GBIC Approval Scheme

Version 1.20

17.05.2024

Content

1 Management Summary

Within an interoperable payment scheme, payment cards are used at terminals of different acquirers. Card issuers rely on the different payment system components of these acquirers to work as described in the respective specifications and to meet the defined security requirements. Issuers are only able to do so if a standardised, transparent approval procedure is installed using state of the art criteria and adequate processes which are agreed on by all issuers and acquirers participating in the scheme. Depending on the system used, payment cards may include not only physical smart cards, but also so-called Digital Cards for storage on a mobile device.

Thus one of the crucial aspects of a payment scheme is its approval procedure.

This document describes the Approval Scheme of the German Banking Industry Committee (GBIC), abbreviated the GBIC Approval Scheme. It focuses on the approval procedure for payment schemes and their components in the GBIC market in order to provide issuers and acquirers with an acceptable level of confidence regarding the functionality of cards and terminals of the payment schemes. The GBIC Approval Scheme must ensure that the approved components

- have a logical behaviour that complies with the specifications of the participating payment scheme,
- will neither harm nor compromise the payment scheme environment and
- are interoperable.

To perform the approval process, GBIC offers an organisational framework developed by the four German Credit Sector Associations. Within this framework, special roles are defined to keep and maintain special tasks throughout the whole process. Both, roles and tasks are described.

The overall approval process includes two processes:

- The maintenance process for identification and integration of new approval objects or approval requirements which are necessary to keep the approval process up to date and
- the approval process itself which includes security evaluation and functional testing of the components, resulting in an approval letter e.g. for the vendor.

Both processes are steered and controlled by the Councils ("Arbeitsstäbe") defined in the respective GBIC interbank agreements. For EMV based Debit/Credit POS approvals also the Acquirers are constantly involved.

To maintain the process, the Councils have to define new approval objects and approval requirements. To ensure that this basic process, which is crucial for the quality of the GBIC Approval Scheme, can be performed in an efficient way, the Councils must use defined forms.

Thus, open questions and further actions can be clearly communicated to other experts. To strengthen the maintenance process, only two committees are assigned to provide for the necessary expertise: GBIC's Security Committee and Technical Committee. Both assist the Councils. The Approval Office coordinates the integration of new or revised requirements into the approval process by informing vendors, providers and all other GBIC Approval Scheme participants.

Routine processes which represent the major part of the approval process are delegated by the Councils to the Approval Office. Questions to be clarified will be analysed and described by the Approval Office in cooperation with the Testing Laboratories and Security Evaluators resulting in a proposal on how to proceed. This proposal is given to the above mentioned committees for decision. Only questions, which cannot be clarified on this level of expertise, will be handled by the Council.

Nevertheless, the Councils will be kept well informed about approval activities through continuous reporting from the Approval Office.

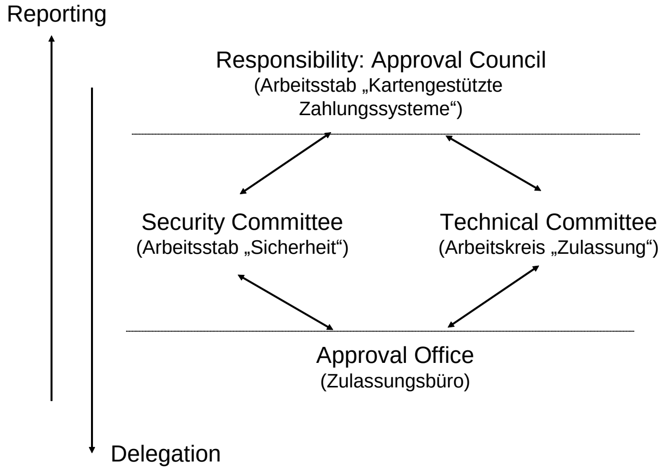

Reporting
Responsibility: Approval Council
(Arbeitsstab „Kartengestützte Zahlungssysteme“)
Security Committee
(Arbeitsstab „Sicherheit“)
Technical Committee
(Arbeitskreis „Zulassung“)
Approval Office
(Zulassungsbüro)
Delegation

Figure 1: GBIC roles and their cooperation

The GBIC Approval Scheme is open for the participation of other payment schemes. The rules and regulations for the participation of these schemes must be agreed on by GBIC and the payment schemes. The payment schemes may use the GBIC Approval Scheme for cards and/or terminals.

Today vendors face and handle numerous different approval schemes offered or mandated by the different payment schemes. Examples are the MasterCard and Visa terminal and processor approval schemes, the EMVCo Type Approvals and the various approval schemes which are necessary for the integration of specific requirements. To achieve an approval for the GBIC market, a POS terminal vendor today must first decide which payment card his terminal shall accept, because each payment scheme defines its own approval scheme including different testing laboratories, test cases and so on. This procedure is costly and time consuming.

Therefore the GBIC Approval Scheme offers the possibility of a common scheme which integrates the requirements of different payment scheme and thus a "one-stop-shopping" for vendors. Even the EMVCo Level 2 Type Approval is integrated. The Level 2 test results achieved during GBIC's functional terminal testing will also be presented to EMVCo to be acknowledged as an EMVCo Type Approval Level 2. Thus vendors can use test results achieved during the GBIC test procedure abroad. On the other hand vendors can reduce testing by presenting an EMVCo Type Approval to the GBIC Testing Laboratories.

To achieve the intended advantages of the GBIC Approval Scheme, it is important that as many payments schemes as possible are supported. Most of the global payment schemes acknowledge the GBIC Approval of terminals. Corresponding letter agreements between the global payment schemes and GBIC are concluded and are part of the approval requirements.

As the approval schemes of the global payment schemes remain unaffected and can still be used, it is crucial for GBIC‘s common approach, that it is efficient, transparent, flexible, provides high quality and keeps consistently close and quick to market. These objectives are achieved by creating synergies using the same infrastructure with common approval rules, a common set of specifications, security requirements, test tools and test cases. Consistent delegation provides for easy administration and high performance of the process.The GBIC Approval Scheme optimises its evaluation and certification processes by using international standards in order to keep up with future requirements and the European standardisation initiative of the European Commission and the European Central Bank (SEPA).

In this context GBIC cooperates with UK Finance for the security certification of POI platforms and with Cartes Bancaires for the functional certification of POI payment applications based on nexo standards.

GBIC and UK Finance founded a Common Security Evaluation and Certification Consortium Common.SECC. Within this Consortium the security evaluation and certification of girocard terminal platforms (hard- and firmware) is performed together following common harmonised processes and rules, e.g. ISO 15 408 Common Criteria. This international cooperation provides vendors with a one stop shopping for their terminal platforms as the Common.SECC certificates are acknowledged by both partners for approval.

Because this document focuses on GBIC's approval scheme the Common.SECC cooperation is only mentioned as far as its interfaces to the GBIC approval scheme are concerned. A detailed information about Common.SECC is given under www.Common-SECC.org.

Together with Cartes Bancaires GBIC founded the Common Functional Certification Framework CFCF, which is based on nexo standards, namely the nexo Implementations Specification (nexo IS). On CFCF level, implementations of this functional specification in terminals and acquirer hosts are tested against a test case catalogue owned by nexo and test tools validated by CFCF. This international cooperation provides vendors with a one stop shopping for their terminal applications, too, as the CFCF certificates are acknowledged by both partners for approval. A detailed information about CFCF is given under www.CFCF.eu.

Where ever possible, simple Type Approvals are issued to leverage the investments and usage of payment scheme components.

2 Introduction

2.1 Scope

This document describes the Approval Scheme of the German Banking Industry Committee (GBIC), the GBIC Approval Scheme. It focuses on the approval procedures of GBIC's payment schemes and their components to provide its members with an acceptable level of confidence. The GBIC Approval Scheme ensures that the product:

- has a logical behaviour that complies with the specifications of the payment scheme;
- will neither harm nor compromise the payment scheme environment;
- is interoperable.

The intended audience for this document includes:

- the approval authorities:

  of payment schemes,

  acquirers or issuers,

  the German credit sector association,

  other interested entities;
- testing laboratories;
- security evaluators;
- certification bodies;
- payment card, terminal, secure application module (SAM) vendors.

2.2 Objectives

Within a payment scheme, payment cards are used at terminals of different acquirers. Card issuers will rely on the different components (terminals, SAMs, network components) of these acquirers to work as described in the respective specifications and to meet the defined security requirements.

Issuers are only able to do so if a standardised, transparent approval procedure is installed ensuring the payment schemes functionality and security through standardised criteria and a process which is agreed upon by all issuers and acquirers participating in a payment scheme.

Therefore, acquirer components must be approved. To protect the schemes also the payment cards, normally in form of integrated circuits (IC's) must be evaluated and certified in the interest of the issuers and the other partners involved in the schemes. The process includes hardware and software as well as aspects related to the hardware and software combination. Reliable evaluation and approval procedures are absolutely necessary to protect the investments being made by both issuers and acquirers participating in payment schemes.

For so-called Digital Cards, specific evaluation requirements are defined which are related to the technology. Thus, the specific requirements may include both, hardware and software aspects or software aspects only.

2.3 GBIC as Approval Authority

In Germany, the banks are represented by four credit sector associations. These are the Association of German Banks (BdB), the Federal Association of German Cooperative Banks (BVR), the German Savings Banks Association (DSGV) and the Association of German Public Sector Banks (VÖB). These four associations form the "German Banking Industry Committee" (GBIC), in German called "Die Deutsche Kreditwirtschaft", (DK). GBIC represents the whole German banking industry as a lobbying organisation towards other interest groups such as retailers, other industry lobbies, data protectionists, consumer protectionists and supervisory authorities of the government or the government itself.

Concerning payment schemes GBIC acts as a standardisation body to define interoperable interfaces for payment system components and technical requirements concerning security. Within GBIC the German banking industry agrees on the design of payment schemes, e.g. the partners involved, the contracts to sign and the technical requirements to use. As the four associations look after the specific interests of their members, GBIC attains payments schemes suitable to the entire banking sector in Germany. In addition it achieves interoperability of cards and terminals independent from the respective issuer and acquirer. The work is performed in various committees comprised of representatives from the four associations. The rules and regulations for a GBIC payment scheme are defined in GBIC agreements, which are legally binding for the associations' member banks. Where the issuing banks are also the acquirers, the contracts in addition include merchant contracts and thus requirements for acceptance devices. These kinds of contracts exist for

- the girocard scheme,
- the German ATM scheme and
- the GeldKarte scheme.

One of the important aspects of payment scheme design is its approval procedure. As GBIC is the governance authority for its payment schemes, GBIC is responsible for the interoperability, security and integrity of the respective schemes. The GBIC Approval Scheme is designed to ensure that these goals are achieved.

Additional to the GBIC requirements there may exist some technical requirements from the existing agreements with global payment schemes in order to accept their cards at the same terminals.

Concerning global payment schemes GBIC agrees to consider the technical requirements of these payment schemes in order to accept their cards at the same terminals.

Figure 2 shows these relationships:

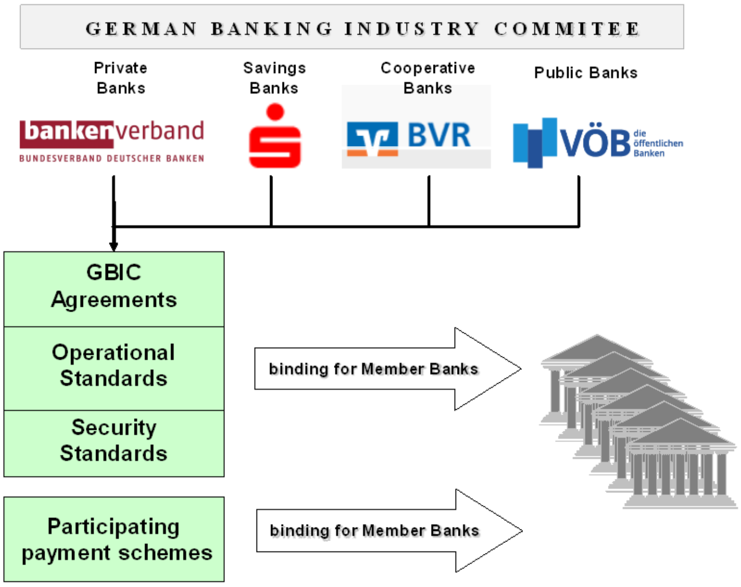


Figure 2: Relationships between GBIC and Payment schemes

2.4 Starting Points

2.4.1 Development of the GBIC Approval Scheme

With the launch of electronic cash in 1990 the former ZKA (ZKA was renamed in GBIC in August 2011) developed its own approval procedure for electronic cash. This procedure covers both the processes (compliance testing of the functional interfaces and the security requirements) and a specific organisational framework. This approval scheme has been gradually extended to other approval objects (PEDs of ATMs and GeldKarte components). Starting the migration to IC technology the approval of ICCs followed. In 2020, the payment scheme "electronic cash" was renamed to "girocard".

The administration of approvals is managed by the GBIC Approval Office, conducted by VÖB.

2.4.2 Extension to Other Payment Schemes and Approval Bodies

With the launch of EMV and the conversion to IC technology MasterCard International and Visa International also have established their own requirements for the approval of system components in order to ensure the integrity of their payment schemes. To provide the compliance they also developed their own approval procedure. The requirements apply to terminals and ICCs as well as to processing centres. For receiving an approval for a terminal it is necessary to obtain the EMVCo Level 1 and 2 Approval by performing functional tests at accredited testing laboratories.

GBIC offers its Approval Scheme to other payment schemes. For participation GBIC and the payment scheme agree on the communication and organisation rules of the scheme via written agreements, the so called Letter Agreements[1]. These agreements are included into the GBIC Approval Scheme. Most of the global payment schemes signed an agreement with GBIC (the former ZKA) and signed Letter Agreements: In view of the existing approval structure in Germany these global payment schemes granted the right to GBIC to include a compliance statement of their terminal requirements in GBIC's approval letters. Thus GBIC offers a single GBIC Approval Scheme covering global payment schemes' compliance, too. The approval procedures of the global payment schemes remain unaffected and can still be used in addition to the GBIC Approval Scheme.

GBIC’s cooperation with UK Finance outsources the terminal platform security certification (hard- and firmware) for the payment scheme "girocard" to the common cross border organisation Common.SECC (Common Security Evaluation and Certification Consortium) whose results are acknowledged for approval. GBIC’s cooperation with Cartes Bancaires where the functional certification of nexo-based payment appliations is outsourced to the CFCF (Common Functional Certification Framework) Consortium follows the same goal.

2.4.3 Necessity of a Common and Uniform Approval Scheme for Payment Schemes

German banks issue debit and credit cards with different brands (e.g. MasterCard and Visa). The terminals of the acquirers should be able to accept all kinds of cards to enable wide acceptance of different payment schemes at POS devices and ATMs. This aim can be achieved a lot easier and faster by means of a harmonised approval scheme for all participating payment schemes. Time to market can be reduced significantly, thus enhancing the acceptance level for all issuers and payment schemes. Therefore German issuers and acquirers established a

[1] The agreements signed under the construction ZKA are agreements of the participating associations and therefore are unaffected by renaming of the GBIC.

harmonised approval scheme for the GBIC market integrating the requirements of the global payment schemes and the different requirements of the GBIC's payment schemes. This allows also for a single, simplified, transparent administration process for all players.

3 Approval Policy

Chapter 2.1 and 2.2 describe the overall aspects of the GBIC Approval Scheme. The approval policy is described in the following by giving more explanations to the overall objectives and by defining specific objectives in addition.

3.1 Overall Objectives

3.1.1 Compliance with Legal Requirements

- The GBIC Approval Scheme ensures adherence to the existing legal and supervisory requirements.
- The GBIC Approval Scheme meets the anti-trust laws and regulations.
- The GBIC Approval Scheme meets the internal requirements of the payment scheme providers involved, e.g. internal audit requirements of the German banking industry.

3.1.2 Interoperability

- The GBIC Approval Scheme provides for interoperability of payment scheme components by verifying the relevant interface specifications defined by the payment scheme.
- This includes basic requirements for the general functionality of the payment scheme components to exclude the danger of component damage, e.g. electrical protocols.

3.1.3 Security

- The GBIC Approval Scheme provides for adequate security defined by the payment schemes and their approval authorities.

3.1.4 System Integrity

- The GBIC Approval Scheme provides adequate means both to ensure the consistency of the protocols used and to enable trust of the market players in the respective systems.
- Thus the GBIC Approval Scheme provides for a sufficient quality according to the requirements of the payment scheme.

3.1.5 Transparency

- The GBIC Approval Scheme is transparent to the market players. Its underlying operational processes are understandable and traceable. Processes of the GBIC Approval Scheme are publicly available. Exceptions to this principle are only in the interest of the payment schemes involved and are avoided as far as possible.

- The competences and responsibilities within the GBIC Approval Scheme are clearly defined.

3.1.6 Integration of International Standards

1. The GBIC Approval Scheme aligns its contents with international standards in order to keep up with future requirements of global payment schemes or European standardisation committees: e.g. integration of Common Criteria and EMV.

3.2 Specific Objectives

- Amount, duration and cost of the GBIC Approval Scheme are based on the guideline "As much as necessary, as little as possible". The duration of the required processes and the costs related to an approval are minimised by attainable synergies.

3.2.1 Easy Administration

- The GBIC Approval Scheme is administrable with appropriate effort. This requirement is met in particular by the defined administration process and the definition of the approval objects.

3.2.2 Flexibility and Modularity

- The GBIC Approval Scheme is expandable to new or modified requirements without major effort. Such requirements can result from inclusion of new functional requirements or security requirements or from integration of further payment schemes and their special requirements.

- Existing approvals are considered in such a way, that users can bring them in with minimum effort. This applies in particular to the consideration of EMVCo Type Approval.

- Depending on the payment schemes participating in the GBIC Approval Scheme, applications and functions can be selected by the approval applicant. A suitable configuration of the component to be approved thus enhances the flexibility in using the modular approach of the GBIC Approval Scheme.

3.2.3 Creation of Synergy Effects

2. The GBIC Approval Scheme gives market players, who want to meet the requirements of different payment schemes in one component, the possibility of "One-Stop-Shopping". This means, that users can obtain an approval for different payment schemes by a single "modular" test procedure.

3. The GBIC Approval Scheme aligns its operating process and its organisation with this aim. This means:

    - Use of a common set of specifications for system components with payment scheme-specific parts.

    - Use of a common set of security requirements for system component with payment scheme-specific parts.

    - Use of a common and uniform approval scheme for system components – according to the requirements of the respective payment scheme.

    - For all system components a Type Approval is issued if possible enabling the use of approved components in each network configuration without further verification.

    - Use of a common set of test tools and a common set of test cases for different products.

    - Use of the same processes for all involved payment schemes.

    - Use of the same approval organisation for different payment schemes.

4 Approval Scheme

4.1 Approval Roles

In this chapter the roles of the GBIC Approval Scheme are described. The institutionalisation of these roles is not part of this section, since an institution may act in different roles for each payment scheme. Additionally an institution may act in more than one role.

4.1.1 Payment Schemes and Licensees

Payment schemes may decide to use the GBIC Approval Scheme (roles and processes). These decisions are laid down in written agreements with GBIC (e.g. GBIC agreements, letter agreements). A fundamental part of these agreements is the delegation of the approval procedure to GBIC. The payment schemes have to acknowledge the functional testing, the security evaluation and all other processes within the GBIC Approval Scheme. The payment schemes can introduce additional requirements to be included into the GBIC Approval Scheme (special test cases, security requirements a.s.o.). They are kept informed about the approval procedure. They may require changes or even may quit the approval agreement.

The payment schemes give acquiring licences to eligible institutions, which have the right to acquire retailers or other service providers for the brand they are licensed for. These acquirers must comply with the rules of the payment scheme and thus must ensure that their contractors comply with the functional and security requirements of the payment scheme. Therefore they may also be involved in the GBIC Approval Scheme, if the respective payment scheme decided to use it.

The payment schemes give issuing licences to banks, which have the right to issue payment cards to their customers called cardholders in the following. These issuers must comply with the rules of the payment scheme and thus must ensure that their contractors comply with the functional and security requirements of the payment scheme. Therefore they may also be involved in the GBIC Approval Scheme, if the respective payment scheme decided to use it.

The payment schemes and their licensees must agree with GBIC on the approval requirements including technical interface specifications and security requirements if they want to participate in the GBIC Approval Scheme. For GBIC payment schemes like girocard GBIC is responsible itself.

4.1.2 GBIC Approval Infrastructure

4.1.2.1 Approval Council

The Approval Council (AC) is the approval authority for the payment schemes and their licensees. Therefore, the Approval Council is responsible for the maintenance of the GBIC Approval Scheme. The Approval Council also prepares approval guidelines.

Based on the recommendations of the Security Committee and the Technical Committee, the Approval Council decides on the approval of an approval object, especially if deviations from the payment scheme's requirements have been detected. If necessary the Approval Council clarifies the handling of a deviation with the global payment schemes.

The Approval Council is responsible to ensure that GBIC approval requirements (e.g. technical interface specifications, migration dates) and any other information relevant for the GBIC Approval Scheme are available to the Approval Applicants and other parties involved in the payment schemes.

4.1.2.2 Security Committee

The Security Committee (SC) is responsible for the maintenance of the security policy for the GBIC Approval Scheme. The Security Committee supports the Approval Council in the GBIC Approval Scheme.

<u>Role of the Security Committee in the Maintenance Process:</u>

The Security Committee gets information about modifications of security requirements and works out the relevant impacts on the security evaluation of the approval process.

<u>Role of the Security Committee in the Approval Process:</u>

The Security Committee assesses on the basis of a security evaluation report and, if necessary, further explanations of the Security Evaluator, whether a product or system complies with the evaluation object of the approval object (i.e. with the security requirements of the payment schemes). Further on, the Security Committee assesses the compliance of the security evaluation report itself with the rules defined within the GBIC Approval Scheme. If defined in the payment scheme, the Security Committee acknowledges external certificates (e.g. according to ISO 15 408 Common Criteria) for the whole or a part of the evaluation object.

For each payment scheme the Security Committee has to base its judgement on the specific security requirements of the payment scheme. The Security Committee provides the Approval Council with a statement concerning the security compliance and a recommendation for decision. The Security Committee informs the Approval Office about the results of the assessment.

The members of the Security Committee must sign a dedicated non disclosure agreement vis-à-vis their association to ensure, that confidential content e.g. of the security evaluation reports is kept secret.

4.1.2.3 Technical Committee

The Technical Committee (TC) determines the requirements for the functional testing. This includes the proposal of definition for the approval objects, the test objects, the testing procedures and migration dates. The Technical Committee supports the Approval Council in the GBIC Approval Scheme.

Role of the Technical Committee in the Maintenance Process:

The Technical Committee is informed about any changes in the technical interface specifications and works out the relevant impacts on the functional test of the approval process.

Role of the Technical Committee in the Approval Process:

The Technical Committee assesses on the basis of a functional test report and, if necessary, further explanations of the Testing Laboratories, whether the product or system complies with the test object of the approval object (i.e. with the technical interface specifications of the payment schemes). If necessary, the Technical Committee provides the Approval Council with a statement concerning the compliance with the technical interface specifications and a recommendation for decision. The Technical Committee informs the Approval Office about the assessment results.

4.1.2.4 Approval Office

The Approval Office (AO) supports the Security Committee, Technical Committee and the Approval Council within the GBIC Approval Scheme. The Approval Office administers the GBIC Approval Scheme. The Approval Office

- administers the communication towards Testing Laboratories and Security Evaluators (e.g. distribution of technical interface specifications, changes in the GBIC Approval Scheme caused by the maintenance process),

- administers the registration process checking the eligibility of objects for approval,

- checks and examines security evaluation reports and functional test reports during the approval process and decides within a framework of rules on the approval based on the assessment results,

- communicates with the Approval Applicants, the Approval Owner, Testing Laboratories and Security Evaluators, and delivers approval letters,
- publishes information about approved objects and lists
- archives all documents used within the GBIC Approval Scheme.

The registration has to be made via the online approval administration tool, when applicable.

4.1.2.5 Security Evaluator

The Security Evaluator (SEV) acts as an independent expert to verify the compliance of the evaluation object with the security requirements of the payment scheme. Several Security Evaluators are listed by GBIC. The Security Evaluator writes security evaluation reports and delivers these reports to the Security Committee, the Approval Office and the Approval Applicant. The Security Evaluator presents the security evaluation reports to the Security Committee. Security Evaluations have to be paid by Approval Applicants.

For Common.SECC evaluations all evaluators accredited at a SOGIS CC Certification Body for the technical domain „Hardware Devices with Security Boxes“ are accepted.

4.1.2.6 Testing Laboratory

The Testing Laboratory (TL) accomplishes the functional testing and thus the functional interoperability of the payment schemes’ products is ensured. The Testing Laboratory has to be paid by Approval Applicants. Via functional testing, the compliance of the test object with the technical interface specifications is examined. The Testing Laboratory writes functional test reports and delivers these to the Approval Office and the Approval Applicant.

4.1.3 Additional Roles

4.1.3.1 Approval Applicant

Approval Applicants (AA) initiate the approval process by registration of their product or system with the Approval Office. The Approval Applicant gets a registration number for each registered product or system by the Approval Office.

4.1.3.2 Approval Owner

The Approval Owner gets the approval for its product or system. E.g. network providers and vendors can be Approval Owners. If the Approval Owner modifies the approved product or system, he is in any case responsible for its compliance with the requirements.

If the Approval Owner is contractually obliged to comply with GBIC "Minimum requirements for the implementation of information security in the girocard system" called "Mindestanforderungen an die Implementierung der Informationssicherheit im girocard-System", the Approval Owner must ensure the secure configuration and validity of all cryptographic certificates used by means of an appropriate certificate management. This must also take into account certificates in third-party components. In the event of the sale of the company or parts of the company of the Approval Owner, the latter shall ensure that the certificate management is transferred to the new owner together with all the data and information required for this purpose and that the new owner is informed of this and made aware of the significance of the certificates the process of proper certificate management for the girocard system. Regardless of this, the new owner will generally need his own approval for the system that will operate with these certificates.

4.1.3.3 Technical Expert

A Technical Expert (TE) acts independently and provides expertise in a special field of competence that can include functional as well as security related aspects. A Technical Expert, nominated by the GBIC for this purpose only, assesses issues and confirms Approval Applicants' statements related to this field of competence. Technical Experts are only required for certain approval objects.

Depending on the approval object, the task for a Technical Expert may be:

- in the Testing and Evaluation process – Functional Test (see chapter 4.4.2.3.2.2), to evaluate and confirm the completeness and correctness of self-test results of the Approval Applicant or

- in the Assessment Process (see chapter 4.4.2.3.4), to consolidate security and functional certificates for one approval process.

4.2 Approval Methodology

The approval is granted based on the verification of the compliance of a product or system with security requirements, technical interface specifications and agreements of GBIC with payment schemes. The compliance with security requirements is verified by independent Security Evaluators. The compliance with the technical interface specifications are verified through functional testing by Testing Laboratories accredited by GBIC.

The testing method is as follows: The functional tests are based on the respective technical interface specifications. For each approval object the GBIC Approval Scheme defines a test object i.e. interfaces to be tested. Existing test results are taken into consideration, if possible (e.g. EMVCo approvals). To ensure compliance with the technical requirements also for approved components in combination with GBIC systems random samples of test cases are tested again. GBIC may add further test cases at any time. In particular GBIC is allowed to react to interoperability issues and may define new test cases. The level of test coverage is defined by GBIC. The Testing Laboratory summarises the test results in a functional test report. The functional test report includes a description of the test object.

In exceptional cases, when the set-up of the functional test for a test object in a Testing Laboratory is not possible with a reasonable effort, a self-test by the Approval Applicant according to a test plan given by GBIC may be defined. In this case, the Applicant declares the successful completion of the self-test in a testing conformance statement, whereby it can be demanded that the test results have to be evaluated by a GBIC accredited Technical Expert and confirmed in a technical expert confirmation.

The security evaluation method is as follows: For each approval object an evaluation object is defined. The security evaluation for the evaluation object is based on the security requirements of the payment scheme. Existing security evaluations, like former evaluations or Common Criteria evaluations, may be used by the Security Evaluator. But the Security Evaluator must write a report where the security requirements of the payment scheme are mapped to the security evaluation results of the evaluation object. If the Approval Applicant divides the evaluation object into different security components with different security evaluations (e.g. separating into a hardware and a software evaluation), then there must be a report summarising the evaluation results of the entire evaluation object. Besides the security requirements of the payment scheme (additional information to the security requirements is published if necessary) no other requirements are prescribed. The assurance level of the security evaluation is defined by GBIC. GBIC proposes at minimum three Security Evaluators to the Approval Applicant.

If the Testing Laboratory detects deviations from the specifications, these deviations are classified and documented in a functional test report. If the Security Evaluator detects deviations, these deviations are explained and documented in the summary of the security evaluation report. The reports are assessed by GBIC. In general deviations from the requirements are not accepted. Depending on the significance of the deviations, GBIC may tolerate deviations. In this case, GBIC may define additional obligations as part of an approval.

If the implementation of an approval object is successfully approved, the Approval Applicant receives an approval letter from the Approval Office. If the Approval Applicant changes the implementation of the approval object, then, depending on the payment scheme and the approval object, the approval may not be valid anymore. The Approval Applicant may apply for an approval of a change, called a "change approval" or an approval of an extension, called an "extended approval", in these cases. For these kinds of approvals only a reduced security evaluation and/or a reduced functional test may be sufficient.

4.3 General Conditions

The following conditions have to be taken into account:

- The approval requirements provided by the Approval Office for the registration process (chapter 4.4.2.3.1) must be fulfilled within the defined approval period. If the approval requirements are modified, GBIC informs the Approval Applicant and the modifications have to be implemented in order to obtain the approval.

- If the approval requirements have to be modified, the Approval Office will examine the impact on open approval requests (see maintenance process in chapter 4.4.1).

- Approvals are exclusively issued on the base of the relevant technical interface specifications and security requirements and if necessary of other documents. Furthermore, only selected properties of the technical interface specifications are tested. Therefore, the approval does not confirm neither the correctness or completeness of the implementation or functionality, interoperability, etc., of the approval object nor the resistance to each known or unknown attack. Under no circumstances should the approval, when granted, be construed to imply any endorsement or warranty regarding approval objects.

- The approval is valid only for the configuration of the approved object regarding the specified technical interface specifications and security requirements written in the approval letter. If the approval owner carries out any modifications of the approved object having an impact on the specified interfaces or security requirements, a new functional test and/or a new security evaluation is required (this rule is refined for GBIC ICC approval objects in chap. 4.4.5.2). The issued approval does not cover a modified configuration. In this case the Approval Applicant has to initiate a new functional test for the test object and/or a new security evaluation for the evaluation object.

- Necessary changes of the interfaces and/or the security requirements have to be met by the Approval Owner within an adequate time period.

- Without prejudice to the manufacturer´s liability for the rest the manufacturer is liable for any damage due to deviations from the specified technical interface specification and security requirements as far as the deviations caused the damage. For avoidance of doubt: In no event GBIC and/or AC, AO, SC, TC, TL will be liable for damages or losses of any kind relating to or arising out of the approval process and all steps of it including but not limited to test results and security evaluation regardless whether or not an approval is granted.

- GBIC, the Security Evaluator and the Testing Laboratory examine and decide in all conscience.

- GBIC can modify the GBIC Approval Scheme at any time.

4.4 Processes within the GBIC Approval Scheme

Within the GBIC Approval Scheme there are the following processes:

1. maintenance process
2. approval process
3. administration process and
4. specific extensions of the approval and maintenance process.

These are described in this chapter.

In the following all tasks are defined which must be met during each process.

4.4.1 Maintenance Process

4.4.1.1 Purpose and Roles

Within the maintenance process the approval and administration process have to be defined and maintained. Approval requirements i.e. the requirements for security evaluation and functional testing of approval objects have to be maintained.

This includes the definition of approval objects and their characteristics, the necessary approval requirements to be met and the required documentation (testing reports, security evaluation reports) as well as the communication of the approval results.

The approval requirements to be met by an implementation of an approval object are split into

- "basic approval requirements" (like the definition of the evaluation object and the test object) defined in chapter 5 and
- "detailed approval requirements" (like technical interface specifications, migration dates, security requirements, functions, agreements or interfaces to be tested) defined in annexes of this document.

Roles involved in the maintenance process are

- Approval Council (AC),
- Approval Office (AO),
- Security Committee (SC) and

- Technical Committee (TC).

4.4.1.2 Process Initiation

The development of payment schemes is an ongoing process. Technical interface specifications, security requirements etc. will always be improved. Therefore approval objects and approval requirements must be modified since

- existing technical interface specifications are changed by the payment scheme,
- new technical interface specifications (e.g. new technology, new functions) are specified together with implementation mandates,
- existing security requirements are changed by the payment scheme or
- new security requirements (e.g. because of new technology) are defined together with implementation mandates.

Additionally it must be possible to introduce new approval objects in the GBIC Approval Scheme.

The committees (CT) of GBIC responsible for technical interface specifications, security requirements, agreements, have to initiate the maintenance process if approval requirements, approval process or approval administration process are affected. TC, SC and AO are not responsible to monitor whether the approval requirements of an existing approval object change or whether a new approval object shall be defined.

4.4.1.3 Sub Processes

The maintenance process consists of following sub processes:

A) Examination and Definition Process.

Examination of the input based on the current approval requirements.

Examination of the effects of the input to the GBIC Approval Scheme.

Examination of the effects of the input to approval objects.

Examination of the effects on ongoing and closed approval requests.

Definition of the approval object and its approval requirements.

Definition of the approval periods.

B) Implementation Process

Information of the TL, implementation of the test cases for the functional test.

Information of the SEV, if necessary implementation of methods to verify new security requirements.

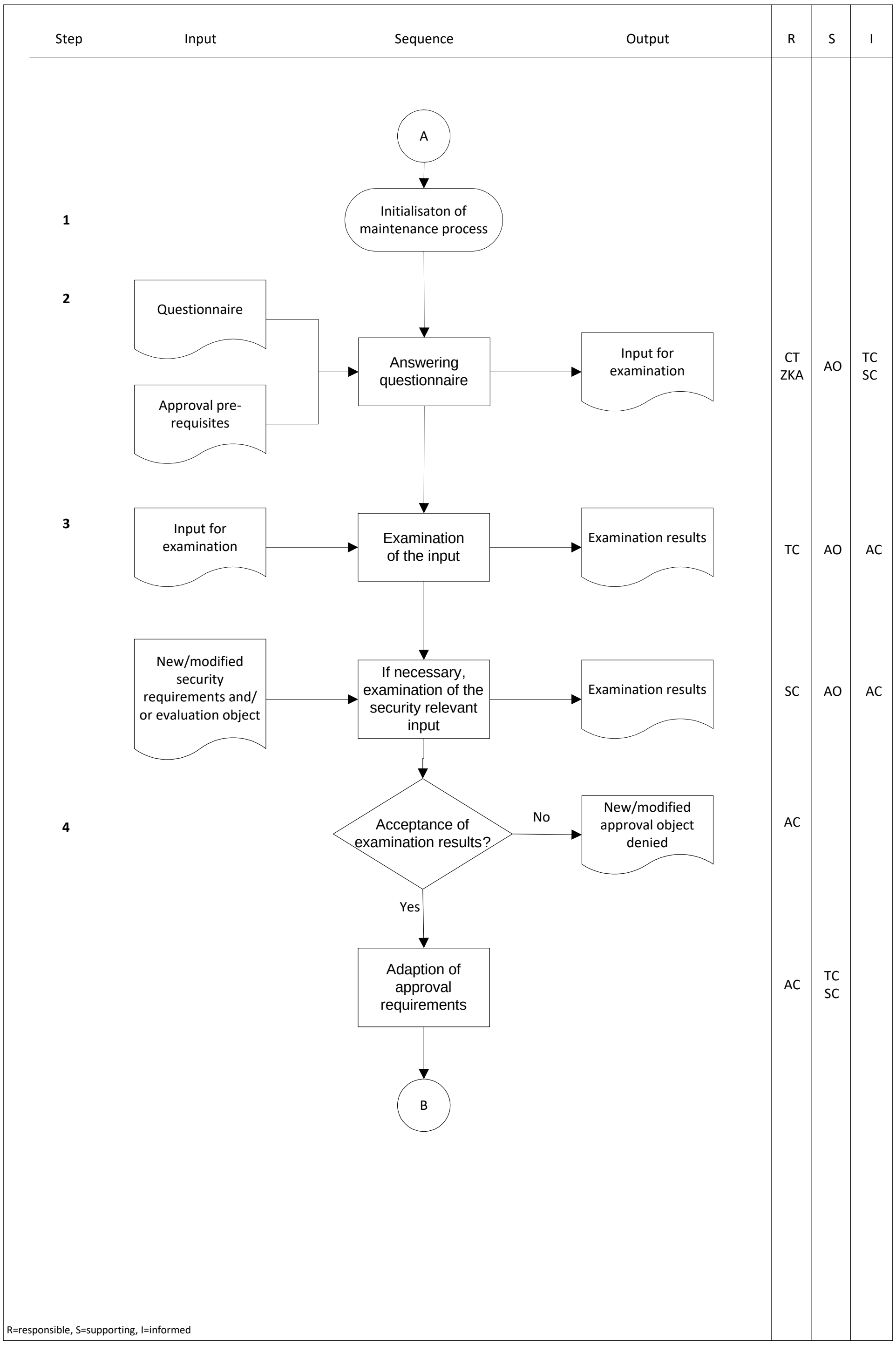
Development/modification of documentation for the approval process.

Communication of the new approval requirements.

Adoption of the approval requirements.

4.4.1.3.1 Examination and Definition Process

4.4.1.3.1.1 Sequence Examination and Definition Process


Step
Input
Sequence
Output
R
S
I
A
1
Initialisaton of maintenance process
2
Questionnaire
Approval pre-requisites
Answering questionnaire
Input for examination
CT
ZKA
AO
TC
SC
3
Input for examination
Examination of the input
Examination results
TC
AO
AC
New/modified security requirements and/ or evaluation object
If necessary, examination of the security relevant input
Examination results
SC
AO
AC
4
Acceptance of examination results?
No
New/modified approval object denied
AC
Yes
Adaption of approval requirements
AC
TC
SC
B
R=responsible, S=supporting, I=informed

4.4.1.3.1.2 Description Examination and Definition Process

Summary

During this first sub process of the maintenance process, the requirements for a new or modified approval object are examined and defined. GBIC´s committees responsible for technical interface specifications, agreements and/or security requirements have to initiate this process by sending necessary information about the new or modified approval object to the TC respective SC. After the assessment of the information the AC decides on the basis of the examination results of the TC and SC whether the new or modified approval object shall be introduced or not. The sub process ends with the decision of the AC.

Steps

1. GBIC´s committees responsible for technical interface specifications, security requirements and/or agreements have to initiate the maintenance process if approval requirements, approval processes or the approval administration process are affected. The maintenance process has to be started if a committee of GBIC recognises

   that a new approval object shall be introduced or

   that for an existing approval object new approval requirements are defined or

   existing approval requirements are modified.

   TC, SC and AO are neither responsible to monitor whether the approval requirements of an existing approval object change nor whether a new approval object shall be defined.

2. To initiate the maintenance process a questionnaire is defined as annex of this document. The questionnaire includes questions concerning all necessary approval requirements and assures that nothing important is neglected.

   The AO maintains for each approval object the respective approval requirements. The committee of GBIC starting the maintenance process for an approval object may ask the AO about the respective approval requirements.

   The committee of GBIC initiates the maintenance process

   by asking the AO about the respective approval requirements, if necessary,

   by answering the questions of the questionnaire and

   by sending necessary input based on the questionnaire to the AC (the new input shall not only consist of the questionnaire answers, but also of new documents like interface specifications, agreements, security requirements, ...).

3. After these steps the effects of the received input on the GBIC Approval Scheme must be examined by the TC and the SC.

The TC and SC examine whether the GBIC approval process itself is affected by the input. Such effects may concern the definition of GBIC roles (e.g. the AO gets a new task) or modifications of the sub processes (e.g. the SEV must use the methodology of Common Criteria) of the approval process.

Afterwards TC and SC examine

which approval objects are affected by the input (this is done by checking the approval requirements of the currently defined approval objects),

whether there are no contradictions and whether the consistency of the approval processes remains when the existing approval requirements of the affected approval objects are modified (e.g. migration dates) and

whether the modification has effects to open approval requests or closed approval requests especially regarding migration dates.

If a new approval object shall be defined, the TC and SC examine whether the input is adequate and sufficient to introduce the new approval object in the GBIC Approval Scheme. The input shall include information on necessary approval requirements. The approval process of the new approval object shall be consistent with the GBIC Approval Scheme.

In general the TC has to examine whether the TL is able to test new or modified approval requirements. The SC has to examine whether the SEV is able to evaluate new or modified approval requirements.

Security relevant new/modified approval requirements like security requirements or the definition of the evaluation object (hardware, software, personalisation environment) are examined by the SC.

Supported by the AO the TC and the SC document the examination results and send them to the AC.

