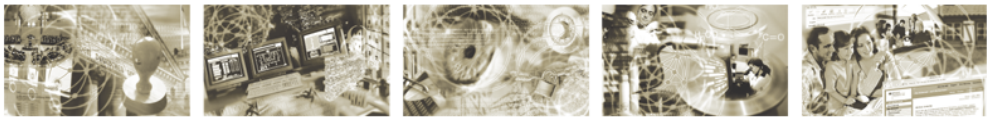
Bundesamt
für Sicherheit in der
Informationstechnik



Technische Richtlinie BSI TR-03109-2

Anhang B: Smart Meter Mini-HSM – Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls

Version 1.0 – 23.06.2017

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Das sogenannte „Smart Meter Mini-HSM“ stellt eine HW-/SW-Komponente mit integriertem Sicherheitsmodul als Cryptographic Service Provider dar, das im Umfeld von Smart Meter-Systemen von verschiedenen Typen von Mini-HSM Usern zur Unterstützung ihrer Aufgaben und Kommunikationstätigkeiten in sicherer Einsatzumgebung verwendet werden kann.

Beispiele für Einsatzmöglichkeiten des Smart Meter Mini-HSM:

Das Smart Meter Mini-HSM kann beim Smart Meter Gateway Administrator (GW-Administrator) in sicherer Einsatzumgebung eingesetzt werden und stellt für den GW-Administrator die Gegenstelle zum SMGW dar, mit dessen Unterstützung der GW-Administrator die Personalisierung und Administration des SMGW und seines Sicherheitsmoduls vornehmen kann. Der GW-Administrator kann das Smart Meter Mini-HSM ferner für die Kommunikation mit dem Autorisierten Externen Marktteilnehmer (EMT) und anderen Parteien nutzen.

Das Smart Meter Mini-HSM kann auch durch den Autorisierten Externen Marktteilnehmer (EMT) in gesicherter Einsatzumgebung eingesetzt werden und stellt dort ebenfalls die Gegenstelle zum SMGW dar, mit dessen Unterstützung der EMT mit dem SMGW kommunizieren kann. Der EMT kann das Smart Meter Mini-HSM ferner für die Kommunikation mit dem GW-Administrator und anderen Parteien nutzen.

Das Smart Meter Mini-HSM kann weiterhin beim Hersteller eines Smart Meter Gateways (GWH) für kryptographische Zwecke im Rahmen seiner Entwicklung und Produktion Verwendung finden.

Das Smart Meter Mini-HSM ist mit einem Applikationsserver verbunden, über den der Mini-HSM User mit dem Smart Meter Mini-HSM und seinem integrierten Sicherheitsmodul kommuniziert. Der Applikationsserver übernimmt für den Mini-HSM User die Kommunikation mit dem Sicherheitsmodul des Smart Meter Mini-HSM auf Kommandoebene. Die weiteren HW-/SW-Bestandteile des Smart Meter Mini-HSM außerhalb des integrierten Sicherheitsmoduls steuern keine weitere (Sicherheits-) Funktionalität bei und dienen lediglich einem Transport Layer für den Zugriff auf das Sicherheitsmodul und für das Durchreichen von Kommandonachrichten und -antworten zwischen Applikationsserver und Sicherheitsmodul.

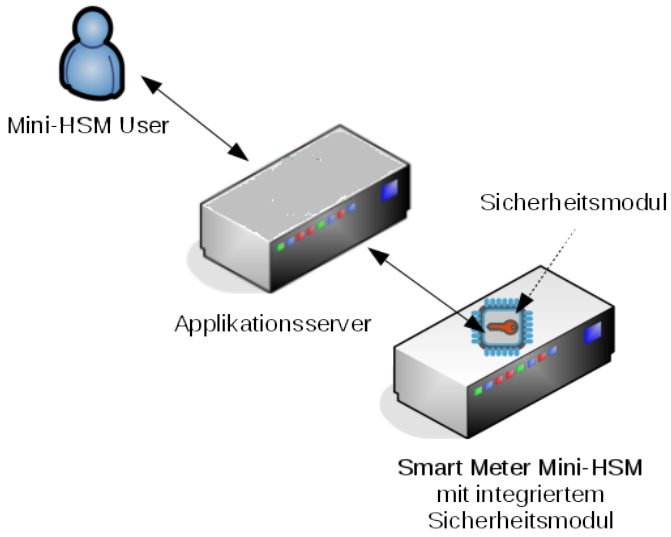


Abbildung 1: Smart Meter Mini-HSM

Zur Implementierung der für den Einsatz in Smart Meter-Systemen benötigten kryptographischen Funktionen bedient sich das Smart Meter Mini-HSM eines gemäß [PP 0095] nach Common Criteria zertifizierten Sicherheitsmoduls. Als zentrale Sicherheitskomponente

- stellt das Sicherheitsmodul die kryptographische Identität des Mini-HSM Users sicher und
- dient dem Mini-HSM User als Service Provider für kryptographische Operationen.

Das Sicherheitsmodul stellt insbesondere Funktionen

- zur Schlüsselgenerierung,
- zur Erzeugung und Verifikation von Digitalen Signaturen und
- zur Schlüsselaushandlung

auf Basis von Kryptographie mit Elliptischen Kurven bereit.

Weiterhin dient das Sicherheitsmodul

- als zuverlässige Quelle für Zufallszahlen und
- als sicherer Speicher von Schlüsseln und Zertifikaten.

Ferner unterstützt das Sicherheitsmodul einen authentisierten und gesicherten Kommunikationskanal zwischen dem Applikationsserver und dem Sicherheitsmodul im Smart Meter Mini-HSM. Der Applikationsserver hat für die Nutzung eines solchen authentisierten und gesicherten Kanals seinerseits entspechende kryptographische Funktionalität (inklusive Handling der Authentisierungsdaten) bereitzustellen.

Im vorliegenden Dokument werden die Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls für das Smart Meter Mini-HSM spezifiziert. Hierzu liefert dieses Dokument neben einer detaillierten Beschreibung des Lebenszyklus-Modells von Sicherheitsmodul bzw. Smart Meter Mini-HSM insbesondere die Spezifikation des Kommandosets, der Zugriffsregelpolitik und des File- und Objektsystems des Sicherheitsmoduls.

Sicherheitstechnische Anforderungen an das Sicherheitsmodul selbst werden darüber hinaus durch das Common Criteria-Schutzprofil [PP 0095] festgelegt.

Es erfolgt im vorliegenden Dokument *keine* Spezifikation der übrigen HW- und SW-Bestandteile des Smart Meter Mini-HSM sowie des Applikationsservers, sofern im Dokument nichts anderes angegeben ist.

Die Anforderungen an die Sicherheit der Einsatzumgebung für das Smart Meter Mini-HSM mit seinem integrierten Sicherheitsmodul und für den damit verbundenen Applikationsserver beim Mini-HSM User liegen außerhalb der vorliegenden technischen Spezifikation.

1.1 Einordnung des Dokuments

Das vorliegende Dokument bildet einen Anhang zur Technischen Richtlinie [TR-03109-2] und spezifiziert in Anlehnung an die dortige Spezifikation für das Sicherheitsmodul des SMGW die Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls für das Smart Meter Mini-HSM.

1.2 Terminologie

Dieses Dokument ist grundsätzlich als normativ anzusehen. Informative Teile werden explizit als solche gekennzeichnet (mit dem Vermerk „informativ“ oder „Hinweis“).

1.3 Abkürzungen

In diesem Dokument werden folgende Abkürzungen verwendet:

Abkürzung	Begriff
AID	Application Identifier
APDU	Application Protocol Data Unit
AT	Authentication Template
ATR	Answer To Reset
ATS	Answer To Select
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authority
CC	Common Criteria
CP	Control Parameter
CRT	Control / Cryptographic Reference Template
DF	Dedicated File
DH	Diffie-Hellman
DST	Digital Signature Template
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECKA	Elliptic Curve Key Agreement
ECKA-DH	Elliptic Curve Key Agreement-Diffie-Hellman
ECKA-EG	Elliptic Curve Key Agreement-ElGamal
EF	Elementary File
EG	ElGamal
EMT	Autorisierter Externer Marktteilnehmer
Enc	Encryption
ENu	Endnutzer (z.B. Externer Marktteilnehmer, GW-Administrator, SMGW, ...)
EVG	Evaluierungsgegenstand
FCP	File Control Parameter
FID	File Identifier
GW	Gateway
GWA	Gateway-Administrator
GWH	Gateway-Hersteller
HAN	Home Area Network
HSM	Hardware Security Module
ID	Identifier
ISO	International Organization for Standardization
KDF	Key Derivation Function
KID	Key Identifier / Key-ID
KM	Kryptografiemodul
LCSI	Life Cycle Status Information
LMN	Local Metrological Network

Abkürzung	Begriff
MF	Master File
MSBit	Most Significant Bit
MT	Marktteilnehmer
NIST	National Institute of Standards and Technology
OID	Object Identifier
OS	Operating System
PIN	Personal Identification Number
PKI	Public Key Infrastruktur
PP	Protection Profile (Common Criteria)
RFU	Reserved for Future Use
RNG	Random Number Generator
SE	Security Environment
SEID	Security Environment ID
SecMod	Security Module / Sicherheitsmodul
SFI	Short File Identifier
SHA	Secure Hash Algorithm
Sign	Signature
SM	Smart Meter
SMGW	Smart Meter Gateway (GW mit integriertem Sicherheitsmodul)
SM-PKI	Smart Metering - Public Key Infrastruktur (SM-PKI)
SP	Security Parameter
TLS	Transport Layer Security
TOE	Target Of Evaluation (Common Criteria)
TR	Technische Richtlinie
WAN	Wide Area Network

Tabelle 1: Übersicht der Abkürzungen

1.4 Änderungshistorie

Version	Datum	Änderung
V 0.1	28.10.2016	Erster Draft
V 0.2	01.12.2016	Einzelne inhaltliche Anpassungen und Ergänzungen
V 0.3	09.02.2017	Bugfixing, Inhaltliche Anpassungen und Ergänzungen: Einführung eines Applikationsservers, Verlagerung des Endpunktes des PACE-Kanals in den Applikationsserver, Erweiterung des initialen File- und Objektsystems für Option 1 durch weitere vordefinierte Key-Objekte
V0.4	07.04.2017	Kleine Ergänzungen
V0.5	14.06.2017	Flexibilisierung bzgl. des Imports von öffentlichen Schlüsseln
V1.0	23.06.2017	Veröffentlichung

Tabelle 2: Änderungshistorie

2 Lebenszyklus-Modell

Das vorliegende Kapitel geht auf das Lebenszyklus-Modell für Sicherheitsmodul und Mini-HSM ein.

