Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche
Kreditwirtschaft

Consultation Paper

Online Banking Payment Website

In the field of e-commerce, various payment processes have been established. During the last year, the so-called "online transfer” has been added. This allows clients to pay the purchase price by means of an online banking transfer involving a so-called online payment service provider. In order to ensure online banking security for the bank’s and the client’s sake, the present approach sets out a technical payment process solution where the client does not have to disclose to the online service provider their online banking identification data - such as user ID and PIN – necessary for initialising the "online transfer"; instead, clients only have to disclose such data directly to their bank.

Hereinafter, this model will be labelled "Online Banking Payment Website” (OBPW). For several years, the principle of the OBPW portal has been practised successfully by online payment service providers in Europe.

1 Model blueprint

This approach is based on an enhancement of the [existing] online banking user interface enabling direct online banking communication between the bank and the client; as a result, authorised online payment service providers will be given special access to the online banking payment interface (OBPW portal) of participating banks so that these online payment service providers can render their services.

Basically, the OBPW portal is an online banking website that has been [optimised or, morover,] streamlined for online payment purposes. Any bank participating in online payment services undertakes to offer such a login site or, moreover online banking interface on the internet.

As a result, registered online payment service providers may access the OBPW Service of participating banks through a standardised interface which will allow them to submit online payments (cf. fig. Figure 1).

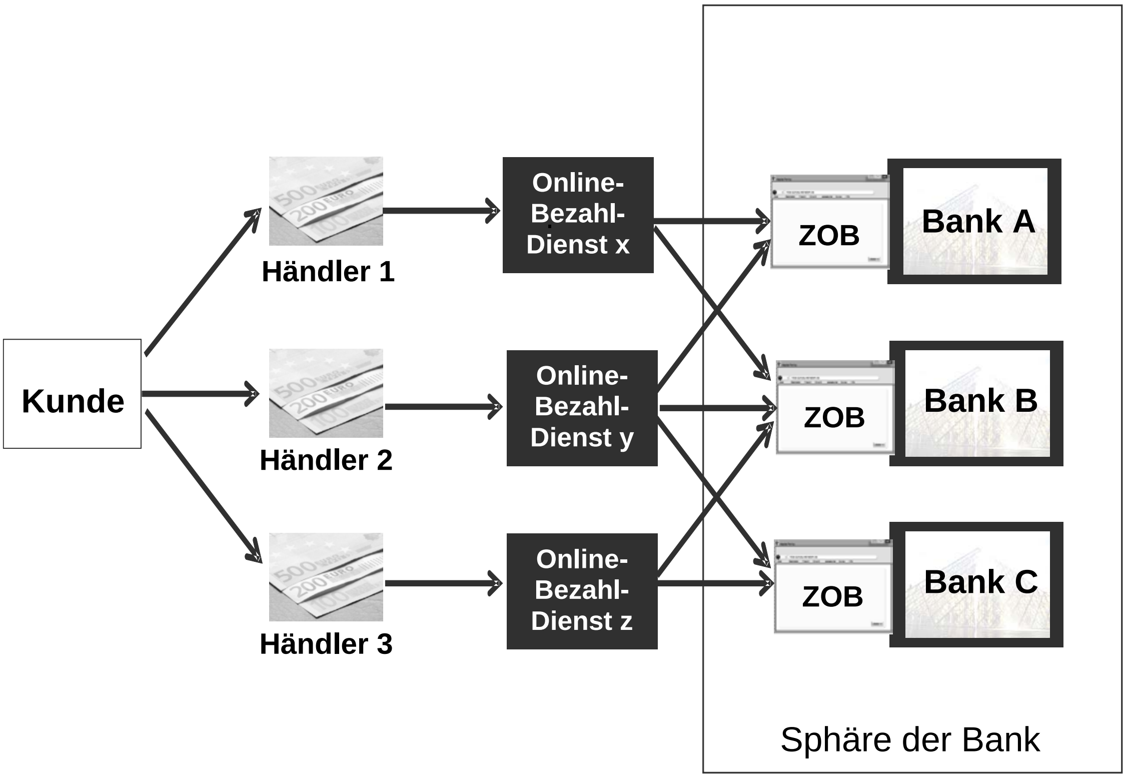

Figure 1: Layer model "Online Banking Payment Website“

Benefits of this approach:

- The online banking login data – such as client ID and PIN – will only be exchanged between the client and the bank in the secure environment [domain]. Third parties will not gain any access to this confidential client data.