4. The AC assesses the results of the TC/SC.

Depending on the assessment results, it could be necessary to change the approval requirements. Supported by TC/SC the AC has to re-define:

the approval object, the evaluation object, the test object,

the technical interface specifications,

the GBIC agreements or the agreement of GBIC with global payment schemes,

the interfaces to be tested,

the set of functions/applications of the approval object (e.g. including/excluding functions/applications),

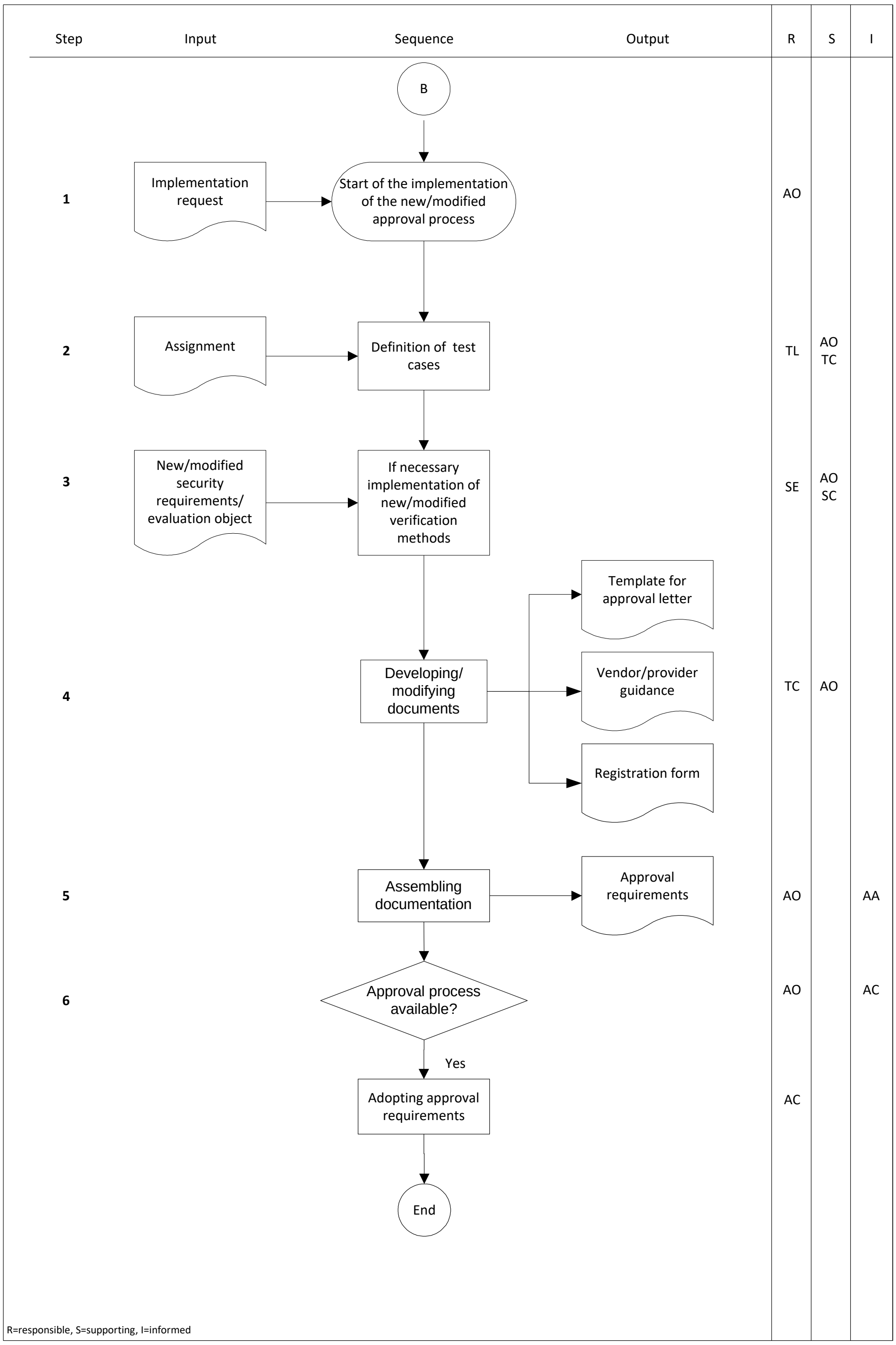
the security requirements,

the migration dates for the new approval object.

If the AC decides that the new approval requirements should be mandatory, an implementation request will be sent to the AO, TC and SC.

4.4.1.3.2 Implementation Process

4.4.1.3.2.1 Sequence Implementation Process


Step
Input
Sequence
Output
R
S
I
B
1
Implementation request
Start of the implementation of the new/modified approval process
AO
2
Assignment
Definition of test cases
TL
AO
TC
3
New/modified security requirements/ evaluation object
If necessary implementation of new/modified verification methods
SE
AO
SC
Template for approval letter
4
Developing/ modifying documents
Vendor/provider guidance
TC
AO
Registration form
5
Assembling documentation
Approval requirements
AO
AA
6
Approval process available?
AO
AC
Yes
Adopting approval requirements
AC
End
R=responsible, S=supporting, I=informed

4.4.1.3.2.2 Description Implementation Process

Summary

During the implementation process the approval process is implemented for the new or modified approval objects. The new approval requirements can only be implemented after successful completion of the examination and decision sub process of the maintenance process.

During the implementation process the AO develops or modifies approval documentation, the AO informs involved parties and SEV and TL implement test and verification methods.

Steps

1. The AO gets the implementation request from the AC to start the implementation of the approval process for the new or modified approval object.

2. If the test object of the approval object is affected, the AO asks the TL to develop and implement correspondent test cases based on the technical interface specifications and the interfaces to be tested.

3. If necessary, the AO informs the SEV about the new evaluation object and about new security requirements. Modification of the evaluation object may concern the scope of security evaluation reports or new limitations of the evaluation object (e.g. not only the PED shall be evaluated but also the correspondent terminal). If necessary, the SEV shall implement verification methods to verify new security requirements.

4. The AO develops or modifies vendor/provider guidance concerning the approval process of the approval object. The AO develops or modifies the registration form for the approval object. The AO develops or modifies the template for the approval letter of the approval object.

5. Based on internal distribution lists the AO sends the modified approval requirements with corresponding migration dates to the Approval Applicants.

6. The AO informs the AC when the new approval process for the affected approval object is available. The approval requirements must not be adopted before the approval process for the approval object is established.

4.4.2 Approval Process

4.4.2.1 Purpose and Roles

The approval process is intended to grant approvals to Approval Applicants (AA) for products or systems. For that purpose, the approval eligibility has to be confirmed, the approval reports (functional test report, security evaluation report) have to be assessed and a decision concerning the approval has to be taken .

This process is supported by the

- Approval Council (AC),
- Approval Office (AO),
- Security Committee (SC),
- Technical Committee (TC),
- Testing Laboratory (TL) and
- Security Evaluators (SEV).

In exceptional cases, if required by the approval object, this process is supported in addition by a

- Technical Expert (TE).

4.4.2.2 Process Initiation

The requirements for the approval process are defined during the maintenance process.

The maintenance process ensures the availability of all necessary documents and procedures, so that the AA is able to pass through the steps of the approval process successfully.

The approval process starts with an incoming registration form at the AO.

4.4.2.3 Sub Processes

The approval process is separated in several sub processes

A) Registration process

Each approval object must be registered. During the registration the approval eligibility is checked with regard to formal requirements, its contents and the adherence to migration dates. The requirements and steps necessary for an approval are determined.

B) Testing and Evaluation processes

- Performing functional tests and security evaluations.
- Delivery of functional test and security evaluation reports to the bodies responsible for assessment.

C) Assessment process

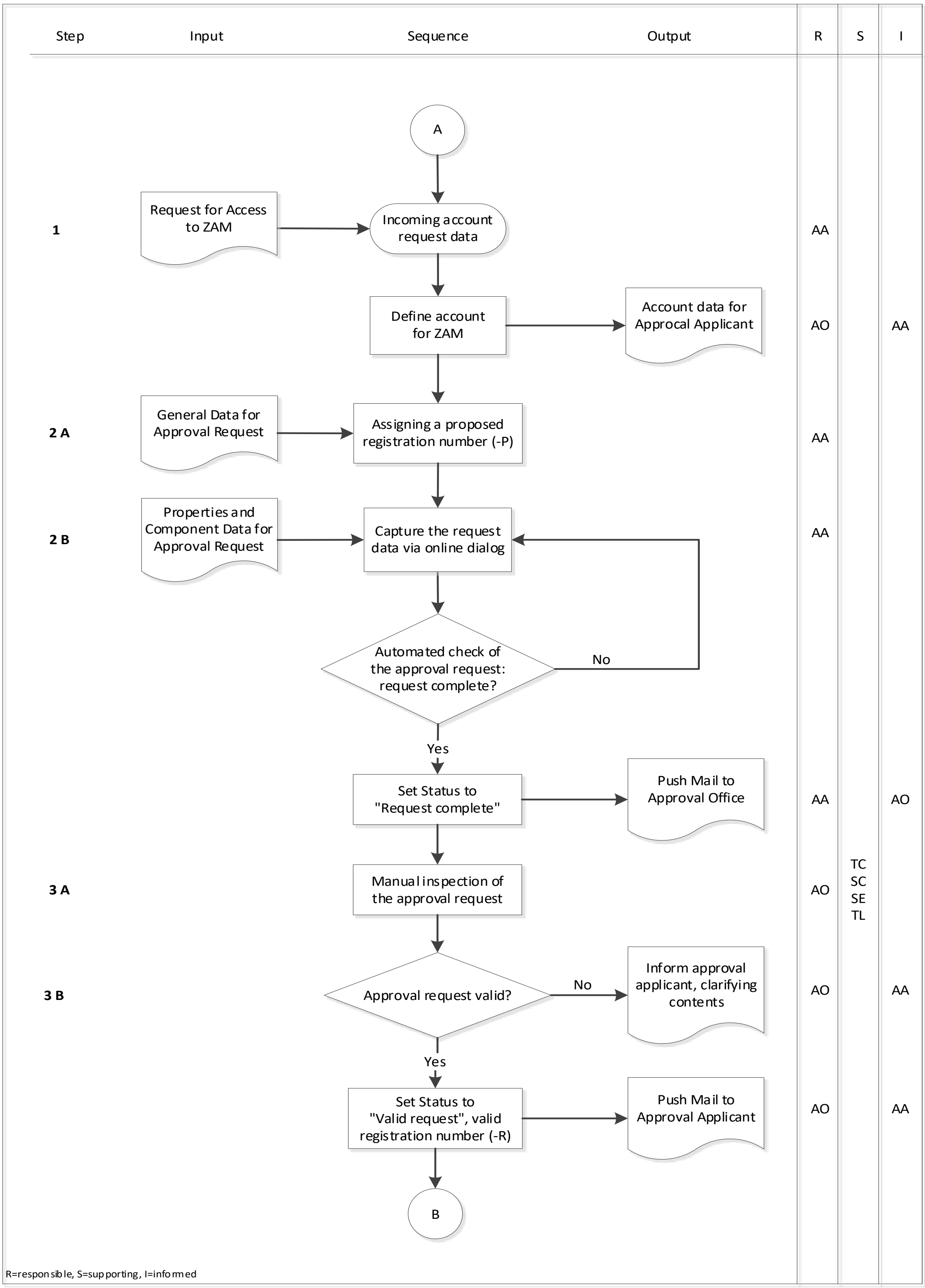
- The approval documents (functional test report, security evaluation report, other documents like signed contracts, certificates or technical expert confirmations) are checked with regard to formal requirements and migration dates.
- The content of each security evaluation and functional test report is assessed and a recommendation (passed/not passed) is passed for decision.

D) Decision taking process

- Based on the delivered documents the decision on the approval of an approval object is taken. An approval letter or a denial letter is sent.

4.4.2.3.1 Registration Process

4.4.2.3.1.1 Sequence Registration Process


Step
Input
Sequence
Output
R
S
I
A
1
Request for Access to ZAM
Incoming account request data
AA
Define account for ZAM
Account data for Approcal Applicant
AO
AA
2 A
General Data for Approval Request
Assigning a proposed registration number (-P)
AA
2 B
Properties and Component Data for Approval Request
Capture the request data via online dialog
AA
Automated check of the approval request: request complete?
No
Yes
Set Status to "Request complete"
Push Mail to Approval Office
AA
AO
3 A
Manual inspection of the approval request
AO
TC
SC
SE
TL
3 B
Approval request valid?
No
Inform approval applicant, clarifying contents
AO
AA
Yes
Set Status to "Valid request", valid registration number (-R)
Push Mail to Approval Applicant
AO
AA
B

R=responsible, S=supporting, I=informed

4.4.2.3.1.2 Description Registration Process

Summary

The registration process is the beginning of the approval process. As a result of the registration process, the AA will be informed on the requirements which have to be met to receive an approval for a product or system. If the information is incomplete, inconsistent or cannot be judged sufficiently, the AO contacts the AA and tries to clarify.

The AO determines whether the described product or system is eligible to be approved.

If necessary, the AO can be supported during the registration process by other roles involved in the approval process (e.g. TC, SC, TL, SEV).

The main task of the registration process has to be done online via approval manager (ZAM). In case that the approval object element is not yet supported by ZAM, a registration form delivered by the AO has to be used.

ZAM creates a file for each testing and evaluation process, called approval request in the following, where all steps are documented. For each approval request a unique registration number is given automatically.

Steps

Each product or system must pass the registration process steps.

1. As presupposition for carrying out a registration the AA needs an access to the online registration tool (ZAM). If not already available, the AA requests the access to ZAM by contacting the AO. The AO adds the reference data of the approval applicant company to ZAM and creates the account data for one or several users of that company. The AO sends the account data to the different users of the AA.

2.A The AA requests a registration by using its access to ZAM. The AA has to select the approval area in the certain version (equal to the version of detailed approval requirements for a payment scheme) and here in the approval object which his product or system shall support. For this selection, the AA has to create a new approval request for which in a first step the general data (name of product or system and planned date of approval) have to be entered. For this input, ZAM generates a unique registration number. Because the request is not yet valid at this time, the registration number will be considered as “proposed” (post fix “-P”).

2.B Via the online dialog masks of ZAM the AA captures all properties and component data which are required for the approval request by the selected approval object. In parallel to the data input the tool automatically performs checks for completeness and plausibility. As soon as no contradictions are found by the tool any more, the AA can complete the approval request. After confirmation by the AA, the status of the approval request will be set to “request complete: manual inspection necessary” and the AO will be informed automatically about the new request by a push mail.

If ZAM cannot be used for the approval request, the AA has to complete the registration form and send it to the AO.

3.A The AO checks the registration information with regard to the responsibility of GBIC for the product or system which an approval is requested for if the status for the approval request is “request complete: manual inspection necessary”. ZAM already provides all necessary details and references of the current approval requirements.

Basic approval requirements which have to be checked (resp. examined) are described in the appropriate section of chapter 5.

The AO checks the eligibility of the product or system with regard to formal aspects. This means:

- valid registration via the approval manager (ZAM),
- the intended approval object fits with the described product or system,
- necessary details are presented and
- migration dates are met.

If not, the AO tries to clarify the content with the AA.

If the approval eligibility cannot be confirmed, the AO contacts the AA.

With ZAM, there is automatically ensured:

- each approval request has a unique registration number,
- the validity of technical interface specifications of the payment scheme and corresponding security requirements,
- consistency of functions, etc. with the approval object,
- consistency of components with the approval object,
- applicability and results of security evaluation reports and
- applicability and results of functional test reports.

If ZAM cannot be used for the approval request, the AO has to perform all checks manually.

If necessary, the AO decides that support by TC, SC, TL or SEV is needed.

If the approval eligibility concerning the contents of the registration information cannot be confirmed, the AO contacts the AA.

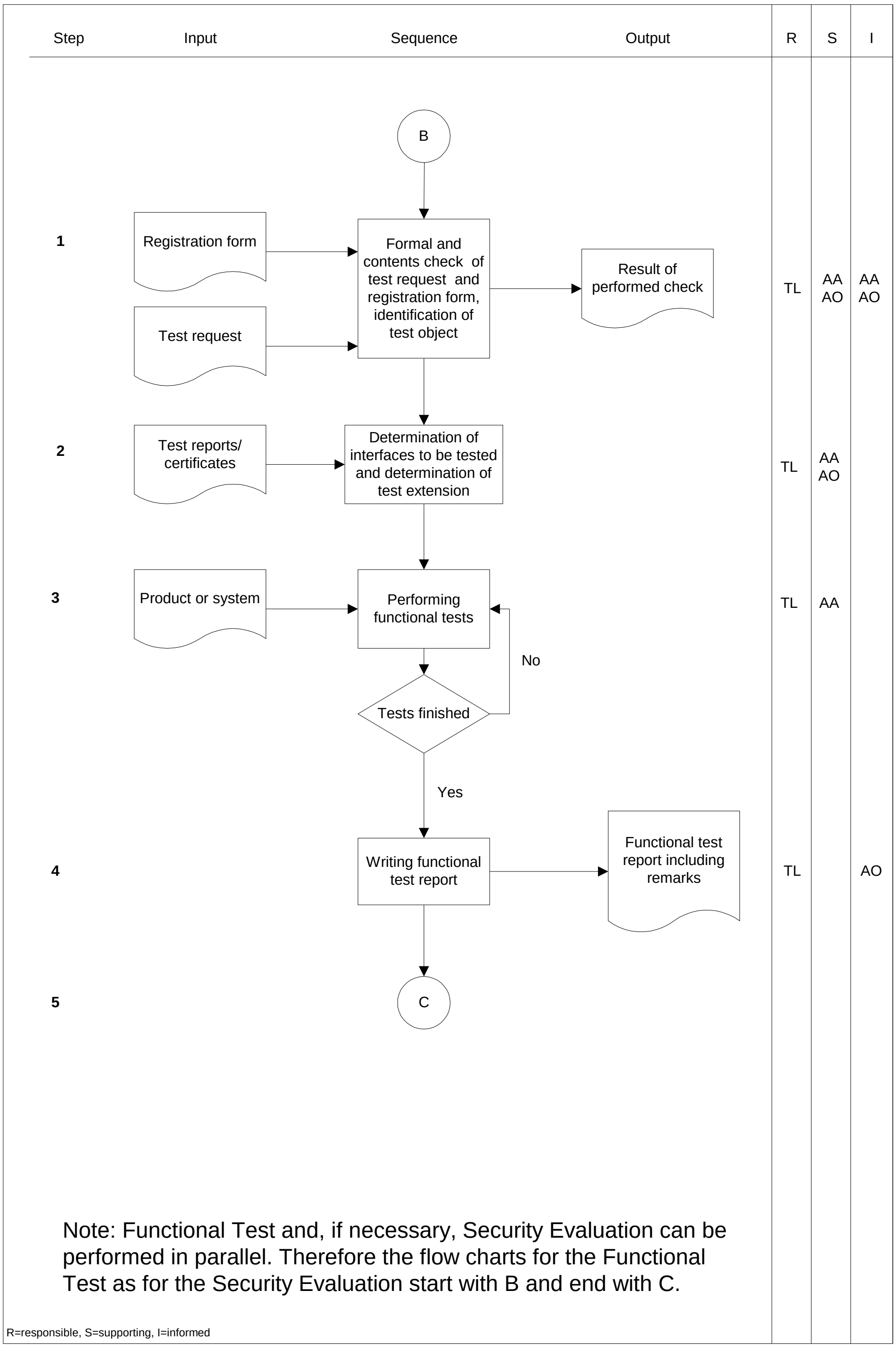
3.B If the approval eligibility is confirmed, the AO determines whether the approval request has to be treated as a first approval, change approval or as an extended approval.

If ZAM can be used, the AO finishes the registration by setting the status to “valid approval request: in evaluation and assessment process”. The AA will be informed automatically about the successful finish of the registration by a push mail. The registration number will now be considered as “registered” (change of post fix to “-R”).

The registration number has to be referred to by the AA in all correspondence with the AO, TL and SEV. The registration number has to be used to refer to the evaluation object, to the test object and to the approval object. Therefore the AA has to inform the TL and the SEV about the assigned registration number.

4.4.2.3.2 Testing and Evaluation Process - Functional Test

4.4.2.3.2.1 Sequence Testing and Evaluation Process - Functional Test


Step
Input
Sequence
Output
R
S
I
B
1
Registration form
Formal and contents check of test request and registration form, identification of test object
Result of performed check
TL
AA AO
AA AO
Test request
2
Test reports/ certificates
Determination of interfaces to be tested and determination of test extension
TL
AA AO
3
Product or system
Performing functional tests
TL
AA
No
Tests finished
Yes
4
Writing functional test report
Functional test report including remarks
TL
AO
5
C

Note: Functional Test and, if necessary, Security Evaluation can be performed in parallel. Therefore the flow charts for the Functional Test as for the Security Evaluation start with B and end with C.

R=responsible, S=supporting, I=informed

4.4.2.3.2.2 Description Testing and Evaluation Process - Functional Test

Summary

The functional test is part of the testing and evaluation process. During the functional test the TL verifies whether the product or system meets the technical interface specifications or not. The TL gets as input the information required to set up the functional test and the product or system to be tested. The information required depends on the functional test object and can be the registration form and/or a special test request. The output of the functional test is the functional test report which is sent to the AO and the Approval Applicant (AA).

The functional test can only be completed after a successful completion of the registration process. Functional test and security evaluations can be performed in parallel. The assessment process starts after the functional test and the security evaluation.

Steps

For each approval object a test object is defined. The functional test is carried out by a TL and is initiated by the AA.

1. The AA has registered its product or system via the approval manager (ZAM). The TL receives from the AA the registration number to refer to within the functional test report of the test object. The TL checks depending on the functional test object the contents of the registration form and/or a special test request with its internal test process requirements.

2. The product or system may have one or more interfaces to be tested. The TL checks and decides about the extent of functional tests on the basis of the information in the test request and/or registration and – if existing and applicable – of former functional tests. If necessary, the TL contacts the AO to confirm the extent of testing.

3. After determining how the product or system has to be tested, the functional test is performed with regard to the technical interface specifications listed as registered. If the product or system fails to comply with the requirements, the functional test can be repeated based on a new release of the product or system. For carrying out the testing, the test environment requirements of the TL must be met. New approval requirements occurring during the testing have to be taken into account.

4. If the functional test confirms the compliance of the product or system to the technical interface specifications on the basis of the tested interfaces, the TL sends the functional test report to the AO. If the compliance of the product or system with the functional requirements are not strictly met from point of view of the TL, the TL explains each unclear point in the report (remarks).

   Within the functional test report the TL has to refer to the registration number assigned to the product or system during the registration process.

5. See assessment process.

Alternative Process

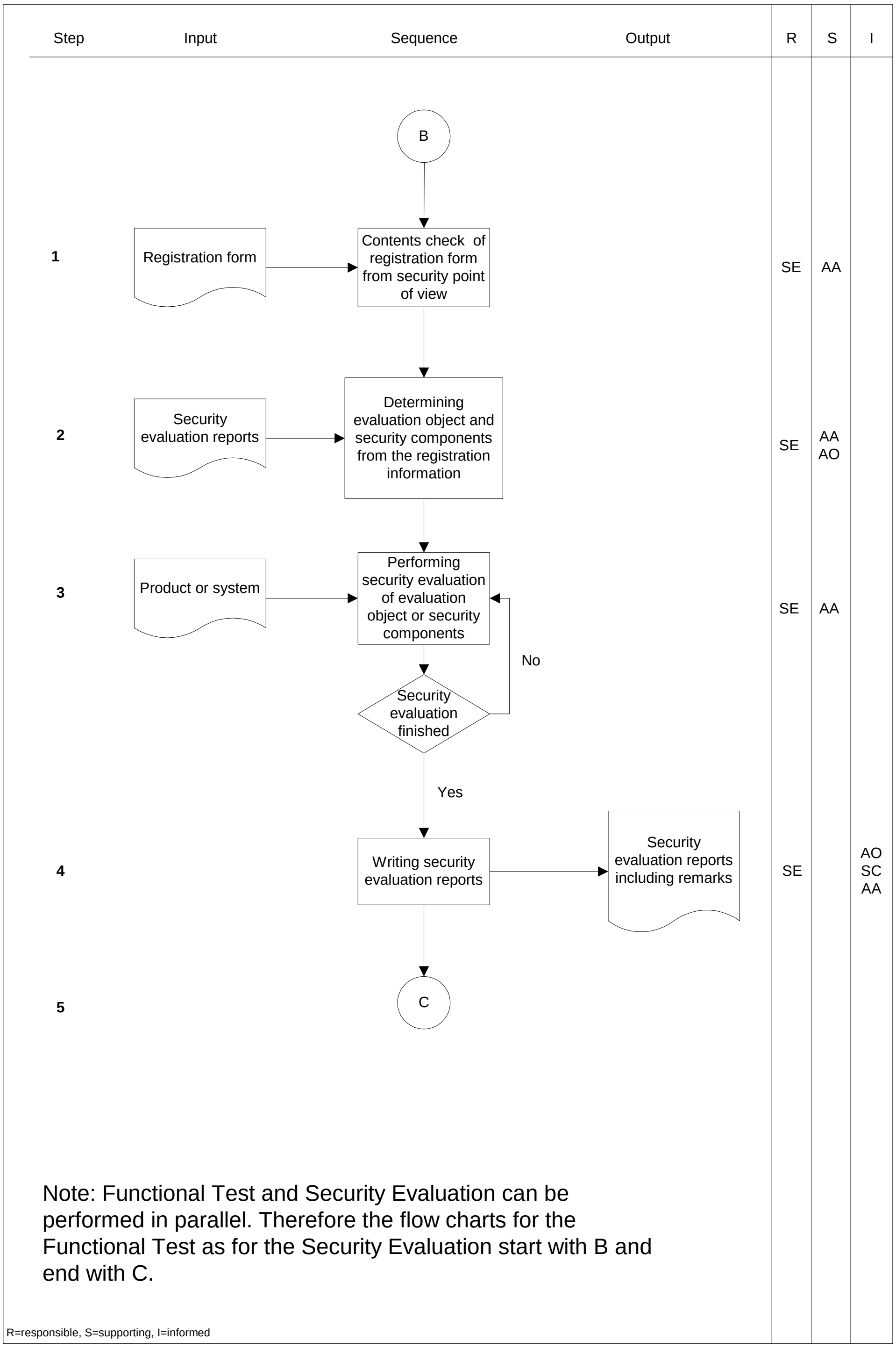
In exceptional cases, if allowed by GBIC and defined accordingly by the test object, the TL can be replaced by the AA itself, who performs a self-test based on a given test plan.

The AA then creates a testing conformance statement (TCS) as output of the functional test (see chapter 4.5.8), whereby it may be required that the correct and complete performance of the self-test must be confirmed by a Technical Expert (TE) by issuing a technical expert confirmation (TEC) (see chapter 4.5.7).

AA sends the TCS, if required together with the TEC, to the AO.

4.4.2.3.3 Testing and Evaluation Process - Security Evaluation

4.4.2.3.3.1 Sequence Testing and Evaluation Process - Security Evaluation


Step
Input
Sequence
Output
R
S
I
B
1
Registration form
Contents check of registration form from security point of view
SE
AA
2
Security evaluation reports
Determining evaluation object and security components from the registration information
SE
AA
AO
3
Product or system
Performing security evaluation of evaluation object or security components
SE
AA
No
Security evaluation finished
Yes
4
Writing security evaluation reports
Security evaluation reports including remarks
SE
AO
SC
AA
5
C

Note: Functional Test and Security Evaluation can be performed in parallel. Therefore the flow charts for the Functional Test as for the Security Evaluation start with B and end with C.

R=responsible, S=supporting, I=informed

4.4.2.3.3.2 Description Testing and Evaluation Process - Security Evaluation

Summary

The security evaluation is part of the testing and evaluation process. During the security evaluation the SEV verifies whether the product or system meets the security requirements. The SEV receives as input the registration information, existing security evaluation reports, product or system from the AA. The output of the security evaluation is the security evaluation report which is sent to the AA, AO and to the SC.

The security evaluation can only be completed after a successful completion of the registration process. Functional test and security evaluations can be performed in parallel. The assessment process starts after the functional test and the security evaluation.

Steps

For each approval object an evaluation object is defined. The SEV performs security evaluations. They are initiated by the AA.

1. The product or system of the AA has to be registered at the AO. The SEV receives from the AA the registration number to refer to within the security evaluation report. The SEV checks the registration information with its internal evaluation process requirements.

2. The product or system can consist of one or more security components. Based on the information in the registration, the SEV determines the security components of the product or system. It is recommended that the AA gets in contact with the evaluators in advance to define the extent of the security evaluation. If necessary, the SEV contacts the AO.

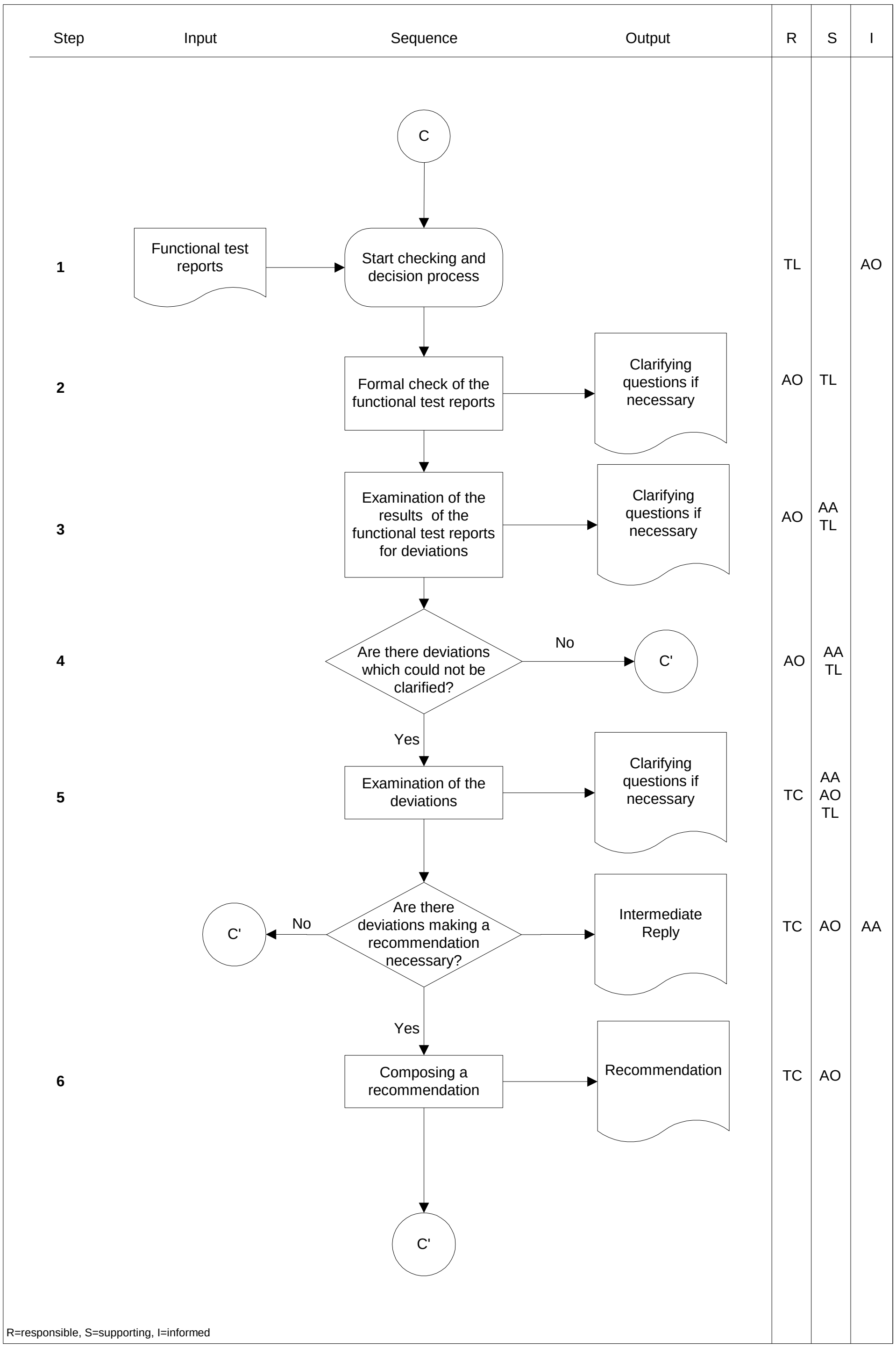
3. The SEV verifies the compliance of the product or system with the security requirements of the payment schemes listed in the registration form. For evaluating the product or system the requirements of the SEV have to be met (e.g. design documentation, software files and hardware samples must be available). New approval requirements occurring during the evaluation have to be taken into account. Each payment scheme can have different security requirements.

4. The SEV documents the results of the security evaluations in reports. Each security component can be evaluated by different SEV. But finally for the complete product or system one security report has to combine and assess all security components of the product or system. The SEV has to refer to the registration number of the product or system in each security evaluation report.

5. See assessment process

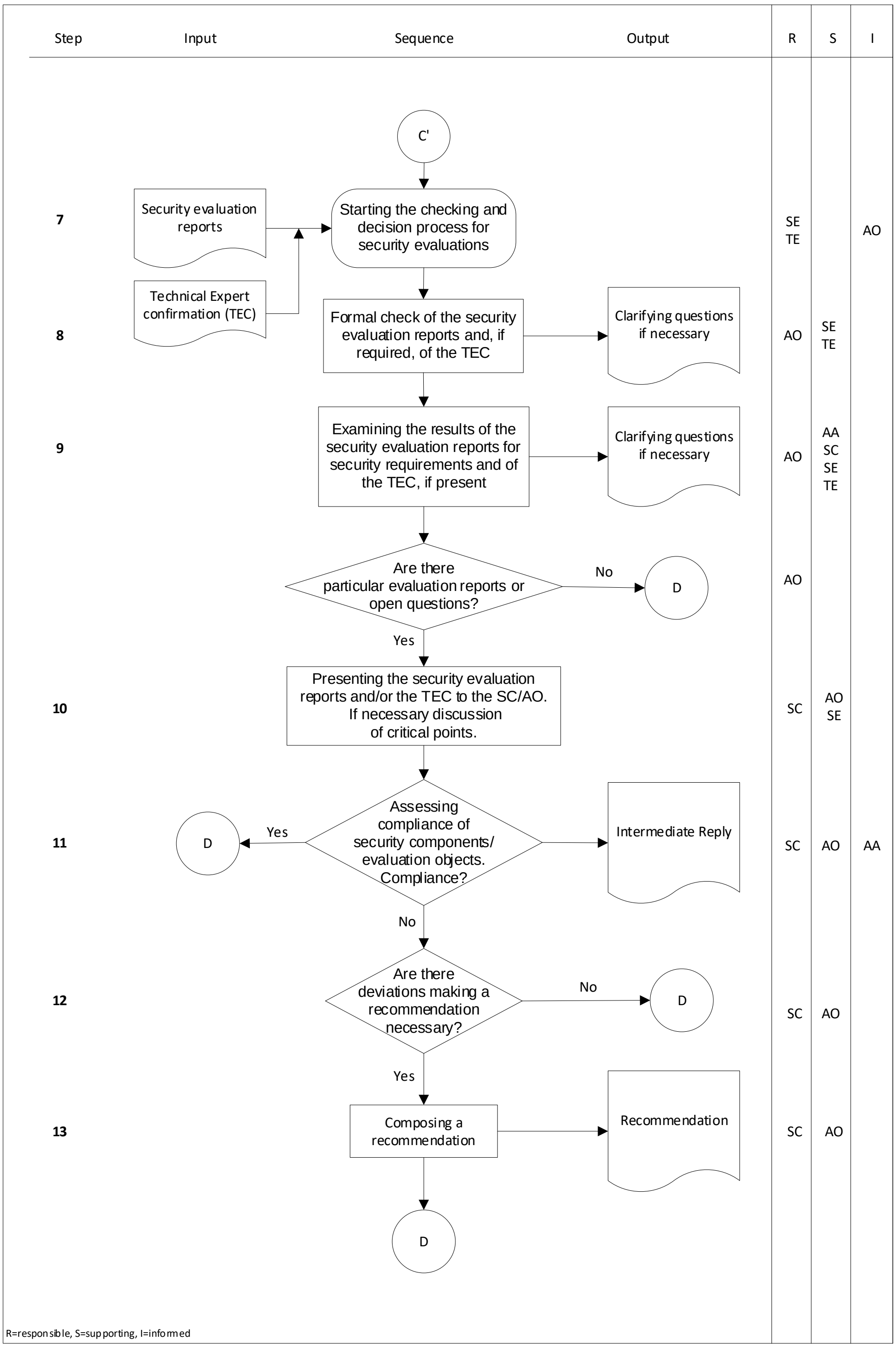
4.4.2.3.4 Assessment Process

4.4.2.3.4.1 Sequence Assessment Process - Functional Test


Step
Input
Sequence
Output
R
S
I
C
1
Functional test reports
Start checking and decision process
TL
AO
2
Formal check of the functional test reports
Clarifying questions if necessary
AO
TL
3
Examination of the results of the functional test reports for deviations
Clarifying questions if necessary
AO
AA
TL
4
Are there deviations which could not be clarified?
No
C'
AO
AA
TL
Yes
5
Examination of the deviations
Clarifying questions if necessary
TC
AA
AO
TL
C'
No
Are there deviations making a recommendation necessary?
Intermediate Reply
TC
AO
AA
Yes
6
Composing a recommendation
Recommendation
TC
AO
C'

R=responsible, S=supporting, I=informed

4.4.2.3.4.2 Sequence Assessment Process - Security Evaluation


Step
Input
Sequence
Output
R
S
I
C'
7
Security evaluation reports
Starting the checking and decision process for security evaluations
SE TE
AO
Technical Expert confirmation (TEC)
8
Formal check of the security evaluation reports and, if required, of the TEC
Clarifying questions if necessary
AO
SE TE
9
Examining the results of the security evaluation reports for security requirements and of the TEC, if present
Clarifying questions if necessary
AO
AA SC SE TE
Are there particular evaluation reports or open questions?
No
D
AO
Yes
10
Presenting the security evaluation reports and/or the TEC to the SC/AO. If necessary discussion of critical points.
SC
AO SE
11
D
Yes
Assessing compliance of security components/ evaluation objects. Compliance?
Intermediate Reply
SC
AO
AA
No
12
Are there deviations making a recommendation necessary?
No
D
SC
AO
Yes
13
Composing a recommendation
Recommendation
SC
AO
D
R=responsible, S=supporting, I=informed

4.4.2.3.5 Description Assessment Process

Summary

The assessment process consists of a functional test part and a security evaluation part. The assessment process prepares the decision taking process. The assessment process can be performed only after completion of the testing and evaluation process. Input of the assessment process are the functional test report and/or the security evaluation report.

During the assessment process the report results are formally checked by the AO.

The functional test report results are examined by the AO and the TC.

The security evaluation report results are examined by the AO and the SC.

If there are deviations which cannot be clarified by the AO, the TC or the SC, a recommendation is given for the AC and the AC has to decide about the approval.

Steps

4.4.2.3.5.1 Functional Test:

1. The TL delivers the functional test reports to the AO and the AA after finishing the testing.

2. The AO checks the results regarding formal aspects i.e. whether the tested interfaces correspond to the test object. If there are any unclear points, the AO is supported by the TL.

3. The AO examines the results of the functional test. This means, the AO examines whether there are deviations from the technical interface specifications of the tested interfaces or not.

4. If there are deviations from the technical interface specifications documented in the reports, the AO clarifies these deviations with the AA and TL. The assessment process for the functional test reports is finished when the AO can clarify these deviations with the AA and TL.

5. If the AO cannot clarify the deviation with the TL, the AO presents the information to the TC for examination. This includes for example:

    - approvals issued with the same deviation,

    - consequences for the practical use in the field and/or

    - duration of use depending on migrations.

Based on the information of the AA, AO and TL, the TC examines the deviations. The AO supports the examination of the TC.

The results of the examination can be:

- approval without condition: toleration of deviation,
- no approval: rework necessary or
- necessity of escalation to other responsible parties (e.g. MasterCard International, VISA International).

Based on the results of the examination the TC decides to give a recommendation for the AC or not. If no recommendation is given, the AO sends an intermediate reply to the AA with the results of the examination.

6. If a recommendation is given, the recommendation must include the results of the examination and a proposal for decision. The AO has to make sure that the recommendation is presented to the AC for the decision on the approval.

The AO documents all checking and examination results and reports them regularly to the TC and to the AC.

4.4.2.3.5.2 Security Evaluation:

7. The SEV must submit a final security evaluation report including external documents (e.g. certificates, if required by the payment scheme), to all the members of the SC and the AO. This final security evaluation report must be submitted at least eight days [without saturdays, sundays and public holidays] before the announced presentation date. If the deadline is not met or the AO identifies deviations from the formal requirements in this final security evaluation report during the formal check according to step 8, the security evaluation report will be rejected by the SC for this presentation date.

   Conditional Supplementary Step for TEC

   If required by the approval object, a TE provides a technical expert confirmation (TEC) for the consolidation of security-related and functional external certificates to GBIC via the AO. Since a TE for this task must always also be a SEV, the technical expert confirmation may be described as a separate chapter in a security evaluation report. If the TE is not the same SEV as for the security evaluation report or at time of the evaluation, a necessary external certificate is not yet available, the technical expert confirmation must be provided later by a separate document.

8. The AO performs a formal check of the submitted final security evaluation reports with regard to the registration number. This includes for example:

- Approval Applicant,
- results of the security evaluation regarding the registration of the product or system,
- applicable requirements and migration dates,
- characteristics of the product or system and
- configuration of hardware and software of the product or system.

If, during the formal check, the AO identifies deviations from the formal requirements in the submitted final security evaluation report (as defined in step 7), the security evaluation report will be rejected by the AO via the SC for the announced presentation date.

