Prof. Dr. Ernst-Günter Giessmann
Institut für Informatik
Humboldt-Universität zu Berlin[1]

Berlin, 2022-11-04

Gutachten zur Äquivalenz der Nachrichten der Online-Personalisierung von Terminals gemäß der Spezifikation der Deutschen Kreditwirtschaft zu den *Key Blocks* entsprechend den Anforderungen der PCI PIN Security

Zusammenfassung:

Im Rahmen der Online-Personalisierung von Terminals der Deutschen Kreditwirtschaft [AES-OPT] werden Triple-DES-Schlüssel an die Sicherheitsmodule (HSM) der Terminals übertragen. Diese Schlüssel werden benötigt, um im Betrieb der Terminals die Kommunikation vor einer Kompromittierung und Verfälschung zu schützen.
Da wurde geprüft, ob durch das Format und die Verwendung der Nachrichten die Anforderung 18-3 der Payment Card Industry (PCI) [PCI PIN-Security]:

„Encrypted symmetric keys must be managed in structures called key blocks. The key usage must be cryptographically bound to the key using accepted methods, such that it must be infeasible for the key to be used if the usage attributes have been altered."

eingehalten wird. Im Ergebnis der vorliegenden Analyse wird bestätigt, dass im Rahmen der Online-Personalisierung Schlüsseldaten in einer Datenstruktur übertragen werden, die die Anforderungen der ANSI X9.143 an einen *key block* erfüllen [TR-31].

Sicherheitsziel der PCI PIN Security

Das zu erfüllende Sicherheitsziel lautet (Control Objective 5 [PCI PIN-Security, S. 58]):

> „Keys are used in a manner that prevents or detects their unauthorized usage."

Die detaillierten Anforderungen der PCI dazu lauten:

> "Encrypted symmetric keys must be managed in structures called key blocks. The key usage must be cryptographically bound to the key using accepted methods.
> Acceptable methods of implementing the integrity requirements include, but are not limited to: A MAC computed over the concatenation of the clear-text attributes and the enciphered portion of the key block, which includes the key itself, e.g., TR-31." [PCI PIN-Security, S. 53].

Weitere akzeptierte Methoden finden sich in beispielsweise in den Standards ASC X9 TR34 und ANSI X9.102.

Diese Anforderung wurde 2022 durch ein Information Supplement ([Supp. 18-3, Q16]) aktualisiert, allerdings nur in Bezug auf die Referenz, die nun nicht mehr TR-31, sondern ANSI X9.143 lautet.

Anhand der vorgelegten Unterlagen [OPT] wurden die zu schützenden geheimen Schlüssel identifiziert und ihre Übertragung und Verwendung untersucht. Dabei sind die Kriterien des ANSI Standards X9.143 [TR-31] zugrunde gelegt worden.

Key Blocks nach X 9.143

Die Datenstruktur der *key blocks* nach TR-31 [TR-31] besteht aus drei Teilen:

[1] E-Mail-Adresse: giessmann@informatik.hu-berlin.de
Postanschrift: Prof. Dr. Ernst-Günter Giessmann, Am Tonberg 28, 16727 Velten

- der *key block header* (KBH)*,* der Attributinformationen über die gesamte Struktur und den Verwendungszweck des auszutauschenden oder zu speichernden Schlüssel enthält,
- die vertraulichen Daten, die ausgetauscht oder gespeichert werden, sowie
- der kryptographische Prüfwert (*Authentication Value*), der den *key block header* und die Schlüsseldaten aneinander bindet.

Sowohl der *key block header* als auch die verschlüsselten Daten haben bis ins Detail standardisierte Formate und verwenden festgelegte Bezeichner. Da der Übergang zu neuen Formaten im Feld eine gewisse Übergangszeit erfordert, sind gegenwärtig auch äquivalente Formate zugelassen. So heißt es in den FAQ der PCI [PIN-FAQ, S. 13] oder aktuell in [Supp. 18-3, S.8]:

> **Q November 2015**: *Is the implementation of TR-31 the only method for meeting the requirement that encrypted symmetric keys must be managed in structures called key blocks?*
>
> **A**: *No. ANSI X9.143 or any equivalent method can be used. Any equivalent method must include the cryptographic binding of the key-usage information to the key value using accepted methods. Any binding or unbinding of key-usage information from the key must take place within the secure cryptographic boundary of the device.*

Personalisierung gemäß [OPT]

Initialisierung und Personalisierung unterscheiden sich aus kryptographischer Sicht nicht, wie betrachten deshalb nur die Personalisierungsschlüssel $\mathbf{K}_{PERS\_T}$. Auf Seiten des eindeutig durch die ZKA-Nummer identifizierbaren Terminals ist dieser Personalisierungsschlüssel $\mathbf{K}_{PERS\_T}$ der Vertrauensanker. Er ist terminalspezifisch, der Initialisierungsschlüssel $\mathbf{K}_{INIT\_T}$ wird zusätzlich durch eine Registrierungsphase abgesichert. Im Fall eines Kompromittierungsverdachts kann der Registrierungsprozess beliebig oft wiederholt werden.

