

DIN/TS 16591

ICS 35.240.40

Ersatz für
DIN SPEC 16591:2016-12**PIN-Verfahren für die deutsche Kreditwirtschaft**

PIN procedure for the credit services sector

Procédure de code PIN pour le secteur allemand du crédit

Gesamtumfang 27 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Inhalt

	Seite
Nationales Vorwort	4
1 Anwendungsbereich	5
2 Normative Verweisungen	5
3 Begriffe	5
3.1 Abkürzungen und Notationen	5
4 Anforderungen an ein kreditwirtschaftliches PIN-Verfahren	8
5 Verfahren PIN-Generierung	9
5.1 Ableitung von Rohdaten	9
5.1.1 Allgemeines	9
5.1.2 Deterministisches Verfahren	9
5.1.3 Generierung aus Zufallsprozess	10
5.2 Ableitung numerischer Stellen für PIN aus Rohdaten	10
5.3 Konkretisierung des deterministischen Verfahrens zur Rohdatengewinnung	11
6 Ausschluss von Trivial-PINs bei der PIN-Generierung und bei der PIN-Selbstwahl	11
7 Bestimmung eines PIN-Referenzwertes (PRW)	11
7.1 Allgemeines	11
7.2 Generische Beschreibung eines Verfahrens zur PRW-Berechnung	11
7.3 PIN-Wechsel	12
7.4 Konkretisierung des Verfahrens zur PRW-Berechnung	12
7.5 Verschlüsselter PIN-Block	12
8 PIN-Verifikation im Rahmen einer Online-Autorisierung	13
9 Übersicht der HSM-Funktionen	13
10 Beschreibung der HSM-Funktionen des PIN-Verfahrens	15
10.1 Allgemeines	15
10.2 PRW-Generierung im Zusammenhang mit der Erst-Ausgabe einer Karte	15
10.3 PRW-Generierung im Zusammenhang mit der Ausgabe einer Folgekarte	17
10.4 PIN-Verifizierung	19
10.5 PIN Prüfung mit abweichenden Kartendaten	20
10.6 PIN-Selbstwahl	21
11 Anforderungen an das Schlüssel-Management	23
Anhang A (normativ) PIN-Block-Formate	25
A.1 Allgemeines	25
A.2 PBF-0	25
A.3 PBF-1	25
Literaturhinweise	27

Bilder

Bild 1 — Ablauf zu PRW_GEN 1 im HSM im Falle der deterministischen PIN-Ableitung	16
Bild 2 — Ablauf zu PRW_GEN2 im HSM im Falle PIN-Ableitung aus einem Zufallsprozess	17
Bild 3 — Ablauf zu PRW_FK im HSM unter Verwendung eines EPB	18
Bild 4 — Ablauf zu PIN_VER	19
Bild 5 — Ablauf zu PIN_CHA im HSM	22

Tabellen

Tabelle 1 — Abkürzungen und Notationen	6
--	---

Tabelle 2 — HSM-Funktionen des PIN-Verfahrens 13
Tabelle 3 — Ein- und Ausgabeparameter der HSM-Funktionen des PIN-Verfahrens 14
Tabelle 4 — Schlüsselverwendung 23
Tabelle 5 — Lebenszyklus der Schlüssel 24

Nationales Vorwort

Dieses Dokument wurde vom NA 043-03-02 AA „Finanzdienstleistungen“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA) erarbeitet.

Technische Spezifikationen sind nicht Bestandteil des Deutschen Normenwerks.

Eine Technische Spezifikation ist das Ergebnis einer Normungsarbeit, das wegen bestimmter Vorbehalte zum Inhalt oder wegen des gegenüber einer Norm abweichenden Aufstellungsverfahrens von DIN noch nicht als Norm herausgegeben wird.

Zur vorliegenden Technischen Spezifikation wurde kein Entwurf veröffentlicht.