Ein integriertes Mini-HSM, d.h. ein Mini-HSM mit eingebautem und verbundenem Sicherheitsmodul wird im vorliegenden Dokument als „Smart Meter Mini-HSM“ bezeichnet.

2.1 Übersicht über das Lebenszyklus-Modell

In den folgenden Abschnitten wird zunächst eine grobe Übersicht über das Lebenszyklus-Modell für Sicherheitsmodul und Mini-HSM gegeben. Insbesondere werden die einzelnen Phasen des Lebenszyklus-Modells und die beteiligten Rollen benannt.

2.1.1 Phasen des Lebenszyklus-Modells

Das Lebenszyklus-Modell für Sicherheitsmodul und Mini-HSM gliedert sich in folgende aufeinander aufbauende Phasen:

1. Herstellungs- und Produktionsprozesse von Mini-HSM und Sicherheitsmodul (siehe Kap. 2.2.1)
2. Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM (siehe Kap. 2.2.2)
3. Installation + Vor-Ort-Inbetriebnahme des Smart Meter Mini-HSM (siehe Kap. 2.2.3)
4. Personalisierung des Smart Meter Mini-HSM (siehe Kap. 2.2.4)
5. Normalbetrieb (End-Usage mit Administration und Smart Meter Wirkbetrieb) des Smart Meter Mini-HSM (siehe Kap. 2.2.5)
6. Außerbetriebnahme des Smart Meter Mini-HSM (siehe Kap. 2.2.6)

In Kap. 2.2 erfolgt eine detaillierte Beschreibung der zuvor genannten Phasen des Lebenszyklus-Modells. In den einzelnen Phasenbeschreibungen werden zum einen die durchzuführenden Aufgaben und Randbedingungen benannt. Zum anderen werden jeweils auch die beteiligten Rollen, die einen Zugriff auf das Mini-HSM bzw. Sicherheitsmodul haben, zugeordnet.

2.1.2 Rollen im Lebenszyklus-Modell

Folgende Rollen sind im Lebenszyklus-Modell für Sicherheitsmodul und Mini-HSM involviert:

- Integrator
- ggf. Techniker für das Smart Meter Mini-HSM bzw. den Applikationsserver
- Mini-HSM User

  (beispielsweise in den Ausprägungen: Smart Meter Gateway Administrator (im Folgenden als GW-Administrator bezeichnet), Autorisierter Externer Marktteilnehmer (EMT), Gateway-Hersteller (GWH))

  Der Mini-HSM User greift über den Applikationsserver auf das Smart Meter Mini-HSM mit seinem Sicherheitsmodul zu.
- Applikationsserver

In Kap. 2.2 erfolgt im Rahmen der Detailbeschreibung der einzelnen Phasen des Lebenszyklus-Modells auch eine Benennung der jeweils beteiligten Rollen und eine detaillierte Beschreibung ihrer Aufgaben.

2.1.3 Weitere Aspekte

2.1.3.1 Life Cycle-Status

Das Sicherheitsmodul verwaltet einen eigenen Life Cycle-Status mit den Werten „nicht-initialisiert“ (d.h. das Sicherheitsmodul ist noch nicht initialisiert), „initialisiert“ (d.h. das Sicherheitsmodul ist initialisiert und mit den für das Smart Meter Mini-HSM bzw. den Applikationsserver vorgesehenen initialen Strukturen und Daten bestückt) und „terminiert“ (d.h. das Sicherheitsmodul ist irreversibel außer Betrieb genommen), siehe [TR-03109-2], Kap. 3.6.1.

Der Applikationsserver kann zusätzlich einen eigenen Life Cycle-Status mitführen und Informationen dazu im Sicherheitsmodul hinterlegen. Eine Auswertung dieses Life Cycle-Status des Applikationsservers durch das Sicherheitsmodul erfolgt jedoch nicht. Siehe Kap. 3.2.3 und [TR-03109-2], Kap. 3.6.1.

2.1.3.2 Zugriffsregelpolitik

Die in den einzelnen Phasen des Lebenszyklus-Modells relevanten Zugriffsregeln für die Restriktion des Zugriffs auf das Sicherheitsmodul, seine Datenfelder und Objekte sowie Kommandos werden über entsprechende sog. Security Environments im Sicherheitsmodul festgelegt, siehe Kap. 3.3.

2.2 Detailbeschreibung des Lebenszyklus-Modells

In den folgenden Abschnitten wird eine Detailbeschreibung des Lebenszyklus-Modells für Sicherheitsmodul und Mini-HSM gegeben, und insbesondere werden die einzelnen Phasen des Lebenszyklus-Modells, die jeweils beteiligten Rollen und die jeweils durchzuführenden Aufgaben genauer beleuchtet.

2.2.1 Herstellungs- und Produktionsprozesse von Mini-HSM und Sicherheitsmodul

Die Herstellungs- und Produktionsprozesse für das Mini-HSM liegen außerhalb des Scopes des vorliegenden Dokuments.

Für die Herstellungs-, Produktions- und Zertifizierungsprozesse des Sicherheitsmoduls sei auf [PP 0095] verwiesen.

Für die in den nachfolgenden Kapiteln dargestellten Phasen des Lebenszyklus-Modells werden die Herstellungs-, Produktions- und Zertifizierungsprozesse von Mini-HSM und Sicherheitsmodul als abgeschlossen vorausgesetzt.

Ausgangspunkt für die in den nachfolgenden Kapiteln dargestellten Phasen des Lebenszyklus-Modells ist genauer:

- Das Sicherheitsmodul liegt als initialisiertes Modul vor, d.h. das Sicherheitsmodul beinhaltet die Betriebssystem-Plattform mit den Kommandos sowie das für das Smart Meter Mini-

HSM bzw. den Applikationsserver vordefinierte initiale File- und Objektsystem mit den vorgesehenen Vorbelegungen. Das Sicherheitsmodul implementiert die vorgesehene Zugriffsregelpolitik. Für Details siehe Kap. 3 und 4.

- Das Mini-HSM liegt vor.

2.2.2 Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM

Die Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ dient der Integration von Mini-HSM und (initialisiertem) Sicherheitsmodul sowie der Vor-Personalisierung des Sicherheitsmoduls zur weiteren Konfiguration des dortigen File- und Objektsystems für den Mini-HSM User und seine Belange.

Die Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ setzt sich aus den Teilphasen „Integration“ und „Vor-Personalisierung“ zusammen und wird beim Integrator durchgeführt. Die „Integration“ kann vor oder nach der „Vor-Personalisierung“ stattfinden.

Der Import öffentlicher Schlüssel in das Sicherheitsmodul wird unter Verwendung sog. Import-Schlüssel realisiert. Entsprechende Key Pair-Objekte und zugehörige Public Key-Objekte für die *initialen* Import-Schlüssel (IMP_PRV_TRANS, IMP_PUB_TRANS) und IMP_PUB_TRANS sowie für die späteren Import-Schlüssel (IMP_PRV, IMP_PUB) und IMP_PUB, die für den Import von Schlüsseln genutzt werden können, sind bereits für das Initialisierungsfile vordefiniert und werden im Rahmen der Produktion (Initialisierung) des Sicherheitsmoduls aufgebracht (siehe auch Kap. 3.1.2).

Für das Befüllen der vorgenannten Key-Objekte mit Schlüsseldaten in der Teilphase „Vor-Personalisierung“ ist Folgendes vorgesehen:

- Soll ein Import von Schlüsseln in das Sicherheitsmodul in den Phasen „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“, „Personalisierung des Smart Meter Mini-HSM“ bzw. „Normalbetrieb (End-Usage) des Smart Meter Mini-HSM“ zur Verfügung stehen, so werden das Key Pair-Objekt für (IMP_PRV_TRANS, IMP_PUB_TRANS) und das zugehörige Public Key-Objekt für IMP_PUB_TRANS im Rahmen der Produktion des Sicherheitsmoduls mit entsprechenden Schlüsseldaten befüllt. Andernfalls können die genannten Key-Objekte leer (d.h. ohne Schlüsseldaten) bleiben.
- Soll ein Import von Schlüsseln in das Sicherheitsmodul in den Phasen „Personalisierung des Smart Meter Mini-HSM“ bzw. „Normalbetrieb (End-Usage) des Smart Meter Mini-HSM“ zur Verfügung stehen, so werden das Key Pair-Objekt für (IMP_PRV, IMP_PUB) und das zugehörige Public Key-Objekt für IMP_PUB in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ unter Nutzung der Transport-Import-Schlüssel (IMP_PRV_TRANS, IMP_PUB_TRANS) und IMP_PUB_TRANS mit entsprechenden Schlüsseldaten befüllt. Andernfalls können die genannten Key-Objekte leer (d.h. ohne Schlüsseldaten) bleiben.

Das Schlüsselpaar (IMP_PRV_TRANS, IMP_PUB_TRANS) hat den Charakter eines Transport-Schlüsselpaares und muss in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ durch den Integrator gegen ein Integrator-eigenes Import-Schlüsselpaar (IMP_PRV, IMP_PUB) ausgetauscht werden. Entsprechend muss auch IMP_PUB_TRANS zu IMP_PUB ausgetauscht werden. Hierzu wird das Import-Schlüsselpaar (IMP_PRV, IMP_PUB) im Sicherheitsmodul generiert und der Schlüssel IMP_PUB unter Nutzung der Transport-Import-Schlüssel (IMP_PRV_TRANS, IMP_PUB_TRANS) und IMP_PUB_TRANS in das Sicherheitsmodul importiert.