In advance to the final submission of a security evaluation report according to step 7, the SEV has the option to present his report to the AO to get a formal check. This premature submission must be done at least fourteen days [without saturdays, sundays and public holidays] prior to the SC meeting. If the report contains any unclear points, the AO contacts the SEV to clarify the open points. This clarification process must be finished before the deadline defined in step 7. If this clarification is not completed before the deadline of eight days defined in step 7, the security evaluation report will be rejected by the AO via the SC for the announced presentation date.

Conditional Supplementary Step for TEC

Technical expert confirmations (TEC) – if required by the approval object – will be formaly checked by the AO with regard to the registration number. If there are any ambiguities, the AO contacts the TE

9. The AO examines the results of the security evaluation reports based on a framework of rules. This means, the AO examines based on these rules whether the product or system meets all security requirements. The AO examines whether the security evaluation reports include the evaluation of a new evaluation object or the evaluation of a particular evaluation object (e.g. smart card operating system, Host Security Module). Based on the results of the examination the AO chooses the security evaluation reports to be presented to the SC and informs the SEV about necessary presentations.

   For security evaluation reports where not all security requirements are met the AO presents information to the SC for examination. This includes for example:

   - existing approvals with the same deviation,
   - consequences/conditions for the practical use in the field and
   - duration of use depending on migrations.

Conditional Supplementary Step for TEC

If required by the approval object, the AO examines the results of the technical expert confirmations (TEC) with regard to the applicability and coherence of the attached external certificates (e.g. Common.SECC and CFCF certificates). If there are any ambiguities, the AO presents these to the SC for examination.

10. The SEV presents the results of the chosen security evaluations in a meeting of the members of the SC. The SC/AO decide on the form of presentation.

    The SEV reports in the meeting the title of the evaluation report, the registration number, the evaluation object or security component. The SEV has to follow the GBIC defined presentation methodology in order to describe testing results uniquely. The SEV explains why the security requirements are met/not met by the product or system. If the compliance of the product or system with the security requirements are not strictly met from point of view of the SEV, the SEV explains each unclear point to the SC during the presentation. If necessary the SEV proposes adequate conditions. The SEV reports unclear points in all conscience during the presentation of the security evaluation report.

    If required, the TE presents the results of the chosen technical expert assessment in a meeting of the members of the SC. The SC/AO decide on the form of presentation.

11. Based on the security evaluation reports and the results of the presentation of the SEV, and, if present, on the additional results of the technical expert assessment of the TE, the SC assesses the compliance of the product or system with the security requirements. The results of the assessment can be:

    - accepted without condition: no deviation,
    - accepted without condition: toleration of deviation,
    - rejected; rework necessary or
    - necessity of escalation to Approval Council.

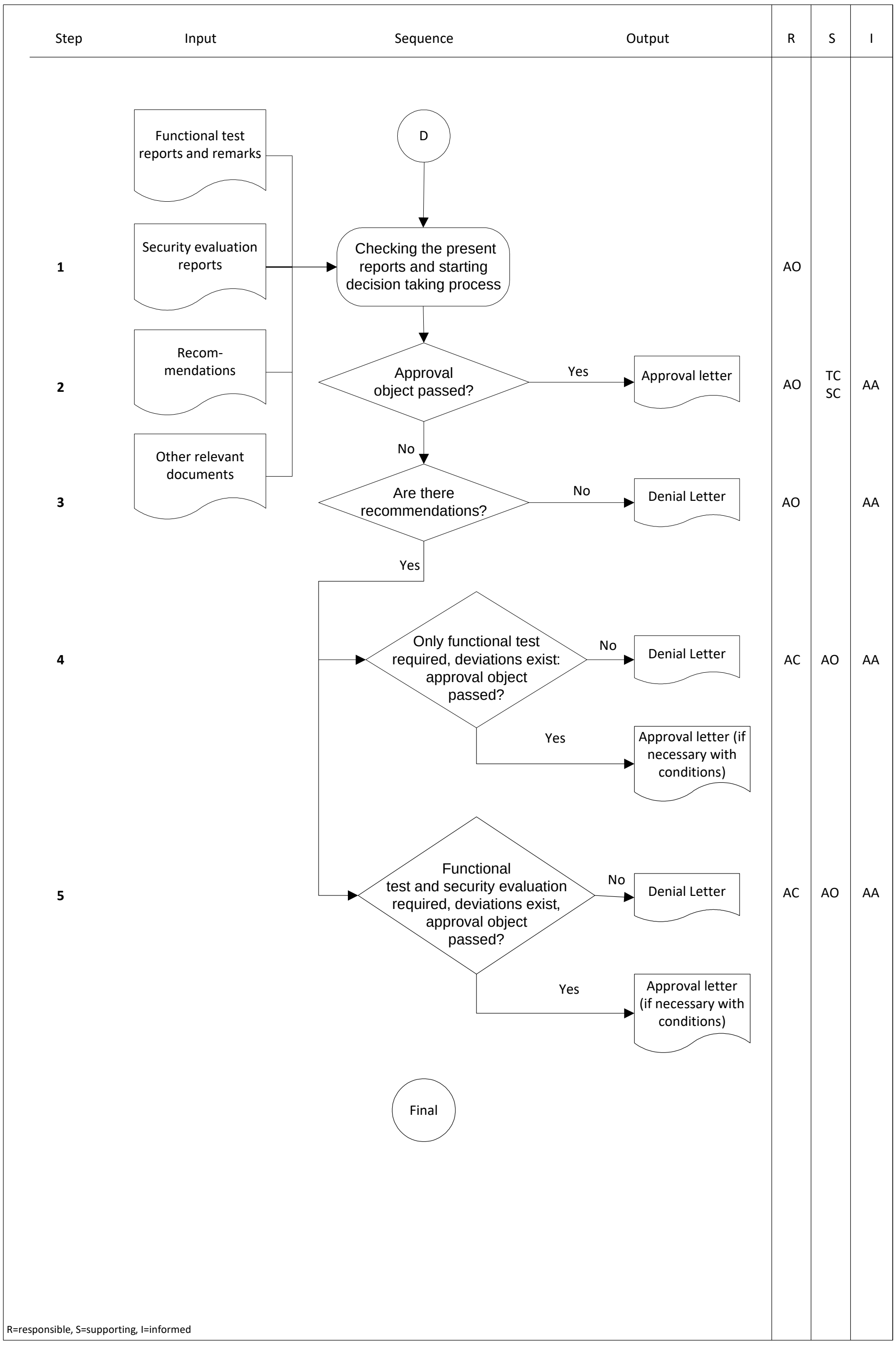
12. If no recommendation is given, the AO gives an intermediate reply for the AA with the results of the assessment.

13. If a recommendation is given, the recommendation must include the results of the examination and a proposal for decision. The AO has to make sure that the recommendation will be presented to the AC for decision on the approval.

The AO documents all checking, examination and assessment results and reports them regularly to the SC and to the AC.

4.4.2.3.6 Decision Taking Process

4.4.2.3.6.1 Sequence Decision Taking Process


Step
Input
Sequence
Output
R
S
I
Functional test reports and remarks
D
Security evaluation reports
1
Checking the present reports and starting decision taking process
AO
Recom-mendations
2
Approval object passed?
Yes
Approval letter
AO
TC
SC
AA
No
Other relevant documents
3
Are there recommendations?
No
Denial Letter
AO
AA
Yes
4
Only functional test required, deviations exist: approval object passed?
No
Denial Letter
AC
AO
AA
Yes
Approval letter (if necessary with conditions)
5
Functional test and security evaluation required, deviations exist, approval object passed?
No
Denial Letter
AC
AO
AA
Yes
Approval letter (if necessary with conditions)
Final
R=responsible, S=supporting, I=informed

4.4.2.3.6.2 Description Decision Taking Process

Summary

The decision of granting the approval is based on the results of the assessment process. In case that recommendations are given during the assessment process, the AC has to decide on the approval. In any other case based on the results of the assessment process, the AO decides supported by SC and TC on the approval. The AA is informed on the results by an approval letter resp. by a denial letter.

Steps

1. If all necessary documents (functional test report, security evaluation reports, etc.) have been presented to the AO, the AO has to decide on the approval or has to prepare the decision of the AC. Therefore the recommendations of the TC and SC and if necessary other documents have to be combined. Recommendations of the TC and SC for one product or system are applied by the AO for further products or systems.

2. If all approval requirements are met by the product or system, the AO sends the approval letter with an approval number to the AA. In case that the approval requirements are not met by the product or system and there is no recommendation, the AO informs the AA about the decision with a denial letter. The AO documents the decisions taken and reports them regularly to the AC.

3. Recommendations have to be treated by the AC.

4. If only a functional test is required for the approval and if the functional test report contains deviations which cannot be clarified, the AO presents the recommendation of the TC to the AC. The AC decides about the approval including conditions if necessary. The decision is documented by the AO. The AO informs the AA about the decision in form of an approval letter with an approval number or of a denial letter.

5. If a functional test as well as a security evaluation is required for the approval and if the functional test report and/or the security evaluation report contain deviations which could not be clarified, the AO presents recommendations of the TC and/or SC to the AC. The AC decides on the approval including conditions if necessary. The decision is documented by the AO. The AO informs the AA about the decision in form of an approval letter with an approval number or of a denial letter.

4.4.3 Administration Process

4.4.3.1 Purpose and Roles

The administration process consists of all administrative processes supporting the preparation and execution of the approval process. During the administration process GBIC open and granted approvals are administered and the adherence to migration dates is monitored.

The Approval Office (AO) is responsible for the execution of the administration process.

4.4.3.2 General Conditions

Tasks of the administration process are defined during the maintenance process. The administration process receives new or modified approval requirements out of the maintenance process (e.g. migration dates or technical interface specifications). Additionally new communication channels may be defined during the maintenance process.

4.4.3.3 Sub Processes

A) Documentation of results of the maintenance process (e.g. GBIC decisions) and of the approval process.

B) Maintaining distribution lists, contact person lists (providers, vendors).

C) Distribution of documents, information and letters with a document release control service.

Depending on the results of the maintenance process the AO provides the information about approval requirements (except technical interface specifications, see below) to vendors and providers. This information process is not restricted to the registration of products or systems to be approved. Also after the registration of products or systems for approval, the approval requirements (e.g. migration dates, technical interface specifications) can change as result of the maintenance process. If the maintenance process is completed for a new or modified approval object, the AA is informed about modifications of the approval requirements by the AO.

For this purpose GBIC provides a web server where technical interface specifications are published. Vendors and providers must sign the license agreement of GBIC, before using the GBIC technical interface specification. The AO is the GBIC contact point for the license agreement.

D) Archiving all approval relevant documents (contracts, agreements, technical interface specifications, forms, protocols, letters, functional test reports, security evaluation reports).

E) Keeping and publication of statistics.

F) Monitoring approval limitations (migration plans, proof of compliance in the field).

4.4.4 Extension of the Approval and Maintenance Process for EMV Debit/Credit

GBIC and Acquirer both act as AC and TC for the approval of EMV based Debit/Credit POS. The coordination and cooperation between these two institutions lead to sub processes for the Approval Process and the Maintenance Process:

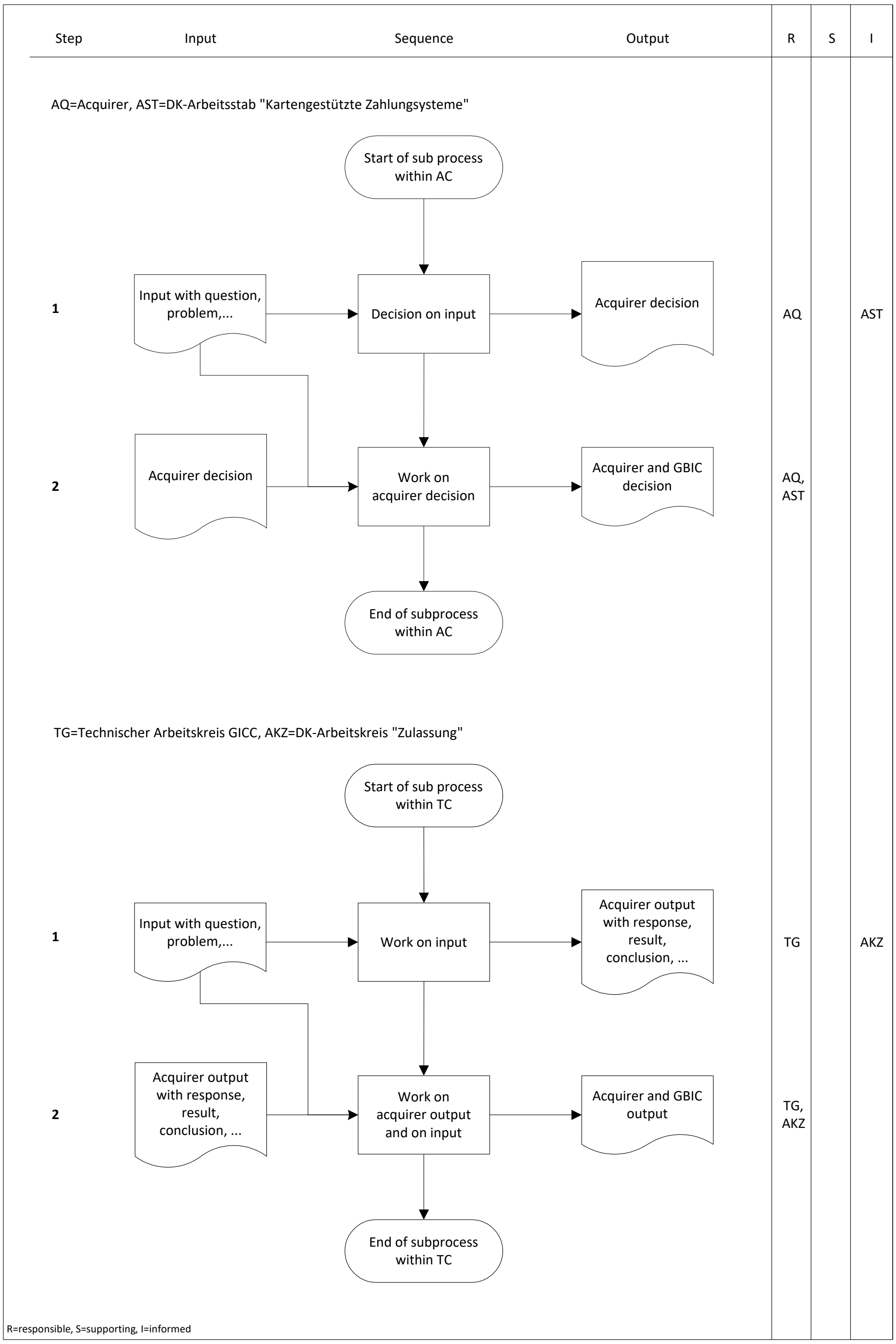
- One sub process shows the mapping of acquirers and GBIC to AC,
- another sub process shows the mapping of acquirers and GBIC to TC.

GBIC and the Acquirers (see chapter 6) defined this extension of the Approval and Maintenance Process.

Whenever AC resp. TC is actively involved within the GBIC Approval Scheme, the sub process shows how acquirers and GBIC cooperate.

After the description of the new sub process of AC resp. TC details of all connection points of AC resp. TC to the approval process and maintenance process are described.

Sequence for the Mapping of Acquirers and GBIC to AC resp. TC


Step
Input
Sequence
Output
R
S
I
AQ=Acquirer, AST=DK-Arbeitsstab "Kartengestützte Zahlungsysteme"
Start of sub process within AC
1
Input with question, problem,...
Decision on input
Acquirer decision
AQ
AST
2
Acquirer decision
Work on acquirer decision
Acquirer and GBIC decision
AQ, AST
End of subprocess within AC
TG=Technischer Arbeitskreis GICC, AKZ=DK-Arbeitskreis "Zulassung"
Start of sub process within TC
1
Input with question, problem,...
Work on input
Acquirer output with response, result, conclusion, ...
TG
AKZ
2
Acquirer output with response, result, conclusion, ...
Work on acquirer output and on input
Acquirer and GBIC output
TG, AKZ
End of subprocess within TC
R=responsible, S=supporting, I=informed

4.4.4.1 Mapping of Acquirers and GBIC to AC

The AC sub process is defined as follows:

1. The Acquirers (AQ) receive information about the occurring question or problem to be decided on. The AQ are informed per e-mail. The AQ internally discuss the question or problem and find a consistent decision. AQ send their consistent decision to the resp. committee of GBIC responsible for girocard (ACEC, see Glossary for the exact definition). The contact person is located at the credit sector association which is in the chair of GBIC (Federführer der Deutschen Kreditwirtschaft). The chair changes on a yearly basis.

2. Based on the decision of the AQ and based on the information about the question or problem, ACEC and AQ together find a consistent solution for the question or problem. The AQ nominate one contact person ("Federführer" AQ*) vis-à-vis to the ACEC. The ACEC communicates via AQ* with the AQ and vice versa. If needed, AQ and the ACEC meet together.

Within the maintenance process this sub process is executed as follows:

- During the examination and definition process (section 4.4.1.3.1) the requirements for a new or modified approval object are examined and defined. If applicable, the requirements of the global payment schemes regarding the handling of major and minor changes have to be taken into account. Committees of GBIC or the acquirers responsible for technical interface specifications, agreements or security requirements have to initiate this process by sending necessary information about the new or modified approval object to the TC and SC for assessment of the information.

  After the assessment of the information the AQ internally decide on the basis of the examination results of the TC and SC whether the new or modified approval object shall be introduced or not. AQ send their consistent decision to the ACEC. ACEC and AQ together find a consistent decision about a new or modified approval object.

- During the implementation process (section 4.4.1.3.2) the AO informs the AQ about the timeframe needed for the new approval process for the affected approval object to be available (e.g. to finalise approval documents and to implement new test procedures). AQ inform ACEC whether the approval document, test procedures, ... are internally accepted by the AQ. ACEC and AQ together adopt the new approval documents and new test cases.

Within the approval process this sub process is executed as follows:

1. The decision to grant an approval is based on the results of the assessment process (section 4.4.2.3.4). In case of escalation from TC to AC, recommendations are given by the TC during the assessment process and the AQ and ACEC decide on the approval (including further requirements if necessary). The AQ inform the ACEC about their consistent decision. If necessary, ACEC and AQ find a new decision together. The decision is documented by the AO. The AO informs the Approval Applicant (AA) about the decision in form of an approval letter with an approval number or in form of a denial letter.

4.4.4.2 Mapping of Acquirers and GBIC to TC

The TC sub process is defined as follows:

1. The acquirers represented by the "Technischer Arbeitskreis GICC" (TG) receive information about the occurring question or problem to be worked on. The TG is informed per e-mail. The TG internally discusses the question or problem and finds a consistent opinion, conclusion or response. Within the approval process (assessment of functional test deviations) the response must be found within 5 days [without saturdays, sundays and public holidays] after having received the information. The TG sends its consistent opinion, conclusion or response to the resp. committee of the GBIC, the "DK Arbeitskreis Zulassung" (AKZ).

2. Based on the opinion, conclusion or response of the TG and based on the information about the question or problem, AKZ and TG together find a consistent solution for the question or problem. The TG nominate one contact person ("Federführer" TG*) vis-à-vis to the AKZ. The AKZ communicates via TG* with the TG and vice versa. In particular cases the TG and the AKZ meet together.

Within the maintenance process the TC sub process is executed as follows:

- During this examination and definition process (section 4.4.1.3.1) the requirements for a new or modified approval object are examined and defined. Committees of GBIC or acquirers responsible for technical interface specifications, agreements or security requirements initiate this process. Whether the new or modified approval object shall be introduced or not is decided by the AC based on the examination results of TG and AKZ (step 3).
- Within the implementation process (section 4.4.1.3.2) TG and AKZ are responsible for the development or modification of
    - vendor/provider guidance concerning the approval process,

- the registration form for the approval object and
- the template for the approval letter.

TG and AKZ have to check the documents given by the AO (step 4).

Within the approval process this TC sub process is executed as follows:

- Within the registration process (section 4.4.2.3.1) TG and AKZ support the AO to check the approval eligibility (To enter the approval process, a product or a system must be able to meet the requirements of an approval object defined in the GBIC Approval Scheme. If the product or the system does not correspond to an approval object, the approval eligibility is denied and the product or the system does not enter into the approval process. The approval eligibility is checked during the registration process by the AO.)
- Within the assessment process (section 4.4.2.3.4) the TG and AKZ examine deviations. Based on the results of the examination the deviations are accepted, are not accepted or a recommendation is given to the AC to escalate the problem. Based on the results of the assessment process the AO is supported by TG and AKZ when the AO finally approves the product or system.

4.4.4.3 Security Committee

The role of the SC is mapped to the "DK Arbeitsstab Sicherheitsfragen". Acquirers and GBIC will discuss general security issues during regular or ad hoc joined meetings.

4.4.5 Refinement of the Maintenance and Approval Process for GBIC ICC Approval Objects

4.4.5.1 Maintenance Process refined for GBIC ICC Approval Objects

Generally all technical interface specifications must be considered during the functional test and the security evaluation of ICC modules resp. ICC products[2] which are to be approved according to the GBIC ICC approval objects. In particular the SEV must not only consider technical specifications related to executable code but also technical interface specifications related to application data structures.

If any technical interface specification mandated by the approval requirements is modified, an ICC product implementing these new technical interface specification must re-entry the GBIC approval process. In order to safe resources, a product must re-entry the GBIC approval process only if major differences between the already approved ICC product and the new ICC product exist in relation to functionality or security. If a new technical interface specification includes only minor changes compared to the old one, then the GBIC Approval Process is refined in order to avoid security evaluations or functional tests.

Therefore the maintenance process for GBIC ICC approval objects is refined as following:

4.4.5.1.1 Modification of Data Structures by GBIC

4.4.5.1.1.1 Impacts to the Functional Test

If GBIC (AC) modifies **data structures** in approval relevant technical interface specifications, GBIC (AC) can determine that **functional tests** already performed based on so far effective technical interface specifications are still valid. The **functional test** of an already approved ICC product based on the so far effective technical interface specification is sufficient for the approval of a successor ICC product configured according to the modified technical interface specification. For GBIC (AC) the modified technical interface specification compared to the so far effective technical interface specification is **equivalent in relation to the functional test**.

If GBIC (AC) determines that functional tests based on the so far effective technical interface specifications are not sufficient, the successor product must pass through Testsuite 2 based on the new data structures.

[2] For the definition of ICC modules and ICC products see glossary of this document.

4.4.5.1.1.2 Impacts to the Security Evaluation

If GBIC (AC) modifies **data structures** in approval relevant technical interface specifications, GBIC (AC) can determine that **security evaluations** already performed based on so far effective technical interface specifications are still valid. The **security evaluation** of an already approved ICC product based on the so far effective technical interface specification is sufficient for the approval of a successor ICC product configured according to the modified technical interface specification. For GBIC (AC) the modified technical interface specification compared to the so far effective technical interface specification is **equivalent in relation to the security evaluation**.

If **security features** are changed, the modified technical interface specification compared to the so far effective technical interface specification is not equivalent in relation to the security evaluation.

Example: A modification of application data structures in technical interface specifications which could affect security features are modifications of initial values for cryptographic key usage counters. If the old initial values for the cryptographic key usage counters are effective, the cryptographic keys are protected against disclosure by SPA/DPA. The attacker is not able to perform sufficient cryptographic operations for a successful SPA/DPA. With higher initial values for the cryptographic key usage counters this could not occur anymore. In this case, the security requirements are met with the so far effective initial values but not with the modified initial values.

GBIC (AC) therefore classifies technical interface specifications in case of a modification as following:

- If GBIC (AC) determines that modified technical interface specifications may have impacts to security features but the security requirements are not changed, then the modified technical interface specification must be considered in the GBIC Approval Scheme and must additionally be considered during the security evaluation. In this case a new security evaluation must be performed. If for the predecessor ICC product a security evaluation based on the so far effective technical interface specifications exists, then the fulfilment of the security requirements can also be demonstrated in form of a Security Evaluator Declaration.

- If GBIC (AC) determines that modified technical interface specifications have no impacts on security features and a security evaluation for the ICC product based on the so far effective technical interface specifications and security requirements exist, then this security evaluation is sufficient for the approval of a product configured according to the modified technical interface specification.

4.4.5.1.2 Modification of Executable Code by GBIC

If GBIC (AC) modifies the specifications for **executable code** in approval relevant technical interface specifications, then a new **functional test** and a new **security evaluation** is necessary. This applies even if an approval exists for the predecessor product implementing the so far effective technical interface specifications. If the modifications do not affect the security features of the ICC module resp. ICC product then a Security Evaluator Declaration is sufficient.

4.4.5.1.3 Modification of the Data Structures (without executable code) by the Card Publishers (Verlage)

If the Card Publishers (Verlage) modify **data structures** of approval relevant technical interface specifications for an ICC product, then GBIC (AC) determines whether the deviations have impact on the approval. The card publishers describe the deviations to GBIC (AC). GBIC (AC) classifies the deviations as following:

4.4.5.1.3.1 Impacts to the Functional Test

If the card publishers modify **data structures** of approval relevant technical interface specifications for a product then GBIC (AC) can determine that **functional tests** already performed on so far effective technical interface specifications are still valid. The **functional test** of an already approved product based on the so far effective technical interface specification is sufficient for the approval of a successor product configured according to the deviating configuration. For GBIC (AC) the deviating configuration compared to the so far effective technical interface specification is **equivalent in relation to the functional test**.

If GBIC (AC) determines that functional tests based on the so far effective technical interface specifications are not sufficient, then the ICC product must pass through Testsuite 2 based on the new data structures. A new approval for the ICC product is necessary.

The card publishers may modify data structures (without **executable code)** in technical interface specifications which are not relevant for any approval on their own.

4.4.5.1.3.2 Impact on the Security Evaluation[3]

If the card publishers modify the **data structures** of approval relevant technical interface specifications for a product then GBIC (AC) can determine that **security evaluations** already performed on so far effective technical interface specifications are still valid. The **security evaluation** of an already approved product based on the so far effective technical interface specification is sufficient for the approval of a product configured according to the deviating configuration. For GBIC (AC) the deviating configuration compared to the so far effective technical interface specification is **equivalent in relation to the security evaluation**.

If GBIC (AC) determines that a security evaluation of an already approved ICC product based on the so far effective technical interface specification is not sufficient for the approval of an ICC product configured according to the deviating configuration then a new security evaluation is necessary. A new approval for the ICC product is necessary. If already a security evaluation exists then the fulfilment of the security requirements can also be demonstrated in form of a Security Evaluator Declaration.

The card publishers may modify data structures without **executable code** in technical interface specifications which are not relevant for any approval on their own.

4.4.5.1.4 Modification of Executable Code by the Card Publishers (Verlage)

If the Card Publishers (Verlage) modify the specifications for **executable code** in approval relevant technical interface specifications then in either case for a product a new **functional test** and a new **security evaluation** is necessary. A new functional test and a new security evaluation is necessary even if an approval exists for the predecessor product implementing the so far effective technical interface specifications. If the modifications does not affect the security features of the ICC module resp. ICC product then a Security Evaluator Declaration is sufficient.

4.4.5.2 Consideration of Patches

The Approval Owner may change the executable code of an ICC module resp. ICC product which is already approved according to GBIC ICC approval objects. For this case new general conditions differing from chap. 4.3 apply for GBIC ICC approval objects: **The modified ICC module resp. ICC product must always be tested (Testsuite 1 and 2) and evaluated independent of the kind of change of the executable code.** The patch must be evaluated by

[3] The card publishers in general do <u>not</u> cause deviations in the data structures having impact on the security of the product. The process is listed here for the sake of completeness.

the SEV although the Approval Owner may consider the patch to be not security relevant. The functional test (Testsuite 1 und 2) must be repeated although the Approval Owner may consider the patch to be not relevant for the interface of the ICC module resp. ICC product. The Approval Owner must inform the AO about the changes using a change registration.

In case of minor changes (e.g. if the Approval Owner considers the changes in the executable code not to be security relevant) after the security evaluation of the patch the SEV summarises its results in a Security Evaluator Declaration. The declaration must describe the patch and its impacts. The Security Evaluator Declaration has to be sent for assessment to the AO.

In case of major changes of the executable code after the security evaluation of the patch a new Security Evaluation Report must be sent to the AO and to the members of the SC as required in step 7 of the assessment process.

In order to differentiate between the ICC module resp. ICC product executable code excluding the patch and the ICC module resp. ICC product executable code including the patch, the version of the executable code has to be changed appropriately by the Approval Owner.

4.4.6 Refinement of the Hardware Security Evaluation for GBIC ICC Approval Objects

4.4.6.1 Introduction

The compliance with the security requirements of the German Banking Industry Committee (GBIC), hereinafter referred to as “Criteria of GBIC” for hardware and firmware of GBIC smart cards, hardware and firmware in the following briefly called hardware, usually may be verified in two alternatives:

1. informally by submission of a GBIC hardware security evaluation prepared by GBIC security evaluators who must be recognised by GBIC for this task.
2. by certificates according to the Common Criteria (CC) Standard, which are issued by governmental national certification bodies, so-called SOGIS CC Certification Bodies[4], as well.

In the following, it is specified how this optional process is embedded in GBIC´s approval process.

[4] “Senior Officials Group Information Systems Security” (SOGIS). The international SOGIS agreement will ensure, that certifications in a SOGIS member country qualified for the implementation of the corresponding certification, will be accepted by every other SOGIS member country.

First, the approval process for an informal GBIC security evaluation without using Common Criteria will be described, followed by an explanation of the optional process based on a CC certificate.

Subsequently, the maintenance process of the hardware security evaluation will be illustrated. Moreover, it will be demonstrated how to proceed in case of the extension of an approval or the change of an approval.

The specific glossary in chapter 4.4.6.7 defines the roles in the above mentioned processes.

4.4.6.2 Process for the Informal Evaluation of GBIC Smart Cards

1. The Hardware Manufacturer orders a GBIC hardware security evaluation from a GBIC Hardware Security Evaluator to prove that the criteria of GBIC are met by the tested hardware.
2. The GBIC Hardware Security Evaluator performs a GBIC hardware security evaluation according to state-of-the-art in science and technology in an informal way. On behalf of the Hardware Manufacturer the GBIC Hardware Security Evaluator provides the **GBIC Smart Card Security Evaluator** with a summarised report of the GBIC hardware security evaluation (i.e. an abstract of the GBIC hardware security evaluation).
3. The Smart Card Manufacturer chooses for its product development a hardware for the GBIC smart card.
4. The Hardware Manufacturer provides the Smart Card Manufacturer with the “Security User Guidance“[5] to ensure the secure usage of the hardware during the development of the software.
5. The Smart Card Manufacturer commissions a **GBIC Smart Card Security Evaluator** with a GBIC smart card security evaluation for its GBIC smart card in accordance with the GBIC criteria and applies for a GBIC approval at the GBIC approval office.
6. The GBIC Smart Card Security Evaluator reviews
    a. the compliance with the criteria of the German Banking Industry Committee,
    b. the validity of the GBIC hardware security evaluation (according to state-of-the-art of science and technology[6]),

[5] The “Security User Guidance“ ensures that the software developer implements the security requirements of the hardware.

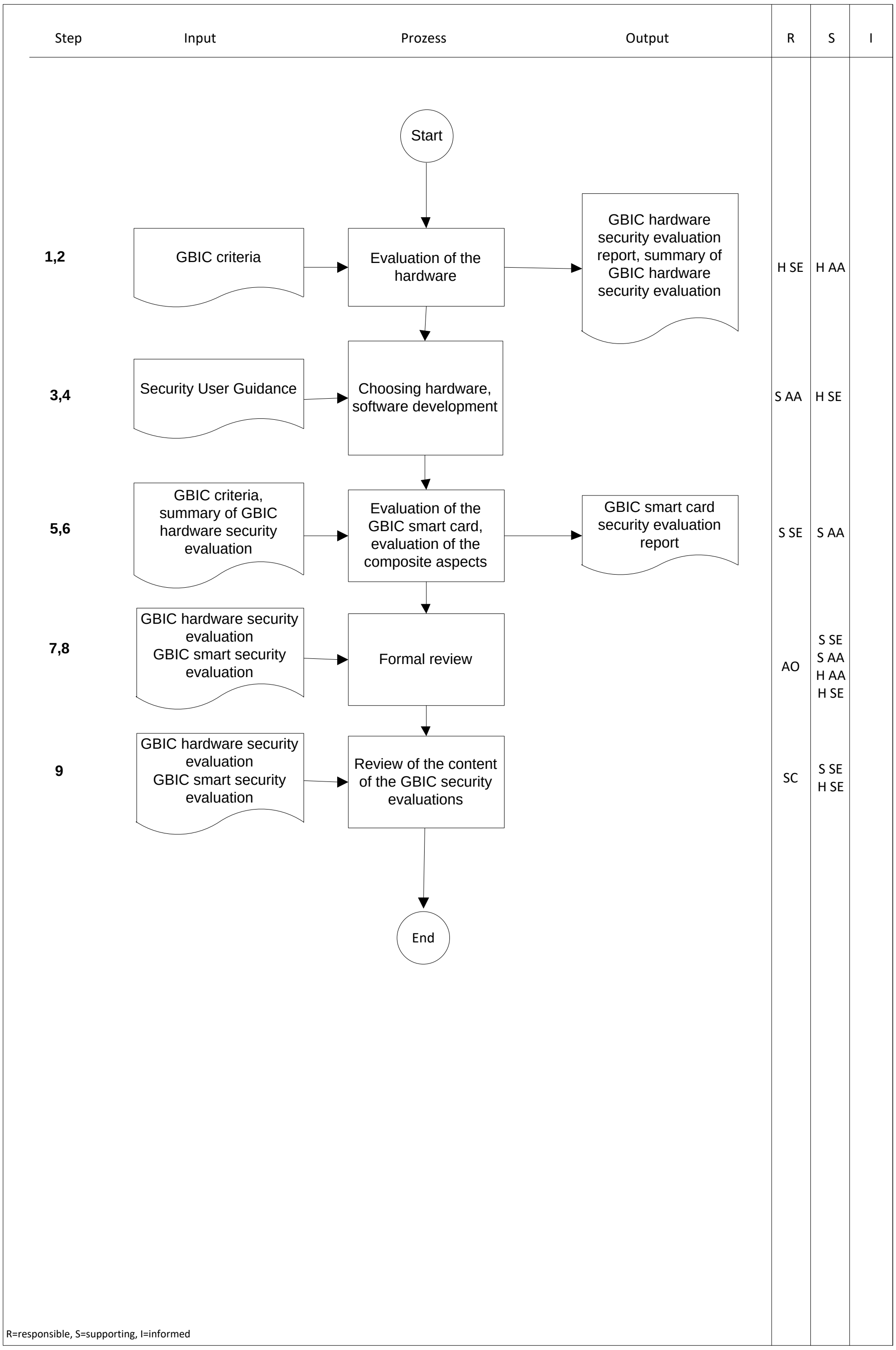
[6] To verify the validity in accordance with today state-of-the-art in science and technology the GBIC Smart Card Security Evaluator checks the summarised report for its age and with regard to the consideration of new attacking techniques. Whenever a decision cannot be reached by the GBIC Smart Card

   c. the compliance with and the validity of the “Security User Guidance”

   d. as well as all obligations possibly mentioned in the GBIC hardware security evaluation.

7. The GBIC Smart Card Security Evaluator submits the GBIC smart card security evaluation to GBIC. The GBIC Hardware Security Evaluator submits the GBIC hardware security evaluation to GBIC.
8. The GBIC Approval Office reviews the formal requirements for the GBIC security evaluation. The security officers or contact persons for hardware are included in the GBIC hardware security evaluation.
9. The technical review of the GBIC security evaluation is realised by the GBIC Security Committee.

Security Evaluator, the GBIC Smart Card Security Evaluator requires a current statement on the validity of the presented GBIC hardware security evaluation from the GBIC Hardware Security Evaluator.


Step
Input
Prozess
Output
R
S
I
Start
1,2
GBIC criteria
Evaluation of the hardware
GBIC hardware security evaluation report, summary of GBIC hardware security evaluation
H SE
H AA
3,4
Security User Guidance
Choosing hardware, software development
S AA
H SE
5,6
GBIC criteria, summary of GBIC hardware security evaluation
Evaluation of the GBIC smart card, evaluation of the composite aspects
GBIC smart card security evaluation report
S SE
S AA
7,8
GBIC hardware security evaluation
GBIC smart security evaluation
Formal review
AO
S SE
S AA
H AA
H SE
9
GBIC hardware security evaluation
GBIC smart security evaluation
Review of the content of the GBIC security evaluations
SC
S SE
H SE
End
R=responsible, S=supporting, I=informed

R = Responsible
S = Support
I = Information

4.4.6.3 Evaluation Process of GBIC Smart Cards based on a CC Certificate

1. The Hardware Manufacturer applies for a CC certification to a CC certificate issuing SOGIS CC Certification Body qualified for "EAL1-7 for Smartcards and similar devices".
2. The Hardware Manufacturer or the Smart Card Manufacturer commissions the CC Hardware Evaluator with a CC evaluation to prove that the security requirements of the Hardware Protection Profiles PP-0035 / PP-0084 are met.[7] The CC Hardware Evaluator performs a CC evaluation in accordance with this PP. On behalf of the Hardware Manufacturer the CC Hardware Evaluator provides with the "ETR for Composition"[8] the **GBIC Smart Card Security Evaluator** who is also licensed for conducting CC evaluations.
3. Following the completion of the evaluation the SOGIS CC Certification Body publishes the certification report of the CC evaluation which includes the certificate for the CC evaluation on its homepage.
4. The Smart Card Manufacturer chooses for its product under development a hardware for the GBIC smart card.
5. The Hardware Manufacturer provides the smart card manufacturer with the "Security User Guidance"[9] for the hardware to develop the software.
6. The Smart Card Manufacturer commissions a GBIC Smart Card Security Evaluator with a security evaluation according to the criteria of the GBIC and applies for a GBIC approval at GBIC for its GBIC smart card.

[7] The PP applicable for the hardware of smart cards, PP-0035 for short, will be replaced by a successor-PP, PP-0084 for short. Hardware that is already PP-0035-certified or hardware that still needs to be certified (i.e. within ongoing proceedings) will remain within the CC certification procedure for the next couple of years. Thus, they can still be used for GBIC approval. The PP-0084 has to be used for new hardware, because the PP-0084 is mandatorily required since January 2015 by the SOGIS CC certification bodies. The evaluation according to the PP does not necessarily cover all security requirements of GBIC mentioned in the detailed approval requirements. Hence, during the modelling of the Security Target the indications in the detailed approval requirements are to be followed.

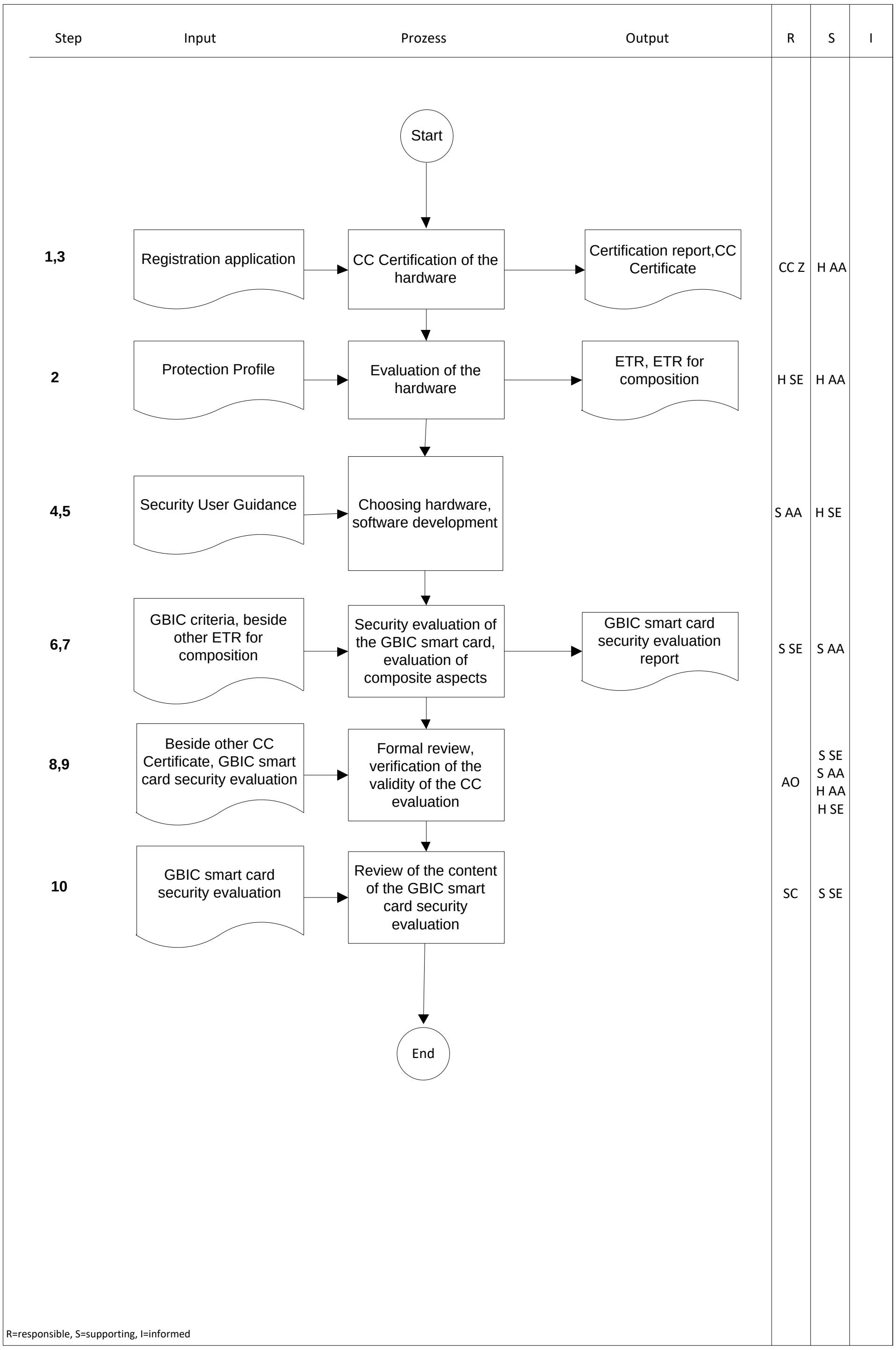
[8] The "ETR for Composition" (Evaluation Technical Report for Composition) summarises the results of the hardware in a way that the GBIC Smart Card Security Evaluator can use these results in the evaluation of the GBIC smart card as a composite product of hardware and software. The CC Hardware Evaluator is asked by the Hardware Manufacturer to provide the GBIC Smart Card Security Evaluator with the "ETR for Composition".