Bei der Erst- und Wiederpersonalisierung werden der Personalisierungsschlüssel $\mathbf{K}_{PERS\_T}$ oder der neue Personalisierungsschlüssel $\mathbf{K'}_{PERS\_T}$ im Terminal gespeichert, die gemäß der Schnittstellenspezifikation der ZKA-Chipkarte aus einem *Key Generation Key* (KGK) erzeugt werden:

$\mathbf{K}_{PERS\_T} = d^*KGK_{PERS}(H(I,ZKA\text{-}Nummer))$.

Dabei sind H eine auf dem Triple-DES basierende standardisierte Hash-Funktion [ISO10118-2] und I ein fixierter Initialwert. Die ZKA-Nummer (16 Byte) ist terminalspezifisch und eindeutig. Mit d* wird die Triple-DES-Entschlüsselung im ECB-Mode bezeichnet.

An dieser Stelle ist es wichtig darauf hinzuweisen, dass es sich hier um die Schlüsselableitung aus einem Hash-Wert und nicht um eine kryptographische Entschlüsselung handelt. Deshalb ist an dieser Stelle die Verwendung des ECB-Mode unkritisch. Durch die Hash-Funktion sind die Eingabedaten sowohl vom jeweiligen Initialwert als auch von der entsprechenden ZKA-Nummer abhängig. Eine zusätzliche Verkettung wie im CBC-Mode ist an dieser Stelle unnötig.

Die jeweiligen Key Generation Keys (KGK) werden an die HSM-Hersteller und Terminalbetreiber im Vier-Augen-Prinzip auf separatem Weg verteilt.

Mit der Erzeugung werden jedem $\mathbf{K}_{PERS\_T}$ (oder $\mathbf{K}_{INIT\_T}$) folgende Daten zugeordnet

- Name $\mathbf{K}_{PERS\_T}$ ($\mathbf{K}_{INIT\_T}$)
- (gegebenenfalls) ID der Personalisierungsstelle PS
- ZKA-Nummer des HSM
- 1 Byte lange, BCD-kodierte Schlüsselgenerationsnummer des $\mathbf{K}_{PERS\_T}$ ($\mathbf{K}_{INIT\_T}$)

- 1 Byte lange, BCD-kodierte Schlüssel-Version des $\mathbf{K}_{PERS\_T}$ ($\mathbf{K}_{INIT\_T}$)
- Aktivierungs- und Verfallsdatum des $\mathbf{K}_{PERS\_T}$ ($\mathbf{K}_{INIT\_T}$) und
- Schlüssellänge und Algorithmus-ID.

Für die Online-Personalisierung werden jedem zu ladenden Personalisierungsdatensatz ein logischer Name, der Logical Data Identifier (LDI) zugeordnet (vier Byte). Damit werden Gruppen-ID, Versionsnummer und eine Datensatz-Nummer innerhalb der Gruppe kodiert.

Nachrichten

Personalisierungsdaten werden in sogenannten Nachrichten übertragen [OPT, Kap. 5]. Diese Nachrichten könnten, soweit sie eine bestimmte Länge überschreiten, auch aufgeteilt werden. Für die Sicherheit ist die Aufteilung allerdings nicht von Bedeutung, da immer nur ein einzelner Datensatz aufgeteilt werden kann. Eine datensatzübergreifende MAC-Berechnung ist daher nicht erforderlich.

Für die kryptographische Sicherung der zu übermittelnden Nachrichten werden verschiedene Schlüssel mit Hilfe des Personalisierungsschlüssel $\mathbf{K}_{PERS\_T}$ abgeleitet.

Die MAC-, Verschlüsselungs- und Import-Schlüssel für die Nachrichtenverschlüsselung und den Integritätsschutz nach folgendem generellen Schema abgeleitet:

$$KS = d^*[\mathbf{K}_{PERS\_T} \text{ XOR } (CV1|CV1)](RND1) \mid d^*[\mathbf{K}_{PERS\_T} \text{ XOR } (CV2|CV2)](RND2).$$

Mit d* wird wie oben die Triple-DES-Entschlüsselung im ECB-Mode bezeichnet.