Mit den Schlüsseln (IMP_PRV_TRANS, IMP_PUB_TRANS) und IMP_PUB_TRANS soll ausschließlich der Import des Schlüssels IMP_PUB in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ durchgeführt werden. Die Key-Objekte für (IMP_PRV_TRANS, IMP_PUB_TRANS) und IMP_PUB_TRANS müssen zum Ende der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ durch den Integrator gelöscht werden, sofern in diesen Key-Objekten Schlüsseldaten vorhanden sind.

Die Key-Objekte für (IMP_PRV, IMP_PUB) und IMP_PUB werden in den nachfolgenden Phasen des Lebenszyklus-Modells für den Import öffentlicher Schlüssel weiter benötigt und verwendet, sofern in diesen Phasen der Import öffentlicher Schlüssel Anwendung findet und für den Import öffentlicher Schlüssel anderweitig keine Import-Schlüssel im Sicherheitsmodul zur Verfügung stehen.

2.2.2.1 Rollen und Aufgaben

Rolle: Integrator

Anforderungen an den Integrator:

- Beim Integrator besteht eine ausreichend durch technische, organisatorische und personelle Sicherheitsmaßnahmen gesicherte Umgebung. Insbesondere sind hierbei die Auflagen aus der CC-Sicherheitszertifizierung des Sicherheitsmoduls, soweit diese die Verwendung des Sicherheitsmoduls durch den Integrator betreffen, zu berücksichtigen und umzusetzen.

  Hinweis: Die Sicherheit der Integrationsumgebung liegt in der Verantwortung des Integrators. Es erfolgt keine Begutachtung der Integrationsumgebung mit ihren technischen, organisatorischen und personellen Sicherheitsmaßnahmen seitens des BSI.
- Sicherheitsmodul-spezifische weitere technische Sicherungsmaßnahmen sind zulässig. Ggf. wird dazu erforderliches Sicherungsmaterial (z.B. Keys, PINs, …) im Rahmen des Initialisierungsprozesses im Sicherheitsmodul hinterlegt und soweit erforderlich an den Integrator zur Nutzung ausgeliefert. Hierzu setzen viele Sicherheitsmodul-Hersteller auf übliche Sicherheitsmechanismen auf. Im Protection Profile [PP 0095] zum Sicherheitsmodul werden keine konkreten Sicherheitsmechanismen festgeschrieben, um den Herstellern von Sicherheitsmodulen genügend Freiraum für ihre spezifischen, ggf. bereits etablierten Sicherheitsmechanismen zu lassen.

2.2.2.1.1 Integration

Voraussetzungen für die „Integration“ von Sicherheitsmodul und Mini-HSM:

- Initialisiertes Sicherheitsmodul und Mini-HSM liegen vor.

Aufgaben in der „Integration“ von Sicherheitsmodul und Mini-HSM:

- Physikalisch-technischer Einbau des Sicherheitsmoduls in das Mini-HSM und elektronische Verbindung der beiden Komponenten.

2.2.2.1.2 Vor-Personalisierung

Voraussetzungen für die „Vor-Personalisierung“ von Sicherheitsmodul und Mini-HSM:

- „Integration“ von Sicherheitsmodul und Mini-HSM ist abgeschlossen, sofern die „Integration“ vor der „Vor-Personalisierung“ stattfindet.

Aufgaben in der „Vor-Personalisierung“ von Sicherheitsmodul und Mini-HSM:

(Hinweis: Der Fokus der Aufgabenbeschreibung liegt auf dem Sicherheitsmodul.)

- Setzen der HSM-System-PIN.

  Zu Beginn der „Vor-Personalisierung“ wird durch den Integrator die HSM-System-PIN generiert und initial im Sicherheitsmodul gesetzt. Die weiteren Schritte der „Vor-Personalisierung“ des Sicherheitsmoduls erfolgen im Rahmen der im Sicherheitsmodul hinterlegten Zugriffsregelpolitik (Verwendung eines PACE-authentisierten sicheren Kommunikationskanals, soweit vorgesehen).
- Sofern nicht schon im Rahmen der Produktion des initialisierten Sicherheitsmoduls geschehen: Anlage von Key-Objekten bzgl. TLS, SIG, ENC, ggf. AUT (nur im Falle des GW-Administrators) für die Schlüsselpaare des Mini-HSM Users.
- Befüllen der Key-Objekte für (IMP_PRV, IMP_PUB) und IMP_PUB mit Schlüsseldaten (sofern vorgesehen).
- Ggf. weitere Administration des initial aufgebrachten File- und Objektsystems (im Rahmen der bestehenden Zugriffsregelpolitik des Sicherheitsmoduls):
  - Anlage weiterer Ordner (DFs) und Datenfelder (EFs)
  - Anlage weiterer Key-Objekte
  - Import von Schlüsselmaterial, Zertifikaten und weiteren Nutzdaten
  - Aktivieren / Deaktivieren und Löschen einzelner Ordner (DFs), Datenfelder (EFs) und Key-Objekte
- Löschen der Key-Objekte für die Transport-Import-Schlüssel (IMP_PRV_TRANS, IMP_PUB_TRANS) und IMP_PUB_TRANS (sofern Schlüsseldaten in diesen Key-Objekten vorhanden sind).

2.2.2.2 Schlüssel- und PIN-Material

Folgendes Schlüssel- und PIN-Material liegt am Ende der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ (mindestens) im Sicherheitsmodul vor:

Im Sicherheitsmodul:

- initiale HSM-System-PIN (Referenzwert)
- ggf. Import-Schlüsselpaar (IMP_PRV, IMP_PUB) und öffentlicher Import-Schlüssel IMP_PUB

2.2.3 Installation + Vor-Ort-Inbetriebnahme des Smart Meter Mini-HSM

Die Phase „Installation + Vor-Ort-Inbetriebnahme des Smart Meter Mini-HSM“ beinhaltet die Installation des Smart Meter Mini-HSM beim Endkunden (Mini-HSM User) und umfasst insbesondere die dabei erforderlichen Installations-, Inbetriebnahme- und Konfigurationstätigkeiten inklusive des Anschlusses an den Applikationsserver.

2.2.3.1 Rollen und Aufgaben

Rolle: Mini-HSM User (unter Nutzung des Applikationsservers), ggf. Techniker für das Smart Meter Mini-HSM bzw. für den Applikationsserver

Voaussetzungen für die „Installation + Vor-Ort-Inbetriebnahme des Smart Meter Mini-HSM“:

- „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ ist abgeschlossen, d.h. das Smart Meter Mini-HSM (also Mini-HSM mit integriertem Sicherheitsmodul) liegt vor.

Aufgaben in der „Installation + Vor-Ort-Inbetriebnahme des Smart Meter Mini-HSM“:

- Installations-, Inbetriebnahme- und Konfigurationstätigkeiten am Smart Meter Mini-HSM gemäß zugehöriger Bedienungsanleitung (z.B. Parametrierung und Konfiguration der physikalischen Kommunikationsschnittstellen des Smart Meter Mini-HSM usw.) inklusive Anschluss an den Applikationsserver.
- Wechsel der HSM-System-PIN.

  Vor Beginn der Nutzung des Smart Meter Mini-HSM und seines integrierten Sicherheitsmoduls im Rahmen der „Personalisierung des Smart Meter Mini-HSM“ generiert der Mini-HSM User oder der Applikationsserver eine neue HSM-System-PIN. Diese wird mittels des Applikationsservers im Sicherheitsmodul gesetzt und ersetzt die im Rahmen der „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ initial gesetzte HSM-System-PIN. Über die (neue) HSM-System-PIN wird eine Bindung zwischen dem Applikationsserver und dem Sicherheitsmodul des Smart Meter Mini-HSM, das sog. „Pairing zwischen Applikationsserver und Sicherheitsmodul des Smart Meter Mini-HSM“, erreicht. Es erfolgt eine permanente Speicherung der HSM-System-PIN im Applikationsserver, sofern der Mini-HSM User die HSM-System-PIN nicht bei jeder Nutzung des Smart Meter Mini-HSM und seines integrierten Sicherheitsmoduls über den Applikationsserver erneut eingeben möchte.

2.2.3.2 Schlüssel- und PIN-Material

Folgendes Schlüssel- und PIN-Material liegt am Ende der Phase „Installation + Vor-Ort-Inbetriebnahme des Smart Meter Mini-HSM“ (mindestens) im Sicherheitsmodul vor:

Im Sicherheitsmodul:

- HSM-System-PIN (Referenzwert)
- ggf. Import-Schlüsselpaar (IMP_PRV, IMP_PUB) und öffentlicher Import-Schlüssel IMP_PUB

2.2.4 Personalisierung des Smart Meter Mini-HSM

Die Phase „Personalisierung des Smart Meter Mini-HSM“ beinhaltet insbesondere die Generierung des Schlüsselmaterials für den Mini-HSM User durch diesen selbst. Je nach Zugriffsregelpolitik des im Smart Meter Mini-HSM integrierten Sicherheitsmoduls kann durch den Mini-HSM User eine weitere Administration des Sicherheitsmoduls bzw. des dort installierten File- und Objektsystems erfolgen.

2.2.4.1 Rollen und Aufgaben

Rolle: Mini-HSM User (unter Nutzung des Applikationsservers)

Voraussetzungen für die „Personalisierung des Smart Meter Mini-HSM“:

- „Installation + Vor-Ort-Inbetriebnahme des Smart Meter Mini-HSM“ ist abgeschlossen, d.h. das Smart Meter Mini-HSM ist installiert und mit dem Applikationsserver verbunden.
- Key-Objekte für die Schlüsselpaare des Mini-HSM Users bzgl. TLS, SIG, ENC, ggf. AUT (nur im Falle des GW-Administrators) sind im Sicherheitsmodul angelegt. Sofern keine Anlage solcher Key-Objekte im Rahmen der Phase der Initialisierung oder „Vor-Personalisierung“ erfolgt sein sollte und die Zugriffsregelpolitik des Sicherheitsmoduls eine Administration durch den Mini-HSM User zulässt, sind die entsprechenden Key-Objekte durch den Mini-HSM User vor Beginn der eigentlichen „Personalisierung“ im Sicherheitsmodul anzulegen.