Erfahrungen mit dieser Technischen Spezifikation sind erbeten:

- vorzugsweise als Datei per E-Mail an nia@din.de in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter <http://www.din.de/stellungnahme> abgerufen werden;
- oder in Papierform an den Normenausschuss Informationstechnik und Anwendungen.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. DIN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Änderungen

Gegenüber DIN SPEC 16591:2016-12 wurden folgende Änderungen vorgenommen:

- a) Anpassung der durchgängigen Verwendung des PIN-Block-Formats 4 nach ISO 9564-1 für die AES gesicherte PIN-Übertragung während der Autorisierung in der Beschreibung;
- b) Definierung eines separaten verschlüsselten Ausgabeformats während des Generierungs- bzw. Karten-erneuerungsprozesses für die Personalisierung von Chipkarten;
- c) Integration einer Prüfroutine zur Prüfung der formalen Korrektheit des Formats 4 nach ISO 9564-1 beim PIN-Prüfungsprozess;
- d) Definieren von Bedingungen, um eine PIN-Prüfung bei abweichenden Kartendaten (z. B. bei Verwendung von Token) sicher zu ermöglichen;
- e) Präzisierung der Hinweise für das Skripting bei der Einbringung einer vom Kunden neu gewählten PIN in den Chip.

Frühere Ausgaben

DIN SPEC 16591: 2016-12

1 Anwendungsbereich

Dieses Dokument legt Verfahren zur PIN-Generierung, PIN-Verifizierung sowie die Möglichkeit des PIN-Wechsels durch den Kunden fest. Es ist das Ziel, kreditwirtschaftlich einheitliche Vorgaben für die Implementierung dieser Prozesse festzulegen. Daher wurde eine generische Beschreibung der Vorgehensweise gewählt, die einerseits ausreichend Flexibilität bei der Umsetzung bietet, andererseits jedoch Rahmenbedingungen vorgibt, die für einen sicheren Betrieb erforderlich sind.

Neben dieser generischen Beschreibung wurde eine Umsetzung mit konkreten Algorithmen formuliert. Hiermit kann das vorliegende Dokument als Input für die Spezifikation einer Sicherheitsmodulschnittstelle verwendet werden.

Bei der Festlegung des Verfahrens wurde das Ziel verfolgt,

- eine strikte und technisch unterstützte Trennung zwischen dem Generierungssystem einer PIN und den Autorisierungssystemen zu erreichen;
- die Verifizierung der PIN auf Basis von Einwegfunktionen zu realisieren, um eine Rückrechenbarkeit z. B. durch Entschlüsselung zu verhindern; und
- die freie PIN-Wahl für den Kunden zu erlauben.

Dieses Dokument macht keine Vorgaben zur sicheren Übertragung der PIN zum Zwecke der Autorisierung. Hierzu muss eine separate Festlegung erfolgen. Die vorliegende DIN/TS 16591 berücksichtigt insbesondere das PIN-Format 4 nach ISO 9564-1 z. B. für Autorisierungsanfragen. In der Migrationszeit bis zur vollständigen Einführung dieses Verfahrens können noch andere Verfahren genutzt werden, wie z. B. die in der Vorgängerversion dieses Dokuments DIN SPEC 16591:2016-12 beschriebenen.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO 9564-1, *Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based systems*

3 Begriffe

In diesem Dokument werden keine Begriffe aufgeführt.

DIN und DKE stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- DIN-TERMinologieportal: verfügbar unter <https://www.din.de/go/din-term>
- DKE-IEV: verfügbar unter <http://www.dke.de/DKE-IEV>

3.1 Abkürzungen und Notationen

Die Abkürzungen und Notationen sind in Tabelle 1 aufgeführt.

Tabelle 1 — Abkürzungen und Notationen

$A B$	Konkatenation zweier Bytefolgen A und B
AD	Account Data
AES	Advanced Encryption Standard
AS	Autorisierungssystem
BCD	Binary Coded Decimal
CBC	Cipher Block Chaining
CD	vom Herausgeber festzulegende Kartendaten
CDp	Teildaten von CD, die eine Unterscheidung von mehreren Karten zu einem Konto erlauben und zeitlich konstant bleiben
CDt	Teildaten von CD, die eine Unterscheidung von Karten hinsichtlich des Gültigkeitszeitraumes erlauben
$CMAC_{AES-k}(K, m, s)$	MAC der Länge von s Byte über eine Nachricht m unter Verwendung des AES [1] mit einem Schlüssel K [2]; bei der Bezeichnung AES-k kann k die Werte der für den AES-spezifizierten Schlüssellängen annehmen (128 Bit, 192 Bit, 256 Bit).
$dec_{ALG}(K, c)$	Entschlüsselung einer Nachricht c mit einem Schlüssel K unter Verwendung eines symmetrischen Algorithmus ALG
$enc_{ALG}(K, m)$	Verschlüsselung einer Nachricht m mit einem Schlüssel K unter Verwendung eines symmetrischen Algorithmus ALG
$dec_{ALG_CBC}(K, IV, c)$	Entschlüsselung eines Kryptogramms c mit einem Schlüssel K und Initialisierungsvektor IV im CBC Modus
$enc_{ALG_CBC}(K, IV, m)$	Verschlüsselung einer Nachricht m mit einem Schlüssel K und Initialisierungsvektor IV im CBC Modus
EPB	verschlüsselter PIN-Block (PAC) im PBF-1 Format ^a ; die Verschlüsselung erfolgt als CBC-Verschlüsselung mit Initialisierungsvektor 0.
EPB-M	8 Byte langer MAC über den EPB verkettet mit den zeitlich konstanten Kartendaten CDp; die Berechnung erfolgt als CMAC [2] nach 7.5.
EPB_{Chip}	verschlüsselter PIN-Block im PBF-1 Format zur Verwendung im Rahmen der Personalisierung von Chipkarten; die Verschlüsselung erfolgt als CBC-Verschlüsselung mit Initialisierungsvektor 0.