Die Schlüsselableitung im ANSI X 9.143 erfolgt durch CMAC-Berechnung der Schlüsselbestandteile auf verschiedenen standardisierten Initialnachrichten und nachfolgende Konkatenation der faktisch im ECB-Modus berechneten Einzelblöcke.

In der vorliegenden Spezifikation der Online-Personalisierung wird die Unterschiedlichkeit der beiden Schlüsselkomponenten durch unterschiedliche Kontrollvektoren (CV1 und CV2) garantiert. Mit so modifizierten Master-Schlüsseln (hier K_{PERS_T}) werden zwei Zufallszahlen (RND1 und RND2) verschlüsselt (im Entschlüsselungsmodus), die ausschließlich durch den entsprechenden Sender generiert werden. Die abgeleiteten Schlüssel werden nicht übertragen, so dass eine known-plaintext-Attack nicht möglich ist.

Wie oben ist hier die Verwendung des Triple-DES im ECB-Mode unkritisch, da es sich um eine Schlüsselableitung und nicht eine Entschlüsselung handelt. Durch jeweilig unterschiedliche Kontrollvektoren für die beiden Schlüsselhälften wird darüber hinaus gewährleistet, dass die beiden Schlüsselhälften trotz ECB-Mode nur in dieser Reihenfolge verwendet und nicht vertauscht werden können.

Die gute Avalanche-Eigenschaft des DES garantiert, dass selbst bei Auswahl identischer Zufallszahlen beide Hälften des abgeleiteten Schlüssel KS verschieden sind und somit die volle Stärke des Triple-DES eingesetzt wird.

Die hier zur Schlüsselableitung eingesetzten Algorithmen sind somit aus kryptographischer Sicht vergleichbar mit dem zur Schlüsselableitung eingesetzten CMAC im ANSI X9.143.

Im Einzelnen werden folgende Sitzungsschlüssel KS erzeugt:

- Nachrichten-MAC-Sessionkey KS_{MES} – zur MAC-Bildung über die für die ZKA-Personalisierung verwendeten Online-Nachrichten,
- MAC-Sessionkey KS_{MAC} – zur MAC-Bildung über die Gruppen von ZKA-Personalisierungsdatensätzen,

- Verschlüsselungs-Sessionkey KS_{ENC} – zur Verschlüsselung von ZKA-Personalisierungsdaten, die keine kryptographischen Schlüssel sind,
- Importer-Sessionkey KS_{IMP} – zur verschlüsselten Übertragung von Betriebsschlüsseln in den ZKA-Personalisierungsnachrichten.

Die Ableitungsmechanismen verwenden verschiedene Kontrollvektoren, so dass die abgeleiteten MAC-Schlüssel und Verschlüsselungsschlüssel untereinander nicht ausgetauscht werden können. Dadurch, dass darüber hinaus unterschiedliche MAC-Schlüssel für Online-Nachrichten und Personalisierungsdaten und unterschiedliche Verschlüsselungsschlüssel für Personalisierungsdaten und den Schlüsselimport verwendet werden, ist eine strenge Bindung des Verwendungszwecks der Schlüssel an die Eingabedaten gewährleistet.

Zusammenfassung von Datensätzen in einer Gruppe

Die Logical Data Identifier (LDI) bestehen aus vier Byte, zwei Byte für eine Gruppen-ID, eine Versionsnummer und einem Byte für die Nummerierung der Datensätze einer Personalisierungsnachricht. Sie charakterisieren die durch die Nachricht zu übertragenen Personalisierungsdaten einer bestimmten Gruppe.

Diese Daten einer Gruppe lassen sich schematisch wie folgt darstellen:

Position	**Länge** (in Byte)	**Wert**	**Erläuterung**
0.1	3	'XX XX VV'	Gruppen-ID und –Versionsnummer
0.2	1	'XX'	Anzahl j+1 der LDIs der Gruppe, binär kodiert
1.1	1	'00'	Nummer des Standard-LDIs (LDI0)
1.2	1	'00'	Algorithmus-Code: unverschlüsselt
1.3	1	'0B'	Länge der übertragenen Daten
1.4	11	'XX XX XX JJJJMMTT JJJJMMTT'	Sperrkennzeichen, Personalisierungszähler, Aktivierungs- und Verfallsdatum der Gruppe
2.1	1	'YY'	Nummer des LDI1
2.2	1	'XX'	Algorithmus-Code für den Datensatz
2.3	1	'XX'	Länge L1 der übertragenen Daten
2.4	L1	'XX..XX'	übertragene Daten
...	...	...	...
(j+1).1	1	'YY'	Nummer des LDIj
(j+1).2	1	'XX'	Algorithmus-Code für den Datensatz
(j+1).3	1	'XX'	Länge Lj der übertragenen Daten
(j+1).4	Lj	'XX..XX'	übertragene Daten
j+2.1	8	'XX..XX'	Retail-CBC-MAC mit KS_{MAC} über die Positionen 0.1 bis (j+1).4