Aufgaben in der „Personalisierung des Smart Meter Mini-HSM“:

(Hinweis: Der Fokus der Aufgabenbeschreibung liegt auf dem Sicherheitsmodul.)

- Generierung der Schlüsselpaare des Mini-HSM Users bzgl. TLS, SIG, ENC, ggf. AUT (nur im Falle des GW-Administrators).
- Der Mini-HSM User kann ggf. – soweit seitens der Zugriffsregelpolitik des im Smart Meter Mini-HSM integrierten Sicherheitsmoduls zulässig – weitere Administrationstätigkeiten am Smart Meter Mini-HSM und seinem Sicherheitsmodul vornehmen. Beispielsweise kann dies das File- und Schlüsselmanagement wie die Anlage weiterer Ordner (DFs) und Datenfelder (EFs), die Anlage weiterer Key-Objekte, den Import von Schlüsselmaterial, Zertifikaten und weiteren Nutzdaten, das Generieren von Schlüsselpaaren, das Aktivieren / Deaktivieren und Löschen einzelner Ordner (DFs), Datenfelder (EFs) und Key-Objekte usw. umfassen.

Mit Abschluss der „Personalisierung“ liegt ein „scharfes“ Smart Meter Mini-HSM vor, das für die Nutzung im Normalbetrieb beim Mini-HSM User und seinem Applikationsserver bereitsteht.

2.2.4.2 Schlüssel- und PIN-Material

Folgendes Schlüssel- und PIN-Material liegt am Ende der Phase „Personalisierung des Smart Meter Mini-HSM“ (mindestens) im Sicherheitsmodul vor:

Im Sicherheitsmodul:

- HSM-System-PIN (Referenzwert)
- ggf. Import-Schlüsselpaar (IMP_PRV, IMP_PUB) und öffentlicher Import-Schlüssel IMP_PUB

- Schlüsselpaare des Mini-HSM Users bzgl. TLS, SIG, ENC, ggf. AUT (nur im Falle des GW-Administrators)

2.2.5 Normalbetrieb (End-Usage) des Smart Meter Mini-HSM

2.2.5.1 Rollen und Aufgaben

Zum „Normalbetrieb des Smart Meter Mini-HSM“ gehören folgende beide Bereiche:

- „Administration des Smart Meter Mini-HSM“
- „Wirkbetrieb des Smart Meter Mini-HSM“

Genauer betrifft dies die Administration und den Wirkbetrieb des im Smart Meter Mini-HSM integrierten Sicherheitsmoduls.

2.2.5.1.1 Administration des Smart Meter Mini-HSM

Rolle: Mini-HSM User (unter Nutzung des Applikationsservers)

Aufgaben in der „Administration des Smart Meter Mini-HSM“:

(Hinweis: Der Fokus der Aufgabenbeschreibung liegt auf dem Sicherheitsmodul.)

- File- und Schlüsselmanagement im Sicherheitsmodul. Je nach Zugriffsregelpolitik des im Smart Meter Mini-HSM integrierten Sicherheitsmoduls umfassen die Administrationstätigkeiten am Smart Meter Mini-HSM und seinem Sicherheitsmodul die Anlage weiterer Ordner (DFs) und Datenfelder (EFs), die Anlage weiterer Key-Objekte, den Import von Schlüsselmaterial, Zertifikaten und weiteren Nutzdaten, das Generieren von Schlüsselpaaren, das Aktivieren / Deaktivieren und Löschen einzelner Ordner (DFs), Datenfelder (EFs) und Key-Objekte im Sicherheitsmodul usw.

Bzgl. der Key-Objekte betrifft die „Administration des Smart Meter Mini-HSM“ die Administration

- der im Sicherheitsmodul hinterlegten Key-Objekte für die Schlüsselpaare des Mini-HSM Users selbst sowie
- der Key-Objekte für die öffentlichen Schlüssel der externen Welt (wie z.B. die TLS-, SIG- und ENC-bezogenen öffentlichen Schlüssel des SMGW, SM-PKI-Root-Keys, SM-PKI-CA-Keys usw.), sofern diese Schlüssel im Sicherheitsmodul des Smart Meter Mini-HSM abgelegt werden.

2.2.5.1.2 Wirkbetrieb des Smart Meter Mini-HSM

Rolle: Mini-HSM User (unter Nutzung des Applikationsservers)

Aufgaben im „Wirkbetrieb des Smart Meter Mini-HSM“:

(Hinweis: Der Fokus der Aufgabenbeschreibung liegt auf dem Sicherheitsmodul.)

- Reguläre Nutzung des Smart Meter Mini-HSM mit seinem integrierten Sicherheitsmodul als Cryptographic Service Provider für die Aufgaben des Mini-HSM Users.

Bzgl. der Key-Objekte betrifft der „Wirkbetrieb des Smart Meter Mini-HSM“ die Nutzung

- der im Sicherheitsmodul hinterlegten Key-Objekte mit den Schlüsselpaaren des Mini-HSM Users selbst sowie
- der öffentlichen Schlüssel der externen Welt (ggf. in Key-Objekten im Sicherheitsmodul abgelegt)

für die kryptographischen Belange in der Kommunikation des Mini-HSM Users mit anderen Komponenten oder Usern im Smart Meter-System.

2.2.6 Außerbetriebnahme des Smart Meter Mini-HSM

Das Sicherheitsmodul stellt für die Außerbetriebnahme des Smart Meter Mini-HSM die Funktionalität zur (irreversiblen) Außerbetriebnahme des Sicherheitsmoduls zur Verfügung, siehe [TR-03109-2], Kap. 3.4.10 und 4.9.

3 File- und Objektsystem, Zugriffsregeln und Kommandoset des Sicherheitsmoduls

3.1 Initialisierung des Sicherheitsmoduls

3.1.1 Initialisierungsverfahren und -kommandos

Die Initialisierung des Sicherheitsmoduls umfasst das Laden fester und kunden- bzw. personenunabhängiger Daten in das Sicherheitsmodul. Insbesondere wird mit dem Initialisierungsfile das initiale File- und Objektsystem des Sicherheitsmoduls mit seinen Sicherheitsstrukturen und Zugriffsregeln geladen. Ggf. beinhaltet das Initialisierungsfile auch im Rahmen der CC-Zertifizierung des Sicherheitsmoduls evaluierte Patches des Sicherheitsmodul-Betriebssystems.

Initialisierungsprozesse und -kommandos für das Sicherheitsmodul werden Hersteller-spezifisch aufgesetzt und implementiert. Zu den Initialisierungsprozessen und -kommandos erfolgen keine funktionalen oder technischen Vorgaben von Seiten des vorliegenden Dokuments. Gleichwohl sind aber die Initialisierungsprozesse und -kommandos Gegenstand der CC-Zertifizierung des Sicherheitsmoduls, siehe [PP 0095].

Das Sicherheitsmodul verwaltet einen eigenen Life Cycle-Status. Zum Abschluss der Initialisierungsphase erfolgt für das Sicherheitsmodul der Übergang vom Status „nicht-initialisiert“ zu „initialisiert“ (Hersteller-spezifische Implementierung), siehe [TR-03109-2], Kap. 3.6.1.

3.1.2 Initialisierungsfile

Der Hersteller des Sicherheitsmoduls erstellt ein Initialisierungsfile, mit dem das Sicherheitsmodul initialisiert wird. Das Initialisierungsfile enthält ein auf das Smart Meter-System und das Lebenszyklus-Modell von Sicherheitsmodul und Mini-HSM zugeschnittenes initiales File- und Objektsystem mit vordefinierten DFs, EFs, Key- und PIN-Objekten, die z.T. eine spezielle Vorbelegung aufweisen (siehe unten).

Der Import öffentlicher Schlüssel in das Sicherheitsmodul wird unter Verwendung sog. Import-Schlüssel realisiert. Entsprechende Key Pair-Objekte und zugehörige Public Key-Objekte für die *initialen* Import-Schlüssel (IMP_PRV_TRANS, IMP_PUB_TRANS) und IMP_PUB_TRANS sowie für die späteren Import-Schlüssel (IMP_PRV, IMP_PUB) und IMP_PUB, die für den Import von Schlüsseln genutzt werden können, sind bereits für das Initialisierungsfile vordefiniert und werden im Rahmen der Produktion (Initialisierung) des Sicherheitsmoduls aufgebracht.

Hinweis: Grund für die doppelte Speicherung des Public Key im Key Pair-Objekt und im korrespondierenden Public Key-Objekt ist das Set der verfügbaren Kommandos des Sicherheitsmoduls.

Für die Verwendung der Import-Schlüssel und zugehörigen Key-Objekte siehe auch Kap. 2.2.2.

Mit dem Initialisierungsfile für die Initialisierung des Sicherheitsmoduls für das Mini-HSM wird mindestens folgendes initiale File- und Objektsystem mit folgenden DFs, EFs, Key- und PIN-Objekten geladen:

MF

|_____ EF.SecModTRInfo
|_____ EF.SecModAccess
|_____ EF.SecModCrypto
|_____ EF.SecModLifeCycle
|_____ PIN.HSM
|_____ Key.EPH_1
|_____ Key.EPH_2
|_____ Key.IMP_TRANS
|_____ Key.IMP_PUB_TRANS
|_____ Key.IMP
|_____ Key.IMP_PUB
|_____ *Key.USR_TLS_1* *(nur für Option 1)*
|_____ *Key.USR _SIG_1* *(nur für Option 1)*
|_____ *Key.USR _SIG_PUB_1* *(nur für Option 1)*
|_____ *Key.USR _ENC_1* *(nur für Option 1)*
|_____ *Key.USR _AUT_1* *(nur für Option 1, nur für den GW-Administrator als Mini-HSM User)*
|_____ *Key.USR _TLS_2* *(nur für Option 1)*
|_____ *Key.USR _SIG_2* *(nur für Option 1)*
|_____ *Key.USR _SIG_PUB_2* *(nur für Option 1)*
|_____ *Key.USR _ENC_2* *(nur für Option 1)*
|_____ *Key.USR _AUT_2* *(nur für Option 1, nur für den GW-Administrator als Mini-HSM User)*

Abbildung 2: Initiales File- und Objektsystem

Für die vorstehend verwendeten Bezeichnungen für die DFs, EFs, Key- und PIN-Objekte sei auf die folgenden Erklärungen bzw. Kap. 3.2.4 und 3.2.5 verwiesen. Für die Beschreibung der im Folgenden genannten Key- und PIN-Attribute siehe ebenfalls Kap. 3.2.4 und 3.2.5.

