

ICS 35.240.40

PIN-Verfahren für die deutsche Kreditwirtschaft

PIN procedure for the credit services sector

Procédure de Code PIN pour le secteur allemand du crédit

Zur Erstellung einer DIN SPEC können verschiedene Verfahrensweisen herangezogen werden:
Das vorliegende Dokument wurde nach den Verfahrensregeln einer Vornorm erstellt.

Gesamtumfang 24 Seiten

Inhalt

	Seite
Nationales Vorwort.....	3
1 Anwendungsbereich.....	4
2 Normative Verweisungen	4
3 Abkürzungen und Notationen.....	4
4 Anforderungen an ein kreditwirtschaftliches PIN-Verfahren	7
5 Verfahren PIN-Generierung.....	8
5.1 Ableitung von Rohdaten.....	8
5.1.1 Allgemeines	8
5.1.2 Deterministisches Verfahren	8
5.1.3 Generierung aus Zufallsprozess.....	9
5.2 Ableitung numerischer Stellen für PIN aus Rohdaten	9
5.3 Konkretisierung des deterministischen Verfahrens zur Rohdatengewinnung	9
6 Ausschluss von Trivial-PINs bei der PIN-Generierung und bei der PIN-Selbstwahl.....	9
7 Bestimmung eines PIN-Referenzwertes (PRW)	10
7.1 Allgemeines	10
7.2 Generische Beschreibung eines Verfahrens zur PRW-Berechnung.....	10
7.3 PIN-Wechsel.....	10
7.4 Konkretisierung des Verfahrens zur PRW-Berechnung	11
7.5 Verschlüsselte PIN Block	11
8 PIN-Verifikation im Rahmen einer online-Autorisierung.....	12
9 Übersicht der HSM-Funktionen.....	13
10 Beschreibung der HSM-Funktionen des PIN-Verfahrens.....	14
10.1 Allgemeines	14
10.2 PRW-Generierung im Zusammenhang mit der Erst-Ausgabe einer Karte	14
10.3 PRW-Generierung im Zusammenhang mit der Ausgabe einer Folgekarte	16
10.4 PIN-Verifizierung.....	17
10.5 PIN-Selbstwahl.....	19
11 Anforderungen an das Schlüssel-Management	20
Anhang A (normativ) PIN-Block-Formate	23
A.1 Allgemeines	23
A.2 PBF-0	23
A.3 PBF-1	23
Literaturhinweise.....	24

Nationales Vorwort

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

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. Das DIN [und/oder die DKE] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Eine DIN SPEC nach dem Vornorm-Verfahren ist das Ergebnis einer Normungsarbeit, das wegen bestimmter Vorbehalte zum Inhalt oder wegen des gegenüber einer Norm abweichenden Aufstellungsverfahrens vom DIN noch nicht als Norm herausgegeben wird.

Zur vorliegenden DIN SPEC wurde kein Entwurf veröffentlicht.

Erfahrungen mit dieser DIN SPEC 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.

1 Anwendungsbereich

Dieses Dokument beschreibt Verfahren zur PIN-Generierung, PIN-Verifizierung sowie die Möglichkeit des PIN-Wechsels durch den Kunden. 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 der Generierungsstelle 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.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. 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 Abkürzungen und Notationen

Tabelle 1 — Abkürzungen und Notationen

A B	Konkatenation zweier Bytefolgen A und B
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

Tabelle 1 (fortgesetzt)

CDt	Teildaten von CD, die eine Unterscheidung von Karten hinsichtlich des Gültigkeitszeitraumes erlauben
$\text{CMAC}_{\text{AES-K}}(\text{K}, \text{m}, \text{s})$	MAC der Länge von s Byte über eine Nachricht m unter Verwendung des AES [1] mit einem Schlüssel K [2]
$\text{dec}_{\text{ALG}}(\text{K}, \text{c})$	Entschlüsselung einer Nachricht c mit einem Schlüssel K unter Verwendung eines symmetrischen Algorithmus ALG
$\text{dec}_{\text{ALG}}(\text{K}, \text{m})$	Verschlüsselung einer Nachricht m mit einem Schlüssel K unter Verwendung eines symmetrischen Algorithmus ALG
$\text{dec}_{\text{ALG_CBC}}(\text{K}, \text{IV}, \text{c})$	Entschlüsselung eines Kryptogramms c mit einem Schlüssel K und Initialisierungsvektor IV im CBC Modus
$\text{dec}_{\text{ALG_CBC}}(\text{K}, \text{IV}, \text{m})$	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]
$\text{EPB}_{\text{Print}}$	Verschlüsselter PIN-Block (PAC) im PBF-1 Format zum Zwecke der Übergabe an einen PIN-Druck Dienstleister. Die Verschlüsselung erfolgt als CBC-Verschlüsselung mit Initialisierungsvektor 0.
EPB_{neu}	Verschlüsselter PIN-Block im PBF-1 Format unter Verwendung eines neuen Verschlüsselungsschlüssels
$\text{EPB-M}_{\text{neu}}$	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