Tabelle 1 (fortgesetzt)

EPB _{Print}	verschlüsselter PIN-Block (PAC) im PBF-1 Format zum Zwecke der Übergabe an einen Dienstleister zur Bereitstellung der PIN an den Kunden (z. B. in Form eines gedruckten PIN-Briefes). Die Verschlüsselung erfolgt als CBC-Verschlüsselung mit Initialisierungsvektor 0.
EPB _{neu}	verschlüsselter PIN-Block im PBF-1 Format unter Verwendung eines neuen Verschlüsselungsschlüssels
EPB-M _{neu}	8 Byte langer MAC über EPB _{neu} verkettet mit den zeitlich konstanten Kartendaten CDP; die Berechnung erfolgt als CMAC [2].
ER	Eingangswerte zur Bestimmung der Rohdaten nach 5.1.2
GS	Generierungssystem
Hex	hexadezimale Darstellung
HSM	Hardware-Sicherheitsmodul
K _{Chip_Pers}	AES-Schlüssel zur Ver-/Entschlüsselung von Daten für die Chip Personalisierung
K _{PRW}	AES-Schlüssel zur Berechnung eines CMAC nach 5.3
K _{PRWneu}	AES-Schlüssel zur Berechnung eines PRW in der Funktion PIN_CHA
K _{DET}	institutsspezifischer Schlüssel zur deterministischen Ableitung von PINs
K _{EPB} , K _{EPBneu}	Schlüssel zur Ver-/Entschlüsselung von EPBs bei der Berechnung von PRWs bei der Ausgabe von Folgekarten oder bei PIN-Wechsel
K _{EPB_MAC}	Schlüssel zur Berechnung des EPB-M
K _{EPB_MACneu}	Schlüssel zur Berechnung eines EPB-M _{neu} im Zusammenhang mit der Ausgabe einer Folgekarte
K _{PAC}	Schlüssel zur Ver-/Entschlüsselung des PIN-Blocks (PAC) einer Autorisierungsnachricht; das Schlüsselformat ist abhängig von dem tatsächlich bei der Übertragung verwendeten Verfahren.
K _{PB}	Schlüssel zur kryptographischen Absicherung der PAN-Bindung nach 10.5
K _{Print}	AES-Schlüssel zur Verschlüsselung des PIN-Blocks im PBF-1 Format zum Zwecke des PIN-Bereitstellung (z. B. PIN-Brief)

Tabelle 1 (fortgesetzt)

Kartendaten _{Script}	Eingabedaten der Funktion PIN_CHA zur Bildung eines Scripts zum Update der PIN in der Karte bei PIN-Selbstwahl
MAC	Message Authentication Code
PAC	verschlüsselter PIN-Block im Format 4 nach ISO 9564-1
PAC _{neu}	verschlüsselter PIN-Block zur Eingabe der neu gewählten PIN bei PIN-Selbstwahl in Funktion PIN_CHA
PAN	Primary Account Number, Bestandteil der PIN-Block-Formate PBF-0 und PBF-1
PD	Dienstleister zur Bereitstellung der PIN an den Endkunden
POS	Point of Sale
PL	PIN-Länge
PRW	PIN-Referenzwert
PRW _{neu}	neu ermittelter PIN Referenzwert nach einem Wechsel der PIN
PS	Personalisierungssystem für Chipkarten
RC	Return-Code, Antwort-Code
RND	Zufallszahl, die zur Bildung des PBF-1 Formats verwendet wurde
RND _{PRW}	Zufallswert zur Berechnung eines PRW nach 7.2
RND _{PRWneu}	neuer Zufallswert im Falle der Neuberechnung eines PRW
Script	Script zum Update der PIN in der Karte bei PIN-Selbstwahl
Scriptschlüssel	Schlüssel zur Verschlüsselung und MAC-Sicherung von Scripten zum Update der PIN in der Karte bei PIN-Selbstwahl. Zur MAC-Sicherung des Scriptes wird ein anderer Schlüssel verwendet als zur Verschlüsselung des PIN-Blocks. Die Schlüssel unterscheiden sich sowohl im Wert als auch in der Verwendbarkeit.
^a siehe Anhang A	