Das Kürzel USR adressiert die Rolle des Mini-HSM Users, die je nach Einsatzzweck des Smart Meter Mini-HSM unterschiedlich besetzt sein kann (siehe Kap. 2.1.2).

Für eine detaillierte Beschreibung der Optionen 1 und 2 für das File- und Objektsystem und der dahinter liegenden Zugriffsregelpolitik siehe Kap. 3.3.3.

Einträge der Art 'XY' in den folgenden Tabellen kennzeichnen Angaben im HEX-Format.

Hinsichtlich der Vorbelegung der DFs und EFs im Initialisierungsfile gilt:

MF/DF/EF	Beschreibung	File-ID	SFI	Vorbelegung
Masterfile (MF)				
MF	Masterfile.	'3F 00'	---	LCSI: „operational state - activated“
EF.SecModTRInfo	Technisches Datenfeld für die Sicherheitsmodul-relevante Spezifikation. Siehe Kap. 3.2.3.	'01 1A'	'1A'	Nutzdaten: … (Eintrag der zutreffenden

MF/DF/EF	Beschreibung	File-ID	SFI	Vorbelegung
				Information) LCSI: „operational state - activated“
EF.SecModAccess	Technisches Datenfeld für die Sicherheitsmodul-relevante PACE-Funktionalität. Siehe Kap. 3.2.3, 3.2.3.1.	'01 1B'	'1B'	Nutzdaten: Siehe [TR-03110-3]. LCSI: „operational state - activated“
EF.SecModCrypto	Technisches Datenfeld für die Sicherheitsmodul-relevante Krypto-Funktionalität. Siehe Kap. 3.2.3, 3.2.3.2.	'01 1C'	'1C'	Nutzdaten: … (Eintrag der zutreffenden Information) LCSI: „operational state - activated“
EF.SecModLifeCycle	Technisches Datenfeld für Life Cycle Status-Informationen. Siehe Kap. 3.2.3.	'01 1D'	'1D'	Nutzdaten: leer LCSI: „operational state - activated“

Tabelle 3: Initialisierungsfile – MF/DFs/EFs

Hinsichtlich der Vorbelegung der Key-Objekte im Initialisierungsfile gilt:

Key-Objekt	Beschreibung	Key-ID / Key-Name	Vorbelegung
Masterfile (MF)			
Key.EPH_1	Key Pair-Objekt für ephemerales Schlüsselpaar des Mini-HSM Users im Rahmen von ECKA-DH (Variante 2.2), siehe [TR-03109-2], Kap. 4.5.5 a), also (USR_PRV_EPH, USR_PUB_EPH).	'7E'	Key-Daten: leer Key-Type: „ECC Key Pair“ Key-LifeCycleStatus: „operational state - activated“ Key-Storage: temporär Key-UsageCounterInit: Wert 1 Key-UsageCounter: Wert 1 Key-Curve: leer Key-Usage: AT Key-CryptoAlg: ECKA-DH Key-SEID: 01 Zugriff über Key Management- und Krypto-Kommandos: siehe Kap. 3.3.3.3, insbesondere Tabellen 18 und 19
Key.EPH_2	Key Pair-Objekt für ephemerales Schlüsselpaar des Mini-HSM Users im Rahmen von ECKA-DH (Variante 2.2), siehe [TR-03109-2], Kap. 4.5.5 a), also (USR_PRV_EPH, USR_PUB_EPH).	'7F'	Key-Daten: leer Key-Type: „ECC Key Pair“ Key-LifeCycleStatus: „operational state - activated“ Key-Storage: temporär Key-UsageCounterInit: Wert 1 Key-UsageCounter: Wert 1 Key-Curve: leer Key-Usage: AT Key-CryptoAlg: ECKA-DH Key-SEID: 01

Key-Objekt	Beschreibung	Key-ID / Key-Name	Vorbelegung
			Zugriff über Key Management- und Krypto-Kommandos: siehe Kap. 3.3.3.3, insbesondere Tabellen 18 und 19
Key.IMP_TRANS	Key Pair-Objekt für Transport-Import-Schlüsselpaar, also (IMP_PRV_TRANS, IMP_PUB_TRANS).	'31'	Key-Daten: ... Key-Type: „ECC Key Pair“ Key-LifeCycleStatus: „operational state - activated“ Key-Storage: persistent Key-UsageCounterInit: … Key-UsageCounter: ... Key-Curve: ... Key-Usage: DST Key-CryptoAlg: ECDSA ohne Hashing Key-SEID: 02 Zugriff über Key Management- und Krypto-Kommandos: siehe Kap. 3.3.3.1, insbesondere Tabellen 15 und 16
Key.IMP_PUB_TRANS	Public Key-Objekt für Transport-Import-Schlüssel, also IMP_PUB_TRANS.	'00 00 00 31'	Key-Daten: ... Key-Type: „ECC Public Key“ Key-LifeCycleStatus: „operational state - activated“ Key-Storage: persistent Key-UsageCounterInit: … Key-UsageCounter: ... Key-Curve: ... Key-Usage: DST Key-CryptoAlg: ECDSA mit Hashing Key-SEID: 02 Zugriff über Key Management- und Krypto-Kommandos: siehe Kap. 3.3.3.1, insbesondere Tabellen 15 und 16
Key.IMP	Key Pair-Objekt für Import-Schlüsselpaar (Integrator-spezifisch), also (IMP_PRV, IMP_PUB).	'32'	Key-Daten: leer Key-Type: „ECC Key Pair“ Key-LifeCycleStatus: „initialisation“ Key-Storage: persistent Key-UsageCounterInit: … Key-UsageCounter: ... Key-Curve: leer Key-Usage: DST Key-CryptoAlg: ECDSA ohne Hashing Key-SEID: 02 und 01 Zugriff über Key Management- und Krypto-Kommandos: siehe Kap. 3.3.3.1 und 3.3.3.3, insbesondere Tabellen 15, 16, 18 und 19
Key.IMP_PUB	Public Key-Objekt für Import-Schlüssel (Integrator-spezifisch), also	'00 00 00 32'	Key-Daten: leer Key-Type: „ECC Public Key“ Key-LifeCycleStatus: „initialisation“

Key-Objekt	Beschreibung	Key-ID / Key-Name	Vorbelegung
	IMP_PUB.		Key-Storage: persistent Key-UsageCounterInit: … Key-UsageCounter: ... Key-Curve: leer Key-Usage: DST Key-CryptoAlg: ECDSA mit Hashing Key-SEID: 02 und 01 Zugriff über Key Management- und Krypto-Kommandos: siehe Kap. 3.3.3.1 und 3.3.3.3, insbesondere Tabellen 15, 16, 18 und 19
Key.USR_TLS_1	Key Pair-Objekt für Schlüssel des Mini-HSM Users bzgl. TLS, also (USR_TLS_PUB, USR_TLS_PRV).	'11'	Key-Daten: leer Key-Type: „ECC Key Pair“ Key-LifeCycleStatus: „initialisation“ Key-Storage: persistent Key-UsageCounterInit: nicht vorhanden Key-UsageCounter: nicht vorhanden Key-Curve: leer Key-Usage: DST Key-CryptoAlg: ECDSA ohne Hashing Key-SEID: 01 Zugriff über Key Management- und Krypto-Kommandos: siehe Kap. 3.3.3.1 und 3.3.3.3, insbesondere Tabellen 15, 16, 18 und 19
Key.USR _SIG_1	Key Pair-Objekt für Schlüssel des Mini-HSM Users bzgl. SIG, also (USR_SIG_PUB, USR_SIG_PRV).	'12'	Key-Daten: leer Key-Type: „ECC Key Pair“ Key-LifeCycleStatus: „initialisation“ Key-Storage: persistent Key-UsageCounterInit: nicht vorhanden Key-UsageCounter: nicht vorhanden Key-Curve: leer Key-Usage: DST Key-CryptoAlg: ECDSA ohne Hashing Key-SEID: 01 Zugriff über Key Management- und Krypto-Kommandos: siehe Kap. 3.3.3.1 und 3.3.3.3, insbesondere Tabellen 15, 16, 18 und 19
Key.USR _SIG__PUB_1	Public Key-Objekt für Signaturprüfschlüssel des Mini-HSM Users bzgl. SIG, also USR_SIG_PUB.	'00 00 00 12'	Key-Daten: leer Key-Type: „ECC Public Key“ Key-LifeCycleStatus: „initialisation“ Key-Storage: persistent Key-UsageCounterInit: nicht vorhanden Key-UsageCounter: nicht vorhanden Key-Curve: leer Key-Usage: DST Key-CryptoAlg: ECDSA mit Hashing