[9] The "Security User Guidance" ensures that the software developer implements the security requirements of the hardware.

7. The GBIC Smart Card Security Evaluator reviews
    a. the compliance with the GBIC criteria taking the "ETR for Composition" into consideration,
    b. the "validity"[10] of the CC certificate (security statement within the selected SOGIS procedure shall not be older than 18 months – date of "ETR for Composition" – and certificate not withdrawn),
    c. the compliance of CC certificate with the PP[11] required by GBIC,
    d. the compliance with and the validity of the "Security User Guidance"
    e. as well as all obligations possibly mentioned in the CC certificate.
    f. The GBIC Smart Card Security Evaluator asks the Smart Card Manufacturer for the contact details of the security officers for hardware and for the contact persons of the Hardware Manufacturer and lists them in the "Overview Section" of the evaluation (Part A). Alternatively, the Hardware Manufacturer´s security officers or contact persons may also be inquired during registration of the GBIC smart card.
8. The GBIC Smart Card Security Evaluator submits the GBIC security evaluation for the GBIC smart card as well as the reference to the CC certificate for the CC hardware evaluation to GBIC.
9. The GBIC Approval Office reviews the formal requirements for a GBIC security evaluation as well as the "validity" of the CC certificate (security statement in the adopted SOGIS procedure shall not be older than 18 months – date of ETR for Composition – and certificate not withdrawn) as well as the formal compliance of the CC certificate with the PP required by GBIC. An independent registration of hardware with GBIC is not necessary.
10. The technical review of the GBIC security evaluation is realised by the GBIC Security Committee.

[10] The validity of the CC certificate refers to the usability of the hardware certificate for a composition evaluation /-certification (regulated e.g. in the German scheme in BSI 7138, point 5.5, AIS36 or in the composite product evaluation for smart cards and similar devices, version 1.2, January 2012, of the JIL). This validity can be determined using the date of the "ETR for Composition".

[11] If the CC certificate does not cover all additionally in the detailed approval requirements mentioned GBIC security requirements, these either have to be handed-in informally in form of a GBIC security evaluation subsequently or the CC certificate has to be extended accordingly. It is assumed that this extension is realised as part of a re-evaluation according to CC, which leads to a new certificate.


Step
Input
Prozess
Output
R
S
I
Start
1,3
Registration application
CC Certification of the hardware
Certification report,CC Certificate
CC Z
H AA
2
Protection Profile
Evaluation of the hardware
ETR, ETR for composition
H SE
H AA
4,5
Security User Guidance
Choosing hardware, software development
S AA
H SE
6,7
GBIC criteria, beside other ETR for composition
Security evaluation of the GBIC smart card, evaluation of composite aspects
GBIC smart card security evaluation report
S SE
S AA
8,9
Beside other CC Certificate, GBIC smart card security evaluation
Formal review, verification of the validity of the CC evaluation
AO
S SE
S AA
H AA
H SE
10
GBIC smart card security evaluation
Review of the content of the GBIC smart card security evaluation
SC
S SE
End
R=responsible, S=supporting, I=informed

R = Responsible
S = Support
I = Information

4.4.6.4 Re-Assessment of Hardware[12]

If the GBIC Smart Card Security Evaluator is asked by the Smart Card Manufacturer to submit a GBIC smart card security evaluation to GBIC but the security statement underlying the CC certificate is older than 18 months – date of ETR for Composition – or in case it is unclear, whether at the discretion of the GBIC Smart Card Security Evaluator the GBIC hardware security evaluation still meets the security requirements considering state-of-the-art in science and technology, it has to be proved that the hardware meets the criteria of GBIC as follows.

4.4.6.4.1 Re-Assessment for the GBIC Hardware Security Evaluation

The GBIC Hardware Security Evaluator submits a recent GBIC hardware security evaluation or a GBIC evaluation declaration on behalf of the Hardware Manufacturer to GBIC in which it is substantially confirmed, that the criteria of GBIC are still met. If a written, informal confirmation from the GBIC Hardware Security Evaluator is considered as sufficient by the GBIC smart card security evaluator, the presentation of a current GBIC hardware security evaluation may be waived.

4.4.6.4.2 Re-Assessment for the CC Certificate

If the CC certificate has not been withdrawn, but the security statement underlying the CC certificate is older than 18 months (date of “ETR for Composition”), the following procedure shall be applied in order to maintain the validity.

For this, the Hardware Manufacturer can pass through the appropriate process of its SOGIS CC Certification Body to maintain the CC certificate.[13]

A written, informal confirmation containing a justification by the CC Hardware Evaluator is sufficient as long as it acknowledges to the GBIC Smart Card Security Evaluator that

a. the security requirements of the PPs are still met and

[12] The considered hardware will not be changed, but simply re-assessed by the evaluators.

[13] In the course of a first approval of the GBIC smart card the Hardware Manufacturer has to pass through the process of its SOGIS CC Certification Body to maintain a CC certificate, because in this case the statements pursuant chapter 2 apply. GBIC accepts the re-assessment statement of every SOGIS CC Certification Body. For renewal of the certificate of a SOGIS CC Certification Body the re-assessment is obligatory once the deadline is expired, which is prescribed by this SOGIS CC Certification Body. This deadline may also be less than 18 months.

b. the “ETR for Composition” underlying the certificate is still valid considering state-of-the-art in science and technology or that an updated “ETR for Composition” is submitted to the GBIC Smart Card Security Evaluator and

c. the “Security User Guidance” underlying the CC certificate is still valid or that the Hardware Manufacturer provides the GBIC Smart Card Security Evaluator with a more recent version of it.

4.4.6.5 Change and Extended Approval of the GBIC Smart Card

The GBIC Smart Card Security Evaluator has to return a verdict on the security of the hardware and the software within the scope of an **Extended Approval** as well as a **Change Approval** of the GBIC smart card.

4.4.6.5.1 Extended Approval of the GBIC Smart Card

To obtain an extension for an already approved GBIC smart card after a certain period specified by GBIC, the Smart Card Manufacturer has to confirm that the security requirements of GBIC are still met. For this purpose the Smart Card Manufacturer commissions a GBIC Smart Card Security Evaluator with the implementation of the assessment and the preparation and presentation of the GBIC evaluator declaration including the result of the evaluation.

In the course of an Extended Approval the GBIC smart card evaluator examines, possibly by means of new penetration tests,

a. the compliance with the latest “Security User Guidance” and

b. whether the security requirements are still met considering state-of-the-art in science and technology.

The evaluator of the hardware is obliged to support the GBIC Smart Card Security Evaluator as described in chapter 4.4.6.4. The GBIC Smart Card Security Evaluator has to perform the assessment taking into account all information provided by the evaluator of the hardware.

4.4.6.5.2 Change Approval of the GBIC Smart Card

If software or data structures of an already approved GBIC smart card have been changed and the GBIC smart card shall be re-approved by a **Change Approval,** the process sequence described in chapter 4.4.5 must be followed.

The GBIC Smart Card Security Evaluator reviews

a. the effects of the change according to the requirements of chapter 4.4.5

b. as well as the compliance of the recent “Security User Guidance” and

c. whether the security requirements are still met considering state-of-the-art in science and technology.

The hardware evaluator is obliged to support the GBIC Smart Card Security Evaluator as described in chapter 4.4.6.4. The GBIC Smart Card Security Evaluator has to perform the assessment taking into account all information provided by the hardware evaluator.

The re-certification may also be required if security relevant parts of the hardware have been changed. If security relevant parts of the hardware have been modified, a summary of a recent GBIC hardware security evaluation or a recent CC certificate with the associated "ETR for Composition" for hardware has to be presented to the GBIC Smart Card Security Evaluator.

If the changes are not security related, the hardware evaluator must support the GBIC Smart Card Security Evaluator analogous to the description in chapter 4.4.6.4. For this, a maintenance certificate covering the non-security-related hardware changes may be used.

4.4.6.6 Tabular Overview Based on a CC Certificate

	Initial Approval GBIC Smart Card	**Change Approval GBIC Smart Card**	**Extended Approval GBIC Smart Card**
Security statement in the hardware certificate not older than 18 months – date "ETR for Composition" – and not withdrawn	GBIC security evaluation for GBIC smart card based on the documents of the CC evaluation of the hardware.	GBIC security evaluation for GBIC smart card based on the documents of the CC evaluation of the hardware. In adherence to chapter 4.4.6.4.2 informal confirmation from the CC Hardware Evaluator to the GBIC Smart Card Security Evaluator of the GBIC smart card, that security statements or maintenance certificate, in case of security-related changes to the hardware, are still valid.	GBIC evaluation declaration for GBIC smart card based on the documents of the CC evaluation of the hardware.
Security statement in the hardware-certificate older than 18 months – date "ETR for Composition" – and not withdrawn	GBIC security evaluation for GBIC smart card based on the documents of the CC evaluation of the hardware. The Hardware Manufacturer has to pass the process of its SOGIS CC Certification Body to maintain a CC certificate.	GBIC security evaluation for GBIC smart card based on the documents of the CC evaluation of the hardware. In adherence to chapter 4.4.6.4.2 informal confirmation from the CC Hardware Evaluator to the **GBIC Smart Card Security Evaluator** of the GBIC smart card, that security statements are still valid.	GBIC evaluation declaration for GBIC smart card based on the documents of the CC evaluation of hardware. In adherence to chapter 4.4.6.4.2 informal confirmation from the CC Hardware Evaluator to the **GBIC Smart Card Security Evaluator** of the GBIC smart card, that security statements are still valid.

4.4.6.7 Glossary – Hardware Security Evaluation for GBIC ICC Approval Objects

GBIC Hardware Security Evaluator (H SEV)

Reviews the hardware for its use in a GBIC smart card. He/She evaluates the hardware with regard to the compliance of the GBIC security requirements.

Hardware Manufacturer (HM)

Develops and produces the hardware for use in a GBIC smart card. Normally the manufacturer does not only provide the semiconductor, but a firmware for the use of the corresponding semiconductor which will be assigned to the "hardware" in the present approval process.

Smart Card Manufacturer (SC M)

Produces GBIC smart cards. The manufacturer develops software, which is used in composition with the hardware in the GBIC smart card and applies for GBIC approval for its GBIC smart card.

CC Hardware Evaluator (H SEV)

Evaluates the hardware for use in a GBIC smart card in accordance with the international Common Criteria Standard. The evaluation facility of the CC hardware evaluator is recognised by a SOGIS CC Certification Body to be qualified to perform the corresponding evaluations in the "Technical Domain Smartcards and similar devices".

SOGIS CC Certification Body (CC CB)

Certifies a hardware CC evaluation. The certificate will be recognised by other SOGIS CC Certification Bodies, if the SOGIS CC Certification Body issuing the certificate is qualified to certify a hardware CC evaluation. Currently, these are the SOGIS CC Certification Bodies BSI, CESG, ANSSI, NLNCSA and CCN.
(See http://www.sogisportal.eu/uk/status_participant_en.html)

GBIC Smart Card Security Evaluator (S SEV)

Reviews a GBIC smart card. He/She tests the integration of the hardware in the GBIC smart card and the software of the GBIC smart card in regard to the compliance with the GBIC security requirements.

GBIC Approval Office (AO)

Manages the GBIC approval process and carries out the formal review of the applications for registration as well as the formal review of the GBIC security evaluations.

GBIC Security Committee (SC)

Performs the technical review of the GBIC security evaluation.

4.5 Approval Process Documentation

The approval documents are archived by the AO.

4.5.1 Approval Information

Approval information describes the approval process for AAs. The approval information consists of a guidance documentation including the approval requirements for each approval object.

4.5.2 Registration

To check the approval eligibility, the product or system must be registered by the AA. The AA has to register and fill in details at the online registration tool (ZAM) or the registration form can be downloaded via internet (www.die-dk.de) or ordered at the AO. Accompanying details are provided by zulassungsbuero@voeb.de for the vendor. The registration provides information about the AA and (future) Approval Owner, the approval object and its approval requirements, the payment schemes an approval is requested for, already presented reports and the implementation planning.

The registration contains the following information:

- name and address of the AA (only once),
- supported payment schemes,
- the approval object,
- information concerning first approval, change approval or approval extension,
- the description of the product or system to be approved (hardware and software configuration, functions and characteristics, interfaces etc.),
- technical interface specification the product or system adheres to (name, version, date),
- evaluation objects of the approval object: if necessary the approval object may consist of several security components - for each security component the AA must indicate the corresponding security evaluation report with its registration number if possible,
- point in time at which the security evaluation report and functional test report are targeted to be finished.

For each product or system a separate registration has to be done.

4.5.3 Information about the Eligibility for Approval

The AO checks the approval eligibility of the product or system once the AA confirms the finalisation of the registration. If ZAM was used for registration and all details are correct and consistent, the AO sets the status “valid approval request: in evaluation and assessment process” and the AA will be informed automatically about the successful finish of the registration by a push mail.

4.5.4 Functional Test Report

The TL summarises the results of the functional test of the product or system in a functional test report. The functional test report describes all tested interfaces. Intermediate functional test report are not relevant within the approval process, therefore in this document functional test reports are always final functional test reports.

4.5.5 Security Evaluator Declaration

The Security Evaluator Declaration is a document where the Security Evaluator is declaring that a product or a system meets security requirements without giving detailed evidence. The Security Evaluator Declaration needs only to be sent for assessment to the GBIC Approval Office. Usually a Security Evaluator Declaration refers to Security Evaluation Reports declaring that security requirements are still met. The Security Evaluator Declaration must be based on security requirements of the respective approval object. Depending on the supported payment schemes, different security requirements may apply. Each Security Evaluator Declaration must be referred to by the registration number of the product or system to be approved. Each Security Evaluator Declaration must meet the formal requirements of GBIC.

4.5.6 Security Evaluation Report

The SEV summarises the results of the security evaluation in a security evaluation report which is sent and presented to the AO/SC. Contents of a security evaluation report is the security evaluation of the entire product or system or of single security components. The security evaluation report must be based on security requirements of the respective approval object. Depending on the supported payment schemes, different security requirements may apply. Each security evaluation report must be referred to by the registration number of the product or system to be approved. Each security evaluation report must meet the formal requirements of GBIC.

4.5.7 Technical Expert Confirmation

The TE summarises the results of his investigation on a subject that required his technical expertise and confirms the result in a Technical Expert Confirmation. Each such confirmation must be referred to by the registration number of the product or system to be approved. In accordance with the defined GBIC requirements, it must declare the exact names and versions of all components and documents which were the subject of the investigation.

If a Technical Expert Confirmation is required as part of the functional test process for a specific approval object (see chapter 4.4.2.3.2.2), then it is provided by the TE to the Approval Applicant as a separate document. The Applicant then uses the Technical Expert Confirmation as a mandatory attachment to a Testing Conformance Statement for submission to GBIC via the AO.

If a Technical Expert Confirmation is required as part of the assessment process for a specific approval object (see chapter 4.4.2.3.5.2), then it is provided by the TE to GBIC via the AO as a separate document or as a separate chapter in the security evaluation report. In the latter case, the TE must be a GBIC-listed Security Evaluator (see chapter 4.1.2.5).

4.5.8 Testing Conformance Statement

The Testing Conformance Statement is a document in which the Approval Applicant declares that the product or system to be approved meets the functional requirements of a test object based on the results of a self-test. The requirements for the self-test are defined by GBIC.

Depending on the test object, requirements for the structure and content of a TCS are predefined and

- the attachment of a technical expert confirmation (TEC) (see chapter 4.5.7) or
- the written confirmation of the appropriate testing of the interfaces by the processing partner (see e.g. chapter 5.4.5.5)

can be demanded.

4.5.9 Intermediate Reply for Approval

During the approval process, security evaluation reports and/or functional test reports might be sent to the AO at different times and/or in different order. The approval can only be given if all necessary documents are presented and assessed with a positive result. During this process, the AO informs the AA about intermediate decisions by approval intermediate replies.

4.5.10 Contracts and other Documents

There are approvals where it is necessary for the AA to sign contracts or other documents. These documents will be sent to the AA together with the approval eligibility letter.

4.5.11 Approval Letter

If the approval is granted by GBIC, the AO issues an approval letter. This approval letter includes the approval number, the approval owner, the payment schemes the approval is issued for, the approval object and its detailed approval requirements, like the technical interface specifications, the security requirements, the results of functional testing and security evaluations and the validity of the approval.

4.5.12 Approval Lists

The lists of approved products or systems are maintained by the AO. These lists are published on the internet (www.die-dk.de).

4.6 Objects of the GBIC Approval Scheme

4.6.1 Approval Object

An approval object is a well defined component as part of one or more payment scheme. Each approval object is defined by its approval requirements. A successful functional test of the test object and if necessary a successful security evaluation of the corresponding evaluation object are required for the approval. Approval objects of the GBIC Approval Scheme are defined in GBIC and/or payment scheme agreements.

Approval objects can be GBIC ICC approval objects with payment scheme applications, ATMs or terminals with payment scheme applications, host systems and provider.

In case there exist different alternative classes of requirements for one approval object, several approval types may be defined for clarification which class requires which kind of validation. Separate approval types could be defined for different reader types which require a security evaluation or not.

During the registration it is checked whether the product or the system of the AA is able to meet the requirements of an approval object. As result of registration a product or system gets a registration number.

4.6.2 Evaluation Object and Security Components

For each approval object with specific security requirements an evaluation object is defined. An implementation of an evaluation object may consist of one or more security components. Each security evaluation report describes the security evaluation of a product or system or of a security component. Therefore for each approval object with specific security requirements there must be one security evaluation report per evaluation object. Additionally there may be security evaluation reports of the security components.

Example for an evaluation object: for the approval object "Automated Teller Machine (ATM)" the evaluation object "Encrypting PIN Pad" is defined.

Examples for security components:

- Security components of the evaluation object "host system" are the security concept of the provider-network, the "Host Security Module (HSM, Sicherheitsbox)" and the operating environment of the network provider.

- Security component of the evaluation object "Terminal" is the PED (security processor inside, operating system, applications and the personalisation environment at the vendor).

The security evaluation verifies the compliance of products, systems or security components with security requirements of the respective evaluation object. Therefore each security evaluation report must deliver a statement of compliance for every security requirement.

The AO refers to evaluation objects and security components based on the information in the registration. Therefore the registration of products or systems includes information about the evaluation object. Each security evaluation report includes the registration number of the product or system to be approved. The security components are defined during the registration. If possible, the security components are referred to by the registration number of the evaluation object. If a security evaluation of a security component is used in other security evaluations, the registration number of the already registered product or system has to be referred to in the registration as well as in the security evaluation report of the new product or system.

4.6.3 Test Object

For each approval object with specific functional requirements a test object is defined. The definition of the test object consists of the definition of interfaces and other well specified requirements of the approval object.

By functional tests it is examined whether the product or system submitted for approval meets the technical interface specifications. Typical interfaces to be tested are the interface between the ICC and the terminal or the interface between the terminal and the host system. Other interfaces to be tested may be the interface between the terminal and the cardholder.

Each functional test report refers to the registration number of the product or system submitted for approval.

5 Basic Approval Requirements

This chapter describes the basic approval requirements for each approval object of the GBIC Approval Scheme. These basic approval requirements are the firm part of the approval requirements which have to be met by any implementation of an approval object. The detailed approval requirements which are defined in annexes of this document may be subject to more frequent modifications.

After the description of the payment scheme where the approval object is used, agreements and contracts, especially the agreements of GBIC with global payment schemes, are described. Afterwards the approval objects with their functions and applications are defined and described. References to interface specifications etc. are not part of this description, but included into the detailed approval requirements.

Afterwards the evaluation object of the approval object is described listing the required security evaluation reports (hardware, software, environment, ...). The security requirements of the scheme (national, global, ...) which have to be met by the evaluation object are referred to whereas the reference to the corresponding security requirements is part of the detailed approval requirements.

Finally the test object of the approval object is described defining required functional tests. The references to the technical interface specifications are part of the detailed approval requirements.

5.1 GeldKarte

5.1.1 System Description

The GeldKarte scheme is a GBIC electronic purse scheme.

5.1.2 Agreements/Contracts

GBIC specifies the functional and security requirements for the GeldKarte scheme in the technical interface specifications of the GeldKarte agreement by GBIC. These technical interface specifications are used for the implementation of components in the GeldKarte scheme. In particular, the interfaces between the purse card, the merchant system ("Händlersystem"), the secure application module for the payment transaction ("Händlerkarte") and the interface between the purse card and the loading terminal ("Ladeterminal") for the loading transaction are specified.

5.1.3 GBIC ICC Approval Objects

The approval object SAM ICC with the application "Händlerkarte" and the Credit ICC or Debit ICC with the application "GeldKarte" are described in chapter 5.3.

5.1.4 Approval Object "Taschenkartenleser"

5.1.4.1 Description of the Approval Object

The approval object personal purse reader ("Taschenkartenleser") represents a device of hardware and software covering the technical interface specifications of the GeldKarte scheme to read free readable data from cardholder ICCs. Regularly these are the actual amount of the GeldKarte in EF_BETRAG as well as the last loading and payment transactions in EF_LLOG and EF_BLOG.

The approval of the "Taschenkartenleser" is issued as a Type Approval.

5.1.4.2 Security Evaluation

5.1.4.2.1 Security Requirements

For the "Taschenkartenleser" there are no security requirements to be verified by a security evaluator.

5.1.4.2.2 Evaluation Object

The "Taschenkartenleser" has no evaluation object.

5.1.4.3 Functional Test

5.1.4.3.1 Functional Test Requirements

The functional test requirements consist of tests according to the technical interface specification for the "Taschenkartenleser".

5.1.4.3.2 Test Object

The interface of the "Taschenkartenleser" to the cardholder ICC and to the cardholder is tested.

5.1.5 Approval Object "Händlersystem" (optionally with "Virtuelle Händlerkarte")

5.1.5.1 Description of the Approval Object

The approval object "Händlersystem" (optional "Händlersystem mit virtueller Händlerkarte") represents a device of hardware and software covering the technical interface specifications of the GeldKarte scheme to perform payment transactions controlling the communication between the cardholder ICC with contact based or contactless interface and the secure application module "Händlerkarte".

A "Händlersystem" respective "Händlersystem mit virtueller Händlerkarte" consists of three components

- "Akzeptanzterminal",
- "Kassenschnittterminal" and
- "Einreichungsterminal".

These components can be implemented in a distributed system.

The approval object "Händlersystem" must be used together with the physical "Händlerkarte". In the "Händlersystem mit virtueller Händlerkarte", the functionality of the physical "Händlerkarte" is virtualy integrated into the merchants system instead of a physical "Händlerkarte". The approval object "Händlersystem mit virtueller Händlerkarte" must be applied together with the functionality "Virtuelle Händlerkarte". The approvals of the "Händlersystem" as well as of the "Händlersystem mit virtueller Händlerkarte" are issued as Type Approvals.

The "Händlersystem mit virtueller Händlerkarte" must support OPT.

5.1.5.2 Security Evaluation

5.1.5.2.1 Security Requirements

Each security relevant component involved in the GeldKarte scheme has to meet the security requirements of the GeldKarte scheme listed in the detailed approval requirements.

Since the "Virtuelle Händlerkarte" is a security relevant component, a "Händlersystem mit virtueller Händlerkarte" has to meet security requirements. For a "Händlersystem" (supporting the physical "Händlerkarte") there are no specific security requirements to be met.

5.1.5.2.2 Evaluation Object

The "Virtuelle Händlerkarte" is the evaluation object of the "Händlersystem mit virtueller Händlerkarte".

5.1.5.3 Functional Test

5.1.5.3.1 Functional Test Requirements

The functional test requirements consist of tests according to the technical interface specification of the GeldKarte scheme for "Händlersysteme" and "Händlersysteme mit virtueller Händlerkarte".

5.1.5.3.2 Test Object

The interface of the "Händlersystem" or "Händlersystem mit virtueller Händlerkarte" to the cardholder ICC, the cardholder, the merchant and the "Händlerevidenzzentrale (HEZ)" is tested. For "Händlersysteme" (i.e. if no "Virtuelle Händlerkarte" is used) the interface to the "Händlerkarte" is tested additionally.

If "Virtuelle Händlerkarte" is supported, the additional interface to the "Personalisierungsstelle" (OPT) is tested.

5.1.6 Approval Object "Internet-Händlersystem" (optionally with "Virtuelle Händlerkarte")

5.1.6.1 Description of the Approval Object

The "Internet-Händlersystem" (optional "Internet-Händlersystem mit virtueller Händlerkarte") is based on the "Händlersystem", designed to support payments on the internet and represents a separate approval object. The differences between the "Internet-Händlersystem" and the "Händlersystem" are described in the detailed approval requirements.

The approval of the "Internet-Händlersystem" or "Internet-Händlersystem mit virtueller Händlerkarte" is issued as a Type Approval. The "Händlersystem mit virtueller Händlerkarte" must support OPT.

5.1.6.2 Security Evaluation

5.1.6.2.1 Security Requirements

Since the "Virtuelle Händlerkarte" is a security relevant component, an "Internet-Händlersystem mit virtueller Händlerkarte" has to meet the security requirements of the GeldKarte scheme. For an "Internet-Händlersystem" (supporting the physical "Händlerkarte") no specific security requirements have to be met.

5.1.6.2.2 Evaluation Object

The "Virtuelle Händlerkarte" is the evaluation object of the "Internet-Händlersystem mit virtueller Händlerkarte".

5.1.6.3 Functional Test

5.1.6.3.1 Functional Test Requirements

The functional test requirements consist of tests according to the technical interface specification of the GeldKarte scheme for "Internet-Händlersysteme" and "Internet-Händlersysteme mit virtueller Händlerkarte".

5.1.6.3.2 Test Object

The interface of the "Internet-Händlersystem" or "Internet-Händlersystem mit virtueller Händlerkarte" to the " Kundenterminal", the merchant and the "Händlerevidenzzentrale (HEZ)" is tested. For "Internet-Händlersysteme" (i.e. if no "Virtuelle Händlerkarte" is used) the interface to the "Händlerkarte" is tested additionally.

5.1.7 Approval Object "Automatenterminal" (optionally with "Virtuelle Händlerkarte")

5.1.7.1 Description of the Approval Object

An "Automatenterminal" is a component intended for integration into an unattended system, e.g. a vending machine. It provides for GeldKarte contact based or contactless based payment transactions according to the technical interface specifications of the "Händlersystem". Since an "Automatenterminal" may support the "Virtuelle Händlerkarte" ("Automatenterminal mit virtueller Händlerkarte"), the technical interface specifications for "Händlersystem mit virtueller Händlerkarte" are also relevant for the "Automatenterminal mit virtueller Händlerkarte".

Additionally specific requirements apply to ensure the correct integration into a vending machine. The machine integrating the terminal is not part of the approval object. The approval for an "Automatenterminal" respective "Automatenterminal mit virtueller Händlerkarte" may include specific conditions for the integration into a machine. If the machine meets these conditions, no separate approval for the machine is needed. The conditions are listed in the approval letter.

For "Automatenterminal mit virtueller Händlerkarte" the OPT function is required.

5.1.7.2 Security Evaluation

5.1.7.2.1 Security Requirements

Since the "Virtuelle Händlerkarte" is a security relevant component, an "Automatenterminal mit virtueller Händlerkarte" has to meet the security requirements of the GeldKarte scheme.

For an "Automatenterminal" supporting a physical "Händlerkarte" no specific security requirements have to be met.

5.1.7.2.2 Evaluation Object

The "Virtuelle Händlerkarte" is the evaluation object of the "Automatenterminal mit virtueller Händlerkarte".

5.1.7.3 Functional Test

5.1.7.3.1 Functional Test Requirements

The functional test requirements consist of tests according to the technical interface specification of the GeldKarte scheme for "Händlersysteme" with/without "virtueller Händlerkarte" and "Automatenterminals".

5.1.7.3.2 Test Object

The interface of the "Automatenterminal" or "Automatenterminal mit virtueller Händlerkarte" to the cardholder ICC, the merchant, the vending machine and the "Händlerevidenzzentrale (HEZ)" is tested. For "Automatenterminals" (i.e. if no "Virtuelle Händlerkarte" is used) the interface to the "Händlerkarte" is tested additionally.

If "Virtuelle Händlerkarte" is supported, the additional interface to the "Personalisierungsstelle" (OPT) is tested.

5.1.8 Approval Object "Einreichungsterminal"

5.1.8.1 Description of the Approval Object

The approval object "Einreichungsterminal" is a device of hardware and software covering the technical interface specifications of the GeldKarte scheme to prepare transaction data for the transfer to the "Händlerevidenzzentrale (HEZ)" and for carrying out the transfer. The format of the file at the interface between "Akzeptanz-/Kassenschnittterminal" and "Einreichungsterminal" has to be the same as it is used at the interface to the "Händlerevidenzzentrale (HEZ)".

The approval of the "Einreichungsterminal" is issued as a Type Approval.

5.1.8.2 Security Evaluation

5.1.8.2.1 Security Requirements

For the "Einreichungsterminal" no specific security requirements have to be met.

5.1.8.2.2 Evaluation Object

The "Einreichungsterminal" has no evaluation object.

5.1.8.3 Functional Test

5.1.8.3.1 Functional Test Requirements

The functional test requirements consist of tests according to the technical interface specification of the GeldKarte scheme for the "Händlersystem".

5.1.8.3.2 Test Object

The interface of the "Einreichungsterminal" to the "Händlerevidenzzentrale (HEZ)" is tested.

5.1.9 Approval Object "Kundenterminal" (KT)

5.1.9.1 Description of the Approval Object

The approval object KT is a device of hardware and software covering the respective technical interface specifications and security requirements of the GeldKarte scheme to perform internet payments. The KT controls the communication between the purse card and the "Internet-Händlersystem" via internet or other open networks and is used as a secure interface to the cardholder.

The approval of the KT is issued as a Type Approval.

5.1.9.2 Security Evaluation

5.1.9.3 Security Requirements

Each component involved in the GeldKarte scheme that performs security relevant operations has to meet the security requirements referred to in the detailed approval requirements for

GeldKarte. The KT is a security relevant component of the GeldKarte scheme and has to meet these security requirements.

The technical interface specification for the KT includes additional information concerning the security requirements (application notes).

5.1.9.3.1 Evaluation Object

The entire KT is the evaluation object of the approval object KT.

The evaluation object includes the hardware, the software and the personalisation environment of the KT. During security evaluation it is verified whether the security requirements for ICC based payment schemes are met considering the application notes in the technical interface specifications.

5.1.9.4 Functional Test

5.1.9.4.1 Functional Test Requirements

The functional test requirements consist of tests according to the technical interface specification of the GeldKarte scheme for the KT.

5.1.9.4.2 Test Object

The interface of the KT to the cardholder ICC, to the cardholder and to the "Internet-Händler-system" are tested.

5.1.10 Approval Object "Secoder 3"

The approval object "Secoder 3" is a device of hardware and software. The German Banking Industry developed a concept and specifications for universal smart card readers under the name of Secoder which shall support a unique solution for secure payments via internet.

Depending of its type the card reader is suitable for the safeguarding of online banking, for internet payments and for the use of electronic signatures.

A "Secoder 3" card reader controls the communication between GBIC ICC and the background system via internet or other open networks and is used as a secure interface to the cardholder.

At time, GBIC defines the requirements for three different types of card readers. Thus, three alternative approval types are defined for the approval object "Secoder 3":

- Secoder 3 Type C (chipTAN-reader),
- Secoder 3 Type G (reader containing multiple Secoder applications).

5.1.10.1 Approval Type "Secoder 3 Type C" (chipTAN-reader)

5.1.10.1.1 Description of the Approval Type

A "Secoder 3 Type C" is a single purpose smart card reader with display and keypad, equal to the known chipTAN-Leser.

As a mandatory application, it supports at least:

- chipTAN (ctn),

as an optional application, it may support:

- Default application.

"Secoder 3 Type C" controls the communication between GBIC ICC and the background system via internet or other open networks and is used as a secure interface to the cardholder.

The approval of a "Secoder 3 Type C" is issued as a Type Approval.

With the issuance of the type approval, the approval applicant receives the right to use the trademark "chipTAN" and the logo for "chipTAN" for the approved "Secoder 3 Type C".

5.1.10.1.2 Security Evaluation

5.1.10.1.2.1 Security Requirements

For the "Secoder 3 Type C" there are no security requirements that must be verified by a security evaluation.

5.1.10.1.2.2 Evaluation Object

The "Secoder 3 Type C" has no evaluation object.

5.1.10.1.3 Functional Test

5.1.10.1.3.1 Functional Test Requirements

For the "Secoder 3 Type C" there are no functional test requirements that must be verified by a functional test.

5.1.10.1.3.2 Test Object

The "Secoder 3 Type C" has no test object.

5.1.10.1.4 Statement of Compliance

The approval applicant has to declare a statement of compliance according the form "Herstellererklärung: Einhaltung der DK-Vorgaben für die Realisierung eines Secoder 3 – Typ C".

5.1.10.2 Approval Type "Secoder 3 Type G" (reader containing multiple Secoder applications)

5.1.10.2.1 Description of the Approval Type

A "Secoder 3 Type G" is a smart card reader with display and keypad. It allows the support of a subset of the following applications:

- chipTAN (ctn),
- Signature application with AUT key (aut),
- EMV Signature (emv),
- Default application.

"Secoder 3 Type G" controls the communication between GBIC ICC and the background system via internet or other open networks and is used as a secure interface to the cardholder.

"Secoder 3 Type G" may contain optionally the so called default application. The default application allows the exchange of ICC commands/ responses, as far as the access rules configured in the reader allow that accesses. If the Secoder 3 Type G contains the application " Signature application with AUT key (aut)" it shall contain also the Default application.

A "Secoder 3 Type G" supports a firmware/ software update.

The approval of a "Secoder 3 Type G" is issued as a Type Approval.

With the issuance of the type approval, the approval applicant receives the right to use the GBIC's seal "Secoder – Empfohlen von den Banken und Sparkassen" for the approved "Secoder 3 Type G".

5.1.10.2.2 Security Evaluation

5.1.10.2.2.1 Security Requirements

The "Secoder 3 Type G" has to fulfill the security requirements, which are defined in the "Sicherheitseigenschaften des Kundenterminals Secoder 3". The compliance with the security requirements concerning the update of the reader software/firmware has to be verified by a security evaluation.

5.1.10.2.2.2 Evaluation Object

The functionality for firmware and/or software update represents the evaluation object for the approval type "Secoder 3 Typ G".

5.1.10.2.3 Functional Test

5.1.10.2.3.1 Functional Test Requirements

For the "Secoder 3 Type G" there are no functional test requirements that must be verified by a functional test.

5.1.10.2.3.2 Test Object

The "Secoder 3 Type G" has no test object.

5.1.10.2.4 Statement of Compliance

The approval applicant has to declare a statement of compliance according the form "Herstellererklärung: Einhaltung der DK-Vorgaben für die Realisierung eines Secoder 3 – Typ G".

5.1.11 Approval Object "Ladeterminal"

5.1.11.1 Description of the Approval Object

The approval object "Ladeterminal" is a device of hardware and software covering the technical interface specifications and security requirements of the GeldKarte scheme for loading devices. The "Ladeterminal" is used by the cardholder of the purse card to transfer value from the cardholders account to the purse. The "Ladeterminal" performs loading transactions and controls the communication between the electronic purse and the backend system. "Ladeterminals" where the cardholder has to enter a PIN include a PED. For loading against other means of payment no PIN may be required, however a security module in the terminal to ensure the correct processing is required. A "Ladeterminal" can be part of a multifunctional system, e.g. an ATM.

The approval of the Ladeterminal is issued as a Type Approval.

5.1.11.2 Security Evaluation

5.1.11.2.1 Security Requirements

The "Ladeterminal" is a security relevant component of the GeldKarte scheme performing sensitive loading transactions and transferring the PIN. It has to meet the security requirements of the GeldKarte scheme.

5.1.11.2.2 Evaluation Object

The PED or the security module is the evaluation object of the approval object "Ladeterminal".

The evaluation object includes the hardware, the software and the personalisation environment of the PED or the security module. During the security evaluation it is verified whether the PED or the security module meets the security requirements of the GeldKarte scheme.

As result of the security evaluation of the PED or the security module the SEV may identify special conditions for the environment of the evaluation object. The SEV must document these conditions in the security evaluation report of the evaluation object. Similar to the ATM the environment conditions may refer to "View protection against PIN disclosure" (if necessary), "Sequence control" or "Software integrity" and "Secure key loading".

The approval letter refers to any additional condition for the operational environment of the evaluation object which cannot be met by the PED or security module alone.

5.1.11.3 Functional Test

5.1.11.3.1 Functional Test Requirements

The functional test requirements consist of tests according to the technical interface specification of the GeldKarte agreement for "Ladeterminal".

5.1.11.3.2 Test Object

The interface of the Ladeterminal to the cardholder ICC, the cardholder, the operator, the "Ladezentrale" and the "Personalisierungsstelle" (OPT) are tested.

5.1.11.3.3 Approval Restrictions

A "Ladeterminal" supporting the function "Laden gegen Bar" has to meet the requirements of German law, especially § 36 "Bundesbankgesetz". Details are available at the AO.

5.2 girocard

5.2.1 System Description

“girocard” is GBIC’s debit POS scheme. The girocard terminals located at the retailer’s side are technically operated by network providers, which are certified and approved by GBIC.

5.2.2 Agreements/Contracts

GBIC specifies the functional and security requirements for the girocard scheme in the technical interface specification of the girocard contract between GBIC and network providers. This technical interface specification, called the technical appendix of the girocard agreement in the following, is used for the implementation of components in the girocard scheme. The interface between the network provider and the girocard terminal is not part of the technical appendix of the girocard agreement.

For the security evaluation of the terminal platform (hard- and firmware), a Common.SECC certificate is mandatory since January 1st, 2017. GBIC together with UK Finance defined a common security evaluation and certification process. For this purpose GBIC and UK Finance founded Common.SECC (the Common Security Evaluation and Certification Consortium) which delivers a Common.SECC certificate as the result of a successful security evaluation according to ISO 15 408 Common Criteria. The Consortium is based on a Consortium Agreement.

For the functional test of a "girocard terminal" GBIC allows two alternative technical interface specifications:

- the technical appendix of the girocard agreement including the EMV POS Debit/Credit requirements specified in the "Schnittstellenspezifikation für chipbasierte EMV-Debit/Credit-Anwendungen, POS-Terminals" (DC POS) or
- the nexo Implementation Specifications (nexo IS).

GBIC is part of the CFCF (Common Functional Certification Framework) Consortium which governs the CFCF documents, the certification process for nexo implementations and the delivery of terminal and acquirer host certifcates based on nexo IS.

The consortium is based on a Consortium Agreement.

5.2.3 GBIC Payment Cards Approval Objects

The approval object Debit ICC with the application "girocard" is described in chapter 5.3.

The approval object "girocard HCE" with a girocard application on a "digitale girocard" using an Host Card Emulation (HCE) solution is described in chapter 5.4.3.

The approval object "Online-Netzbetreiber", which are responsible for the processing of "digitale girocard" E-Commerce transaction on the merchant's side, is described in chapter 5.4.5.

5.2.4 Approval for "girocard Terminal"

5.2.4.1 Description of the Approval Object

The approval object "girocard Terminal" represents a device defined as a platform (hardware and firmware) and software combination covering technical interface specifications and security requirements defined by GBIC to carry out payment transactions. A terminal equipped with a PED must either support contact based transactions or support contactless transactions or support both kinds of transaction. A terminal without PED (TOPP) may support contactless transactions and may support contact based transactions. The allowed contactless/ contact support combination depends on the choseable type of TOPP.

The approval of a "girocard Terminal” is granted as a Type Approval. The approved terminal is allowed to be operated in the field only after the integration into a "girocard Network" as described in chapter 5.2.5.

Already existing certifications for the hardware and software combination will be taken into account (if applicable) during the Type Approval process to minimise efforts:

- EMVCo Type Approval Contact Level 1 as well as Level 2 certification for the contact based transactions,
- EMVCo Type Approval Contactless Level 1 for the contactless based transactions,
- CFCF certificate for nexo IS implementations and
- Common.SECC certificate (mandatory since January 1st, 2017).

The corresponding EMVCo approval letters, CFCF certificates and Common.SECC certificates have to be delivered for verification.

The platform certificate issued by Common.SECC has to be delivered by the SEV as one part of the terminal evaluation report which is assessed by the SC.

If a CFCF certificate for a nexo IS implementation is delivered, then a technical expert confirmation (see chapter 4.5.7) for the consolidation with the Common.SECC certificate for the hardware/firmware (terminal platform) and software combination to be approved has to be delivered by a Technical Expert (TE). The TE is a SEV listed by GBIC and has to be nominated by the GBIC for the consolidation of certificates for the approval object "girocard Terminal”.