Der Algorithmus-Code für den Datensatz ist entweder 00 – für unverschlüsselt, 01 – für CBC-Mode mit dem Verschlüsselungsschlüssel KS_{ENC} und 02 – für die Schlüsselverschlüsselung von K_{INIT_T} oder K_{PERS_T} mit dem Importer-Schlüssel KS_{IMP}.

Die übertragenen LDI (*logical data identifier*) erfüllen zusammen mit den Gruppen-ID die Anforderungen des ANSI X9.143 nach den Attribut-informationen in einem *key block header.* Die kryptographische Bindung wird durch die MAC-Berechnung gewährleistet.

Da sich die Längeninformation bereits im ersten Eingabeblock der MAC-Berechnung befindet (Position 1.3 in der obigen Tabelle), ist eine Anforderung des ANSI X 9.143

> *The key block will have a fixed key length for a given header.*

für die Triple-DES-Verwendung erfüllt ([X9.143, 7.3.1.2]).

Sicherheitsbewertung

Der Schutzmechanismus Triple-DES und Retail-MAC sind durch den ANSI X 9.143 aus Gründen der Abwärtskompatibilität ausdrücklich zugelassen.

Der Abschnitt 7.3 des ANSI-Standards entspricht dabei genau dem bei der Online-Personalisierung verwendeten Verfahren des kryptographischen Schutzes der übertragenen Nachrichten.

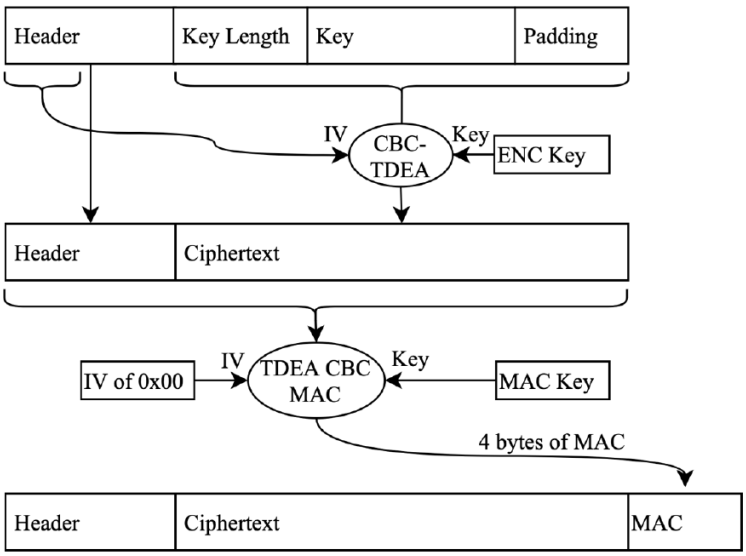

Figure 11 - Key Variant Binding Method [X9.143, S. 58]

Für die Nachrichtenverschlüsselung wird der CBC-Mode verwendet, der ebenfalls den Anforderungen des ANSI Standards X 9.143 genügt. Die verwendeten Algorithmen machen jegliche Veränderung einzelner Bits erkennbar. Das Entfernen und der Tausch einzelner Bits oder ganzer Datengruppen untereinander wird bei der MAC-Prüfung erkannt. Die Blocklänge wird durch den Header bestimmt, woraus sich die MAC-Länge zweifelsfrei ergibt.

Für zukünftige Anwendungen liegt nach Auskunft der Deutschen Kreditwirtschaft ein Migrationsplan und entsprechende Spezifikationen zu stärkeren Algorithmen und größeren Schlüssellängen (AES-256) bereits vor [AES-OPT].

Die bekannte Schwäche des Triple-DES, seine relativ kurze Schlüssellänge, bleibt ein gewisses Risiko. Allerdings werden die verwendeten Schlüssel bei der Online-Initialisierung und -Personalisierung jeweils gewechselt, durch Sperrung und zwischenzeitliche Außerbetriebsetzung können zu jedem Zeitpunkt Maßnahmen ergriffen werden, die Schäden durch eine Kompromittierung verhindern. Durch die Verwendung abgeleiteter Schlüssel wird eine wesentliche Anforderung des ANSI X 9.143 erfüllt.