Key-Objekt	Beschreibung	Key-ID / Key-Name	Vorbelegung
			Key-SEID: 01 Zugriff über Key Management- und Krypto-Kommandos: siehe Kap. 3.3.3.1 und 3.3.3.3, insbesondere Tabellen 15, 16, 18 und 19
Key.USR _ENC_1	Key Pair-Objekt für Schlüssel des Mini-HSM Users bzgl. ENC also (USR_ENC_PUB, USR_ENC_PRV).	'13'	Key-Daten: leer Key-Type: „ECC Key Pair“ Key-LifeCycleStatus: „initialisation“ Key-Storage: persistent Key-UsageCounterInit: nicht vorhanden Key-UsageCounter: nicht vorhanden Key-Curve: leer Key-Usage: AT Key-CryptoAlg: ECKA-EG und ECDSA ohne Hashing Key-SEID: 01 Zugriff über Key Management- und Krypto-Kommandos: siehe Kap. 3.3.3.1 und 3.3.3.3, insbesondere Tabellen 15, 16, 18 und 19
Key.USR _AUT_1	Key Pair-Objekt für Schlüssel des Mini-HSM Users bzgl. AUT also (USR_AUT_PUB, USR_AUT_PRV).	'10'	Key-Daten: leer Key-Type: „ECC Key Pair“ Key-LifeCycleStatus: „initialisation“ Key-Storage: persistent Key-UsageCounterInit: nicht vorhanden Key-UsageCounter: nicht vorhanden Key-Curve: leer Key-Usage: AT Key-CryptoAlg: ECDSA ohne Hashing Key-SEID: 01 Zugriff über Key Management- und Krypto-Kommandos: siehe Kap. 3.3.3.1 und 3.3.3.3, insbesondere Tabellen 15, 16, 18 und 19
Key.USR _TLS_2	Key Pair-Objekt für Schlüssel des Mini-HSM Users bzgl. TLS, also (USR_TLS_PUB, USR_TLS_PRV).	'21'	Key-Daten: leer Key-Type: „ECC Key Pair“ Key-LifeCycleStatus: „initialisation“ Key-Storage: persistent Key-UsageCounterInit: nicht vorhanden Key-UsageCounter: nicht vorhanden Key-Curve: leer Key-Usage: DST Key-CryptoAlg: ECDSA ohne Hashing Key-SEID: 01 Zugriff über Key Management- und Krypto-Kommandos: siehe Kap. 3.3.3.1 und 3.3.3.3, insbesondere Tabellen 15, 16, 18 und 19

Key-Objekt	Beschreibung	Key-ID / Key-Name	Vorbelegung
Key.USR _SIG_2	Key Pair-Objekt für Schlüssel des Mini-HSM Users bzgl. SIG, also (USR_SIG_PUB, USR_SIG_PRV).	'22'	Key-Daten: leer Key-Type: „ECC Key Pair“ Key-LifeCycleStatus: „initialisation“ Key-Storage: persistent Key-UsageCounterInit: nicht vorhanden Key-UsageCounter: nicht vorhanden Key-Curve: leer Key-Usage: DST Key-CryptoAlg: ECDSA ohne Hashing Key-SEID: 01 Zugriff über Key Management- und Krypto-Kommandos: siehe Kap. 3.3.3.1 und 3.3.3.3, insbesondere Tabellen 15, 16, 18 und 19
Key.USR _SIG__PUB_2	Public Key-Objekt für Signaturprüfschlüssel des Mini-HSM Users bzgl. SIG, also USR_SIG_PUB.	'00 00 00 22'	Key-Daten: leer Key-Type: „ECC Public Key“ Key-LifeCycleStatus: „initialisation“ Key-Storage: persistent Key-UsageCounterInit: nicht vorhanden Key-UsageCounter: nicht vorhanden Key-Curve: leer Key-Usage: DST Key-CryptoAlg: ECDSA mit Hashing Key-SEID: 01 Zugriff über Key Management- und Krypto-Kommandos: siehe Kap. 3.3.3.1 und 3.3.3.3, insbesondere Tabellen 15, 16, 18 und 19
Key.USR _ENC_2	Key Pair-Objekt für Schlüssel des Mini-HSM Users bzgl. ENC also (USR_ENC_PUB, USR_ENC_PRV).	'23'	Key-Daten: leer Key-Type: „ECC Key Pair“ Key-LifeCycleStatus: „initialisation“ Key-Storage: persistent Key-UsageCounterInit: nicht vorhanden Key-UsageCounter: nicht vorhanden Key-Curve: leer Key-Usage: AT Key-CryptoAlg: ECKA-EG und ECDSA ohne Hashing Key-SEID: 01 Zugriff über Key Management- und Krypto-Kommandos: siehe Kap. 3.3.3.1 und 3.3.3.3, insbesondere Tabellen 15, 16, 18 und 19
Key.USR _AUT_2	Key Pair-Objekt für Schlüssel des Mini-HSM Users bzgl. AUT also (USR_AUT_PUB, USR_AUT_PRV).	'20'	Key-Daten: leer Key-Type: „ECC Key Pair“ Key-LifeCycleStatus: „initialisation“ Key-Storage: persistent Key-UsageCounterInit: nicht vorhanden Key-UsageCounter: nicht vorhanden

Key-Objekt	Beschreibung	Key-ID / Key-Name	Vorbelegung
			Key-Curve: leer Key-Usage: AT Key-CryptoAlg: ECDSA ohne Hashing Key-SEID: 01 Zugriff über Key Management- und Krypto-Kommandos: siehe Kap. 3.3.3.1 und 3.3.3.3, insbesondere Tabellen 15, 16, 18 und 19

Tabelle 4: Initialisierungsfile - Key-Objekte

Zur Notation in vorstehender Tabelle 4:

1) „Key-Daten: ...“ bedeutet, dass konkrete Schlüsseldaten einzutragen sind (Hersteller-spezifische Wahl).
2) „Key-Curve: ...“ bedeutet, dass eine konkrete Elliptische Kurve einzutragen ist (Hersteller-spezifische Wahl).
3) „Key-UsageCounterInit: ...“, „Key-UsageCounter: ...“ bedeuten, dass ein konkreter Wert für den Usage Counter und seinen Initialwert einzutragen ist (Hersteller-spezifische Wahl).

Hinweis zu Option 1: Optional können im Initialisierungsfile Key Pair-Objekte bzgl. TLS, SIG, ENC und AUT für die Schlüsselpaare des Mini-HSM Users bereits eingebracht sein, um die Vor-Personalisierung zu verschlanken. Entsprechendes gilt für die Anlage von Public Key-Objekten bzgl. SIG für die Unterstützung des Imports öffentlicher Schlüssel durch den Mini-HSM User. Um im laufenden Betrieb des Smart Meter Mini-HSM bzw. Sicherheitsmoduls einen Wechsel der Schlüssel des Mini-HSM Users technisch zu unterstützen, bietet es sich an, im Initialisierungsfile dazu sogleich zwei Sätze von Key Pair-Objekten und Public Key-Objekten für den Mini-HSM User anzulegen. Vorgeschlagen wird die Anlage der Key Pair-Objekte Key.USR_TLS_x, Key.USR_SIG_x, Key.USR_ENC_x und Key.USR_AUT_x (nur für den GW-Administrator als Mini-HSM User) sowie die Anlage der Public Key-Objekte Key.USR_SIG_PUB_x (jeweils x = 1 bzw. 2) mit den in Tabelle 4 genannten Vorbelegungen für die Key-Attribute.

Hinweis: Der GW-Administrator in der Rolle des Mini-HSM Users benötigt im Rahmen der externen Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul im SMGW sein Authentisierungsschlüsselpaar für die Erstellung eines signierten Authentisierungstokens. Für dieses Authentisierungsschlüsselpaar vorgesehen ist eigentlich das entsprechende Key Pair-Objekt bzgl. AUT. Werden jedoch seitens des GW-Administrators für das Authentisierungsschlüsselpaar seine TLS-Schlüsseldaten verwendet, so bleiben die AUT Key Pair-Objekte für den GW-Administrator im Sicherheitsmodul des Smart Meter Mini-HSM ungenutzt und das für die externe Authentisierung gegenüber dem SMGW-Sicherheitsmodul benötigte signierte Authentisierungstoken wird unter Verwendung der TLS-Schlüsseldaten erzeugt.

Hinsichtlich der Vorbelegung der PIN-Objekte im Initialisierungsfile gilt:

PIN-Objekt	Beschreibung	PIN-ID	Vorbelegung
PIN.HSM	PIN-Objekt für HSM-System-PIN (PACE-PIN).	'01'	PIN-Daten: leer PIN-LifeCycleStatus: „initialisation“

PIN-Objekt	Beschreibung	PIN-ID	Vorbelegung
			PIN-Mindestlänge: 10 Dezimalziffern SEID: 01 und 02 Zugriff über PIN Management- und Krypto-Kommandos: für SEID = 02 siehe Kap. 3.3.3.1, insbesondere Tabellen 15 und 16, für SEID = 01 siehe Kap. 3.3.3.3, insbesondere Tabellen 18 und 19

Tabelle 5: Initialisierungsfile - PIN-Objekte

3.2 File- und Objektsystem des Sicherheitsmoduls

3.2.1 Übersicht über das File- und Objektsystem

Das Sicherheitsmodul stellt eine Applikation, die auf der unterliegenden Betriebssystem-Plattform des Sicherheitsmoduls (HW/SW) mit ihren Funktionalitäten und Sicherheitsmechanismen aufsetzt und auf die Belange des Mini-HSM Users bzw. des Applikationsservers zugeschnitten ist, bereit. Diese Applikation mit ihren Sicherheitsstrukturen, Zugriffsregeln, Ordnern, Datenfeldern, PIN- und Key-Objekten ist im MF (und eventuellen späteren zugehörigen Unterordnern) angesiedelt.

Eine Übersicht über das File- und Objektsystem des Sicherheitsmoduls im initialen Zustand (mit den mindestens enthaltenen Ordnern, Datenfeldern und Key- und PIN-Objekten sowie ihrer Vorbelegung) ist in Kap. 3.1.2 gegeben. Insbesondere befinden sich direkt im MF das PIN-Objekt für die HSM-System-PIN und die mindestens für die Phasen der Produktion (Integration und Vor-Personalisierung), der Installation und Inbetriebnahme, der Personalisierung und des Normalbetriebs des Smart Meter Mini-HSM und seines Sicherheitsmoduls erforderlichen Key-Objekte.

Für Zugriffe auf die im MF (und ggf. in Unterordnern) liegenden Ordner, Datenfelder, Key- und PIN-Objekte stellt das Sicherheitsmodul ein auf die Belange des Smart Meter Mini-HSM zugeschnittenes Set an Kommandos zur Verfügung. Siehe hierzu Kap. 3.4 und 4.