5.2.4.2 Security Evaluation

5.2.4.2.1 Security Requirements

Each component involved in the girocard system and performing sensitive operations has to meet the security requirements of the technical appendix.

5.2.4.2.2 Evaluation Object "girocard Terminal"

The evaluation object has to meet the security requirements defined by GBIC. For the CC evaluation of the terminal platform (hard- and firmware) the requirements are defined in Protection Profiles applicable for terminals equipped with a PED or for a TOPP which are published via the Common.SECC web site.

The Common.SECC certificate covers the terminal platform. Therefore the SEV must deliver the evaluation report for the payment application – taking into account the results of the platform evaluation - and the evaluation of the personalisation site in addition. All three parts form the complete terminal evaluation report which must be delivered by the SEV of the payment application.

Consolidation of security and functional certificates for nexo IS terminals

If a terminal supporting nexo IS functionality has been evaluated, a technical expert confirmation (see chapter 4.5.7) for the consolidation with Common.SECC certificates and CFCF certificates is mandatory.

By the technical expert confirmation, the TE confirms:

1. that the implementations of the application software with respect to the evaluated and tested requirements as examined in the

    a. the evaluation of the payment application, proven by a GBIC evaluation report and

    b. the CFCF application functional test, proven in the CFCF certificate

    do not differ and

2. that the terminal platform (hardware and firmware) as assessed in the

    a. the Common.SECC evaluation for the terminal platform, proven in the Common.SECC certificate and

    b. the application certified under 1

interact in such a way that the security requirements and functional requirements underlying the single certifications are fully complied with by the terminal, without the joint interaction restricting or changing the respective certified functional and security-relevant configurations and properties, or otherwise defining any conditions to be fulfilled for the joint secure and functional interaction.

If any security requirement or functional requirement could be affected by the combination of the present certified functional and security configuration, the exact conditions for the joint secure and functional interaction must be defined. In this case, a presentation of the technical expert confirmation in the SC is mandatory.

If the SEV of the payment application and the TE are the same instance, the technical expert confirmation can be described as a separate chapter in the complete terminal evaluation report. Nevertheless a technical expert confirmation as a separate document can be provided.

5.2.4.3 Functional Test

5.2.4.3.1 Functional Test Requirements

The functional test requirements consist of tests according to the technical appendix including the EMV POS Debit/Credit requirements or the nexo IS requirements. For the validation of the nexo IS requirements, the CFCF certificate (including the nexo ICS) based on nexo IS has to be provided. The CFCF certificate will be taken into account for a girocard approval if the certificate is sufficient to fulfil the GBIC functional test requirements.

5.2.4.3.2 Test Object "girocard Terminal"

The test object "girocard Terminal" assigned to the approval object "girocard Terminal" has to pass

- a terminal functional test to proof compliance with the requirements of the technical appendix including the EMV POS Debit/Credit specifications or

- a CFCF certification alternatively.

Compliance with the Technical Appendix including the EMV POS Debit/Credit Specification

In the following the proof of the compliance with the technical appendix including the EMV POS Debit/Credit specification is described:

- The EMV POS Debit/Credit and the common online test interface (TAI) requirements for girocard EMV processing as well as the terminal management.

- An additional terminal functional test for online personalisation of the public keys in case this should be supported.

If the test object has already an EMVCo Level 1 or an EMVCo Level 2 approval, this approval is taken into account (if applicable). Due to integration necessities, a sample of EMV Level 1 test cases is tested again.

Compliance with nexo IS

For the compliance with nexo IS the CFCF certificate together with the nexo ICS has to be presented only. The functional test includes the validation of the nexo FAST application including mandatory functions (e. g. contact based "Payment" and "Manual Reversal" ("Manuelles Storno", called "Cancellation" in nexo IS)), and the nexo Acquirer as well as Terminal Management System (TMS) protocols.

5.2.5 Approval for "girocard Network"

5.2.5.1 Description of the Approval Object

According to the network provider contract ("Netzbetreibervertrag") with the subtitle "Vertrag über die Zulassung als Netzbetreiber im girocard-System der deutschen Kreditwirtschaft", the network provider is entitled to operate girocard terminals within the girocard scheme only if he has an approval for its network and all terminals connected to it. The approval of the network provider cannot be transferred to other companies.

For the approval of "girocard Network" the following mandatory approval objects are defined:

- "girocard Network" (defined in this chapter) and
- "girocard Terminal" equipped with a PED and supporting at least contact based transactions (see chapter 5.2.4),

For the approval of "girocard Network" the following optional approval objects are defined:

- "girocard Terminal" without a PED (TOPP) (see chapter 5.2.4),
- "girocard Terminal" equipped with a PED and supporting contactless transactions (see chapter 5.2.4).

The approval object "girocard Network" represents a system consisting of

- the host of the network provider,
- the hardware and software of the network provider Host Security Module,
- the operating environment of the network provider and
- at least one or more terminals having a type approval as a "girocard Terminal" (see chapter 5.2.4).

The "girocard Network" must be in compliance with the technical appendix of the girocard agreement. Note: The technical appendix of the girocard agreement includes also details of the approval process for the approval of an "girocard Network".

The interfaces to be examined within the approval process include basically the interface to the authorisation system and, optional, the OPT interfaces. Since the interface between the terminals and the host system is network provider specific, the approval of the "girocard Network" is issued as a provider specific approval.

The approval objects "girocard Network" and "girocard Terminal" must be in compliance with the technical appendix including the EMV POS Debit/Credit requirements (see chapter 5.7).

5.2.5.2 Security Evaluation

5.2.5.2.1 Security Requirements

Each component in the girocard system which performs sensitive operations has to meet the security requirements of the technical appendix and the security requirements for the pure chip-based girocard system. Therefore the "girocard Network" has to meet these security requirements.

One evaluation object is defined for the approval object "girocard Network".

5.2.5.2.2 Evaluation Object "Network Provider System"

This evaluation object is assigned to the approval object "girocard Network" consists of

- the operating environment of the host system,
- the terminal network concept including the interface between the girocard terminal and the host and
- the hardware and software of the Host Security Module.

For the evaluation object "Network Provider System" the following security evaluation reports are necessary:

- The security evaluation report for the terminal network concept describing the technical interface between the host system and the girocard terminals considering the girocard security requirements.
- The security evaluation report for the hardware and software of the Host Security Module based on the network concept and referring to the security requirements of the Host Security Module’s operating environment considering girocard.
- The integrative security evaluation report for all security relevant components of the terminal network ("Integrationsgutachten") including the terminal network concept, the

Host Security Module, the evaluation of the operating environment of the host system (provider site inspection and nomination of the provider security manager) and the girocard terminal.

- The integrative security evaluation report for all security relevant components of the terminal network ("Integrationsgutachten") must be submitted for the first product approved according to "girocard Terminal" being included into the network. After having included the first product according to "girocard Terminal" any new product according to "girocard Terminal" can be included into the network without the necessity to update the integrative security report. This rule holds as long as the approval office is informed about the initial operation.

The integrative security evaluation report for the terminal network ("Integrationsgutachten") refers to the evaluation object whereas the other security evaluation reports listed above are security evaluation reports for security components. In addition the integrative security evaluation report contains the result of integrative security tests.

The evaluation object has to meet the requirements of the technical appendix and the security requirements for the girocard system.

The GBIC security requirements to be complied with are described in the chapter "Sicherheitsanforderungen an girocard-Terminal-Netze" of the technical appendix.

5.2.5.3 Functional Test

5.2.5.3.1 Functional Test Requirements

The functional test requirements consist of tests according to the technical appendix including the EMV POS Debit/Credit requirements.

Two different test objects are defined for the approval object "girocard Network". From these one test object is defined additionally for the approval object "girocard Terminal".

5.2.5.3.2 Test Object "Network Provider System"

This test object is assigned to the approval object "girocard Network".

The test object "Network Provider System" includes interfaces to the authorisation system, to cardholder and card and to the OPT personalisation centre. The interfaces to be tested are referred to in the detailed approval requirements. A functional test is required to test whether the host system meets the requirements of the technical appendix of the girocard agreement. In this functional test the interface to the authorisation system, the format of clearing and fee collection data, the interfaces to the OPT personalisation centre and the interfaces to card and cardholders are tested. Additionally a proof of conformance with the technical appendix must be provided for the girocard EMV interfaces. Therefore the test object has to meet the EMV POS Debit/Credit requirements (see chapter 5.7).

5.2.5.3.3 Test Object "girocard Terminal Integration"

The test object "girocard Terminal Integration" as part of the approval object "girocard Network" has to pass an integrative functional test according to the corresponding technical appendix.

No functional test of the host system as well as no further integrative functional test is necessary for each additional terminal to be included where the referenced specification including the interfaces have already been tested.

This rule holds as long as the approval office is informed about the initial operation.

Compliance with the Technical Appendix including the EMV POS Debit/Credit Specification

The test object "girocard Terminal Integration" includes the test interface for girocard EMV including the online-personalisation of the public keys in case this should be supported, when the first "girocard Terminal" is included into the "girocard Network". In this case an integrative functional test according to the corresponding technical appendix is necessary.

If the terminal has to be used in a network supporting with optional functions, e.g. "Manual Reversal" ("Manuelles Storno"), "Pre-Authorisation" ("Reservierung eines Maximalbetrags"), “Cashback” or “girocard EMV contactless”, these options must be tested within the terminal functional test according to the test object "girocard Terminal" and the integrative functional test according to the test object "girocard Terminal Integration".

Compliance with the Technical Appendix and additionally with nexo IS

Within the test object "girocard Terminal Integration" for the first terminal which shall be included into the "girocard Network" additional function requirements must be tested within the integrative functional test, e.g. the display messages for the response codes sent by the host system which are shown to the cardholder as well as to the merchant and printed on the receipts.

If the terminal has to be used in a network supporting with optional functions, e.g. “girocard EMV contactless”, “Payment with Cashback” or "Pre-Authorisation" (called "Deffered Payment" in nexo IS), these options must be certified with a CFCF certificate according to the test object "girocard Terminal" and tested within the integrative functional test according to the test object "girocard Terminal Integration".

5.3 GBIC ICC Approval Objects

For ICC modules resp. ICC products which implement a GBIC operating system and applications four kind of approval objects are defined:

- SECCOS ICC
- Debit ICC
- Credit ICC
- SAM ICC

As overall name these approval objects are called GBIC ICC approval objects.

ICC modules consist of hardware (IC) and executable code. ICC modules meet technical interface specifications and security requirements specified by GBIC. The executable code of an ICC module is either fully stored in Read Only Memory (ROM) or stored in ROM and in Electronically Erasable Read Only Memory (EEPROM) or in comparable memory. The executable code includes the operating system. Depending on the chosen configuration the executable code additionally includes application specific commands (e.g. EMV commands, girocard commands, GeldKarte commands or any other commands).

An approval of an ICC module according to SECCOS ICC is the necessary pre-condition (basic approval) for an approval of an ICC product according to Debit ICC, Credit ICC or SAM ICC.

ICC modules are not operable. For operability the applications must be completed. The approval objects Debit ICC, Credit ICC and SAM ICC extend the approval object SECCOS ICC to technical interface specifications for application data structures.

The approval object Debit ICC is used for

- the payment scheme girocard (pay now, GBIC),
- the payment scheme GeldKarte (electronic purse),
- the German ATM scheme,
- the payment and cash withdrawal schemes Maestro, V PAY, Cirrus and Plus
- the value added service applications "Marktplatz", "Fahrschein", "TAN-Anwendung" and "Signatur-Anwendung".

The approval object Credit ICC is used for

- the payment and cash withdrawal scheme MasterCard or
- the payment and cash withdrawal scheme VISA,

- the payment scheme GeldKarte (electronic purse),
- the value added service applications "Marktplatz", "Fahrschein", "TAN-Anwendung" and "Signatur-Anwendung".

The approval object SAM ICC is used for

- the payment scheme GeldKarte (electronic purse) based on the application "Händlerkarte" and
- the value added service applications "Marktplatz" and "Fahrschein".

The applications are used together with a GBIC defined ICC operating system (e.g. GBIC Operating System SECCOS 7.0) referred to in the detailed approval requirements for the GBIC ICC approval objects.

The applications "TAN-Anwendung" and "Signatur-Anwendung" are not part of the GBIC ICC approval objects, but successful interaction testing (between the approved applications and the additional applications) is mandatory.

5.3.1 Agreements/Contracts

GBIC specifies the functional and security requirements for the GBIC ICC approval objects in the technical interface specifications and security requirements.

Technical interface specifications exist to be used for the implementation of SECCOS ICC on an ICC module. Within these specifications the operating system and the application specific commands of the respective schemes are defined. The operating system and the application commands are evaluated and tested within the GBIC approval scheme. Technical interface specifications exist to be used for the initialisation and personalisation of ICC products according to Debit ICC, Credit ICC and SAM ICCs.

5.3.2 Description of the Approval Objects

The approval object SECCOS ICC is implemented by an ICC module. The approval object SECCOS ICC covers the technical interface specifications and security requirements of a GBIC operating system (e.g. SECCOS) including application specific commands. Since different GBIC operating systems and application commands exist different configurations are defined for the approval object SECCOS ICC. The GBIC operating systems and the application commands to be included into the approval object SECCOS ICC are listed in the detailed approval requirements for the respective configuration of the approval object.

The approval objects Debit ICC, Credit ICC and SAM ICC are implemented by an ICC product. The approval objects Debit ICC, Credit ICC and SAM ICC include a configuration of the approval object SECCOS ICC and additionally requires the conformance with technical interface specifications for payment schemes and acceptance schemes specifying application data structures. The combinations of configurations of the approval object SECCOS ICC and application data structures leading to the approval objects Debit ICC, Credit ICC and SAM ICCs are listed in the detailed approval requirements.

Approvals of the SECCOS ICC, Debit ICC, Credit ICC and SAM ICC are granted as issuer independent Type Approvals for the respective schemes.

The approval for an ICC module according SECCOS ICC is granted only for the time period of one year for the production of the approved ICC module. ICC modules approved firstly in the first quarter of a year are allowed to be produced until the end of the year. ICC modules approved starting with the second quarter of a year are allowed to be produced until the end of the following year. After this period the ICC module has to be re-evaluated according to the effective security requirements. For this purpose the ICC module must pass again the approval process (consisting of registration and security evaluation). The Approval Owner is responsible for the re-initiation of the approval process if the approval runs out. The prolonged approval is re-granted for a period of twelve months if the approval is granted prior to the expiration of the existing approval. The prolongation of the approval of an ICC modul is also possible at any time in that year which follows the expiring approval period, but not thereafter. The approval of an ICC modul is not granted retroactively. Only the time period remaining until the end of the year is approved - so a period of less than twelve months. The repetition of this procedure is allowed without restrictions. Note: The time period for the production of such a prolonged approval always ends at the end of a year.

Approvals for ICC products are allowed to be based on an approved ICC module. Therefore the approval of an ICC product terminates when the approval of the correspondent ICC module runs out.

The prolongation of the approval of an ICC product is possible. The Approval Owner is responsible for the re-initiation of the approval process if the approval runs out. The prolongation of the approval should be finished before the existing approval expires.

The prolongation of the approval of an ICC product is also possible at any time in that year which follows the expiring approval period, but not thereafter. The approval of an ICC product is not granted retroactively. Only the time period remaining until the expiration date of the approval for the ICC module is approved.The repetition of this procedure is allowed without restrictions. Note: The time period for the production of such a prolonged approval always ends at the end of a year.

5.3.2.1 Security Evaluation

5.3.2.1.1 Security Requirements

The ICC modules and ICC products have to meet the security requirements of the respective schemes assigned to the approval object. If a scheme does not define specific security requirements, the GBIC security requirements for ICC based payment schemes must be met.

The Approval Owner of an ICC product is obliged to ensure that all card manufacturers responsible for initialisation and personalisation of that product are currently listed as compliant with PCI CP (Payment Card Industry - Card Production and Provisioning) and fullfill the requirements of the DK “Mindestanforderungen an die Implementierung der Informationssicherheit im girocard-System” as far as not covered by PCI CP. For every card manufacturer commissioned with the production of girocard cards equipped with the respective ICC product, an approval applicant must provide the GBIC Approval Office also on an annual basis on the occasion of an approval prolongation with evidence of compliance of the card manufacturer with the PCI CP standard. Before an approval the Approval Office verifies the provided evidence by checking whether the card manufacturer is currently listed as a PCI CP compliant card manufacturer by the stated approval body (e.g. Mastercard or Visa).

The Approval Owner of an ICC product is obliged to ensure contractually that all card manufacturers provide GBIC (AC) via the Approval Office with information on major control and audit function findings with relevance to girocard.

5.3.2.1.2 Evaluation Object

The evaluation object of the approval object SECCOS ICC is the hardware and any executable code of an ICC module. The executable code is stored in ROM and if necessary, additionally in EEPROM or in comparable memory. Not only that part of the executable code which implements security features of the technical interface specifications must meet the security requirements. Additionally, any executable code of the ICC module implementing security features must be securely separated from any other executable code of the ICC module.

Two alternative evaluation processes for the approval object SECCOS ICC are described as refinement in chapter 4.4.6. The first alternative includes the submission of a separate GBIC hardware security evaluation provided by GBIC security evaluators, the second alternative includes a Common Criteria (CC) certificate for the hardware, which is embedded into the GBIC approval process.

The application data structures are not part of the evaluation object of the approval object SECCOS ICC. The Security Evaluator verifies the security requirements independent of the application data structures. The evaluation object of SECCOS ICC includes the production and development environment of the hardware vendor.

The Security Evaluator for an ICC module implementing SECCOS ICC shall state whether the results of the security evaluation of the ICC module implementing SECCOS ICC have impacts on the application data structures. This may concern bounds for usage counters or error counters or any other security relevant data structure.

If an ICC product implementing Debit ICC, Credit ICC or SAM ICC is based on an ICC module which is approved according to SECCOS ICC the Security Evaluator must confirm in some cases that the results leading to the ICC module approval are still valid:

1. If the evaluator stated for the ICC module that no impact on application data structures exists then no additional security evaluation is necessary for the approval of that ICC product.

2. If the evaluator stated for the ICC module that impacts on application data structures exist or no statement of the SEV exists then an additional security evaluation is necessary for the approval of that ICC product. The Security Evaluation for the ICC product can be done in form of a Security Evaluator Declaration.

3. If the ICC product includes additional executable code compared to the ICC module then an additional security evaluation is necessary for the approval of that ICC product. The Security Evaluation for the ICC module resp. product can be done in form of a Security Evaluator Declaration if the requirements of chap. 4.4.5.2) are met.

   According to chap. 4.4.5, GBIC (AC) may determine that application data structures are not security relevant or that a set of application data structures is equivalent to another set of application data structures:

4. If application data structures are not security relevant then no additional security evaluation is necessary for the approval of that ICC product.

5. If the ICC product is a successor of an ICC product which is approved according to Debit ICC, Credit ICC or SAM ICC and the application data structures are equivalent as defined in chap. 4.4.5 then no additional security evaluation is necessary for the approval of that ICC product.

The personalisation environment is not part of any evaluation object.

Executable code or application data structures as part of an ICC product may exist which do not need to meet security requirements besides the requirements for secure separation. This applies for non-payment schemes like "Marktplatz", "Fahrschein", "TAN-Anwendung" and "Signatur-Anwendung". Secure separation means that executable code and application data structures only used by these non-payment schemes must not have any security impact on executable code and application data structures of an evaluation object which is part of a GBIC ICC approval object.

If the GBIC ICC approval object includes a non-GBIC-application of a global scheme, it could be necessary that during the security evaluation additional security requirements of the respective scheme have to be verified. If mandatory, such security requirements are part of the detailed approval requirements for the GBIC ICC approval objects for this non-GBIC-application.

In addition to software and hardware evaluations integrative security testing is necessary to evaluate the security measures against side channel attacks. In this security test the effectiveness of the combination of hardware countermeasures and software countermeasures are examined. This concerns at least Simple Power Analysis (SPA), Differential Power Analysis (DPA) and Differential Fault Analysis (DFA).

In order to identify ICC modules approved according to SECCOS ICC, the byte 22 of the elementary file EF_ID includes a readable identification number. Based on a decision of the SC, the AO assigns a new value for EF_ID byte 22, if the hardware or the ROM mask is new or modified compared to a predecessor ICC module. Therefore approved ICC modules with the same hardware and the same ROM mask have the same EF_ID byte 22. Thus changes of the executable code of ICC modules which do not affect neither the ROM mask nor the hardware itself do not lead to a new EF_ID byte 22. No EF_ID byte 22 is assigned to ICC products approved as Debit ICC, Credit ICC or SAM ICC. Certificates may indicate the EF_ID byte 22 of the correspondent ROM mask and hardware.

5.3.2.2 Functional Test

The functional test requirements consist of tests according to the technical interface specification of the operating system and the applications of the approval object. The functional test is performed with real ICC modules resp. ICC products and not with emulators. All relevant technical interface specifications are tested. The ICC module is tested with Testsuite 1. Testsuite 1 tests consist of interface tests of the ICC module (which is not personalised) according to SECCOS ICC. The ICC product is tested with Testsuite 2. Testsuite 2 tests consist of interface tests of the ICC product (which is personalised) according to Debit ICC, Credit ICC or SAM ICC.

5.3.2.2.1 Test Object

Based on the two-stage functional test ("Testsuite 1" and "Testsuite 2") the test object is defined as follows:

"Testsuite 1": The test object for the "Testsuite 1" consists of (non-personalised) ICC modules. The non-personalised ICC modules includes commands of the operating system and commands of the applications of the respective approval object. The code implementing the commands of the respective technical interface specifications is located in the Read Only Memory (ROM) as well as in the Electronically Erasable Programmable Read Only Memory (EEPROM) or in comparable memory. Besides minimal data structures required for the functional tests, the non-personalised ICC module does not include the Master File (MF), Dedicated Files (DF) and Elementary Files (EF) with its data structures as specified in the technical interface specifications of the approval object.

The test object of (non-personalised) ICC modules with dual interface includes next to the contact interface also contactless interface. The contactless interface to applications with contactless access is tested according to correspondent technical interface specifications. The transport protocol is also tested based on a set of pre-elected tests. Since applications exist which must not be accessed via the contactless interface in addition the obeying of access rules for the contactless interface is also verified.

"Testsuite 2": The test object for the "Testsuite 2" consists of the (personalised) ICC product. The (personalised) ICC product includes all commands and application data structures as specified in the technical interface specifications of the respective approval object. The test object is identical with the initialised and personalised ICC product as produced in the final initialisation and personalisation environment.

The test object of a (personalised) ICC product with dual interface includes the contact interface like personalised contact only ICC products. Further test cases are used to test the contactless interface of (personalised) ICC products with dual interface.

According to chap. 4.4.5, GBIC (AC) may determine that application data structures are not functional relevant or that a set of application data structures is equivalent to another set of application data structures: If the ICC product is a successor of an ICC product which is approved according to Debit ICC, Credit ICC or SAM ICC and the application data structures are equivalent as defined in chap. 4.4.5 then no additional functional test is necessary for the approval of the successor ICC product.

5.4 digitale girocard

5.4.1 System Description

The German Banking Industry operates the girocard system, which includes cashless payments by the payment scheme girocard and cash withdrawals by the German ATM system. Transactions within the girocard system, called girocard transactions, are carried out by means of payment cards which are assigned to the customer and which guarantee an acceptable level of trust for the parties involved. Payment cards for girocard transactions can be issued in the form of physical cards ("smart cards") or emulated cards. The approval requirements for physical cards are described in chapter 5.3 "GBIC ICC Approval Objects".

An emulated payment card stored in and operated by a mobile device or other dedicated device as described in this chapter is called a "digitale girocard". The set of data needed to emulate a "digitale girocard" is called a Digital Card.

"digitale girocard" transactions can be carried out

- as girocard contactless transactions at POS terminals or ATMs or
- as E-Commerce transactions at retail and service companies. The technical infrastructure and the related legal contracts that enable such transactions are called "girocard im Online-Handel".

"digitale girocard" transactions can be supported either

- by mobile devices based on Host Card Emulation (HCE), which is a method of card emulation in software that enables a Mobile Payment Application to be carried out as a girocard contactless transaction or to communicate with the systems of the card issuer enabling E-Commerce transactions, or
- by mobile devices based on Secure Element (SE), which is a secure hardware component integrated into the device where sensitive data can be stored and sensitive processes can be executed. For the processing of "digitale girocard" transactions, a CPA applet with the Digital Card must be installed in the SE. A CPA applet supports girocard contactless transactions as well as E-Commerce.

"digitale girocards" are operated by Digital Card Providers who are entitled to personalise and operate "digitale girocards" on behalf of card-issuing banks within the girocard system. For this purpose, a Digital Card Provider must be approved by GBIC after providing evidence that the security and functional requirements of the approval object defined by GBIC are met.

The approval objects "girocard HCE" and "girocard SE" define the approval requirements for Digital Card Providers implementing the technical solutions HCE and SE respectively and are defined in chapters 5.4.3 and 5.4.4.

For the acceptance of "digitale girocard" transactions in E-Commerce, the role of the "Online-Netzbetreiber" is defined, which is responsible for the connection of merchants, their technical operation in E-Commerce and their technical support. An "Online-Netzbetreiber" is connected to the central entry points of the girocard system for E-Commerce based on HCE and/or SE and exchanges incoming payment-related data with them. In addition, clearing data is transmitted from the card issuers to the merchant banks. An "Online-Netzbetreiber" must be approved by GBIC after providing evidence that the security and functional requirements of the approval object defined by GBIC are met.

The approval objects defined for "digitale girocard" transactions in E-Commerce refer to the requirements for the technical solutions and do not cover the appearance of the customer interface or the acceptance trademark under which the E-Commerce transaction is processed.

Chapter 5.4.5 defines the approval object "Online-Netzbetreiber" which requires to support at least one of two technical solutions, the variant for HCE or the variant for iOS. The variant for HCE is based on Digital Cards in the Mobile Payment App on Android devices. The variant for iOS defines a SE-based mobile payment solution for digital purses (wallets) operated by a third party.

As the central entry point of the card-issuing institutes in the girocard system for E-Commerce based on HCE, the role of the "Lookup-Server" is defined, which distributes the payment requests coming from an "Online-Netzbetreiber" to the systems of the responsible card issuer. Further, clearing data is transmitted from the card issuer to the "Online-Netzbetreiber" and by the latter to the merchant banks. The role of the "ONB-Hub" was defined for the corresponding central entry point of the card-issuing institutes in SE-based E-Commerce. A "Lookup-Server" and an "ONB-Hub" must be approved by GBIC after providing evidence that the functional requirements of the respective approval object defined by GBIC are met.

Chapter 5.4.6 defines the approval object "Lookup-Server", chapter 5.4.7 defines the approval object "ONB-Hub".

Chapter 5.4.2 states the agreements and contracts that form the legal basis for the approval objects.

A specific glossary in chapter 5.4.8 defines the terms used in the area of "digitale girocards".

5.4.2 Agreements/Contracts

For Digital Card Providers, GBIC specifies the technical interface specifications and the security requirements for systems providing "digitale girocards" as referenced by the provider contract for Digital Cards called "Vertrag über die Zulassung als Betreiber digitaler Karten im girocard-System der Deutschen Kreditwirtschaft". The operation of "digitale girocards" has to fulfil the requirements of this contract.

For "Online-Netzbetreiber", GBIC specifies the technical interface specifications and the security requirements for systems providing electronic remote payment transactions (called E-Commerce) as referenced by the provider contract for "Online-Netzbetreiber" called "Vertrag über die Zulassung als Online-Netzbetreiber im girocard-System der Deutschen Kreditwirtschaft". The operation of E-Commerce transactions has to fulfil the requirements of this contract.

For "Lookup-Server", GBIC specifies the technical interface specifications as referenced by the provider contract for "Lookup-Server-Betreiber" called "Vertrag über die Zulassung als Lookup-Server-Betreiber im girocard-System der Deutschen Kreditwirtschaft". For "ONB-Hub", GBIC specifies the technical interface specifications as referenced by the provider contract for "ONB-Hub-Betreiber" called "Vertrag über die Zulassung als ONB-Hub-Betreiber im girocard-System der Deutschen Kreditwirtschaft". The operation of E-Commerce transactions has to fulfil the requirements of these contracts.

Furthermore, all mentioned contracts require compliance with the minimum requirements for the implementation of information security in the girocard system called "Mindestanforderungen an die Implementierung der Informationssicherheit im girocard-System" and with the emergency management called "Notfallmanagement-Handbuch - Organisatorische Prozesse und technische Maßnahmen bei wesentlichen Störfällen im girocard-System".

5.4.3 Approval Object "girocard HCE"

5.4.3.1 Definition of the Approval Object and the Approval Owner

The approval object "girocard HCE" is a system implementing the system architecture "girocard HCE solution" enabling "digitale girocard" transactions based on Host Card Emulation. The system provides the basic set-up for POS transactions as described in chapter 5.4.3.2 and an extended set-up for E-Commerce transactions as described in chapter 5.4.3.3.

The approval owner is the provider of a system operating one type of digital cards within such a HCE solution and is called a Digital Card Provider for "girocard HCE". The Digital Card Provider is entitled to personalise and operate the approved type of Digital Cards for "girocard HCE" on behalf of card issuing banks within the girocard system. The approval cannot be transferred to other companies.

5.4.3.2 Basic System Architecture "girocard HCE solution"

The basic system architecture for the approval object "girocard HCE" that enables a girocard contactless transaction at a POS terminal or an ATM is based on the model shown in the following figure:

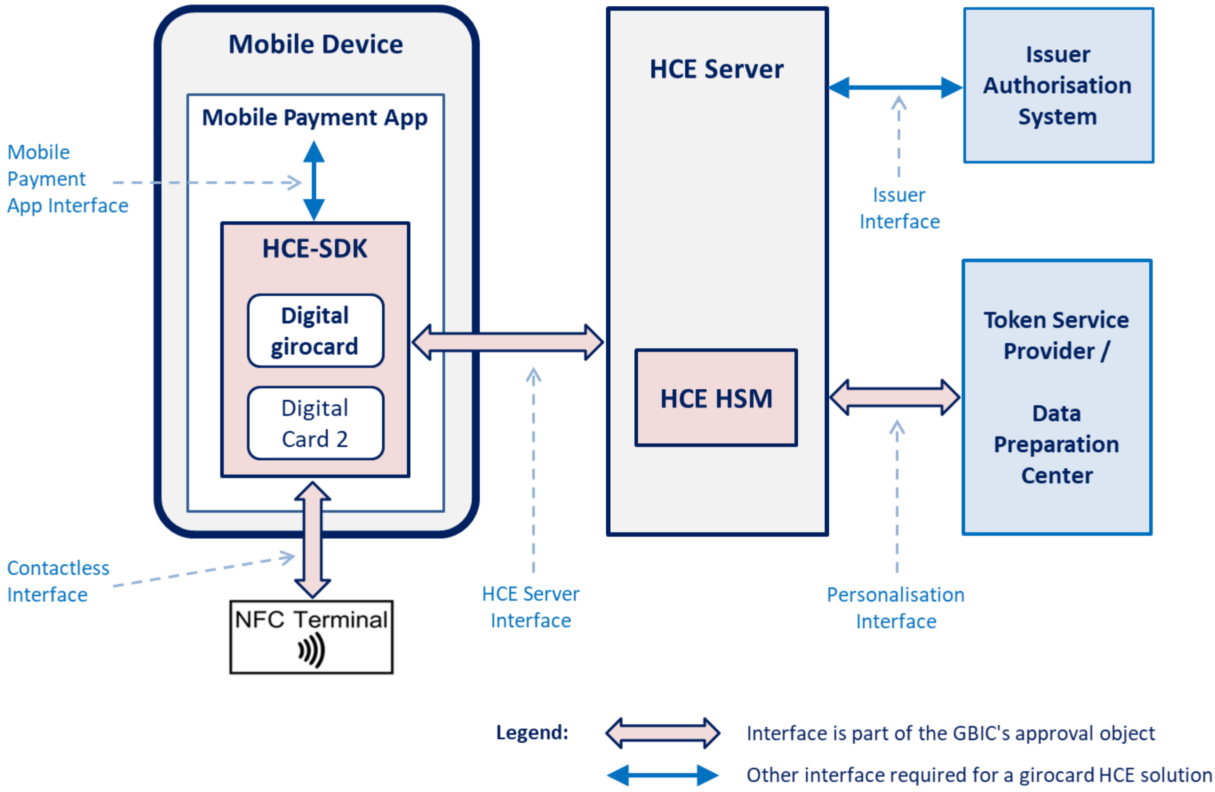

Mobile Device
Mobile Payment App
Mobile Payment App Interface
HCE-SDK
Digital girocard
Digital Card 2
Contactless Interface
NFC Terminal
HCE Server
HCE HSM
HCE Server Interface
Issuer Authorisation System
Issuer Interface
Token Service Provider / Data Preparation Center
Personalisation Interface
Legend:
Interface is part of the GBIC's approval object
Other interface required for a girocard HCE solution

Figure 3: Basic System Architecture for a "girocard HCE solution"

Note: The extension to the system architecture for the approval object "girocard HCE" enabling E-Commerce transactions is described later in chapter 5.4.3.3.

The **Mobile Payment App** is a mobile app, which has indicated to the platform of the **Mobile Device** that it implements an HCE service for payment, thus emulating one or several payment cards. The set of data needed to emulate a girocard payment card for HCE represents the Digital Card for "girocard HCE".

The user (the owner, to be precise) of the Mobile Device is considered to be the cardholder of the Digital Cards. The **Mobile Payment App** offers and controls the interface to the cardholder, i.e. cardholder information and cardholder input.

The **HCE SDK** is software integrated in the Mobile Payment App, which implements the functions needed

- for Digital Card processing over the contactless interface,
- for Digital Card storage and
- for Digital Card management over the Mobile Payment App interface and the HCE Server interface.

These functions are referred to as **Digital Card Handling** in the following. Normally, the HCE SDK supports storage and processing of several Digital Cards.

The Mobile Payment App accesses Digital Card Handling over the Mobile Payment App interface to modify data of the Digital Cards and to receive information on the stored Digital Cards including information on transactions performed with Digital Cards. The Mobile Payment App offers and controls the interface to the cardholder. In particular, it must support a method for **CDCVM** cardholder verification.

The **HCE Server** accesses Digital Card Handling over the HCE Server interface for administration processes, e.g. loading of Digital Cards (also called personalisation or provisioning), loading of cryptographic keys (also called key replenishment) and update of Digital Card data according to issuer requirements.

The **Contactless Interface** is an interface of the HCE SDK, which has to be implemented according to the requirements of the technical interface specifications to work with any contactless girocard terminal. The technical interface specifications of the HCE SDK are called in following as CPACE HCE Device Specifications. As contactless interface the Near Field Communication (NFC) interface is used, about which the HCE SDK communicates (through the NFC controller and platform of the mobile device) with an NFC terminal.

The **Mobile Payment App Interface** between HCE SDK and Mobile Payment App is an In-App interface that is currently not described in a formal way. The CPACE HCE Device Specifications only define requirements for the functionality to be made available at this interface.

The **HCE Server Interface** between HCE SDK and HCE Server is based on a secured Web Service and the HCE SDK has to support push notifications to allow the HCE Server to initiate the communication. Beyond this, this interface is currently not described in a formal way. The CPACE HCE Device Specifications only define requirements for the functionality to be made available at this interface.

The HCE Server interface between the HCE Server and the **Token Service Provider/ Data Preparation Center**, called the **Personalisation Interface**, is used to process on behalf of a card issuer encrypted personalisation data for a Digital Card to the HCE SDK via the HCE Server. The personalisation interface is to be agreed and to be tested bilaterally. It is out of scope of the approval. The HCE Server owns a hardware security module (HCE HSM) which provides cryptographic mechanisms required for the personalisation, the key replenishment and the update of a Digital Card and which provides the cryptographic protection of all interfaces of the HCE Server.

Finally, the "girocard HCE solution" should have an **Issuer Interface** between the HCE Server and the **Issuer Authorisation System** to allow the card issuer to get status information about a Digital Card (e.g., transaction counter) and to update a Digital Card (e.g., transaction limits). The issuer interface could be combined with the personalisation interface, in that case the HCE server and the Issuer Authorisation System will communicate via the Token Service Provider. The issuer interface is to be agreed and to be tested bilaterally. The optional technical interface specification for the update of Digital Cards over the HCE server can be used to realise the issuer interface. In any case, it is out of scope of the approval.

5.4.3.3 Extension to the Basic System Architecture enabling E-Commerce

For enabling E-Commerce transactions, an extension to the basic system architecture for the approval object "girocard HCE" is required as shown in the following figure:

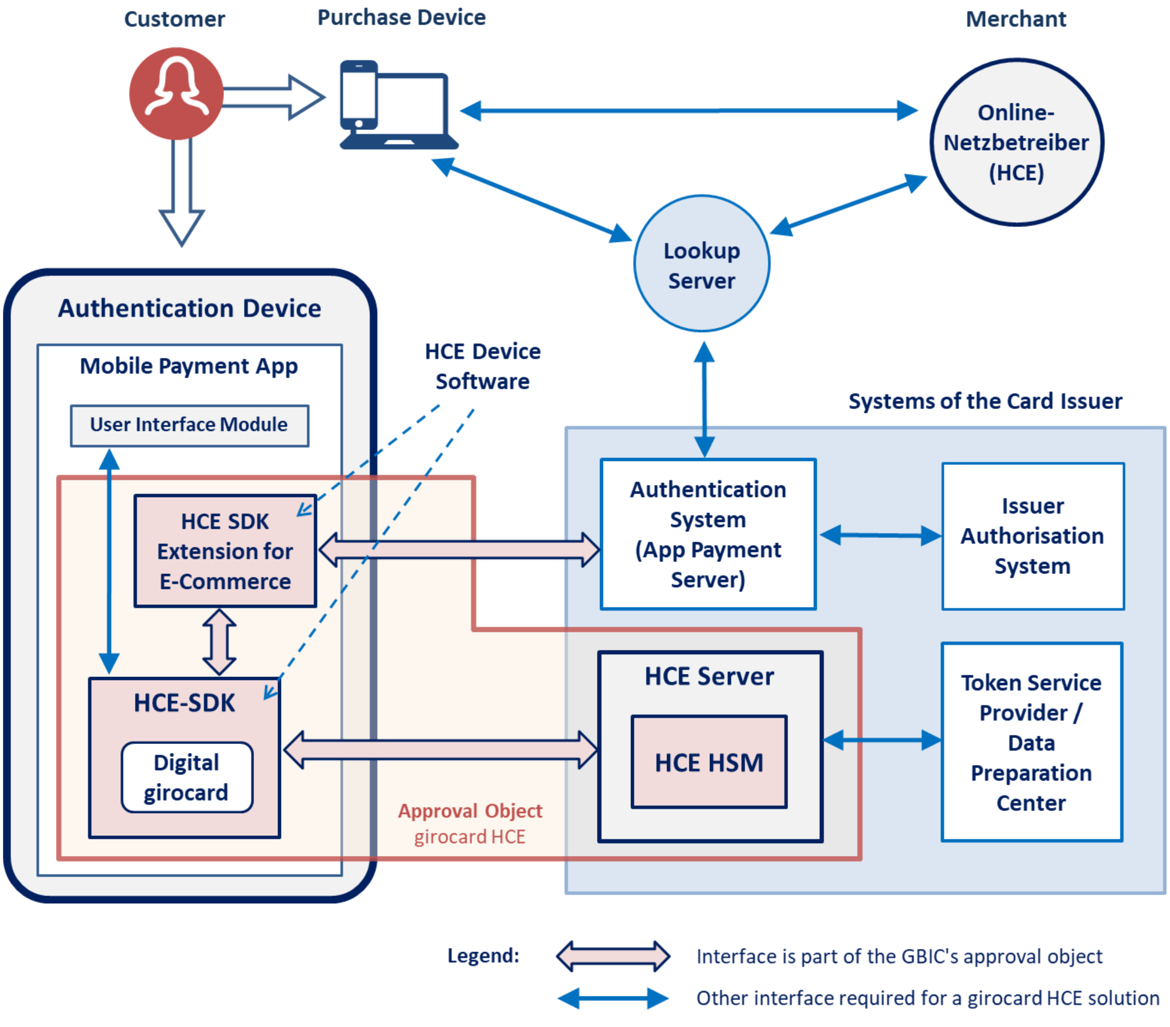

Customer
Purchase Device
Merchant
Online-Netzbetreiber (HCE)
Lookup Server
Authentication Device
Mobile Payment App
User Interface Module
HCE SDK Extension for E-Commerce
HCE-SDK
Digital girocard
HCE Device Software
Systems of the Card Issuer
Authentication System (App Payment Server)
Issuer Authorisation System
HCE Server
HCE HSM
Token Service Provider / Data Preparation Center
Approval Object
girocard HCE
Legend:
Interface is part of the GBIC's approval object
Other interface required for a girocard HCE solution

Figure 4: Extension to a "girocard HCE solution" enabling E-Commerce

For E-Commerce transactions, the customer's Android mobile device is used as **Authentication Device** to confirm and to authenticate a remote payment transaction. An E-Commerce transaction works according following basic principle:

The customer selects on the checkout page of an online shop to pay with girocard. On merchant's site, the "Online-Netzbetreiber (HCE)" assembles the transaction data, including the amount and the merchant's name, determines the environmental data from the cardholder's **Purchase Device** and sends both pieces of information to the **Lookup-Server**.

