

DIN/TS 16591:2020-11 (D)

PIN-Verfahren für die deutsche Kreditwirtschaft

Inhalt	Seite
Nationales Vorwort	4
1 Anwendungsbereich.....	5
2 Normative Verweisungen	5
3 Begriffe	5
3.1 Abkürzungen und Notationen	6
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	14
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	20
Bild 5 — Ablauf zu PIN_CHA im HSM	22

Tabellen

Tabelle 1 — Abkürzungen und Notationen	6
Tabelle 2 — HSM-Funktionen des PIN-Verfahrens	14
Tabelle 3 — Ein- und Ausgabeparameter der HSM-Funktionen des PIN-Verfahrens.....	14
Tabelle 4 — Schlüsselverwendung	23
Tabelle 5 — Lebenszyklus der Schlüssel	24