- Online payment service providers will not receive any information on clients’ account status or their transaction data; instead, they will merely be informed whether the payment order was accepted. Usually, this information will be sufficient for finalising the purchase transaction. Depending on the respective agreement between the online payment service provider and the bank, the bank may include further information in this confirmation (for instance a payment guarantee).

- Provided they will receive an execution confirmation upon the submission of a payment order, there will be no need for online payment service providers to engineer sophisticated systems for assessing the execution likelihood (scoring / credit rating approaches).

- Online payment service providers no longer have to analyse any client data. As a result, they can dispense with the data protection measures which they would otherwise have to adopt in such a scenario. Especially for smaller providers, such an approach lowers the barriers to market entry.

- The user interfaces to the OBPW services are subject to a standard interface specification (cf. chapter 3 **Fehler! Verweisquelle konnte nicht gefunden werden.**)promulgated by the German Banking Industry Committee (GBIC). This greatly facilitates market access for online payment service providers. They only have to implement one single interface thus receiving access to the OBPW portals of all participating banks in a standardised manner.

- Clients’ alertness regarding phishing and Trojan attacks will remain undiminished; this is due to the fact that clients can still be instructed to only enter their login data on familiar (URL, certificate) websites belonging to their banks.

- Due to the fact that the online payment service provider is not directly involved in the client's payment authorisation process, it is only the client and their bank who will have to agree a secure protocol for handling identification data. This also resolves a number of liability issues.
- The principle of the OBPW portal is separate from the security protocols offered by banks thus allowing the use of both TAN based and also signature based approaches.
- The certification protocol used by the payment service provider in order to prove compliance with the requirements for processing security relevant data is being simplified (cf. chapter 4 **Fehler! Verweisquelle konnte nicht gefunden werden.**).
- The use of standardised interfaces renders the automated processing of websites (screenscraping) redundant. This helps to prevent customer complaints as well as transmission errors which occasionally occurred in the past.

2 Technical model

The flowchart below illustrates an OBPW transfer:

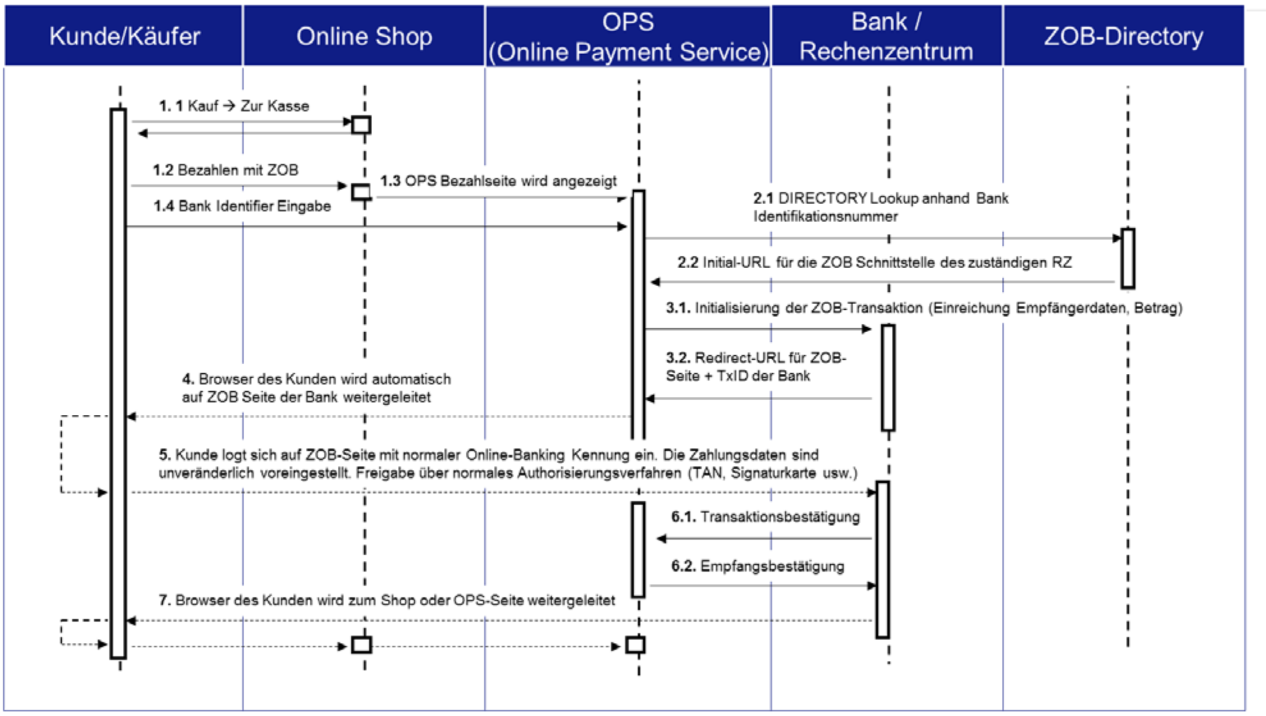
Kunde/Käufer
Online Shop
OPS (Online Payment Service)
Bank / Rechenzentrum
ZOB-Directory
1. 1 Kauf → Zur Kasse
1.2 Bezahlen mit ZOB
1.3 OPS Bezahlseite wird angezeigt
1.4 Bank Identifier Eingabe
2.1 DIRECTORY Lookup anhand Bank Identifikationsnummer
2.2 Initial-URL für die ZOB Schnittstelle des zuständigen RZ
3.1. Initialisierung der ZOB-Transaktion (Einreichung Empfängerdaten, Betrag)
3.2. Redirect-URL für ZOB-Seite + TxID der Bank
4. Browser des Kunden wird automatisch auf ZOB Seite der Bank weitergeleitet
5. Kunde logt sich auf ZOB-Seite mit normaler Online-Banking Kennung ein. Die Zahlungsdaten sind unveränderlich voreingestellt. Freigabe über normales Authorisierungsverfahren (TAN, Signaturkarte usw.)
6.1. Transaktionsbestätigung
6.2. Empfangsbestätigung
7. Browser des Kunden wird zum Shop oder OPS-Seite weitergeleitet