Tabelle 1 (fortgesetzt)

HSM	Hardware-Sicherheitsmodul
K_{PRW}	AES Schlüssel zur Berechnung eines CMAC nach 6.3
$K_{PRW_{neu}}$	AES Schlüssel zur Berechnung eines PRW in der Funktion PIN_CHA
K_{DET}	Institutsspezifischer Schlüssel zur deterministischen Ableitung von PINs
$K_{EPB}, K_{EPB_{neu}}$	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
$K_{EPB_MAC_{neu}}$	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_{Print}	AES-Schlüssel zur Verschlüsselung des PIN-Blocks im PBF-1 Format zum Zwecke des PIN-Drucks
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 ISO-1 Format
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	PIN-Druck-Dienstleister
POS	Point of Sale
PL	PIN Länge
PRW	PIN Referenzwert

Tabelle 1 (fortgesetzt)

PRW_{neu}	Neu ermittelter PIN Referenzwert nach einem Wechsel der PIN
RC	Return-Code, Antwort-Code
RND	Zufallszahl, die zur Bildung des PBF-1 Formats verwendet wurde
RND_{PRW}	Zufallswert (4 Byte binär)
$RND_{PRW_{neu}}$	Neuer Zufallswert (4 Byte binär) 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:

- 1) 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.
- 2) Innerhalb des Verfahrens ist für unterschiedliche Zwecke unterschiedliches Schlüsselmaterial zu verwenden.
- 3) 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.
- 4) Das Verfahren ist unabhängig vom Krypto-Algorithmus (Nachhaltigkeit).
- 5) PIN-Generierung erfolgt in einer zertifizierten Krypto-Hardware (gilt analog für alle anderen Funktionen mit einer Klartext-PIN).
- 6) 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 PIN-Druck (erfordert geeignete organisatorische Sicherheitsvorkehrungen).

- 7) 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.
- 8) Das Verfahren erfordert keine dauerhafte Speicherung der PIN (auch nicht verschlüsselt) in der Autorisierungsstelle. Es muss ein ausreichender Schutz vor Codebook-Attacken und vor Kollisionen (gleiche Prüfdaten zu verschiedenen PINs bei identischen Kartendaten, Geburtstags-Paradoxon) gegeben sein.
- 9) Die Gleichverteilung aller PIN-Ziffern bei der PIN-Generierung wird gefordert.
- 10) PIN-Längen zwischen 4 und 12 Ziffern müssen unterstützt werden.
- 11) 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.

Als kryptographische Einwegfunktion wird beispielsweise ein CMAC ([2]) oder ein HMAC ([3]) gewählt. Aus dem Ergebnis der Anwendung dieser Einwegfunktion auf die Eingangswerte werden $b \geq 16$ Byte als Rohdaten für die PIN-Ableitung verwendet.

Die Eingangswerte müssen sich aus einer Kombination von Daten zur Kontoinformation und zur Kartenidentifikation zusammensetzen. Die Eingangswerte beginnen mit 19 Stellen der PAN kodiert als Dezimalziffern in Halbbytes (BCD). Ist die PAN kürzer als 19 Ziffern, geht sie links mit Nullen auf 19 Stellen gefüllt in die Generierung der Rohdaten ein. Es ist sicherzustellen, dass die Eingangswerte für verschiedene Karten sich auch tatsächlich unterscheiden. Die Eingangswerte zur Gewinnung der Rohdaten werden mit ER bezeichnet.

Mögliche Eingangswerte für einen Algorithmus zur Ableitung von Rohdaten zur deterministischen PIN-Generierung sind Kartenidentifikationsdaten wie z. B.:

- PAN (19 Dezimalstellen, BCD);
- Kartenfolgennummer (3 Dezimalstellen, BCD);
- Freizügigkeitsschlüssel (2 Dezimalstellen, BCD);
- Kontoart (1 Dezimalstelle, BCD);
- Benutzungseinschränkung (2 Dezimalstellen, BCD);
- Filter z. B. '00 00'.