The Lookup-Server represents the central entry point of the card-issuing institutes for "girocard im Online-Handel" based on HCE and distributes the payment request to the **Authentication Systems** of the card issuers which are responsible to find a suitable Authentication Device belonging to the customer.

The Authentication Device contains a **Mobile Payment App** supporting E-Commerce transactions. The Mobile Payment App offers processing functions for both, the functions for communication via the contactless interface at a POS terminal according to chapter 5.4.3.2 and the functions for communication with an **App Payment Server** to support E-Commerce transactions. The HCE SDK as described in chapter 5.4.3.2 implements at least the functions to communicate with a POS terminal over the NFC interface. The functions for the exchange with an App Payment Server can be outsourced to a separate software "**HCE SDK Extension for E-Commerce"**, which also has to be integrated into the Mobile Payment App, whereby the HCE SDK remains unchanged compared to the implementation according to chapter 5.4.3.2. In this case, the HCE SDK Extension communicates with the HCE SDK via an existing internal software interface of the HCE SDK by emulating the contactless interface. It means that the HCE SDK Extension software converts the requests it receives from the App Payment Server into a sequence of internal executions of card application commands that the HCE SDK already provides for the execution over the NFC interface for the communication with a POS terminal.

The HCE-SDK must store a **Digital Card** for girocard for which the card issuer may decide whether E-Commerce transactions are enabled.

A **User Interface (UI) Module** must be integrated into the Mobile Payment App in which the transaction data such as the amount, the merchant name and the **Digital Card** involved are displayed to the customer for confirmation. The Mobile Payment App controls the communication between the UI module and the HCE-SDK and other modules as the SDK extension for E-Commerce. The UI module and its interfaces are not subject of the approval object.

For the processing on the Authentication Device, the Authentication System checks whether a CDCVM is required and forwards the transaction data and the CDCVM decision to the Mobile Payment App. The part of the Authentication System that controls the Mobile Payment App is also called the **App Payment Server**.

The Mobile Payment App transmits the cryptographic evidence of the customer's confirmation to the App Payment Server, which forwards it to the **Issuer Authorisation System**. The Authentication System informs the Lookup Server about the result of the authorisation which returns the result to the system of the "Online-Netzbetreiber (HCE)".

Currently, the GBIC technical interface specifications only define the "girocard HCE solution" where the functionality for E-Commerce is outsourced to a separate software "HCE SDK Extension for E-Commerce" as shown in Figure 4. A "girocard HCE solution" must comply with these specifications. The technical interface specifications of the HCE SDK extension are called in following as CPACE HCE Device Extension for E-Commerce.

5.4.3.4 Components of the Approval Object

The approval object "girocard HCE" is a system implementing a "girocard HCE solution". It consists of the following components, which have to be considered in the evaluation objects and the functional test object:

- the component "HCE Server" as a system, including
    - the hardware and software of the sub component "HCE HSM" as part of the component "HCE Server",
    - the operational environment of the sub component "HCE HSM" and
- and the two software components, which can be integrated together in Mobile Payment Apps,
    - the component "HCE SDK" as a software library and
    - the component "HCE SDK Extension for E-Commerce" as a special software.

Note 1: The Mobile Payment App as well as the hardware and the operating system of the mobile device are not part of the approval object.

Note 2: The functionality of the component "HCE SDK Extension for E-Commerce" may be integrated into the software component "HCE SDK" in the future.

The approval object "girocard HCE" contains exactly one component "HCE Server", one component "HCE SDK" and one component "HCE SDK Extension for E-Commerce". Note: If several components "HCE Server", several components "HCE SDK" or several components of "HCE SDK Extension for E-Commerce" exist which could work together within a "girocard HCE" system, then each triple of one component "HCE Server", one component "HCE SDK" and one component "HCE SDK Extension for E-Commerce" requires an own registration and approval.

5.4.3.5 Security Evaluation

5.4.3.5.1 Security Requirements

The components "HCE Server" and "HCE SDK" of the approval object "girocard HCE" have to meet the security requirements referenced by the provider contract for digital cards referred to in the detailed approval requirements for "digitale girocard".

For the component "HCE SDK Extension for E-Commerce" there are no security requirements that must be verified by a security evaluation.

5.4.3.5.2 Evaluation Objects

The security requirements referenced by the provider contract for digital cards define requirements for both the component "HCE Server" including the sub component "HCE SDK" as well as the component "HCE SDK". Thus, for the approval object "girocard HCE", following evaluation objects are defined:

- the evaluation object "HCE Server/HCE HSM" and
- the evaluation object "HCE SDK".

The component "HCE SDK Extension for E-Commerce" has no evaluation object.

Figure 5 illustrates the evaluation objects and the required evaluation reports for them as described in the next two chapters:

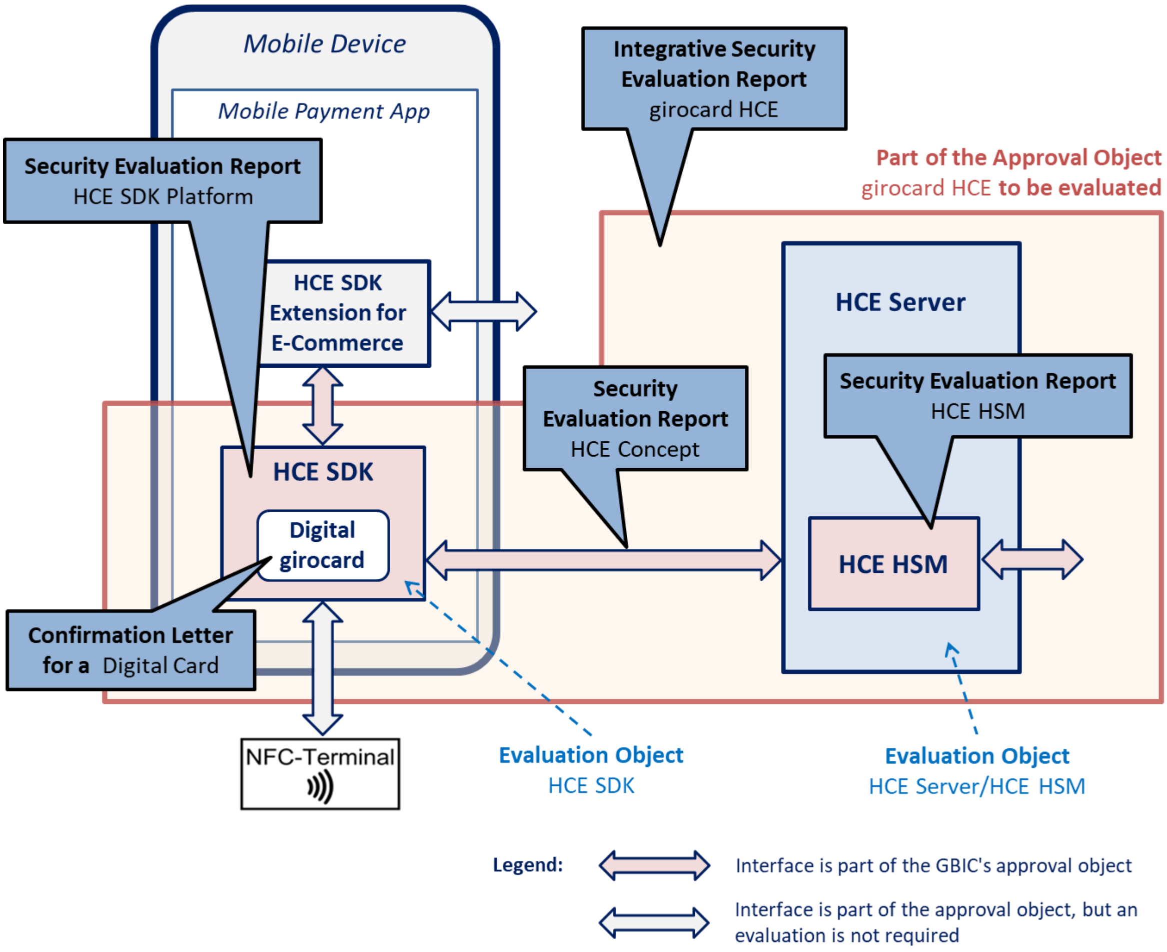

Mobile Device
Mobile Payment App
Integrative Security Evaluation Report girocard HCE
Security Evaluation Report HCE SDK Platform
Part of the Approval Object girocard HCE to be evaluated
HCE SDK Extension for E-Commerce
HCE Server
Security Evaluation Report HCE Concept
Security Evaluation Report HCE HSM
HCE SDK
Digital girocard
HCE HSM
Confirmation Letter for a Digital Card
NFC-Terminal
Evaluation Object HCE SDK
Evaluation Object HCE Server/HCE HSM
Legend:
Interface is part of the GBIC's approval object
Interface is part of the approval object, but an evaluation is not required

Figure 5: Security Evaluation Reports for "girocard HCE"

5.4.3.5.2.1 Evaluation Object "HCE Server/HCE HSM"

The evaluation object "HCE Server/HCE HSM" considers

- the concept for the interface between the sub component "HCE SDK" and the component "HCE server" in interaction with the HCE SDK,
- the hardware and the software of the sub component "HCE HSM" as part of the component "HCE server" and
- the operational environment of the sub component "HCE HSM".

For the evaluation object "HCE Server/HCE HSM", the following security evaluation reports are required:

- the "Security Evaluation Report HCE concept" which describes the technical interface between the HCE SDK and the HCE server in interaction with the HCE SDK,
- the "Security Evaluation Report HCE HSM" for the hardware and the software of the sub component HCE HSM, which implements the HCE concept. Further, the interfaces of the HCE HSM to the external world required especially for the personalisation and update of digital cards have to be evaluated,
- the "Integrative Security Evaluation Report girocard HCE" which integrates the reports for the HCE concept, the hardware and the software of the sub component HCE HSM and the HCE Device Software (including Confirmation Letter) defined in chapter 5.4.3.5.2.2
- and which contains an audit report assessing the operational environment of the sub component HCE HSM. Further, the integrative security evaluation report references to the manufactures documentation forming the basis for all security evaluation reports for the approval object "girocard HCE".

Any security relevant modification of the HCE HSM of an approved "girocard HCE solution" has to be re-evaluated.

5.4.3.5.2.2 Evaluation Object "HCE SDK"

The evaluation object "HCE SDK" considers the components "HCE SDK". The HCE SDK implements amongst other things the HCE concept evaluated according to chapter 5.4.3.5.2.1.

It has to be evaluated, whether the implementation of the evaluation object "HCE SDK" meets the security requirements of the provider contract.

The security evaluation for the HCE SDK has to be separated in

- the "Security Evaluation Report HCE SDK Platform" covering the platform part of the CPACE HCE Device Specifications implemented by the HCE SDK and
- the "Confirmation Letter for a Digital Card" covering one certain type of Digital Cards within the HCE SDK determined according to the application part of the CPACE HCE Device Specifications and the CPACE HCE Device Extension for E-Commerce.

In the "Security Evaluation Report HCE SDK Platform", the Security Evaluator has to confirm that the HCE SDK meets the security requirements independent from any chosen type of Digital Card. If there is a dependency, this dependency has to be indicated in the report. In the "Confirmation Letter for a Digital Card" covering one type of Digital Cards, the Security Evaluator has to confirm that any Digital Card of this type meets the security requirements based on the evaluated platform and considers possible dependencies indicated in the platform security evaluation. The template for a "Confirmation Letter for a Digital Card" will be provided by the Approval Office.

For an approved "girocard HCE solution" 12 months after the validation of the "Security Evaluation Report HCE SDK platform" by the Security Committee, a Security Evaluator has to confirm in an assessment by a confirmation letter that the security requirements are still met according to state-of-art of science and technology. The Approval Owner is responsible for the re-initiation of the approval process and has to provide the confirmation letter eight weeks before the end of a period to the Security Committee (SC). Therefore the approval for a "girocard HCE solution" is granted only for the period of 12 months after the validation of the "Security Evaluation Report HCE SDK platform" by the Security Committee. The prolonged approval is re-granted for a period of twelve months. The repetition of this procedure is allowed without restrictions. Without prolongation the approval of a "girocard HCE solution" terminates.

Any security relevant modification of the HCE SDK of an approved "girocard HCE solution" has to be re-evaluated.

5.4.3.6 Functional Test

5.4.3.6.1 Functional Test Requirements

The functional test requirements of the approval object "girocard HCE" can be separated into two parts:

- the component "HCE SDK" has to meet the CPACE HCE Device Specifications,
- the component "HCE SDK Extension for E-Commerce" has to meet the CPACE HCE Device Extension for E-Commerce,

both as part of the appendixes of the provider contract for digital cards referred to in the detailed approval requirements for "digitale girocard".

The CPACE HCE Device Specifications define the behaviour on the contactless interface between a mobile device and a POS terminal and define requirements only for the Mobile Payment App Interface and the HCE Server Interface (see Figure 3). Therefore, a test object "HCE SDK" is defined to validate the behaviour on the contactless interface by functional tests and to validate the other interfaces by checking the compliance with the requirements.

The CPACE HCE Device Extension for E-Commerce define the behaviour on the network interface between a authentication device and an App Payment Server and define requirements for the sub component "HCE SDK Extension for E-Commerce" (see Figure 4). Therefore, a test object "HCE SDK Extension for E-Commerce" is defined to validate the behaviour on the network interface by integration functional tests and to validate the other interfaces by checking the compliance with the requirements.

5.4.3.6.2 Test Object "HCE SDK"

Figure 6 illustrates the test set up for the test object "HCE SDK" with the data to be provided and the technical components to perform the functional test.

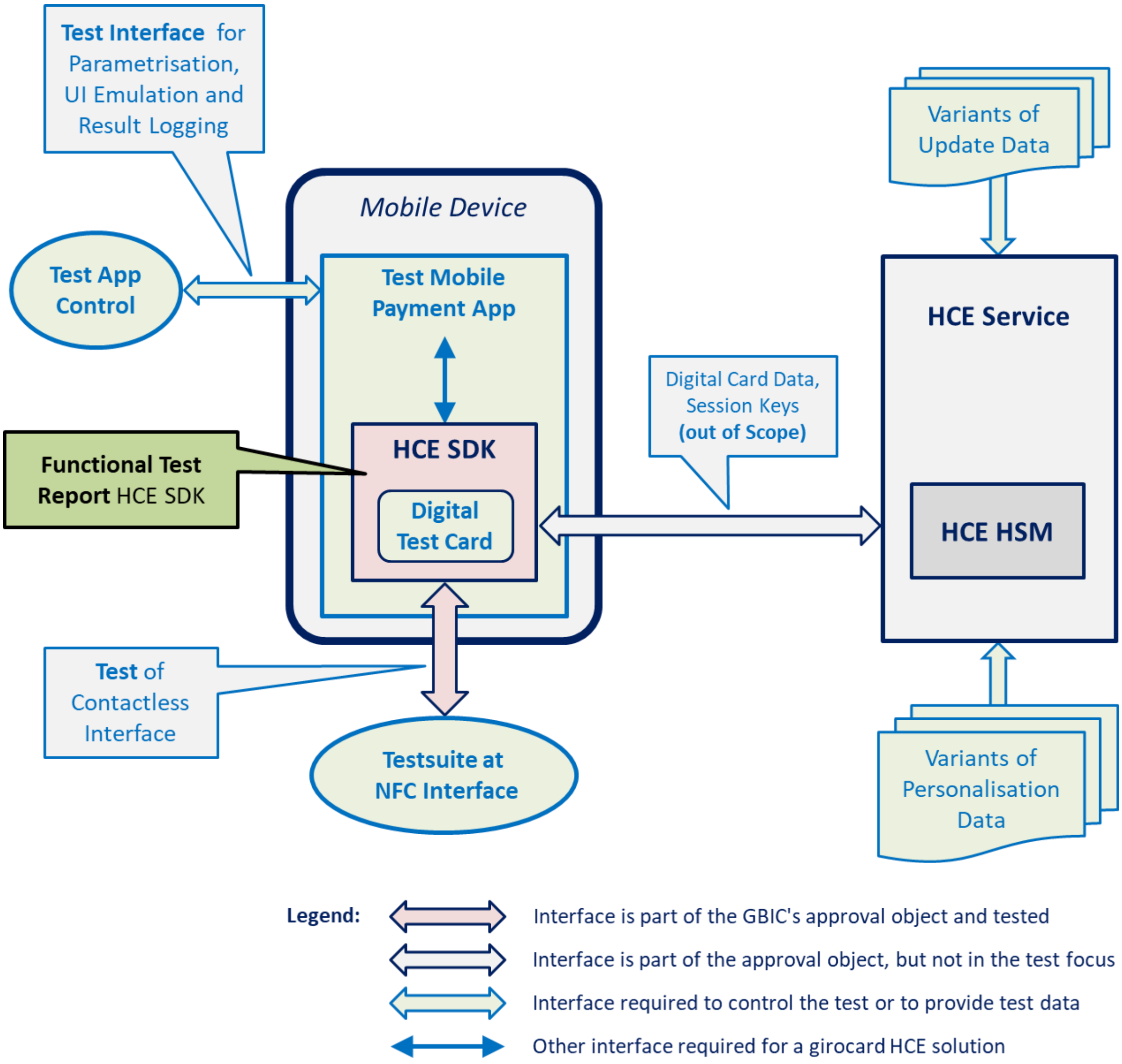

Test Interface for Parametrisation, UI Emulation and Result Logging
Variants of Update Data
Mobile Device
Test App Control
Test Mobile Payment App
HCE Service
Digital Card Data, Session Keys (out of Scope)
Functional Test Report HCE SDK
HCE SDK
Digital Test Card
HCE HSM
Test of Contactless Interface
Testsuite at NFC Interface
Variants of Personalisation Data
Legend:
Interface is part of the GBIC's approval object and tested
Interface is part of the approval object, but not in the test focus
Interface required to control the test or to provide test data
Other interface required for a girocard HCE solution

Figure 6: Functional Test Set Up for the test object "HCE SDK"

The test object "HCE SDK" consists of the component "HCE SDK" which shall be linked as software library within a Mobile Payment App. Since the Mobile Payment App itself is not a component of the approval object, it can be substituted by a Test Mobile Payment App. This approach allows a wider coverage of the technical interface specifications for the contactless interface by the functional test.

Because the interface between the Mobile Payment App and the component "HCE SDK" (see Mobile Payment App interface in Figure 3) is not defined by the CPACE HCE Device Specifications, a Test Mobile Payment App has to support the specific interface to the HCE SDK. The proof of the correct interoperability between the components "HCE SDK" and "HCE Server" will be obtained implicitly (see HCE Server interface in Figure 3) by executing the Test Mobile Payment App.

The Approval Applicant has to implement a test application according to requirements provided by the Testing Laboratory, has to link it with the software library of the component "HCE SDK" and has to provide the completed Test Mobile Payment App in an appropriate way for the installation into a mobile device in preparation of the functional test. The Test Mobile Payment App should provide a remote interface (e.g., an IP connection or a special command set via the NFC interface) to a control instance called Test App Control. That test interface should allow the Test App Control to activate or parametrise certain functionalities as required by a test plan of the Testing Laboratory. The Test Mobile Payment App should allow emulating the communication with the cardholder to avoid the need of any user interaction at the mobile device during the test. Via the test interface, the Test App Control should be able to read results of the test functions of the Test Mobile Payment App.

For the execution of the functional test, the Approval Applicant has to provide an HCE Service, which means an HCE Server in form of a simulation or the access to a real component "HCE Server". The HCE service has to be able to be configured according the requirements of the Testing Laboratory. That includes an interface to process different variants of complete personalisation data for a Digital Card and to process variants of update data for a Digital Card. As result of the processing of such data a Digital Test Card will be installed or will be updated within the component "HCE SDK". Further, the HCE service has to provide the key replenishment (session keys) required for the execution of "digitale girocard" transactions on the component "HCE SDK".

Different Digital Test Cards personalised during the functional tests shall cover a wide range of the functional requirements of the platform part and the application part of the CPACE HCE Device Specifications and the CPACE HCE Device Extension for E-Commerce.

The Test App Control should be realised as a part of a Testsuite HCE. Further, this Testsuite HCE should be able to access the HCE service to configure personalisation or update data for Digital Cards.

The Approval Applicant has to fulfill all requirements stated by the Testing Laboratory to support the functional test set up for the test object "HCE SDK".

The results of the functional tests are assembled in the functional test report "HCE SDK".

5.4.3.6.3 Test Object "HCE SDK Extension for E-Commerce"

Figure 7 illustrates the test set up for the test object "HCE SDK Extension for E-Commerce" to perform the integration functional test.

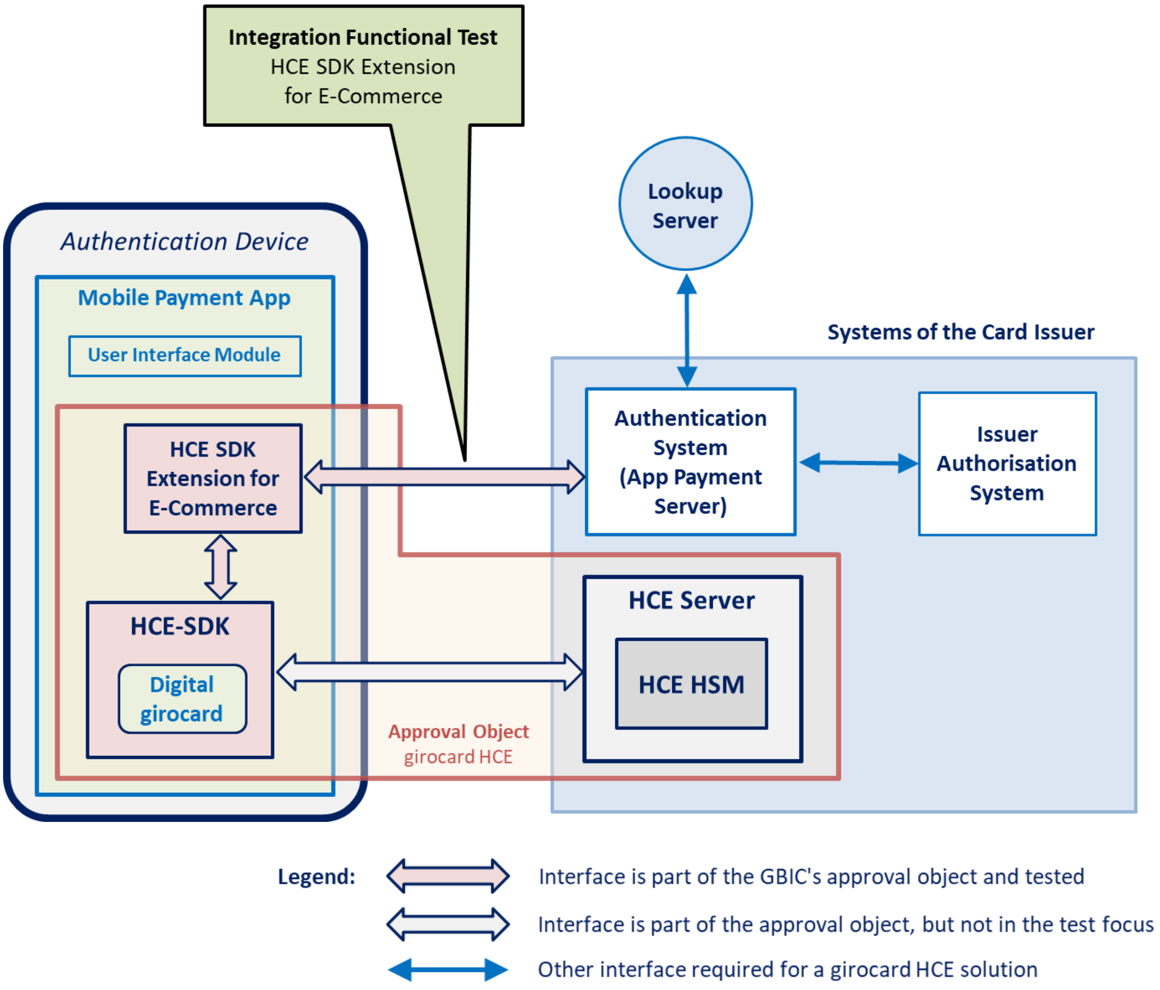

Integration Functional Test
HCE SDK Extension
for E-Commerce
Lookup Server
Authentication Device
Mobile Payment App
User Interface Module
HCE SDK Extension for E-Commerce
HCE-SDK
Digital girocard
Systems of the Card Issuer
Authentication System (App Payment Server)
Issuer Authorisation System
HCE Server
HCE HSM
Approval Object
girocard HCE
Legend:
Interface is part of the GBIC's approval object and tested
Interface is part of the approval object, but not in the test focus
Other interface required for a girocard HCE solution

Figure 7: Functional Test Set Up for the test object "HCE SDK Extension for E-Commerce"

The test object "HCE SDK Extension for E-Commerce" consists of the component "HCE SDK Extension for E-commerce" which shall be linked as software library together with the corresponding component "HCE SDK" within a Mobile Payment App. It is not necessary to use a special test app for the integration function test. The test set-up should provide the connection to the Authentication System (access to a real test system) to be used by the Approval Applicant, which in turn must connect to the Lookup-Server.

During the integration functional test, several E-Commerce transactions, as described in chapter 5.4.3.3, must be performed manually, which should cover the full range of behavior supported by a Digital girocard.

The integration functional test based on the test set-up has to be performed by the approval applicant. The catalogue of test cases to be mandatory performed during this test is defined and provided by the Testing laboratory. The approval applicant documents the results of the integration functional test in a pre-written format and submits it to the Testing laboratory.

The Testing laboratory checks the completeness of the submitted test results and the achievement of the test objectives. In case a documented deviation, the plausibility of the applicant's assessment is evaluated. The results of these checks are assembled by the Testing laboratory into the integration functional test report "HCE SDK Extension for E-Commerce".

5.4.4 Approval Object "girocard SE"

5.4.4.1 Definition of the Approval Object and the Approval Owner

The approval object "girocard SE" is a system implementing the system architecture "girocard SE solution" enabling girocard mobile transactions based on Secure Element (SE). The system provides the set-up as described in chapter 5.4.4.2.

The approval owner is the provider of a system operating one type of Digital Cards within such a SE solution and is called a Digital Card Provider for "girocard SE". The Digital Card Provider is entitled to personalise and operate the approved type of Digital Cards for "girocard SE" on behalf of card issuing banks within the girocard system. The approval cannot be transferred to other companies.

5.4.4.2 System Architecture "girocard SE solution"

The approval object "girocard SE" is based on the model shown in the following figure:

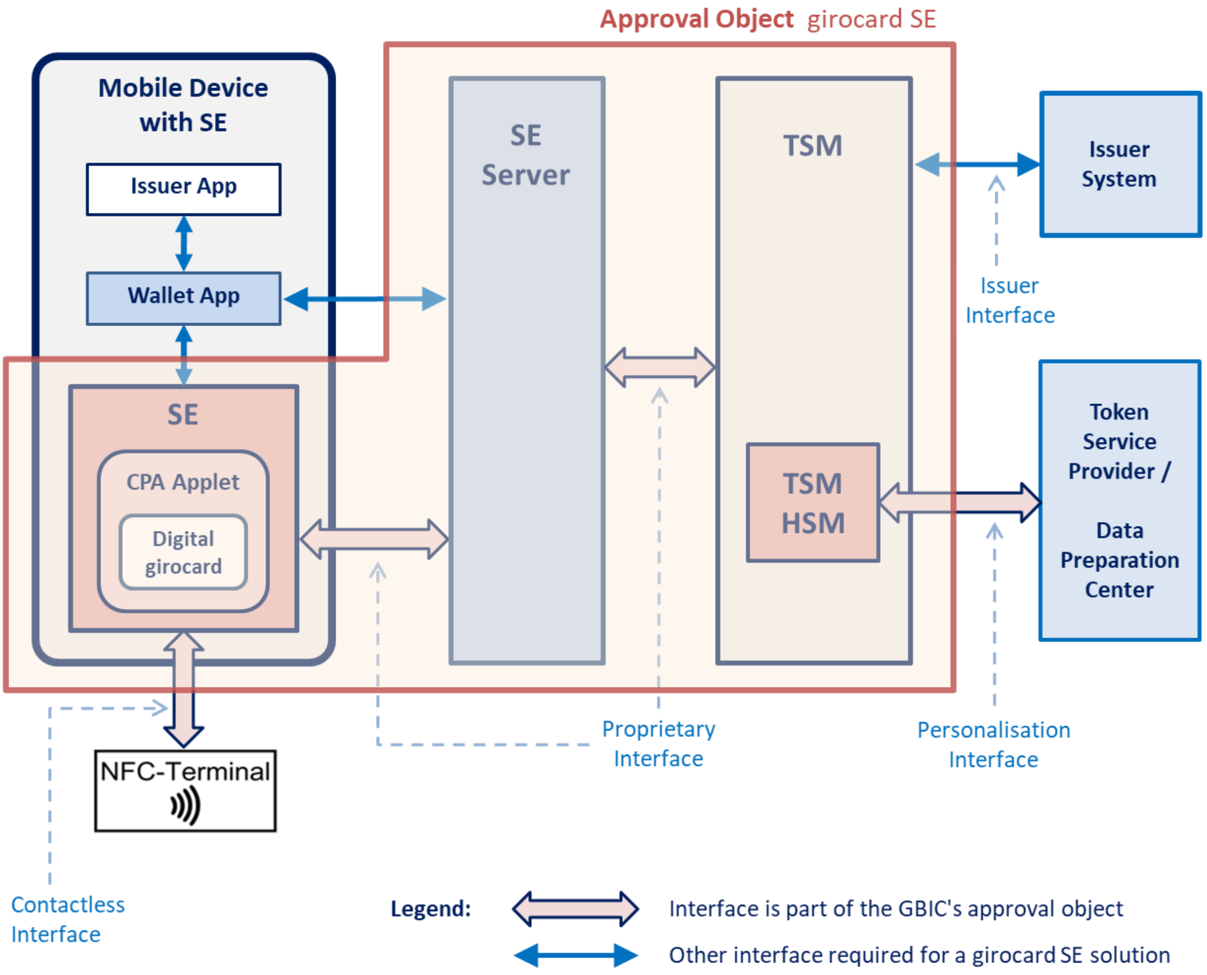

Approval Object girocard SE
Mobile Device with SE
Issuer App
Wallet App
SE
CPA Applet
Digital girocard
SE Server
TSM
TSM HSM
Issuer System
Issuer Interface
Token Service Provider / Data Preparation Center
NFC-Terminal
Proprietary Interface
Personalisation Interface
Contactless Interface
Legend:
Interface is part of the GBIC's approval object
Other interface required for a girocard SE solution

Figure 8: System Architecture for a "girocard SE solution"

On the SE a CPA Applet is installed that includes a girocard Digital Card. The CPA Applet can also contain digital cards from other payment systems at the same time. The CPA Applet communicates on the mobile device side with the Wallet App of the SE, which in turn has an interface with the card issuer's Payment App. The background system provides a secure channel from the SE to the Trusted Service Manager (TSM). The corresponding cryptographic keys are managed in the TSM-HSM. In particular, the TSM manages the keys to access the CPA Applet. The TSM is the connection between the card issuer and the Digital Card Provider for "girocard SE", and this role can be exercised by both the Digital Card Provider for "girocard SE" or a third party.

The TSM loads and deletes the CPA Applet, personalizes the Digital Card, and sends commands to manage the life cycle of the Digital Card. Therefore, there is an interface to the TSM from both the token service provider and the card issuer.

The set of data needed to emulate a girocard payment card for SE represents the Digital Card for "girocard SE".

The user (the owner, to be precise) of the mobile device is considered to be the cardholder of the Digital Cards. The Payment App as well as the Wallet App offer and control the interface to the cardholder, i.e. cardholder information and cardholder input.

The SE implements the functions needed

- for Digital Card processing over the contactless interface beside the EMV transaction itself,
- for Digital Card storage and
- for key management for the Digital Card with the TSM.

The CPA Applet itself implements the EMV transaction, either at an EMV terminal or in the form of an E-Commerce transaction.

Normally, the SE supports storage and processing of several CPA Applets and Digital Cards.

The TSM accesses Digital Cards over the SE Server interface for administration processes, e.g. loading of Digital Cards (also called personalisation or provisioning) and update of Digital Card data according to issuer requirements.

The contactless interface is an external interface of the SE, which has to be implemented according to the requirements of the technical interface specifications to work with any contactless EMV terminal. The technical interface specifications of the SE are called in following as girocard mobile SE specifications. As contactless interface the Near Field Communication (NFC) interface is used, about which the SE communicates (through the NFC controller and platform of the mobile device) with an NFC terminal. In case of an E-Commerce transaction, the CPA Applet calculates a cryptogram over transaction data that is passed through background systems for authorisation (see chapter 5.4.5.3).

The interfaces between Payment App and Wallet App as well as between Wallet App and the SE are device dependent interfaces.

The interface between the TSM and the Token Service Provider/ Data Preparation Center, called the personalisation interface, is used to process on behalf of a card issuer encrypted personalisation data for a Digital Card to the SE via the TSM. The personalisation interface is to be agreed and to be tested bilaterally. The test is out of scope of the approval, but a specification how to secure the card data during the personalisation is mandated. The TSM owns a hardware security module (TSM-HSM) which provides cryptographic mechanisms required for the personalisation, the key replenishment and the update of a Digital Card and which provides the cryptographic protection of all interfaces of the TSM.

5.4.4.3 Components of the Approval Object

The approval object "girocard SE" is a system implementing a "girocard SE solution". It consists of the following components, which have to be considered in the evaluation objects and the functional test object:

- the component "TSM" as a system, including
  - the hardware and software of the sub component "TSM HSM",
  - the operational environment of the sub component "TSM HSM";
- the component "SE" consisting of hardware and a software-platform:
- the component "CPA Applet" as a piece of software running within the SE and executing the EMV transaction.

The approval object "girocard SE" contains exactly one component "TSM" and one component "SE" with the "CPA Applet". Note: If several components "TSM" work together within a "girocard SE" system, then each pairing of one component "TSM" and one component "SE" requires an own registration and approval.

5.4.4.4 Security Evaluation

5.4.4.4.1 Security Requirements

Each component of the approval object "girocard SE" has to meet the security requirements referenced by the provider contract for digital cards referred to in the detailed approval requirements for Evaluation Objects

The security requirements referenced by the provider contract for digital cards define requirements for both the component "TSM" including the sub component "TSM HSM" as well as the component SE with its CPA applet. Thus, for the approval object "girocard HCE", following evaluation objects are defined:

- the evaluation object "TSM/TSM HSM" and
- the evaluation object "SE".

The following figure illustrates the evaluation objects and the required evaluation reports for them as described in the next two chapters:

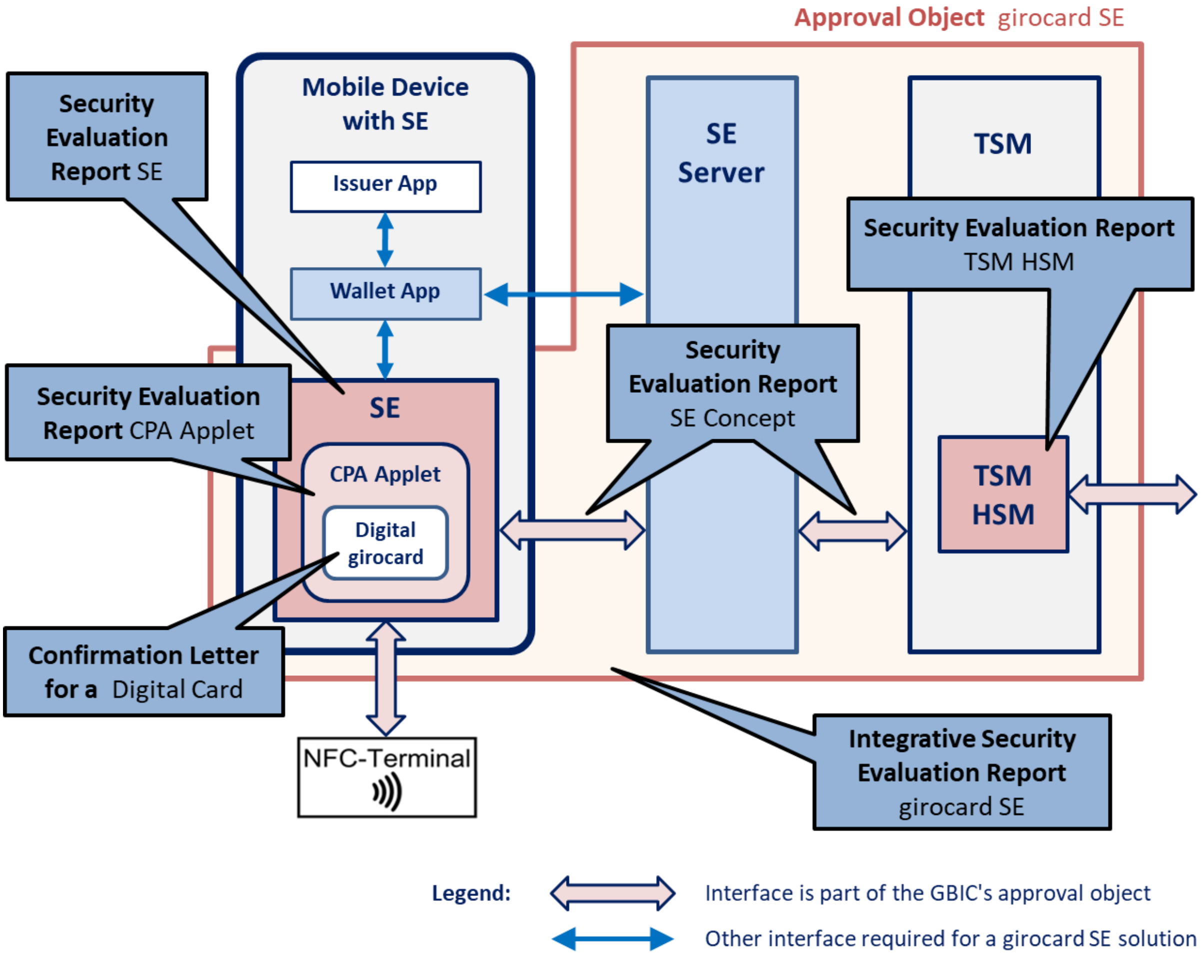

Approval Object girocard SE
Security Evaluation Report SE
Mobile Device with SE
Issuer App
Wallet App
SE
Security Evaluation Report CPA Applet
CPA Applet
Digital girocard
Confirmation Letter for a Digital Card
NFC-Terminal
SE Server
Security Evaluation Report SE Concept
TSM
Security Evaluation Report TSM HSM
TSM HSM
Integrative Security Evaluation Report girocard SE
Legend:
Interface is part of the GBIC's approval object
Other interface required for a girocard SE solution

Figure 9: Security Evaluation Reports for "girocard SE"

5.4.4.4.1.1 Evaluation Object "TSM/TSM HSM"

The evaluation object "TSM/TSM HSM" considers

- the concept for the interface between the component SE and the component "TSM" in interaction with the SE,
- the hardware and the software of the sub component "TSM HSM" as part of the component "TSM" and
- the operational environment of the sub component "TSM HSM".

For the evaluation object "TSM/TSM HSM", the following security evaluation reports are required:

- the "Security Evaluation Report SE concept" which describes the technical interface between the SE and the TSM in interaction with the SE,
- the "Security Evaluation Report TSM HSM" for the hardware and the software of the sub component TSM-HSM, which implements the SE concept. Further, the interfaces of the TSM-HSM to the external world required especially for the personalisation and update of digital cards have to be evaluated,
- the "Integrative Security Evaluation Report SE Solution" which integrates the reports for the SE concept, the hardware and the software of the sub component TSM-HSM and the SE and the CPA Applet (including Confirmation Letter) defined in chapter 5.4.4.4.1.2,
- and which contains an audit report assessing the operational environment of the sub component TSM-HSM. Further, the integrative security evaluation report references to the manufactures documentation forming the basis for all security evaluation reports for the approval object "girocard SE".

Any security relevant modification of the TSM-HSM of an approved "girocard SE solution" has to be re-evaluated.

5.4.4.4.1.2 Evaluation Object "SE"

The evaluation object "SE" considers the component SE. The SE implements amongst other things the SE concept evaluated according to chapter 5.4.5.4.2.

It has to be evaluated, whether the implementation of the evaluation object "SE" meets the security requirements of the provider contract.

The security evaluation for the SE has to be separated in

- the "Security Evaluation Report SE" covering the hardware and platform part of the girocard mobile SE specifications implemented by the SE (this may also consist of one for the hardware and one for the platform),
- the "Security Evaluation Report CPA Applet" covering the CPA Applet part of the girocard mobile SE specifications implemented by the CPA Applet and
- at least one "Confirmation Letter for a Digital Card" each covering one certain type of Digital Cards within the SE determined according to the application part of the girocard mobile SE specifications.

In the "Security Evaluation Report CPA Applet", the Security Evaluator has to confirm that the CPA applet meets the security requirements independent from any chosen type of Digital Card. If there is a dependency, this dependency has to be indicated in the report. In the "Confirmation Letter for a Digital Card" covering one type of Digital Cards, the Security Evaluator has to confirm that any Digital Card of this type meets the security requirements based on the evaluated CPA Applet and considers possible dependencies indicated in the platform security evaluation. The template for a "Confirmation Letter for a Digital Card" will be provided by the Approval Office.