Insbesondere enthält das Sicherheitsmodul im MF durch den Applikationsserver bzw. den Mini-HSM User / Integrator auslesbare bzw. schreibbare Datenfelder, in denen technische Informationen zum Sicherheitsmodul und seiner Applikation hinterlegt sind. Siehe hierzu Kap. 3.2.3.

Für die für das Sicherheitsmodul und seine Ordner, Datenfelder und Key- und PIN-Objekte gesetzten Zugriffsregeln siehe Kap. 3.3.

3.2.2 Ordner und Datenfelder

Das Sicherheitsmodul verwaltet ein hierarchisches, aus Ordnern (MF, DFs), Datenfeldern (EFs) und Key- und PIN-Objekten bestehendes File- und Objektsystem, das sich konform zur [ISO 7816-4] verhält.

Für jedes DF und EF wird ein LCSI gemäß [ISO 7816-4] mitgeführt, der (mindestens) folgende Werte annehmen kann: „initialisation“ / „operational state – activated“ / „operational state – deactivated“ / „terminated“. Von den Zuständen „operational state – activated“ und „operational state – deactivated“ gibt es keinen Schritt zurück auf den Wert „initialisation“, und vom Zustand „terminated“ gibt es keinen Schritt zurück auf einen der übrigen Werte.

Übergänge zwischen den verschiedenen Werten für den LCSI eines DFs oder EFs durch die Ausführung eines auf das betreffende Objekt zugreifenden Kommandos werden abgesehen von den zuvor gemachten Vorgaben und sofern von Seiten des vorliegenden Dokuments in den Kap. 3.4 und 4 zu den Kommando-Spezifikationen keine weitere explizite Vorgabe erfolgt, Hersteller-spezifisch festgelegt und implementiert.

3.2.3 Technische Datenfelder

Das Sicherheitsmodul enthält im MF insbesondere durch den Applikationsserver bzw. den Mini-HSM User / Integrator auslesbare bzw. schreibbare Datenfelder, in denen technische Informationen zum Sicherheitsmodul und seiner Applikation hinterlegt sind:

- EF.SecModTRInfo: Record-orientiertes Datenfeld mit technischen Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation (insbesondere Angabe der Version des vorliegenden Dokuments, auf Basis derer das vorliegende Sicherheitsmodul implementiert wurde)
- EF.SecModAccess: Transparentes Datenfeld mit technischen Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität; hier Speicherung der SecurityInfos-Datei (für weitere Detailinformationen zu diesem Datenfeld siehe Kap. 3.2.3.1)
- EF.SecModCrypto: Transparentes Datenfeld mit technischen Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität; hier Speicherung der KryptoSecurityInfos-Datei (für weitere Detailinformationen zu diesem Datenfeld siehe Kap. 3.2.3.2)
- EF.SecModLifeCycle: Record-orientiertes Datenfeld mit technischen Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls (für weitere Detailinformationen zu diesem Datenfeld siehe Kap. 3.6 bzw. [TR-03109-2], Kap. 3.6.1)

Die Technischen Datenfelder EF.SecModTRInfo, EF.SecModAccess und EF.SecModCrypto zum Hinterlegen von Informationen zu der für das Sicherheitsmodul relevanten Spezifikation und zu der vom Sicherheitsmodul unterstützten PACE- und Krypto-Funktionalität werden insbesondere im Hinblick auf mögliche spätere Migrationsschritte im Smart Meter-System als sinnvoll erachtet. Für die Verwendung des Technischen Datenfeldes EF.SecModLifeCycle siehe Kap. 3.6 bzw. [TR-03109-2], Kap. 3.6.1.

Der Zugriff auf die Technischen Datenfelder erfolgt über die üblichen Kommandos READ / UPDATE BINARY bzw. READ / UPDATE RECORD gemäß der. gesetzten Zugriffsregeln, siehe Kap. 3.3.

3.2.3.1 Technisches Datenfeld zur PACE-Funktionalität

Das Sicherheitsmodul beinhaltet im MF eine auslesbare Info-Datei zu der vom Sicherheitsmodul unterstützten PACE-Funktionalität und ihren Protokollparametern.

Für die im Folgenden verwendeten Bezeichnungen der Info-Datei siehe [TR-03110-3], Abschnitt A.1.

SecurityInfo-Datei:

- Die Datei enthält ein oder mehrere PACEInfo-Dateien (siehe unten).

- Die SecurityInfo-Datei kann vom Applikationsserver bzw. Mini-HSM User / Integrator ausgelesen werden, um Informationen darüber zu erhalten, welche PACE-Protokollparameter das Sicherheitsmodul prinzipiell unterstützt.

Das Sicherheitsmodul kann mehrere SecurityInfo-Dateien enthalten, die in der SecurityInfos-Datei zusammengefasst sind. Die SecurityInfos-Datei wird im EF.SecModAccess (siehe Kap. 3.2.3) gespeichert.

PACEInfo-Datei:

- Die Datei beinhaltet Informationen zur Implementierung von PACE und seinen Protokollparametern.
- Inhalte der Datenstruktur:
  - OID des PACE-Protokolls mit seinen Protokollparametern (siehe auch [TR-03109-3])
  - Protokoll-Version
  - Parameter-ID = ID der Elliptischen Kurve (Standardized Domain Parameter, gemäß [TR-03110-3], Abschnitt A.2.1.1)

Hinweis: Das für das Smart Meter Mini-HSM verwendete PACE-Protokoll nutzt ausschließlich das sog. Generic Mapping, siehe auch [TR-03109-3] bzw. [TR-03116-3].

Es ist keine Signatur über die SecurityInfos-Datei und kein alternativer Sicherungsmechanismus für die Authentizität dieser Datei explizit vorgesehen. Jedoch ist die SecurityInfos-Datei Betriebssystem-intern integritätsgeschützt abzulegen (Hersteller-spezifische Implementierung).

3.2.3.2 Technisches Datenfeld zur Krypto-Funktionalität

Das Sicherheitsmodul beinhaltet im MF eine auslesbare Info-Datei zu den vom Sicherheitsmodul unterstützten Krypto-Algorithmen und Elliptischen Kurven.

KryptoSecurityInfo-Datei:

- Die Datei enthält ein oder mehrere KryptoInfo-Dateien (siehe unten).
- Die KryptoSecurityInfo-Datei kann vom Applikationsserver bzw. Mini-HSM User / Integrator ausgelesen werden, um Informationen darüber zu erhalten, welche Krypto-Algorithmen und Elliptischen Kurven das Sicherheitsmodul prinzipiell unterstützt.

Das Sicherheitsmodul kann mehrere KryptoSecurityInfo-Dateien enthalten, die in der KryptoSecurityInfos-Datei zusammengefasst sind. Die KryptoSecurityInfos-Datei wird im EF.SecModKrypto (siehe Kap. 3.2.3) gespeichert.

KryptoInfo-Datei:

- Die Datei beinhaltet Informationen zum Krypto-Algorithmus und zur Elliptischen Kurve.
- Inhalte der Datenstruktur:
  - OID des Krypto-Algorithmus
  - Parameter-ID = OID der Elliptischen Kurve (Standardized Domain Parameter)

Hinweis: Die SecurityInfos-Datei ist als eigenständige Info-Datei ausspezifiziert, und es ist keine Zusammenfassung der KryptoSecurityInfos-Datei und SecurityInfos-Datei (siehe Kap. 3.2.3.1) vorgesehen. Die KryptoSecurityInfos-Datei wird als eigenständige Datei spezifiziert (in Anlehnung an die Spezifikation der SecurityInfos-Datei).

Es ist keine Signatur über die KryptoSecurityInfos-Datei und kein alternativer Sicherungsmechanismus für die Authentizität dieser Datei explizit vorgesehen. Jedoch ist die KryptoSecurityInfos-Datei Betriebssystem-intern integritätsgeschützt abzulegen (Hersteller-spezifische Implementierung).

3.2.4 Sicherheitsmodul als Speicher und Nutzer asymmetrischer Schlüssel

3.2.4.1 Schlüsselkonzept

Für das Smart Meter Mini-HSM wird die Zielsetzung eines möglichst flexiblen Schlüsselkonzeptes verfolgt. Das Sicherheitsmodul setzt hierzu auf der Idee von Key-Objekten auf, für die das Sicherheitsmodul entsprechende Key Management-Funktionen, insbesondere zum Anlegen, Löschen, Aktivieren und Deaktivieren von Key-Objekten bereitstellt.

Prinzipiell geht das Sicherheitsmodul des Smart Meter Mini-HSM mit folgendem Schlüsselmaterial um:

a) Keys des Mini-HSM Users:
   - Die Schlüsselpaare des Mini-HSM Users für TLS, SIG, ENC und AUT (nur im Falle des GW-Administrators) werden im Sicherheitsmodul gespeichert.
   - Alle Schlüsselpaare des Mini-HSM Users werden onboard im Sicherheitsmodul generiert. Öffentliche Schlüssel des Mini-HSM Users können zusätzlich im Sicherheitsmodul abgelegt werden.
   - Die öffentlichen Schlüssel des Mini-HSM Users für TLS, SIG, ENC und AUT (nur im Falle des GW-Administrators) werden in der SM-PKI zertifiziert. Die Zertifikate können im Sicherheitsmodul gespeichert werden.

b) Keys der externen Welt (z.B. des SMGW):
   - Die Schlüsselpaare der externen Welt für TLS, SIG und ENC werden durch diese selbst generiert.
   - Die Zertifikate zu den öffentlichen Schlüsseln entstammen der jeweils zugehörigen PKI (z.B. für die WAN-Kommunikation also der SM-PKI). Die öffentlichen Schlüssel und Zertifikate können im Sicherheitsmodul gespeichert werden. Die privaten Keys verbleiben bei der externen Welt.
   - Für die Nutzung der öffentlichen Keys der externen Welt in Krypto-Operationen werden diese Keys in das Sicherheitsmodul importiert, entweder innerhalb des jeweiligen Krypto-Kommandos oder aber vorab durch ein entsprechendes Import-Kommando.

c) Über die zuvor in a) und b) genannten Schlüssel hinaus generiert und verarbeitet das Sicherheitsmodul (im Rahmen der Unterstützung des Mini-HSM Users beim TLS Handshake) Diffie-Hellman-Schlüssel (DH).