4 Anforderungen an ein kreditwirtschaftliches PIN-Verfahren

An ein kreditwirtschaftliches PIN-Verfahren werden die folgenden konzeptionellen Anforderungen gestellt:

- a) Die Prozesse der PIN-Generierung und PIN-Prüfung müssen organisatorisch und technisch voneinander getrennt sein; insbesondere darf die PIN-Prüfung nicht darauf beruhen, dass der PIN-Generierungsprozess nochmals durchlaufen wird.
- b) Innerhalb des Verfahrens ist für unterschiedliche Zwecke unterschiedliches Schlüsselmaterial zu verwenden.
- c) Die PIN-Generierung aus einem Zufallsprozess und als deterministisches Ableitungsverfahren (auf Basis des unterliegenden Blockverschlüsselungsalgorithmus) ist vorzusehen. Aus juristischer Sicht sind sogenannte Trivial-PINs nicht relevant. Als geschäftspolitische Option sollte es jedoch möglich sein, bei der Generierung bestimmte PINs auszuschließen.
- d) Das Verfahren ist unabhängig vom Krypto-Algorithmus (Nachhaltigkeit).
- e) Die PIN-Generierung erfolgt in einer zertifizierten Krypto-Hardware (gilt analog für alle anderen Funktionen mit einer Klartext-PIN).
- f) Die Verwendung der PIN erfolgt außerhalb der Krypto-Hardware nur verschlüsselt, hierfür ist die Definition geeigneter PIN-Formate für die Ausgabe der PIN erforderlich. Einzige Ausnahme ist die Klarrechnung für die Übergabe der PIN an den Kunden (wobei diese geeignete organisatorische Sicherheitsvorkehrungen erfordert).
- g) Die PIN-Prüfung wird anhand von Prüfdaten vorgenommen, aus denen die PIN auch bei Kenntnis kryptographischer Schlüssel nicht rückrechenbar sein darf. Es dürfen keinerlei PIN-bezogene Prüfdaten auf dem Magnetstreifen einer Karte gespeichert werden.
- h) Das Verfahren erfordert keine dauerhafte Speicherung der PIN (auch nicht verschlüsselt) im Autorisierungssystem. Es muss ein ausreichender Schutz vor Codebook-Attacken und vor Kollisionen (gleiche Prüfdaten zu verschiedenen PINs bei identischen Kartendaten, Geburtstags-Paradoxon) gegeben sein.
- i) Die Gleichverteilung aller PIN-Ziffern bei der PIN-Generierung wird gefordert.
- j) PIN-Längen zwischen 4 und 12 Ziffern müssen unterstützt werden.
- k) Die PIN-Selbstwahl durch den Kunden muss grundsätzlich möglich sein. Aus juristischer Sicht sind sogenannte Trivial-PINs nicht relevant. Als geschäftspolitische Option sollte es jedoch möglich sein, bei der PIN-Selbstwahl bestimmte PINs auszuschließen.

5 Verfahren PIN-Generierung

5.1 Ableitung von Rohdaten

5.1.1 Allgemeines

Zunächst werden zwei Varianten zur Gewinnung von Binärdaten beschrieben, aus denen anschließend mit Hilfe des in 5.2 beschriebenen Verfahrens die Ziffern der PIN abgeleitet werden. Die Binärdaten werden daher als Rohdaten bezeichnet.

5.1.2 Deterministisches Verfahren

Ein deterministisches Verfahren zur Gewinnung der Rohdaten basiert auf der Anwendung einer kryptographischen Einwegfunktion auf bestimmte Eingangswerte. Die Anwendung der kryptographischen Einwegfunktion muss mittels einer geheimen Komponente parametrisiert werden, da sonst bei bekanntem Algorithmus und bekannten Eingangswerten die PIN auch von Unberechtigten „nachgerechnet“ werden könnte.