For an approved "girocard SE solution" 12 months after the validation of the "Security Evaluation Report SE " by the Security Committee, a Security Evaluator has to confirm in an assessment by a confirmation letter that the security requirements are still met according to state-of-art of science and technology. The Approval Owner is responsible for the re-initiation of the approval process and has to provide the confirmation letter four weeks before the end of a period. Therefore, the approval for a "girocard SE solution" is granted only for the period of 12 months after the validation of the "Security Evaluation Report SE" by the Security Committee. The prolonged approval is re-granted for a period of twelve months. The repetition of this procedure is allowed without restrictions. Without prolongation, the approval of a "girocard SE solution" terminates.

Any security relevant modification of the SE or CPA Applet of an approved "SE" has to be re-evaluated.

5.4.4.5 Functional Test

5.4.4.5.1 Functional Test Requirements

The functional test requirements of the approval object "girocard SE" consist of the technical interface specifications, which are part of the appendixes of the provider contract for digital cards referred to in the detailed approval requirements for "digitale girocard".

The test object "Digital Card" consists of the verification that by provisioning a type of Digital Card for girocard into a CPA Applet running in the SE, all functional test requirements for the components on the mobile device are fulfilled by the girocard SE solution to be approved.

The provider contract for digital cards may require that more than one version of CPA Applets has to be supported by a girocard SE solution. Such, for each required CPA Applet version, the functional test requirements has to be verified.

5.4.4.5.2 Test Object "Digital Card"

The test object is a Digital Card for girocard as it is inserted into a CPA Applet based on the personalisation data of the Data Preparation Center. The test objective is to ensure the correct functionality of the digital card for the customer in interaction with the terminal types and acceptance technologies (e.g. E-Commerce) in the field.

For the type of Digital Card inserted into a CPA Applet, an functional test has to be performed by the approval applicant. The functional test must be based on a common catalogue of test scenarios, which will be provided by the Testing Laboratory.

According to the requirements of his girocard SE solution, the Approval Applicant derives concrete test cases from the prescribed test scenarios and executes these test cases independently. The test results must be assembled in a prescribed format and submitted to the Testing Laboratory for review. In the case of a failure, the deviations are to be documented accordingly.

The common catalogue of test scenarios must cover the following sub-objectives:

- Tests for provisioning and updating Digital Cards,
- Payment with the Digital Card,
- Interoperability and field tests and
- Life cycle processes of the Digital Card.

The Testing Laboratory validates the test results submitted by the Approval Applicant against the requirements of the test scenarios. In the result, the Testing Laboratory creates a functional test report.

5.4.5 Approval Object "Online-Netzbetreiber"

5.4.5.1 Description of the Approval Object

The "Online-Netzbetreiber" is a participant in "girocard im Online-Handel" and is entitled to operate a system responsible for the processing of E-Commerce transactions on behalf of its commissioned merchants. The system of the "Online-Netzbetreiber" transmits payment requests from online shops to the systems of the German banking industry, which are responsible for processing with the card-issuing banks.

The approval object "Online-Netzbetreiber" consists of

- the technical system (host) of the "Online-Netzbetreiber" and
- the operating environment of the system of the "Online-Netzbetreiber".

For the approval object "Online-Netzbetreiber", two technical variants are supported:

1. "Online-Netzbetreiber (HCE)": The variant Host Card Emulation ("HCE") is based on Digital Cards in the Mobile Payment App of the card issuer on Android devices.

2. "Online-Netzbetreiber (iOS)": The variant based is on the mobile payment solution for digital purses (wallets) containing Digital Cards and which are operated by a third party in the technical variant iOS ("iOS").

The approval owner is the provider of a system operating either the technical variant "HCE" or the technical variant "iOS" or both of them.

The approval cannot be transferred to other companies.

5.4.5.2 "Online-Netzbetreiber" in an E-Commerce solution based on HCE

The technical variant "Online-Netzbetreiber (HCE)" of the approval object "Online-Netzbetreiber" is embedded in an HCE based E-Commerce solution as shown in the following figure:

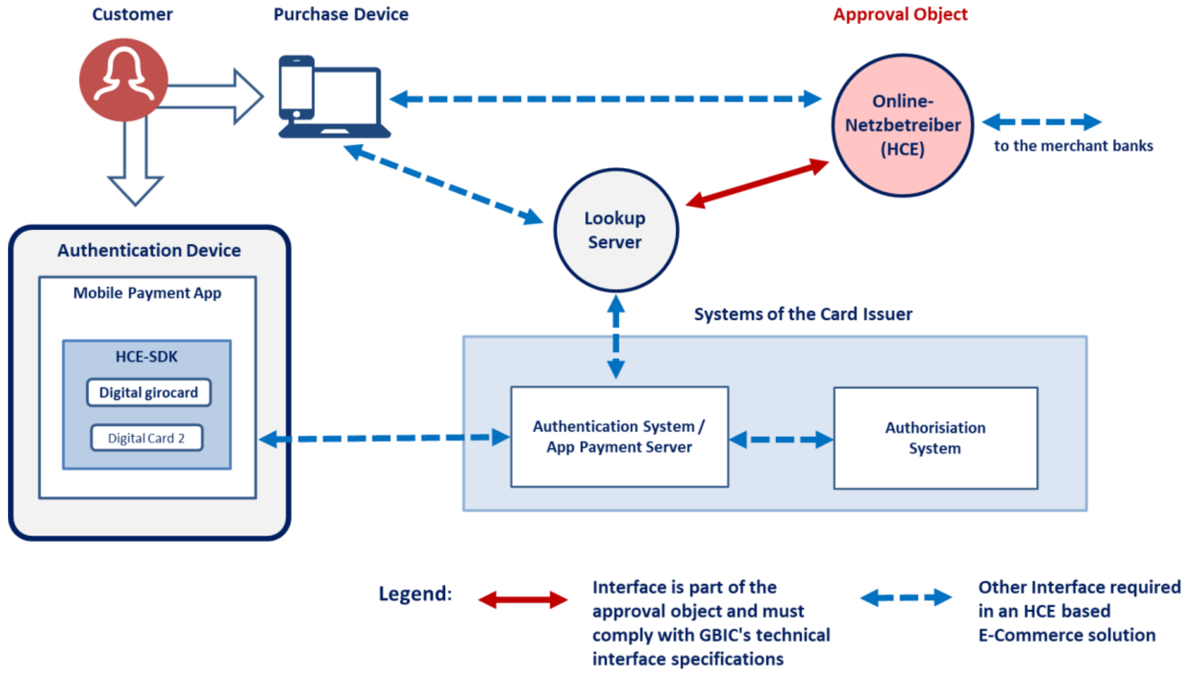

Customer
Purchase Device
Approval Object
Online-Netzbetreiber (HCE)
to the merchant banks
Lookup Server
Authentication Device
Mobile Payment App
HCE-SDK
Digital girocard
Digital Card 2
Systems of the Card Issuer
Authentication System / App Payment Server
Authorisiation System
Legend:
Interface is part of the approval object and must comply with GBIC's technical interface specifications
Other Interface required in an HCE based E-Commerce solution

Figure 10: "Online-Netzbetreiber (HCE)" in an E-Commerce solution based on HCE

To understand the role of the "Online-Netzbetreiber (HCE)" in an E-Commerce solution based on HCE, the basic principle of the interaction of its components is described:

The customer selects on the checkout page of an online shop to pay with girocard. The "Online-Netzbetreiber (HCE)" assembles the transaction data, which include the amount and the merchant's name, determines the environmental data from the cardholder's **Purchase Device** and sends both pieces of information to the **Lookup-Server**.

The Lookup-Server represents the central entry point of the card-issuing institutes for "girocard im Online-Handel" based on HCE and distributes the payment request to the **Authentication Systems** of the card issuers which are responsible to find a suitable Authentication Device belonging to the customer. The **Authentication Device** is an Android mobile device containing a **Mobile Payment App** that the customer uses to confirm and to authenticate the transaction. The Mobile Payment App contains a **HCE SDK** where a **Digital Card** for girocard must be stored. For the processing on the Authentication Device, the Authentication System checks whether a **CDCVM** is required and forwards the transaction data and the CDCVM decision to the Mobile Payment App. The part of the Authentication System that controls the Mobile Payment App is also called the **App Payment Server**.

The Mobile Payment App transmits the cryptographic evidence of the customer's confirmation to the App Payment Server, which forwards it to the **Authorisation System** of the card issuer.

The Authentication System informs the Lookup Server about the result of the authorisation which returns the result to the system of the "Online-Netzbetreiber (HCE)".

A further task of the system of the "Online-Netzbetreiber (HCE)" is to forward the clearing data received from the Lookup-Server to the different merchant banks.

The interface between the system of the "Online-Netzbetreiber (HCE)" and the Lookup-Server must comply with the technical interface specifications of GBIC.

5.4.5.3 "Online-Netzbetreiber" in an E-Commerce solution based on iOS

The technical variant "Online-Netzbetreiber (iOS)" of the approval object "Online-Netzbetreiber" is embedded in an iOS based E-Commerce solution as shown in the following figure:

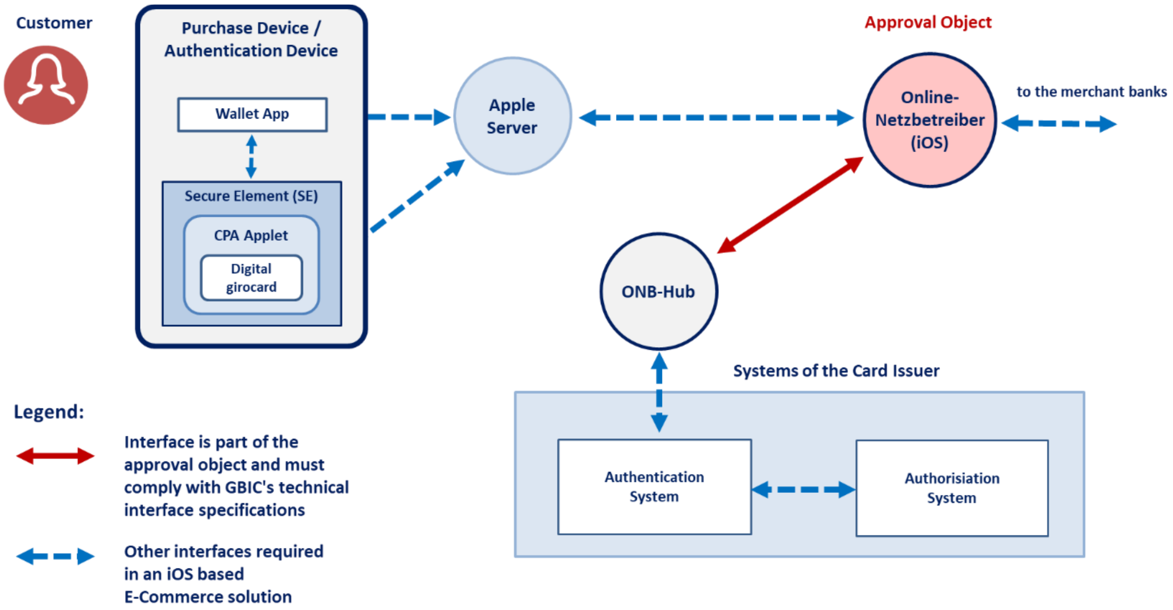

Customer
Purchase Device / Authentication Device
Wallet App
Secure Element (SE)
CPA Applet
Digital girocard
Apple Server
Approval Object
Online-Netzbetreiber (iOS)
to the merchant banks
ONB-Hub
Systems of the Card Issuer
Authentication System
Authorisiation System
Legend:
Interface is part of the approval object and must comply with GBIC's technical interface specifications
Other interfaces required in an iOS based E-Commerce solution

Figure 11: "Online-Netzbetreiber (iOS)" in an E-Commerce solution based on iOS

To understand the role of the "Online-Netzbetreiber (iOS)" in an E-Commerce solution based on iOS, the basic principle of the interaction of its components is described:

In an Apple Pay E-Commerce transaction, the iOS mobile device displays the amount and the merchant's name, the cardholder confirms this data and performs CDCVM. Apple systems determine whether the customer and the merchant together support, among other things, the girocard payment method. Then, when a customer selects the "digitale girocard" in the **Wallet App**, the **CPA Applet** calculates the application cryptogram based on the Digital Card. CPA applet and Digital Card are always stored in the **Secure Element (SE)**, the hardware component for storing and processing of sensitive data.

The system of the "Online-Netzbetreiber (iOS)" receives an encrypted message from the **Apple Server** containing the girocard transaction data and the application cryptogram. This information is forwarded to the **ONB-Hub** which represents the central entry point of the card-issuing institutes for "girocard im Online-Handel" based on iOS.

The ONB-Hub transmits the transaction-related data to the **Authentication Systems** of the card-issuing institutes. Each Authentication System checks whether it is responsible for the Digital Card involved in the payment transaction and if so, it transmits the transaction data to the associated **Authorisation System** of the card issuer. The Authentication System informs the ONB-Hub about the result of the authorisation which forwards the result to the system of the "Online-Netzbetreiber (iOS)".

A further task of the system of the "Online-Netzbetreiber (iOS)" is to forward the clearing data received from the ONB-Hub to the different merchant banks.

The interface between the system of the "Online-Netzbetreiber (iOS)" and the ONB-Hub must comply with the technical interface specifications of GBIC.

5.4.5.4 Security Evaluation

5.4.5.4.1 Security Requirements

The "Online-Netzbetreiber" performs sensitive operations for the processing of E-Commerce transactions. Therefore, the system of the "Online-Netzbetreiber" must comply with the security requirements "Sicherheitskriterien für Dienstleister für girocard im Online-Handel", which are part of the appendix of the contract for "Online-Netzbetreiber".

The security requirements must be met regardless of which technical variant "HCE" or "iOS" is used.

5.4.5.4.2 Evaluation Object "Online-Netzbetreiber"

The evaluation object assigned to the approval object "Online-Netzbetreiber" consists of the security concept of the "Online-Netzbetreiber" including the interfaces as well as their configuration, personal responsibilities and the onboarding process for merchants.

For the evaluation object "Online-Netzbetreiber", a security evaluation report for the security concept is required, describing the technical interfaces, personnel responsibilities and sensitive processes.

5.4.5.5 Functional Test

5.4.5.5.1 Functional Test Requirements

GBIC specifies the functional requirements of an "Online-Netzbetreiber" in the technical appendix of provider contract for "Online-Netzbetreiber" called "Technischer Anhang zum Vertrag über die Zulassung als Online-Netzbetreiber im girocard-System der Deutschen Kreditwirtschaft".

If the technical variant "HCE" is used, the functional requirements of the technical appendix assigned to "Variante HCE" are to be fulfilled.

If the technical variant "iOS" is used, the functional requirements of the technical appendix assigned to "Variante Apple Pay" are to be fulfilled.

5.4.5.5.2 Test Object "Online-Netzbetreiber (HCE)"

If the "Online-Netzbetreiber" implements the technical variant "HCE", the interface of the technical system (host) of the "Online-Netzbetreiber (HCE)" to the Lookup-Server must be tested.

An integration functional test has to be performed by the Approval Applicant in co-operation with the provider of the central Lookup-Server. The test plan "TP ONB (HCE)" which is mandatory to be performed during the integration functional test is created and is made available by the provider of the Lookup-Server. The test plan is developed based on the requirements of the test case catalogue for the connection of the "Online-Netzbetreiber (HCE)" to the Lookup-Server defined by GBIC, called "GBIC TCC ONB (HCE)". The assessment of the test plan "TP ONB (HCE)" is part of the approval of the provider of the Lookup-Server (see chapter 5.4.6.3.2). An accredited Technical Expert verifies the content of the test plan and examines the results of its run in the integration functional test of the first "Online-Netzbetreiber" applicant with regard to the approval of the Lookup-Server.

After completion of the integration functional test, the Approval Applicant submits a "Testing Conformance Statement for the Integration Functional Test" to GBIC via the Approval Office, which must contain the confirmation from the provider of the Lookup-Server about the successful execution of the test plan "TP ONB (HCE)".

5.4.5.5.3 Test Object "Online-Netzbetreiber (iOS)"

If the "Online-Netzbetreiber" implements the technical variant "iOS", the interface of the technical system (host) of the "Online-Netzbetreiber (iOS)" to the ONB-Hub must be tested.

An integration function test has to be performed by the Approval Applicant in co-operation with the provider of the central ONB-Hub. The test plan "TP ONB (iOS)" which is mandatory to be performed during the integration functional test is created and is made available by the provider of the ONB-Hub. The test plan is developed based on the requirements of the test case catalogue for the connection of the "Online-Netzbetreiber" to the ONB-Hub defined by GBIC, called "GBIC TCC ONB (iOS)""GBIC TCC ONB (iOS)". The assessment of the test plan "TP ONB (iOS)" is part of the approval of the provider of the ONB-Hub (see chapter 5.4.7.3.2). An accredited Technical Expert verifies the content of the test plan and checks the results of its run in the integration functional test of the first "Online-Netzbetreiber" applicant with regard to the approval of the ONB-Hub.

After completion of the integration functional test, the Approval Applicant submits a "Testing Conformance Statement for the Integration Functional Test" to GBIC via the Approval Office, which must contain the confirmation from the provider of the ONB-Hub about the successful execution of the test plan "TP ONB (iOS)".

5.4.6 Approval Object "Lookup-Server"

5.4.6.1 Description of the Approval Object

The "Lookup-Server" is a participant in "girocard im Online-Handel" and is required as the central entry point of the card-issuing institutes in the girocard system for E-Commerce based on HCE to distribute the payment requests coming from an "Online-Netzbetreiber" to the Authentication System of the responsible card issuer. The central entry point allows the card issuer to control the type of authentication as well as the design of the customer's connection independently of the merchant system.

The approval object "Lookup-Server" consists of the technical system of the "Lookup-Server". The approval owner is the provider operating that technical system.

The approval cannot be transferred to other companies.

The approval object "Lookup-Server" is embedded in an HCE based E-Commerce solution as shown in the following figure:

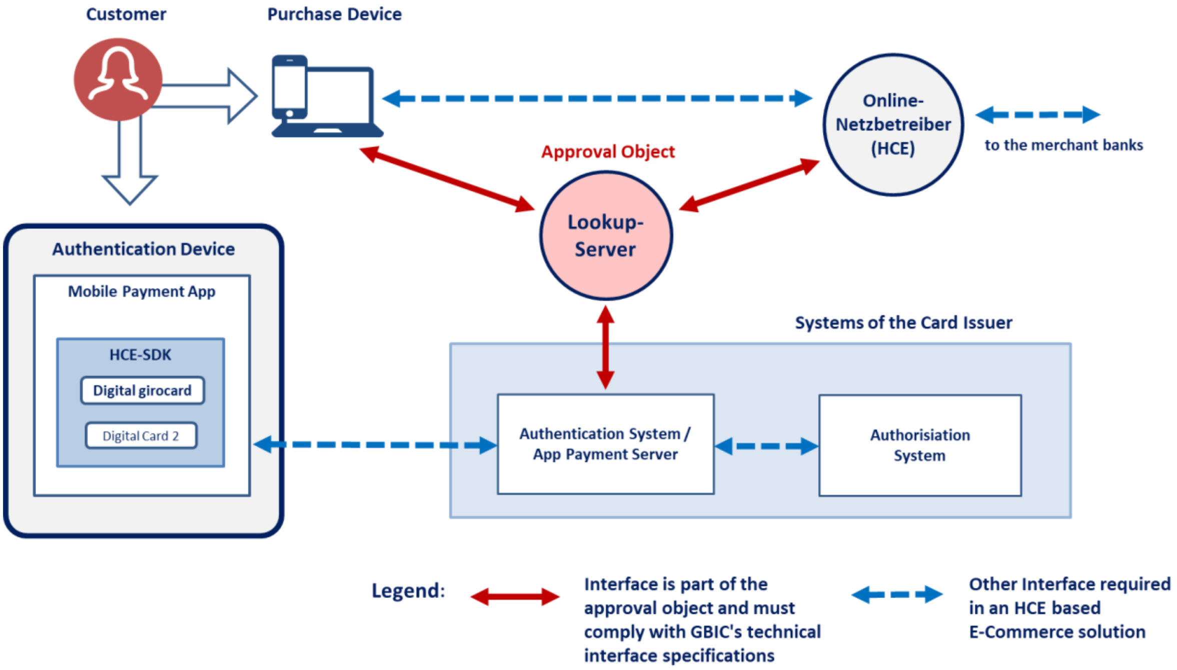

Customer
Purchase Device
Online-Netzbetreiber (HCE)
to the merchant banks
Approval Object
Lookup-Server
Authentication Device
Mobile Payment App
HCE-SDK
Digital girocard
Digital Card 2
Systems of the Card Issuer
Authentication System / App Payment Server
Authorisiation System
Legend:
Interface is part of the approval object and must comply with GBIC's technical interface specifications
Other Interface required in an HCE based E-Commerce solution

Figure 12: "Lookup-Server" in an E-Commerce solution based on HCE

The role of the "Lookup-Server" in an E-Commerce solution based on HCE represents the link between the sphere of the merchants and the sphere of the card issuers. That E-Commerce solution has already been described in chapter 5.4.5.2 from the perspective of the merchants and in chapter 5.4.3.3 from the perspective of the customers and card issuers.

Three sub-processes may be triggered by the "Online-Netzbetreiber (HCE)" at the "Lookup-Server": release of a payment transaction, capture and payment cancellation. The "Lookup-Server" distributes the respective type of request to the Authentication System of the card issuers which is responsible. In response, the "Lookup-Server" transmits the result of the authentication or cancellation and clearing data from the card issuer to the "Online-Netzbetreiber (HCE)".

In the response of a payment request, the Authentication System may require the selection of the authentication method by the customer. In this case, the "Lookup-Server" builds a web page on the Purchase Device for the method selection, whereby the URL for this is requested from the "Online-Netzbetreiber (HCE)".

5.4.6.2 Security Evaluation

5.4.6.2.1 Security Requirements

For the approval object "Lookup-Server", there are no security requirements that must be verified by a security evaluation.

5.4.6.2.2 Evaluation Object

The approval object "Lookup-Server" has no evaluation object.

5.4.6.3 Functional Test

5.4.6.3.1 Functional Test Requirements

GBIC specifies the functional requirements of a "Lookup-Server" in the technical appendix of provider contract for "Lookup-Server-Betreiber" called "girocard Online-Handel Lookup-Server Systembeschreibung".

5.4.6.3.2 Test Object

The test object consists of the interfaces to the "Online-Netzbetreiber (HCE)", the Authentication System and to the Purchase Device.

A functional test has to be performed by the Approval Applicant based on the catalogue of provider-independent test cases defined by GBIC, called "GBIC TCC Lookup-Server". Inline with its existing technical system, the Approval Applicant derives concrete test cases from the prescribed test scenarios and executes these test cases autonomously. All test results, including interim results, must be submitted to a GBIC authorised Technical Expert for review.

To support the integration functional test for an Approval Applicant of the approval object "Online-Netzbetreiber (HCE)" (see chapter 5.4.5.5.2) a test plan "TP ONB (HCE)" has to be developed based on the requirements of the test case catalogue for the connection of the "Online-Netzbetreiber (HCE)" to the Lookup-Server defined by GBIC, called "GBIC TCC ONB (HCE)". Inline with its existing technical system, the Approval Applicant derives concrete test cases from the prescribed test scenarios which form the specific test plan "TP ONB (HCE)". The content of the test plan "TP ONB (HCE)" and its first successful use during an integration functional test by an "Online-Netzbetreiber (HCE)" has to be confirmed by a GBIC accredited Technical Expert.

The Approval Applicant submits a "Testing Conformance Statement for the Functional Test" to GBIC via the Approval Office, which must contain the following three Technical Expert Confirmations:

1. Confirmation of Functional Test "Lookup-Server": a successful completion of the functional test based on test cases that were correctly and completely derived from the "GBIC TCC Lookup-Server" test case catalogue,

2. Confirmation of Test Plan "TP ONB (HCE)": a complete and correct description of the test plan "TP ONB (HCE)" in derivation of the test case catalogue "GBIC TCC ONB

(HCE)" for the connection of the "Online-Netzbetreiber" to the Lookup-Server defined by GBIC and

3. Confirmation of Test Implementation for "TP ONB (HCE)": a successful use of the test plan "TP ONB (HCE)" in a first integration functional test by an approved "Online-Netzbetreiber (HCE)" or an Approval Applicant of this approval object.

5.4.7 Approval Object "ONB-Hub"

5.4.7.1 Description of the Approval Object

The "ONB-Hub" is a participant in "girocard im Online-Handel" and is required as the central entry point of the card-issuing institutes in the girocard system for E-Commerce based on iOS to distribute the payment requests coming from an "Online-Netzbetreiber" to the Authentication System of the responsible card issuer.

The approval object "ONB-Hub" consists of the technical system of the "ONB-Hub". The approval owner is the provider operating that technical system.

The approval cannot be transferred to other companies.

The approval object "ONB-Hub" is embedded in an iOS based E-Commerce solution as shown in the following figure:

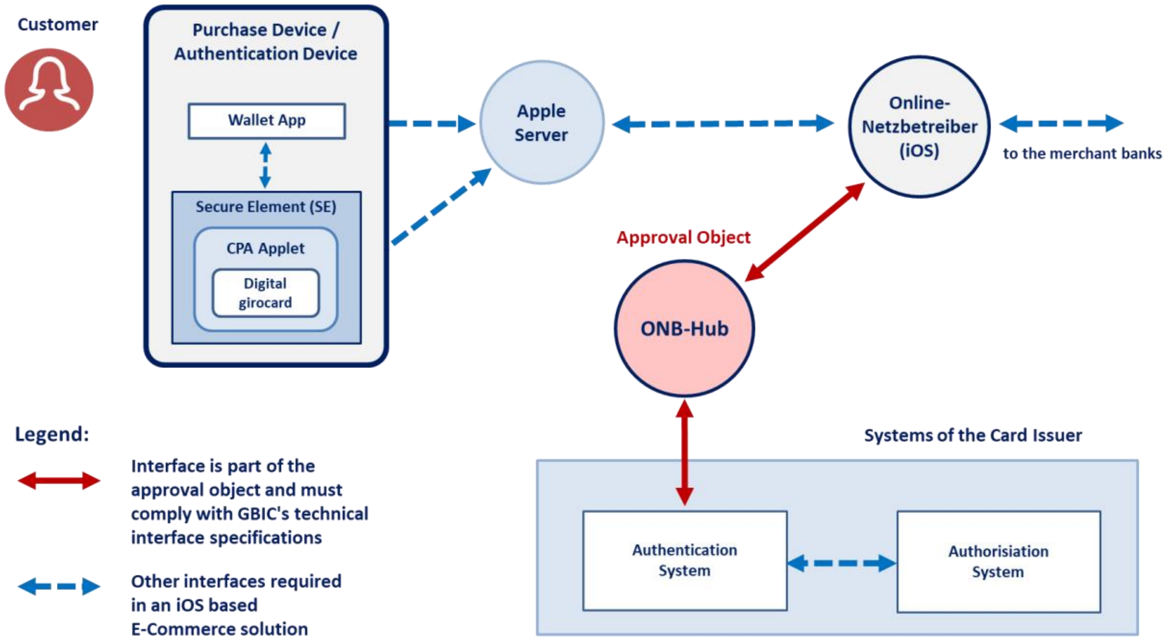

Customer
Purchase Device / Authentication Device
Wallet App
Secure Element (SE)
CPA Applet
Digital girocard
Apple Server
Online-Netzbetreiber (iOS)
to the merchant banks
Approval Object
ONB-Hub
Systems of the Card Issuer
Authentication System
Authorisiation System
Legend:
Interface is part of the approval object and must comply with GBIC's technical interface specifications
Other interfaces required in an iOS based E-Commerce solution

Figure 13: "ONB-Hub" in an E-Commerce solution based on iOS

The role of the "ONB-Hub" in an E-Commerce solution based on iOS represents the link between the sphere of the merchants and the sphere of the card issuers. That E-Commerce solution has already been described in chapter 5.4.5.3.

Three sub-processes may be triggered by the "Online-Netzbetreiber (iOS)" at the "ONB-Hub": release of a payment transaction, capture and payment cancellation. In response, the "ONB-Hub" transmits the result of the authentication or cancellation and clearing data from the card issuer to the "Online-Netzbetreiber (iOS)".

5.4.7.2 Security Evaluation

5.4.7.2.1 Security Requirements

For the approval object "ONB-Hub", there are no security requirements that must be verified by a security evaluation.

5.4.7.2.2 Evaluation Object

The approval object "ONB-Hub" has no evaluation object.

5.4.7.3 Functional Test

5.4.7.3.1 Functional Test Requirements

GBIC specifies the functional requirements of a "ONB-Hub" in the technical appendix of provider contract for "ONB-Hub-Betreiber" called "girocard Online-Handel ONB-Hub Systembeschreibung".

5.4.7.3.2 Test Object

The test object consists of the interfaces to the "Online-Netzbetreiber (iOS)" and the Authentication System.

A functional test has to be performed by the Approval Applicant based on the catalogue of provider-independent test cases defined by GBIC, called "GBIC TCC ONB-Hub". Inline with its existing technical system, the Approval Applicant derives concrete test cases from the prescribed test scenarios and executes these test cases autonomously. All test results, including interim results, must be submitted to a GBIC authorised Technical Expert for review.

To support the integration functional test for an Approval Applicant of the approval object "Online-Netzbetreiber (iOS)" (see chapter 5.4.5.5.3) a test plan "TP ONB (iOS)" has to be developed based on the requirements of the test case catalogue for the connection of the "Online-Netzbetreiber (iOS)" to the ONB-Hub defined by GBIC, called "GBIC TCC ONB (iOS)". Inline with its existing technical system, the Approval Applicant derives concrete test cases from the prescribed test scenarios which form the specific test plan "TP ONB (iOS)". The content of the test plan "TP ONB (iOS)" and its first successful use during an integration functional test by an "Online-Netzbetreiber (iOS)" has to be confirmed by a GBIC accredited Technical Expert.

The Approval Applicant submits a "Testing Conformance Statement for the Functional Test" to GBIC via the Approval Office, which must contain the following three Technical Expert Confirmations:

1. Confirmation of Functional Test "ONB-Hub": a successful completion of the functional test based on test cases that were correctly and completely derived from the "GBIC TCC ONB-Hub" test case catalogue,

2. Confirmation of Test Plan "TP ONB (iOS)": a complete and correct description of the test plan "TP ONB (iOS)" in derivation of the test case catalogue "GBIC TCC ONB (iOS)" for the connection of the "Online-Netzbetreiber" to the ONB-Hub defined by GBIC and

3. Confirmation of Test Implementation for "TP ONB (iOS)": a successful use of the test plan "TP ONB (iOS)" in a first integration functional test by an approved "Online-Netzbetreiber (iOS)" or an Approval Applicant of this approval object.

5.4.8 Glossary – Digital Cards

Application Part (of the HCE specifications) – The part of the technical specifications which define the concrete setting of data elements introduced in the Platform Part of the HCE specification ("CPACE for Host Card Emulation (HCE) in a Consumer Device") to fulfil the requirements of an application.

Authentication Device – A mobile device containing the cardholder's Digital Card that carries out the authentication for a "girocard im Online-Handel" transaction and calculates the application cryptogram.

Authentication System – A system that is responsible for authentication on behalf of the issuer for E-Commerce transactions over the Internet. The Authentication System exchanges payment-related messages between the Lookup-Server or ONB-Hub, the cardholder's Authentication Device and the Issuer Authorisation System. The part of the Authentication System that controls the Mobile Payment App for HCE based transactions is called the **App Payment Server**.

Consumer Device Cardholder Verification Method (CDCVM) – A Cardholder Verification Method in which authentication is performed by verifying a passcode or a biometric feature on the cardholder's Authentication Device.

CPA Applet – A software running in the Secure Element (SE) and executing an EMV transaction. The CPA Applet includes one or more Digital Cards, in particular a Digital Card for its use within the girocard system.

Digital Card – The set of personalisation data and cryptographic keys required to emulate a card in a mobile device that allows payments at a Point Of Sale (POS) terminal or E-Commerce payments within the girocard system.

Digital Card Provider – A Digital Card Provider is the approval owner of a system providing a certain type of Digital Cards. He is entitled to personalise and operate that type of Digital Cards on behalf of card issuing banks within the girocard system.

digitale girocard – An emulated payment card stored in and operated by a mobile device or other dedicated device. The set of data needed to emulate a "digitale girocard" is called a Digital Card.

E-Commerce – The term refers to payment transactions that involve the purchase and sale of goods or services over the internet.

girocard im Online-Handel – The technical infrastructure and the related legal contracts that enable E-Commerce transactions via the internet at retail and service companies on the basis of the girocard system.

Host Card Emulation (HCE) – A method of card emulation on a mobile device that enables a Mobile Payment App to emulate a card and communicate with a POS terminal or with the card issuer's Authentication System for E-Commerce transactions.

HCE SDK – Software integrated into the Mobile Payment App that implements the functions required for processing transactions based on Digital Cards and their storage and management. The processing functions to be offered include, on the one hand, the functions for communication via the contactless interface at a POS terminal and, on the other hand, the functions for communication with an App Payment Server to support E-Commerce transactions. The latter can be outsourced to a separate software "Extension for E-Commerce", which communicates with the HCE SDK by emulating the contactless interface and then also has to be integrated into the Mobile Payment App. Digital card storage and management take place over the Mobile Payment App interface and the HCE Server interface.

HCE Server - A server operated by or on behalf of the issuer of Digital Cards to which the HCE SDK connects for provisioning and management of a Digital Card.

Issuer Authorisation System – A system responsible for processing online authorisation requests for payment transactions within the girocard system on behalf of the issuer.

Lookup-Server – The central entry point of the card-issuing institutes in "girocard im Online-Handel" based on HCE which constitutes the link between the system of the "Online-Netzbetreiber (HCE)" and the Authentication System of the card issuer.

Mobile Payment App – A mobile app which has been declared to the platform of the mobile device that it implements an HCE service for payment, thus emulating one or several payment cards.

ONB-Hub – The central entry point of the card-issuing institutes in "girocard im Online-Handel" based on SE which constitutes the link between the system of the "Online-Netzbetreiber (iOS)" and the Authentication System of the card issuer.

Online-Netzbetreiber – An online network provider (in English) is a participant at "girocard im Online-Handel", who must have a contractual relationship with both the merchant and the German banking industry and who is responsible for the processing of an E-Commerce transaction on the merchant's side. The Online-Netzbetreiber and the merchant can be identical.

Platform Part (of the HCE specifications) – The part of the technical specifications which define the functionality of a HCE SDK without a concrete setting of its data elements. For "digitale girocards" based on HCE the requirements of the "CPACE for Host Card Emulation (HCE) in a Consumer Device" specification are to be fulfilled.

Platform (of the mobile device) – A manufacturer independent operating system and its minimum version that provides the functionality and the resources required to execute a Mobile Payment App.

Secure Element (SE) – A secure hardware component integrated into a mobile device in which sensitive data can be stored and sensitive processes executed. For processing of girocard transactions, a CPA Applet containing the Digital Card must be installed in the SE.

Trusted Service Manager (TSM) – Entity having the access right to load CPA applets and Digital Cards on a SE.

Token Service Provider / Data Preparation Center – A system that provides the encrypted personalisation data for a Digital Card on behalf of a card issuer.

5.5 German ATM System

5.5.1 System Description

The German ATM system is a scheme for cash withdrawals with payment cards using a PIN. Besides GBIC further licensors of global payment schemes may be involved (VISA, MasterCard, JCB, Amex, ...). The data processing centres of the Acquirers operate ATMs based on contracts between acquirers and the respective payment schemes.

5.5.2 Agreements/Contracts

GBIC specifies the functional and security requirements for the German ATM system in the technical interface specification of the German ATM agreement. This technical interface specification is used for the implementation of components of the German ATM system. Especially the interface between debit card issuer and acquirer gateway (Nationaler Online-Verbund) as well as the interface between the ATM and accepted ICCs are specified. The technical interface specification of the German ATM agreement covers EMV and the respective technical interface specifications of the payment schemes.

GBIC and MasterCard International have agreed on a procedure for the approval of ICCs and terminals using MasterCard debit and credit applications (see detailed approval requirements for ATM). Based on this agreement, MasterCard International acknowledges the GBIC approval for its payment schemes. As JCB-cards are processed as Cirrus-cards a separate agreement with JCB for ATM acceptance is not needed.

GBIC is in negotiation with other payment schemes to agree on a procedure for the approval of ICCs and terminals using their applications. As long as no agreement between GBIC and these payment schemes is achieved, ICCs and terminals of the German ATM network using applications of these payment schemes must pass the approval process of the respective payment scheme.

5.5.3 GBIC ICC Approval Object

The approval objects Credit ICC or Debit ICC are described in chapter 5.3.

5.5.4 Approval Object "Automated Teller Machine (ATM)"

5.5.4.1 Description of the Approval Object

The approval object "Automated Teller Machine (ATM)" consists of hardware and software covering the technical interface specification of the German ATM agreement and the corresponding security requirements to carry out cash withdrawals for the schemes as defined in the detailed approval requirements for ATMs.

The interfaces to be checked within the approval process include the online interface of the ATM, the communication between the ATM and the ICC and to the cardholder.

The approval of an ATM is issued as a Type Approval and will be granted for ATMs of the German ATM system.

5.5.4.2 Security Evaluation

5.5.4.2.1 Security Requirements

Each component of the German ATM system has to meet the security requirements of the German ATM Agreement and the ec-PIN-Agreement referred to in the detailed approval requirements for ATMs. Therefore the ATM as a component of the German ATM system has to meet these security requirements.

Since the ATM supports the acceptance of cards of global payment schemes - called functions in the detailed approval requirements for ATM - the ATM has to meet the security requirements of the global payment schemes, too.

The PIN security requirements of each payment scheme to be supported by German ATMs are referred to in the detailed approval requirements for ATMs.

JCB, MasterCard International and VISA International require that EPPs must meet specific EPP security requirements. The JCB, MasterCard and VISA EPP security requirements are referred to in the detailed approval requirements for ATMs. If necessary, the EPP security requirements of any other payment scheme are referred to in the approval requirements for ATMs.

5.5.4.2.2 Evaluation Object "EPP for ATM"

The EPP is the evaluation object of the approval object ATM. Note: In the GBIC Approval Scheme the EPP includes components and functions securing the integrity of messages.

The evaluation object includes the hardware, the software and the personalisation environment of the EPP.

The Security Evaluator verifies whether the EPP meets the GBIC security requirements. Additionally the Security Evaluator shall testify in the security evaluation report whether the EPP security requirements of other payment schemes are met. It is expected that a EPP meeting the security requirements of the German ATM agreement also meets the specific EPP security requirements of other payment schemes.

As a result of the security evaluation of the EPP the Security Evaluator may identify conditions to the operational environment of the EPP. The Security Evaluator must document these conditions in the security evaluation report. Environmental conditions may concern "View protection against PIN disclosure", "Sequence control" respective "Software integrity" and "Secure key loading".

The approval letter for the approval owner refers to the tested technical interface specifications and the evaluated security requirements. Additionally the approval letter refers to the specific conditions to the operational environment of the EPP which are not met by the EPP alone.

5.5.4.3 Functional Test

5.5.4.3.1 Functional Test Requirements

The functional test requirements consist of tests according to the technical interface specification of the German ATM agreement.

5.5.4.3.2 Test Object "ATM"

The ATM is fully tested by a Testing Laboratory if no EMVCo Type Approval exists.

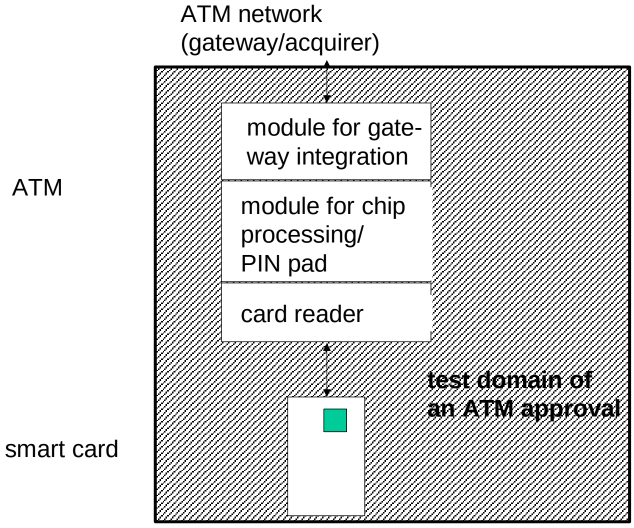

ATM network
(gateway/acquirer)
ATM
module for gateway integration
module for chip processing/ PIN pad
card reader
test domain of an ATM approval
smart card

Figure 14: Test Domain

If the test object has already an EMVCo Level 1 or Level 2 approval based on the vendor Implementation Conformance Statement (ICS), this approval is taken into account. Due to integration necessities, a sample of EMV Level 1 and Level 2 test cases is tested again. The approval process includes payment scheme specific test cases in addition to EMV test cases.

The connection to the backend system is tested including error handling.

Further test cases may be added at the discretion of the TC in order to react to interoperability issues encountered in service.

The definition of the interfaces to be tested is part of the detailed approval requirements for ATMs.

5.6 GBIC Acceptance Schemes

5.6.1 System Description

The GBIC acceptance schemes are non-payment schemes for miscellaneous applications. "Marktplatz", "Fahrschein", "TAN-Anwendung" and "Signatur-Anwendung" are GBIC acceptance schemes. Besides GBIC further licensors of the acceptance scheme may be involved (e.g. merchants).

5.6.2 Agreements/Contracts

GBIC specifies the functional requirements for the GBIC acceptance schemes in the GBIC agreement for acceptance schemes.