Figure 2: OBPW transaction flowchart

1. The client purchases something on an e-commerce website. The online merchant forwards the online purchase invoice data to the online payment service provider. Clients enter their name or, moreover, their bank's ID on the website of the payment service provider (step 1).

2. Based on the OBPW directory, the online payment service provider works out which bank is in charge (step 2).

3. The online payment service providers prove their identity to the client's bank using the provider ID issued as part of the GBIC certification process along with any further identification data that may have been agreed; through the client's bank, the online payment service provider accesses the respective OBPW service, transfers the payment order data and obtains the URL of the OBPW portal (step 3).

4. The client will be forwarded by the payment service provider to the OBPW interface of their bank. Based on the familiar features (website layout, address (URL), security certificate) the client will be able to recognise that they are on their bank’s OBPW portal, i.e. in the credit institution's [internet] domain (step 4).

5. On the OBPW portal, clients enter their login data and identification data for online banking purposes. Once they have logged on, in order to ascertain that everything is correct, the client will be shown the payment transaction data. During the next step, the client authorises the transaction by entering the authentication data generated by means of the respective security protocol or, respectively, approves it by using their signature card (step 5).

6. Through the OBPW service, the bank sends a payment order acceptance confirmation to the online payment service provider. This message includes the status of the payment order. Provided further message elements have been agreed with the online payment service provider, the message of the bank will contain a confirmation of the payment order execution or a payment guarantee by the bank. The online banking transaction is thus completed (step 6).

7. After leaving the OBPW portal, the client will be redirected to the site of the online payment service provider or of the merchant. If applicable, the online payment service provider will forward the bank’s payment message to the online merchant (step 7).

3 Interface specification

As has been mentioned above, the user interfaces to the individual bank's OBPW portals are being standardised by the German Banking Industry Committee (GBIC). Hence, an online payment service provider will only have to implement this interface once.

The following XML schema file contains a proposal for the interface specifications of the individual communication steps between the online payment service provider and banks' OBPW service presented under Figure 2. The structure of the data listed hereunder will still be fine-tuned with a view to technical and database engineering details.

http://www.fints.org/spec/xmlschema/4.0/transactions/ZOB-2.xsd

The draft XML schema below will provide an online payment service provider with a complete list of all banks and savings banks that offer an OBPW service.

The list contains the requisite access information, e.g. particularly the URL of the OBPW service.

http://www.fints.org/spec/xmlschema/4.0/transactions/ZOBBankList-3.xsd

4 Certification requirements

Due to the fact that, under the OBPW model, the online payment service provider neither receives nor processes any security relevant data (e.g. banking login data or identification data), the online payment service provider will only have to meet moderate security requirements.

However, in order to participate in the OBPW process, online payment service providers will still have to undergo a registration process. This is necessary because it has to be ensured that the online payment service integrates banks' OBPW portals correctly and that their own identity authentication is tamper proof. Upon proof of their registration, the online payment service provider will receive a provider ID and a personal ID allowing the online service providers to prove their identity towards the OBPW service. Based on this registration, subsequently a participation agreement may be concluded between the online payment service provider and the bank or aggregators on the basis of which additional services, e.g. payment guarantees, may be agreed.