Das bei der Personalisierung verwendete Nachrichtenformat garantiert eine strikte Bindung der Schlüssel an ihren Verwendungszweck. Eine Verfälschung der Schlüsseldaten ist durch die MAC-Berechnung ausgeschlossen.

Da die Initialisierung und Personalisierung durch entsprechende Dialoge als Nachrichtenfolgen umgesetzt werden, ist eine vorgegebene Reihenfolge einzuhalten. Mit einem Personalisierungszähler wird das Wiedereinspielen alter Personalisierungsdaten wirksam erkannt und verhindert.

Durch Aktivierungs- und Verfallsdaten können Schlüssel gegen eine zu lange Verwendung geschützt werden. Schlüssel können auch kurzfristig gesperrt und Terminals neu initialisiert werden. Damit stellen auch Triple-DES-Schlüssellängen kein Sicherheitsrisiko dar.

Der ANSI-Standard X 9.143 empfiehlt für die Übertragung von TDES- und AES-Schlüsseln die Schlüssellänge zu verschleiern ([X9.143, S. 6]). TDES-Schlüssel sind dann bis auf 192 Bits, AES-Schlüssel bis auf 256 Bits aufzufüllen. Aus kryptographischer Sicht ist eine solche Empfehlung im Allgemeinen sinnvoll, da sie einem Angreifer keine unnötigen Schlüsseldetails preisgibt. In dem speziellen Fall der Online-Personalisierung ist ein Padding zur Verschleierung des Schlüsseltyps und der Schlüssellänge allerdings unnötig, da im OPT-Verfahren nur ein einziger Schlüsseltyp (TDES) mit fixierter Schlüssellänge (128 Bit) verwendet wird. Da nicht ausgeschlossen werden kann, dass diese Information aus anderen Quellen bekannt ist, bringt eine Verschleierung der Schlüssellänge keinen zusätzlichen Sicherheitsgewinn. Da es nur eine Empfehlung ist (SHOULD), ist ihre Umsetzung nicht zwingend erforderlich.

Abschließende Beurteilung

Die Struktur der Nachrichten, die im Rahmen der Online-Initialisierung und -Personalisierung ausgetauscht werden, ist klar und eindeutig beschrieben. Sie gestattet die kryptographische Bindung der übermittelten Schlüsseldaten an den vorgesehenen Verwendungszweck. Der Schutz der Schlüsseldaten gegen Verfälschung und Kompromittierung ist durch die verwendeten Algorithmen Triple-DES und Retail-MAC gewährleistet. Der kryptographische Schutz der Nachrichten durch abgeleitete Schlüssel und die dafür eingesetzten Algorithmen sind äquivalent zu dem im ANSI-Standard X 9.143 beschriebenen Verfahren.

Die Umsetzung eines entsprechenden Migrationskonzepts auf stärkere Algorithmen und größere Schlüssellängen wird dessen ungeachtet empfohlen.

Literaturverzeichnis

[OPT] Online-Personalisierung von Terminal-HSMs, Schnittstellenspezifikation für die ZKA-Chipkarte, Version 3.1, 26.10.2004

[PCI PIN-Security] Payment Card Industry (PCI) PIN Security Requirements and Testing Procedures, Version 3.1, March 2021

[X9.143] Retail Financial Services Interoperable Secure Key Block Specification (ANSI X9.143-2022), Accredited Standards Committee X9, American National Standards Institute, 2022-05

[ISO10118-2] ISO/IEC 10118-2:2010, Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an *n*-bit block cipher

[AES-OPT] Schnittstellenspezifikation für chipbasierte DK-Anwendungen, Online-Personalisierung von Terminal-HSMs, Unterstützung von AES, Version 1.0, 19.04.2018

[PIN-FAQ] PTS PIN Security Requirements, Technical FAQs for use with Version 3, Payment Card Industry (PCI), September 2021

[HSM-FAQ] PTS HSM Security Requirements, Technical FAQs for use with Version 3, Payment Card Industry (PCI), August 2022

[Supp. 18-3] Information Supplement: PIN Security Requirement 18-3 − Key Blocks, PIN Assessment Working Group PCI Security Standards Council, July 2022

[TR-31] Interoperable Secure Key Exchange Key Block Specification (ASC X9 TR 31-2018), , Accredited Standards Committee X9, American National Standards Institute, 2018