5.6.3 GBIC ICC Approval Objects

The approval objects Credit ICC, Debit ICC and SAM ICC including the applications of the supported acceptance schemes are described in chapter 5.3.

5.6.4 Approval Object "Zusatzanwendungsterminal"

5.6.4.1 Description of the Approval Object

The approval object "Zusatzanwendungsterminal" consists of hardware and software covering the technical interface specifications of the supported acceptance schemes to carry out operations defined in the detailed approval requirements.

The interfaces to be checked within the approval process include the interface to the GBIC ICC approval objects.

The approval of an "Zusatzanwendungsterminal" is issued as a Type Approval and will be granted for "Zusatzanwendungsterminal" for the German GBIC acceptance schemes.

5.6.4.2 Security Evaluation

5.6.4.2.1 Security Requirements

For the "Zusatzanwendungsterminal" no specific security requirements have to be met.

5.6.4.2.2 Evaluation Object

The "Zusatzanwendungsterminal" has no evaluation object.

5.6.4.3 Functional Test

5.6.4.3.1 Functional Test Requirements

The "Zusatzanwendungsterminal" must meet the detailed approval requirements for the electromechanical interface and the T=1 protocol.

If the product is approved as terminal for a GBIC payment scheme, then the approval as "Zusatzanwendungsterminal" is granted without additional functional test.

5.6.4.3.2 Test Object

The test object consists of the interfaces to the Debit ICC resp. Credit ICC and the interface to the SAM ICC.

5.7 EMV based Debit/Credit POS

5.7.1 System Description

The EMV standard specified by EMVCo in EMV Book 1 to 4 covers POS as well as ATM transactions and unifies the technical requirements for debit and credit transactions. It mainly describes the requirements for the communication between the smart card and the terminal to ensure interoperability including the security mechanisms and the interfaces to the card- holder and the Host Systems supporting an EMV payment application. In addition the pay- ment schemes American Express, Discover, JCB, MasterCard, VISA and UnionPay In- ternational (UPI) have defined own requirements by using this standard, e.g. by choosing op- tions defined in the EMV standard.

The EMV specifications are functional specifications focusing on the description of successfully standardised EMV transactions. Error handling, the fallback process to magnetic stripe, and further processing details are not described completely.

All these issues especially the interface to the Host Systems and functional definitions of an EMV POS Debit/Credit terminal and its configuration must be clarified by the acquirers in additional technical interface specifications for POS Terminals and Host Systems.

- EMV and additional requirements have therefore been integrated in the specifications of the acquirers using the GENERAL ISO-8583-CREDIT Card (GICC) Proto- col for POS Authorisation or the Key Accounts Authorisation Interface (KAAI).

Approvals will be granted for a

- "POS Terminal (EMV Debit/Credit)", and
- "Provider (EMV Debit/Credit)" as the processing party of POS Terminals and Host Systems.

The approval of a "POS Terminal (EMV Debit/Credit)” is granted as a Type Approval.

Type Approvals issued according to the rules of the GBIC Approval Scheme allow for deployment and use of the approved devices in the respective acquirer markets.

The approval of the "Provider (EMV Debit/Credit)" is issued as a provider specific approval.

The approval object "Provider (EMV Debit/Credit)" represents the entity that processes

- the Host System consist of the hardware platform, operating system and all relevant application software of the provider Host including the hardware and software of the “Host Security Module” in a secure environment and
- the Approval Object "POS Terminal (EMV Debit/Credit)"

covering the technical interface specifications especially GICC or KAAI to the acquiring hosts and the security criteria. "Security Officers" of the "Provider (EMV Debit/Credit)" are responsible for the operating environment of the Host System including the "Host Security Module".

Due to the specific behaviour of the different Host Systems an additional integration testing is necessary to start operations using a GBIC approved "POS Terminal (EMV Debit/Credit)" in combination with a GBIC approved "Provider (EMV Debit/Credit)" for POS Debit/Credit transactions in global payment schemes. This integration testing is not part of the GBIC Approval Scheme and is therefore not a prerequisite for a GBIC Type Approval. Further details are described in section 5.7.4.3.

5.7.2 Agreements/Contracts

American Express, Discover, JCB, MasterCard, VISA and UPI delegated the approval of EMV based Debit/Credit-POS-Terminals to GBIC. The delegation and its basic rules and regulations are defined in a bilateral Letter Agreement between each payment scheme and GBIC respectively. Note, most of the agreements with GBIC were closed with the former ZKA.

GBIC worked out the detailed concept of its Approval Scheme in cooperation with acquirers as listed in chap. 4.4.4. The ideas and arrangements are synchronised with American Express, Discover, JCB, MasterCard, VISA and UPI on a regular basis to assure alignment with the Letter Agreements. GBIC and acquirers agree on the system description in this handbook. Further contracts or agreements do not exist up to now.

The acquirers oblige the "Provider (EMV Debit/Credit)" via individual contracts to mandate the approval process described here.

5.7.3 Approval Object "POS Terminal (EMV Debit/Credit)"

5.7.3.1 Description of the Approval Object

The approval object "POS Terminal (EMV Debit/Credit)" represents a device defined as a hardware and software combination covering technical interface specifications and security requirements defined by the acquirers and GBIC to carry out EMV-based contact/ contactless POS Debit/Credit transactions in the global payment schemes.

The approval of "POS Terminal (EMV Debit/Credit)" is granted as a GBIC Type Approval.

If an EMVCo Type Approval Contact Level 1 or Level 2, EMVCo Type Approval Contactless Level 1 as well as certificates for the integrated contactless kernels already exist for the hardware and software combination these will be taken into account during the Type Approval process to minimise efforts. The corresponding EMVCo approval letters and the certificates of the contactless kernels have to be delivered for verification.

Vice versa the vendor may use the GBIC Type Approval as a prerequisite for an EMVCo Type Approval Contact Level 2. In this case the Testing Laboratory issues a test report according to EMVCo rules and sends it to EMVCo for further decision.

5.7.3.2 Security Evaluation

5.7.3.2.1 Security Requirements

The approval object "POS Terminal (EMV Debit/Credit)" has to meet the "Security Requirements for PIN Processing" referred to in the detailed approval requirements for "POS Terminal (EMV Debit/Credit)".

Since the approval object supports global payment schemes - called functions in the detailed approval requirements for EMV Debit/Credit - the "POS Terminal (EMV Debit/Credit)" must meet the security requirements of the global payment schemes, too.

The Payment schemes require that POS Terminals and Secure (encrypting) Card Readers must meet specific Payment Card Industry (PCI) PIN security and Point of Interaction (POI) Modular Security Requirements for PIN Transaction Security (PTS) devices and Secure Card Readers. These documents are referenced in the "Security requirements for PIN Processing".

If necessary, the security requirements of any other payment scheme are referred to in the detailed approval requirements for EMV Debit/Credit.

5.7.3.2.2 Evaluation Object "POS Terminal (EMV Debit/Credit)"

The "POS Terminal (EMV Debit/Credit)" includes components and functions securing the confidentiality of secret data and the integrity of messages, configuration data and software. Each component of the "POS Terminal (EMV Debit/Credit)" performing sensitive operations is part of the evaluation object "POS Terminal (EMV Debit/Credit)".

The evaluation object includes the hardware, the software including the mechanisms for loading cryptographic keys and software as well as the personalisation environment of the "POS Terminal (EMV Debit/Credit)" to ensure that the environment is under supervised control and ensures the necessary confidentiality and integrity.

The Security Evaluator verifies whether the "POS Terminal (EMV Debit/Credit)" meets the "Security Requirements for PIN Processing". Additionally the Security Evaluator shall testify in the security evaluation report whether the PIN or PTS security requirements of other payment schemes are met. It is expected that a "POS Terminal (EMV Debit/Credit)" meeting the "Security requirements for PIN Processing" also meets the specific PIN, and PTS security requirements of other payment schemes.

As a result of the security evaluation of a "POS Terminal (EMV Debit/Credit)" the Security Evaluator may define further conditions to the operational environment of the "POS Terminal

(EMV Debit/Credit)" as a prerequisite to go operational. The Security Evaluator must document these conditions in the security evaluation report. Such additional conditions may concern e.g. "protection against PIN disclosure (so called privacy shield)", "Software integrity" and "Secure key loading".

The Approval Letter to the Approval Owner refers to the tested technical interface specifications and the evaluated security requirements. Further on the Approval Letter refers to the additional requirements on the operational environment of the "POS Terminal (EMV Debit/Credit)", which are not met by the "POS Terminal (EMV Debit/Credit)" alone.

5.7.3.3 Functional Testing

5.7.3.3.1 Functional Test Requirements

The functional test requirements are defined in the technical interface specifications for "POS Terminal (EMV Debit/Credit)", in the "Terminal Type Approval Interface" (TAI) as well as in the "Terminalmanagement für EMV-Applikationen" (TM DC).

For the approval object the "POS Terminal (EMV Debit/Credit)" is the test object and it is tested by performing the terminal functional test.

5.7.3.3.2 Test Object "POS Terminal (EMV Debit/Credit)"

The test object "POS Terminal (EMV Debit/Credit)" must comply with the technical interface specifications for "POS Terminal (EMV Debit/Credit)" the online test interface "TAI" and the terminal management debit/credit "TM DC". The following interfaces of the test object "POS Terminal (EMV Debit/Credit)" are tested within the terminal functional test:

- interface to the cardholder (display of the cardholder unit, cardholder receipt),
- interface to the merchant (display of the merchant unit, transaction log, merchant receipt),
- electro-mechanical properties (ICC based processing),
- ICC protocol contact and/or contactless based (ICC based processing),
- EMV application layer for transaction flows (ICC contact and/or contactless based processing),
- terminal delivered data elements in the online messages according to the Online test interface "TAI".

If OPT is supported:

- interface to the personalisation centre (OPT)
- interface to the online pre-initialiser (OPT)

All interfaces listed above must be tested by the Testing Laboratory. If an EMVCo Level 1 or Level 2 approval already exists for the "POS Terminal (EMV Debit/Credit)" it will be taken into account to minimise efforts. The corresponding EMVCo approval letters have to be delivered for verification.

The technical interface specifications for EMV-based POS Terminals cover the requirements of all participating payment schemes. Thus, all these requirements are tested together. In addition GBIC brands may be tested within the respective domestic approval schemes.

The interfaces of the "POS Terminal (EMV Debit/Credit)" are tested via component simulations by the Testing Laboratory.

5.7.4 Approval Object "Provider (EMV Debit/Credit)"

5.7.4.1 Description of the Approval Object

The Approval Object "Provider (EMV Debit/Credit)" processes the approval object "POS Terminal (EMV Debit/Credit)" and the "Host System (EMV Debit/Credit)" consisting of

- the host system of the provider (a combination of hardware and software of the host) ,
- a combination of the hardware and software of the "Host Security Module"

<u>and</u>

- the operating environment of the provider.

The approval of the "Provider (EMV Debit/Credit)" is issued as a provider specific approval (per provider entity). The "Provider (EMV Debit/Credit)" has to be approved in order to start his operation. The approval of the provider cannot be transferred to other companies.

5.7.4.2 Security Evaluation

5.7.4.2.1 Security Requirements

The approval object "Provider (EMV Debit/Credit)" must meet the "Security Requirements for PIN Processing" referred to in the detailed approval requirements for EMV Debit/Credit.

Since this Approval Object supports global payment schemes - called functions in the de- tailed approval requirements for EMV Debit/Credit – the "Provider (EMV Deb- it/Credit)" must meet the security requirements of the global payment schemes, too.

If necessary, the security requirements of any other payment scheme are referred to in the detailed approval requirements for EMV Debit/Credit.

5.7.4.2.2 Evaluation Object

The evaluation object “Provider (EMV Debit/Credit)” consist of

- the operating environment of the provider host including the hardware and software of the "Host Security Module", and
- the "Security Officers".

For the evaluation object a site inspection of the operating environment of the provider host including the "Host Security Module" has to be performed. The operating environment shall meet the security relevant documentation of the "Provider (EMV Debit/Credit)", especially the "Security Requirements for PIN Processing" referred to in the detailed approval requirements for "Provider (EMV Debit/Credit)".

The "Host Security Module" is an integrated evaluation object of the "Provider (EMV Debit/Credit)".

The evaluation object "Host Security Module" consists of the hardware and software of the "Host Security Module" based on the interface specification between the "Host Security Module" and the provider host.

For the evaluation object "Host Security Module" the security evaluation report for the hardware and software according to the interface specification between the "Host Security Module" and the host is necessary.

The results of the evaluation are summarised in evaluation reports.

The following security evaluation reports are necessary:

- The security evaluation report for the hardware and software of the Host Security Module referring to the security requirements of the Host Security Module’s operating environment considering EMV Debit/Credit.
- The integrative security evaluation report for all security relevant components of the provider network ("Integrationsgutachten") including the Host Security Module, the evaluation of the operating environment of the provider host (provider site inspection and nomination of the provider security officers).

If an evaluation report covering the above mentioned security requirements already exists, e.g. from a former girocard approval, it can be reused and delivered to the acquirer for verification.

The Approval Letter to the Approval Owner refers to the tested technical interface specifications and the evaluated security requirements. Additionally the approval letter refers to the further requirements on the operational environment of the provider host or the "Host Security Module" which are not met by the module alone.

5.7.4.3 Functional Test

5.7.4.3.1 Functional Test Requirements

The functional test requirements consist of the technical interface specifications for the "Provider (EMV Debit/Credit)" especially GICC or KAAI.

In each case a test object is defined for the approval object "Provider (EMV Debit/Credit)". The test object "Host System (EMV Debit/Credit)" is tested within the provider functional test. This test object-is described in the following section.

5.7.4.3.2 Test Object "Host System (EMV Debit/Credit)"

The test object "Host System (EMV Debit/Credit)" must comply with the technical interface specification for "Host System (EMV Debit/Credit)".

The following interfaces of the test object "Host System (EMV Debit/Credit)" are tested within the host system functional test for each “Provider (EMV Debit/Credit)” to be approved:

- the "Host System" interface to the authorisation system/ acquirer processor,
- the impact of the "Host System" interface on
  - the cardholder (display of the cardholder unit, cardholder receipt),
  - the merchant (display of the merchant unit, merchant receipt),
  - the cardholder contact/contactless card.

The interface to the authorisation system/acquirer processor is tested using simulations of these systems supporting the online-interfaces used in production by each acquiring host.

The interfaces to the merchant, cardholder and the card are tested using an already suc- cessfully tested "POS Terminal (EMV Debit/Credit)". The interface between the "Host System (EMV Debit/Credit)" and the "POS Terminal (EMV Debit/Credit)" shall be based on the proto- col used in production.

5.7.4.4 Global testing Surplus

The global card schemes implemented approval schemes by themselves, which can be replaced by the GBIC Approval Scheme. Only very limited requirements of the global schemes are left e.g. the contactless kernel certificates or the End-to-End-Tests.

For the GBIC Approval Scheme the former ZKA and MasterCard made the following agreement: "For EMV-POS terminals the Terminal Integration Process (TIP) will be reduced to the first newly EMV terminal with a ZKA Type Approval for each acquiring processor. Thus, the TIP will be performed once per acquirer / processor."

Organisation and design of the starting phase are up to the acquirers. The functional requirements, test specification and test planning for the integration test are defined by the acquirers themselves as well as the organisation of the provider evaluation and the processing of the TIP.

The Approval Owner is informed via the GBIC Approval Letter about the necessity of additional integration testing (see chapter 5.7.1).

5.8 Approval Object on Self Service Machines Encrypting PIN Pad

The electronic purse scheme GeldKarte, the debit payment scheme girocard and the German ATM system as well as Self Service Machines of the Germany banking industry use the same PIN for user authentication. Therefore for Self Services Machines of the German banking industry using the PIN the approval object "Self Service Machine Encrypting PIN Pad (Self Service Machine EPP)" is defined. An example for a Self Service Machine is a machine placed within a bank where the cardholder may transfer money from one account to another.

5.8.1 Agreements/Contracts

The security requirements of the ZKA[14] PIN Agreement are the security requirements for the approval object Self Service Machine EPP. No other requirements are defined for the approval object Self Service Machine EPP.

[14] Agreements signed under the construction ZKA are agreements of the participating associations and therefore are unaffected by renaming of the GBIC.

5.8.2 Approval Object Self Service Machine EPP

5.8.2.1 Description of the Approval Object "Self Service Machine EPP"

The approval object Self Service Machine EPP represents a device of hardware and firmware covering the security requirements of the ZKA PIN Agreement to carry out cryptographic operations on the PIN within Self Service Machines of the Germany banking industry. The approval of a product implementing a Self Service Machine EPP is issued as a type approval.

5.8.2.2 Security Evaluation

5.8.2.2.1 Security Requirements

The security requirements of the German PIN Agreement are the security requirements for the approval object Self Service Machine EPP.

5.8.2.2.2 Evaluation Object

The evaluation object is identical to the approval object. The Security Evaluator verifies whether the Self Service Machine EPP meets the security requirements of the German PIN Agreement.

5.8.2.3 Functional Test

Neither test object nor functional test requirements are defined for the approval object Self Service EPP.

5.9 "Kopf- und Übergabestellen"

5.9.1 System Description

GBIC operates the German ATM system and the girocard system. Both schemes require the function of

- "Kopfstellen", which bundle transactions sent by different sources as the Acquirer bank, the girocard network provider or the "Online-Netzbetreiber" in order to be further transmitted to the issuer for authorisation or to provide for authorisation by themselves. The “Kopfstelle” operates on behalf of the issuer.
- "Übergabestellen", which provide for the correct routing of transactions to and from cooperation partners of GBIC.

Based on a contract with GBIC, providers of a "Kopfstelle", of an "Übergabestelle" or of a combined "Kopf- und Übergabestelle" operate host systems to provide the respective tasks either for one or both of the two schemes, the German ATM system and the girocard system.

5.9.2 Agreements/Contracts

GBIC’s approval of "Kopf- und Übergabestellen" is granted by issuing an approval certificate, that is based on the approval contract called "Vertrag über die Zulassung als Kopf- und/oder Übergabestelle im girocard-System der Deutschen Kreditwirtschaft". This contract is signed by GBIC and the “Kopf- / Übergabestelle”.

GBIC specifies the functional and security requirements for the "Kopf- und Übergabestellen" in the technical appendix of this approval contract called "Anlage 1 Technischer Anhang zum Vertrag über die Zulassung als Kopf- und/ oder Übergabestelle im girocard-System der Deutschen Kreditwirtschaft".

5.9.3 Approval Object "Kopfstelle of the girocard system"

5.9.3.1 Description of the Approval Object

According to the Approval contract ("Kopfstellen-Vertrag"), subtitle "Vertrag über die Zulassung als Kopf- und/ oder Übergabestelle im girocard-System der Deutschen Kreditwirtschaft" a "Kopfstelle" is entitled to exchange online messages with network providers or with a "Passiv-Übergabestelle" in the girocard system only, if it - among other things – proved, that it meets the defined security and functional requirements. According to the Approval contract this proof is the condition for approval. Only if the approval is granted, a "Kopfstelle" can start operations.

The "Kopfstelle of the girocard system" must be in compliance with the technical appendix of the "Kopfstellen-Vertrag" (short TA KÜS).

The approval of a "Kopfstelle" can not be transferred to other companies.

The "Kopfstelle" has to support the two functions in consideration of conditions:

- "Kopfstelle (Netzbetreiber)", mandatory according to the requirements in TA KÜS, chapter 2.1, which exchanges online messages with network providers approved for the girocard system (see this document, chapter 5.2.5) and exchanges E-Commerce transactions with the related authentication system (see this, chapter 5.4.5), both to forward the messages to the dedicated authorisation systems,
- "Passiv-Kopfstelle (Kooperation)" according to the requirements in TA KÜS, chapter 4.2, which exchanges online messages with an approved "Übergabestelle of the girocard system" supporting the function "Passiv-Übergabestelle (Kooperation)" to forward the messages to the dedicated authorisation systems. This function is only to be supported when girocard cards are accepted from cooperation partners.

The approval process, as it is specified here, is the process followed by the "Kopfstelle" to prove that it meets the security and functional requirements.

The approval object "Kopfstelle of the girocard system" represents a system consisting of

- the host of the "Kopfstelle",
- the hardware and software of the "Kopfstelle" Host Security Module and
- the operating environment of the "Kopfstelle".

5.9.3.2 Security Evaluation

5.9.3.2.1 Security Requirements

Each component of the "Kopfstelle of the girocard system" performing sensitive operations has to meet the security requirements of the technical appendix of the Approval contract.

5.9.3.2.2 Evaluation Object "Host System supporting Kopfstelle of the girocard system"

The approval object "Kopfstelle of the girocard system" consists of the operating environment of the host system and the hardware and software of the Host Security Module.

For the evaluation object "Host System supporting Kopfstelle of the girocard system" a security evaluation report is necessary containing:

- the security evaluation of the hardware and software of the Host Security Module referring to the security requirements of the Host Security Module’s operating environment,
- the evaluation of the operating environment of the host system (provider site inspection and nomination of the provider security manager) and referring to the security relevant documentation of the host system.

5.9.3.3 Functional Test

5.9.3.3.1 Functional Test Requirements

The "Kopfstelle" ensures the interoperability of the implementation of all requirements described in the technical appendix of the Approval contract. The appropriate interoperability testing must be confirmed in written form according the testing conformance statement (TCS)

- for the "Kopfstelle (Netzbetreiber)" with at least one network provider approved as "girocard Network" for the girocard,
- for the "Passiv-Kopfstelle (Kooperation)" by all approved "Übergabestelle of the girocard system" supporting the function "Passiv-Übergabestelle (Kooperation)".

5.9.4 Approval Object "Übergabestelle of the girocard system"

5.9.4.1 Description of the Approval Object

The approval object "Übergabestelle of the girocard system" corresponds to chapter 5.9.3.1 with the difference that the "Übergabestelle" has to support at least one of the two functions:

- "Übergangsstelle (Netzbetreiber)" according to the requirements in TA KÜS, chapter 3.1, which exchanges online messages with network providers approved for the girocard system to forward them to systems of cooperation partners,
- "Passiv-Übergabestelle (Kooperation)" according to the requirements in TA KÜS, chapter 4.1, which exchanges online messages with systems of cooperation partners to forward them to an accredited "Kopfstelle of the girocard system" supporting the function "Passiv-Kopfstelle (Kooperation)".

5.9.4.2 Security Evaluation

5.9.4.2.1 Security Requirements

Each component of the "Übergabestelle of the girocard system" performing sensitive operations has to meet the security requirements of the technical appendix of the Approval contract.

5.9.4.2.2 Evaluation Object "Host System supporting Übergabestelle of the girocard system"

The security requirements correspond to chapter 5.9.3.2.2 with the difference that according to the technical appendix of the "Kopf- und Übergabestellen" contract instead of the security requirements for "Kopfstelle" the security requirements for "Übergabestelle" have to be supported.

The evaluation object "Host System supporting Übergabestelle of the girocard system" consists of the same hardware, software and environmental components as required for a "Kopfstelle". Therefore, the same security evaluation reports are necessary as described in chapter 5.9.3.2.2.

5.9.4.3 Functional Test

5.9.4.3.1 Functional Test Requirements

The "Übergabestelle" ensures the interoperability of the implementation of all requirements described in the technical appendix of the Approval contract. The appropriate interoperability testing must be confirmed in written form according the testing conformance statement (TCS)

- for the "Übergabestelle (Netzbetreiber)" by at least one network provider approved as "girocard Network" for the girocard system,
- for the "Passiv-Übergabestelle (Kooperation)" by all accredited "Kopfstelle of the girocard system" supporting the function "Passiv-Kopfstelle (Kooperation)".

5.9.5 Approval Object "Kopfstelle of the German ATM system"

5.9.5.1 Description of the Approval Object

The approval object "Kopfstelle of the German ATM system" corresponds to chapter 5.9.3.1 with the difference that the "Kopfstelle" has to support at least one of the two functions:

- "Aktiv-Kopfstelle", which exchanges online messages from ATM providers (see TA KÜS, chapter 2.2) and online messages from an "Übergabestelle of the German ATM system" supporting the function "Aktiv-Übergabestelle" (see TA KÜS, chapter 3.2), both to forward them to an approved "Kopfstelle of the German ATM system" supporting the function "Passiv-Kopfstelle",
- "Passiv-Kopfstelle", which exchanges online messages with an approved "Kopfstelle of the German ATM system" supporting the function "Aktiv-Kopfstelle" (see TA KÜS, chapter 2.2) and with an approved "Übergabestelle" of the German ATM System supporting the function "Passiv-Übergabestelle" (see TA KÜS, chapter 4.2), both to forward them to the authorisation systems of the mandating issuing payment service provider.

The exchange of online messages coming from an "Übergabestelle of the German ATM system" is only to be supported when girocard cards are accepted from cooperation partners.

5.9.5.2 Security Evaluation

5.9.5.2.1 Security Requirements

Each component of the "Kopfstelle of the German ATM system" performing sensitive operations has to meet the security requirements of the technical appendix of the Approval contract.

5.9.5.2.2 Evaluation Object "Host System supporting Kopfstelle of the German ATM system"

The evaluation object "Host System supporting Kopfstelle of the German ATM system" consists of the same hardware, software and environmental components as required for a "Kopfstelle" in the girocard System. Therefore, the same security evaluation reports are necessary as described in chapter 5.9.3.2.2.

5.9.5.3 Functional Test

5.9.5.3.1 Functional Test Requirements

The "Kopfstelle" ensures the interoperability of the implementation of all requirements described in the technical appendix of the Approval contract. The appropriate interoperability testing must be confirmed in written form according the testing conformance statement (TCS)

- for the "Aktiv-Kopfstelle" by all "Übergabestelle of the German ATM system" supporting the function "Aktiv-Übergabestelle" and by all approved "Kopfstelle of the German ATM system" supporting the function "Passiv-Kopfstelle",
- for the "Passiv-Kopfstelle" by all approved "Kopfstelle of the German ATM system" supporting the function "Aktiv-Kopfstelle" and by all "Übergabestelle of the German ATM system" supporting the function "Passiv-Übergabestelle".

5.9.6 Approval Object "Übergabestelle of the German ATM system"

5.9.6.1 Description of the Approval Object

The approval object "Übergabestelle of the German ATM system" corresponds to chapter 5.9.3.1 with the difference that the "Übergabestelle" has to support at least one of the two functions:

- "Aktiv-Übergabestelle" according to the requirements in TA KÜS, chapter 3.2, which exchanges online messages with an approved "Kopfstelle of the German ATM system" supporting the function "Aktiv-Kopfstelle" to forward them to systems of cooperation partners,
- "Passiv-Übergabestelle" according to the requirements in TA KÜS, chapter 4.1, which exchanges online messages with systems of of cooperation partners to forward them to an approved "Kopfstelle of the German ATM system" supporting the function "Passiv-Kopfstelle".

5.9.6.2 Security Evaluation

5.9.6.2.1 Security Requirements

Each component of the "Übergabestelle of the German ATM system" performing sensitive operations has to meet the security requirements of the technical appendix of the Approval contract.

5.9.6.2.2 Evaluation Object "Host System supporting Übergabestelle of the German ATM system"

The evaluation object "Host System supporting Übergabestelle of the German ATM system" consists of the same hardware, software and environmental components as required for a "Kopfstelle" in the girocard System. Therefore, the same security evaluation reports are necessary as described in chapter 5.9.3.2.2.

5.9.6.3 Functional Test

5.9.6.3.1 Functional Test Requirements

The "Übergabestelle" ensures the interoperability of the implementation of all requirements described in the technical appendix of the Approval contract. The appropriate interoperability testing must be confirmed in written form according the testing conformance statement (TCS)

- for the "Aktiv-Übergabestelle" by all approved "Kopfstelle of the German ATM system" supporting the function "Aktiv-Kopfstelle",

- for the "Passiv-Übergabestelle" by all approved "Kopfstelle of the German ATM system" supporting the function "Passiv-Kopfstelle".

6 Glossary

Acquirer (AQ) – AMERICAN EXPRESS PAYMENT SERVICES LIMITED, PAYONE GMBH, VR PAYMENT GMBH, NEXI GERMANY GMBH, GLOBAL PAYMENTS INC., ELAVON FINANCIAL SERVICES DAC, FIRST DATA GMBH, VERIFONE PAYMENTS GMBH and TRANSACT ELEKTRONISCHE ZAHLUNGSSYSTEME GMBH.

GBIC and Acquirer act as AC (see chapter 4.1.2.1) and TC (see chapter 4.1.2.3) within the Approval and Maintenance Process with its extensions for EMV based Debit/Credit POS.

Acquirer Contact Person (AQ*) – Acquirer nominated contact person vis-à-vis to GBIC.

Administration Process (Administrationsprozess) – The administration process consists of all administrative processes supporting the preparation and execution of the approval process. During the administration process open and granted approvals are administered and the adherence to migration dates is monitored. See also chapter 4.4.3.

Approval Applicant (Antragsteller) – The Approval Applicant initiates the registration of its product or system and gets a registration number, if the product or system is eligible for approval. During the registration and approval process, the Approval Applicant is contacted by the Approval Office. The Approval Applicant can be a network provider, an ATM vendor, a terminal vendor or an ICC vendor (see chapter 4.1.3.1).

Approval Change (Änderungszulassung) – If the requirements for the approval of an approval object have not changed compared to the already granted approval, if the interfaces, functions and applications have not changed (same basic and detailed approval requirements for an approval object) but the implementation of the approval object is partly changed then the result of an approval change is an approval of the new implementation with another approval number.

Approval Council (AC) - see chapter 4.1.2.1.

Approval Council responsible for girocard (ACEC) – The approval authority for the payment scheme girocard. In the "Detailed Approval Requirements" the responsible GBIC institution is mapped to this role.

Approval Extension (Erweiterungszulassung) – If the requirements for the approval of an approval object have not changed compared to the already granted approval, but the interfaces, functions or applications have changed (new basic and/or detailed approval requirements for an approval object) then the result of an approval extension is an approval of the new implementation with another approval number.

Approval First (Erstzulassung) – see First Approval in this glossary.

Approval Eligibility (Zulassungsfähigkeit) – To enter the approval process a product or a system must be able to meet the requirements of an approval object defined in the GBIC Approval Scheme. If the product or the system does not correspond to an approval object, the approval eligibility is denied and the product or the system does not enter into the approval process. The approval eligibility is checked during the registration process by the Approval Office.

Approval Eligibility Letter (Schreiben zur Zulassungsfähigkeit) – see chapter 4.5.3.

Approval Letter (Zulassungszertifikat*)* – see chapter 4.5.11.

Approval Lists – see chapter 4.5.12.

Approval Number (Zulassungsnummer) – After a successful approval each implementation of an approval object receives an approval number. There are payment schemes, where the approval number is important for the handling of payment transactions (especially in the GeldKarte scheme). The approval number is assigned after the decision on the approval.

Approval Object (Zulassungsgegenstand) – see chapter 4.6.1.

Approval Office (AO, Zulassungsbüro) – The Approval Office is an administrative role in the GBIC Approval Scheme (see chapter 4.1.2.4).

Approval Owner (Zulassungsinhaber) – The approval owner gets the approval for its product or system, submitted for approval. Network providers and vendors can be approval owners.

Approval Period (Zulassungszeitraum) – The time period within an approval concerning to a certain version of the detailed approval requirements (see there) can be granted. For an approval period three dates are defined:

1. the **Valid From** is the first date on which a registration of a new product or system is allowed and an approval can be granted,
2. the **New Registration Until** is the last date on which the registration of a new product or system is allowed,
3. the **Valid Until** is the last date on which an approval can be granted.

Approval Process (Zulassungsprozess) – The approval procedures of the GBIC Approval Scheme defined in chapter 4.4.2. During the approval process the compliance of the implementation of an approval object with the approval requirements consisting of basic approval requirements and detailed approval requirements is verified. Approval requirements are particularly technical interface specifications and security requirements.

Approval Requirements (Zulassungsvoraussetzungen) – To get an approval, the implementation of an approval object must meet the approval requirements which are split into basic approval requirements (see there) and detailed approval requirements (see there).

Approval Types (Zulassungstyp zu einem Zulassungsgegenstand) – see chapter 4.6.1.

Basic Approval Requirements (Allgemeine Zulassungsvoraussetzungen) – The general part of the approval requirements including the approval object and its characteristics defined in this document (like the supported payment scheme and the definition of the evaluation object and the test object). The basic approval requirements are the firm part of the approval requirements, which is rarely subject to modification during the maintenance process.

Card Publishers (Verlage) – The Card Publishers are consitituted by the four German banking sector’s publishing companies Bank-Verlag, Deutscher Genossenschafts-Verlag, Deutscher Sparkassen Verlag and VÖB-ZVD Processing. The publishers are responsible for the definition of the data structures for the different ICC products.

CFCF – Common Functional Certification Framework Consortium (www.CFCF.eu) for the governance of the nexo CFCF documents, the certification process for nexo implementations and the delivery of terminal and acquirer host certifcates based on nexo Implementation Specifications (nexo IS).

CFCF certificate – A certificate issued by the CFCF stating the conformance of a nexo POI (Point Of Interaction) or an nexo Acquirer Host with the referenced version of nexo IS.

Common Criteria for Information Technology Security Evaluation (short **Common Criteria** or **CC**) – International Standard about criteria for the evaluation and certification of the security of IT products.

Common.SECC – Common Security Evaluation and Certification Consortium founded by GBIC and UK Finance. Within this Consortium, the security evaluation and certification of terminal platforms (hard- and firmware) is performed regarding common harmonised processes and rules, e.g. ISO 15 408 Common Criteria.

Credit ICC – Approval object including a GBIC operating system, a credit application and optionally other applications.

CVM – Cardholder Verification Method

Debit ICC – Approval object including a GBIC operating system, a debit application and optionally other applications.

Denial Letter (Ablehnungsbescheid) – The Approval Office sends a denial letter to the Approval Applicant at the end of the approval process, if the approval process could not be completed successfully due to the product or system submitted for approval not meeting the approval requirements of the corresponding approval object.

Detailed Approval Requirements – (Spezifische Zulassungsvoraussetzungen) – The specific part of the approval requirements like technical interface specifications, approval periods, security requirements, functions, agreements or interfaces to be tested. The detailed approval requirements are more often subject to modification during the maintenance process.

Encrypting PIN Pad (EPP) – A device for secure PIN entry and encryption without a display or card reader. An EPP is typically used in an ATM for PIN entry and controlled by an ATM device controller. An EPP has a tamper responsive shell.

Evaluation Object (Begutachtungsgegenstand) – The security relevant part of an approval object, subject to security evaluation by a security evaluator, is referred to as evaluation object. The Security Evaluator verifies the compliance of the security relevant components of a product or system submitted for approval with the security requirements of an evaluation object of the corresponding approval object (see chapter 4.6.2).

Evaluation Technical Report (ETR) for Risk Management – A report be produced by the evaluator, is provided in support of the final certificate, to enable certificate users to understand the details of the residual vulnerabilities.

Fee for Administration (Bearbeitungsentgelt) – By sending the registration form to the Approval Office and before getting the approval eligibility letter, the Approval Applicant has to pay a fee for processing.

First Approval (Erstzulassung) – Result of a first approval of a product or system is a new approval number.

Functional Test Report (Funktionstestbericht) – see chapter 4.5.4.

GBIC Approval Scheme (DK-Zulassungsverfahren) – The GBIC Approval Scheme consists of the approval process, the maintenance process and the administration process. The GBIC Approval Scheme is implemented with the following basic roles: Security Evaluator, Testing Laboratory, Security Committee, Technical Committee, Approval Office and Approval Council.

GBIC ICC Approval Objects – The overall name for the approval objects Debit ICC, Credit ICC and SAM ICC.

Host Security Module (Sicherheitsbox) – The Host Security Module is a security device signing message data with a Message Authentication Code (MAC) as well as decrypting and encrypting sensitive data like PINs in backend systems of authorisation systems or intermediate hosts. The Host Security Module is a security component in the payment schemes girocard and EMV based Debit/Credit POS.

ICC module – An Integrated Circuit Card (ICC) including the IC processor and executable code stored in ROM. Additional executable code may be stored in EEPROM. Data structures are not covered by an ICC module. Therefore ICC modules are not functional because the applications are not complete. An ICC module can be approved according to the approval object SECCOS ICC.

ICC product – An Integrated Circuit Card (ICC) including the IC processor, any executable code (stored in ROM and EEPROM) and data structures (stored in EEPROM). ICC products are fully functional. An ICC product is approved according to the three approval objects Debit ICC, Credit ICC and SAM ICC.

Intermediate Reply (Zwischenbescheid) – The Approval Office informs the Approval Applicant in form of an intermediate reply about the status of the approval process for a product or system submitted for approval. (see chapter 4.5.9.)

JTEMS PP – Protection Profile (PP) developed by the Common Approval Scheme Initiative (CAS) in co-operation with the Joint Interpretation Library Terminal Evaluation Subgroup (JTEMS) to be used for the Common Criteria (CC) evaluation of Point of Interaction.

Maintenance Process – The maintenance procedures of the GBIC Approval Scheme are defined in chapter 4.4.1.

nexo ICS – The nexo Implementation Conformance Statement declares the support of optional functionality of a nexo POI (Point Of Interaction) allowed by the referenced version of the nexo IS which has to be stated by the approval applicant together with the CFCF certificate during the registration process. The nexo ICS will be owned by CFCF (www.CFCF.eu).

nexo IS – The nexo Implementations Specifications is the set of specifications defining the functional requirements for a nexo POI (Point Of Interaction) or a nexo Acquirer Host. The nexo IS will be owned by nexo standards (www.nexo-standards.org).

Online-Personalisierung für Terminal-HSMs (OPT) – A scheme for the online personalisation of terminals in Germany with sensitive data like cryptographic keys. OPT consists of the terminal functions "Online-Vor-Initialisierung und Online-Anzeige einer Außerbetriebnahme von Terminal-HSM" and "Online-Initialisierung und Online-Personalisierung von Terminal-HSMs" and the host functions "Online-Registrierung und Online-Abmeldung von Terminal-HSMs".

Payment Scheme (Zahlungssystem) – A product or system is approved for payment schemes (e.g. Maestro, girocard, GeldKarte, ...). Approval objects are components of payment schemes. GeldKarte, POZ, Maestro, girocard, ... are payment schemes. The approval process is payment scheme-specific.

PIN Entry Device (PED, PIN-Eingabegerät) – A device for secure PIN entry and processing. The PED typically consists of a keypad for PIN entry, laid out in a prescribed format, a display for user interaction, a processor and storage for PIN processing sufficiently secure for the key management scheme used, and firmware. A PED has a clearly defined physical and logical boundary, and according to the correspondent security requirements a tamper resistant, tamper evident or tamper responsive shell.

Registration form (Registrierungsformular) – see chapter 4.5.2.

SAM ICC – Approval object including a GBIC operating system, a secure application module application and optionally other applications.

SECCOS ICC – Approval object including a GBIC operating system and application commands but not covering any application data structures.

Security Committee (SC) – see chapter 4.1.2.1.

Security Components – An evaluation object may consist of one or more security components. The Security Evaluator may create single security evaluation reports for each security component. In the end there must be an integrative security evaluation report covering the entire evaluation object where the results of the evaluations of the security components are summarised (see chapter 4.6.2).

Security Evaluator (SEV, Sicherheitsgutachter) – see chapter 4.1.2.5.

Security Evaluator Declaration (Gutachtererklärung) **–** see chapter 4.5.5.

Security Evaluation Report (Sicherheitsgutachten) – see chapter 4.5.5.

SOGIS CC Certification Body – Accredits security evaluators within the Common Criteria certification scheme for a certain technical domain as „Hardware Devices with Security Boxes". A accredited evaluator is allowed to deliver a CC conformant security evaluation report to Common.SECC for certification.

Statement of Compliance (Herstellererklärung) – A formal statement where the approval applicant declares the compliance with a certain set of requirements defined by the approval object.

Technical Committee (TC) – see chapter 4.1.2.3.

Technical Expert (TE, Technischer Sachverständiger) – see chapter 4.1.3.3

Technical Expert Confirmation (TEC, Sachverständigenerklärung) – see chapter 4.5.7

Technical Interface Specification (Schnittstellen-Spezifikationen) – Technical specification of the communication interfaces between system components. The communication interfaces between system components are specified in GBIC specifications and/or in specifications of the payment schemes. The interface between the ICC and the terminal is an example for a technical interface specification.

Technischer Arbeitskreis GICC (TG, TAK GICC) – Working Committee of Acquirer involved in the Maintenance and Approval Process for EMV based Debit/Credit POS.

Testing Conformance Statement (TCS) – see chapter 4.5.8

Testing Laboratory (TL, Funktionstestlabor) – see chapter 4.1.2.6.

Test Object (Testgegenstand) – see chapter 4.6.3.

Type Approval (Typzulassung) – An approval which is granted independent from the operating environment. For each implementation of the approval object the same interfaces are tested.

Annex Detailed Approval Requirements

See www.die-dk.de or contact "Zulassungsbüro Die Deutsche Kreditwirtschaft":

Bundesverband Öffentlicher
Banken Deutschlands e.V.
Lennéstraße 11, D-10785 Berlin
phone +49 (0) 30/81 92-1 86
email zulassungsbuero@voeb.de

Annex Questionaire

See www.die-dk.de or contact "Zulassungsbüro Die Deutsche Kreditwirtschaft":

Bundesverband Öffentlicher
Banken Deutschlands e.V.
Lennéstraße 11, D-10785 Berlin
phone +49 (0) 30/81 92-1 86