3.2.4.2 Key-Objekte

Für die im Sicherheitsmodul gespeicherten und verwalteten Schlüssel gilt Folgendes:

- Speicherformen von Keys:

  - Persistent oder temporär im Sicherheitsmodul gespeicherte Key-Paare und Public Keys werden vom Betriebssystem des Sicherheitsmoduls in Form von Key-Objekten abgelegt.
  - Hinweis: Die Speicherorganisation der im Sicherheitsmodul gespeicherten Key-Objekte fällt generell unter die Administration des Sicherheitsmoduls (vor und ggf. nach Auslieferung des Smart Meter Mini-HSM, je nach Zugriffsregelpolitik).
  - Unterschieden werden je nach Speicherort globale und lokale Key-Objekte (im Sinne der [ISO 7816-4]).
  - Die Sicherheitsmodul-interne Speicherung der Key-Objekte erfolgt Betriebssystem-spezifisch, d.h. es erfolgt keine weitere technische Vorgabe zu den Betriebssystem-internen Speicherstrukturen und -mechanismen von Seiten des vorliegenden Dokuments.
- Key-Objekte werden im Sicherheitsmodul integritätsgeschützt abgelegt. Vor der Nutzung eines Key-Objektes wird dieses vom Betriebssystem auf Integrität geprüft. Siehe hierzu auch die Anforderung nach Integritätsschutz im Protection Profile [PP 0095] für das Sicherheitsmodul.
- Folgende Typen von Key-Objekten werden unterschieden:
  - Key Pair-Objekte (zur persistenten/temporären Speicherung von Schlüsselpaaren)
  - Public Key-Objekte (zur persistenten/temporären Speicherung von öffentlichen Schlüsseln)
- Referenzierung von Key-Objekten:
  - Key Pair-Objekte: Key-ID von 1 Byte Länge.
  - Public Key-Objekte: Key-Name von 4-8 Byte Länge.
  - Für Kommandos, die auf ein Key-Objekt zugreifen, wird das betreffende Key-Objekt über die sog. Key Reference referenziert. Für den Zusammenhang zwischen Key Reference und Key-ID bei Key Pair-Objekten bzw. Key-Name bei Public Key-Objekten siehe Kap. 3.2.4.2.1 bzw. 3.2.4.2.2.
- Schlüsselsuche von Key-Objekten:
  - Die Schlüsselsuche erfolgt über die Key Reference und ggf. die Anwendungsklasse des Key-Objektes (je nach Hersteller-spezifischer Implementierung des Betriebssystems des Sicherheitsmoduls).
  - Die Implementierung der Schlüsselsuche erfolgt Betriebssystem-spezifisch.
  - In Kommandos, in denen Key-Objekte zu referenzieren sind, wird neben der Key Reference auch der Parameter AT / DST zur Anzeige der Anwendungsklasse des betreffenden Key-Objektes mitgegeben. Ob das jeweilige Betriebssystem des Sicherheitsmoduls diese Information bei der Schlüsselsuche auswertet oder nicht, hängt von der Implementierung des Betriebssystems ab.
  - Die Schlüsselsuche beginnt bei lokaler Suche im aktuell selektierten DF. Wird das gesuchte Key-Objekt unter der Key Reference, ggf. zusammen mit der Anwendungsklasse, im selektierten DF nicht gefunden, so bricht die Suche ab oder wird sukzessive in den übergeordneten DFs fortgesetzt (Hersteller-spezifische Implementierung).

    Bei globaler Suche erfolgt die Schlüsselsuche im MF, ebenfalls unter der Key Reference, ggf. zusammen mit der Anwendungsklasse.

Für Key Pair-Objekte ist sowohl eine lokale wie auch globale Suche möglich (Anzeige über die Key Reference).

Für Public Key-Objekte beginnt die Suche immer im aktuell selektierten DF (lokale Suche).

- Bei der Referenzierung von Key-Objekten in Kommandos werden Key Pair-Objekte mit Tag '84' und Public Key-Objekte mit Tag '83' referenziert. Die Anwendungsklasse des Key-Objektes wird über ein entsprechendes CRT-Template (AT / DST) angezeigt.

- Management von Key-ID/Key-Name:
  - Für Key Pair-Objekte:

    Das Betriebssystem erkennt und lehnt i.a. die mehrfache Vergabe von Key-IDs innerhalb desselben Ordners für im Sicherheitsmodul gespeicherte Key Pair-Objekte ab. Hersteller-spezifisch können ggf. aber auch doppelt vergebene Key-IDs für Key Pair-Objekte im selben Ordner zulässig sein, sofern sich die Keys in ihrer Anwendungsklasse (AT / DST im Key-Attribut Key-Usage) unterscheiden.
  - Für Public Key-Objekte:

    Das Betriebssystem erkennt die doppelte Vergabe von Key-Names im Pfad eines Public Key-Objektes (auch über Anwendungsklassen von Public Key-Objekten hinweg) und lehnt eine solche doppelte Vergabe bei der Ausführung des Kommandos CREATE KEY ab.
  - Hinweis: Zum Auffinden von im Sicherheitsmodul persistent gespeicherten Key-Objekten kann z.B. eine Cryptographic Information Application (DF.CIA) nach ISO/IEC 7816-15 (siehe auch [EN 14890-1]) verwendet werden (optional). Im DF.CIA kann eine Übersicht über die im Sicherheitsmodul vergebenen Key-ID/Key-Name hinterlegt werden.

Die beiden folgenden Kapitel enthalten eine detailliertere Beschreibung der Key-Objekte, gegliedert nach den beiden Typen Key Pair-Objekt und Public Key-Objekt.

3.2.4.2.1 Key Pair-Objekte

Für die im Sicherheitsmodul gespeicherten und verwalteten Key Pair-Objekte gilt Folgendes:

- Es erfolgt ausschließlich eine onboard-Generierung von Key-Paaren im Sicherheitsmodul, die dann in einem Key Pair-Objekt abgelegt werden.
- Key Pair-Objekte werden persistent oder temporär im Sicherheitsmodul gespeichert.
- Im Key Pair-Objekt gespeichert werden die Daten des Key-Paares:
  - Private Key-Daten (Zufallszahl aus dem zugelassenen Wertebereich)
  - Public Key-Daten (Kurvenpunkt) (Speicherung optional)
- Bei der Speicherung von Key-Paaren erfolgt Hersteller-spezifisch die Ablage des Public Key-Parts oder nicht. Erfolgt keine Speicherung des Public Key im Sicherheitsmodul, so ist dieser, wenn er z.B. in Krypto-Kommandos benötigt wird, vom Betriebssystem erneut aus dem Private Key-Part zu berechnen.
- Gespeichert werden mindestens folgende Key-Paar-Zusatzinformationen (Key-Attribute):

- Key-ID (1 Byte Länge): zur Identifikation des Key Pair-Objektes, relevant für die Schlüsselsuche

  Für die eigentliche Schlüsselnummer stehen nur die untersten 7 Bit in der Key-ID zur Verfügung. Wird in einem Kommando ein Key Pair-Objekt referenziert, so wird im Sinne der [ISO 7816-4] nicht die Key-ID, sondern die sog. Key Reference übergeben. Die Key Reference stimmt in ihren untersten 7 Bit mit den untersten 7 Bit der Key-ID überein, während über das MSBit der Key Reference die Steuerung der Schlüsselsuche (1 für lokale Suche, 0 für globale Suche) erfolgt.
- Key-Type: hier „ECC Key Pair“
- Key-LifeCycleStatus: Key-Paar „initialisation“ / „operational state – activated“ / „operational state – deactivated“ (LCSI des Key Pair-Objektes)

  Für temporäre Key-Paare wird im Sicherheitsmodul nur der Wert „operational state – activated“ genutzt.
- Key-Storage: persistente / temporäre Speicherung des Key-Paars
- Key-UsageCounterInit: Initialwert eines Bedienungszählers für das Key-Paar (optionales Attribut)
- Key-UsageCounter: Aktueller Wert des Bedienungszählers für das Key-Paar (optionales Attribut)
- Key-Curve: Informationen zu den zum Key-Paar zugehörigen Kurvenparametern (OID oder Hersteller-spezifische Codierung/Speicherung, siehe hierzu auch Kap. 3.2.4.4 und [TR-03109-2], Kap. 3.4.6.1)
- Key-Usage: Informationen zum Verwendungszweck bzw. zur Anwendungsklasse des Key-Paares, hier AT = authentication bzw. DST = digital signature; ggf. relevant für die Schlüsselsuche (Hersteller-spezifische Implementierung der Schlüsselsuche)
- Key-CryptoAlg: Informationen zum Krypto-Algorithmus (ohne Bezug zur Elliptischen Kurve bzw. Schlüssellänge), für den das Key-Paar eingesetzt werden darf; hier ECDSA ohne Hashing / ECKA-EG / ECKA-DH, siehe Kap. 3.2.4.3, insbesondere Tabelle 6, und Kap. 3.2.4.5, [TR-03109-3], [TR-03111] bzw. [EN 14890-1] (OID oder Hersteller-spezifische Codierung/Speicherung, siehe hierzu auch [TR-03109-2], Kap. 3.4.6.1)

  Für ein Key Pair-Objekt müssen in Key-CryptoAlg mehrere Krypto-Algorithmen eingetragen werden können.
- Key-SEID: Information, in welchem Security Environment (SE) das Key-Paar nutzbar ist

- Für temporäre Key Pair-Objekte, deren Key-UsageCounter zu Beginn der Ausführung eines dieses Key Pair-Objekt nutzenden Kommandos einen Wert trägt, der eine einmalige weitere Nutzung dieses Key Pair-Objektes erlaubt, werden die Schlüsseldaten des Key Pair-Objektes nach ihrer Nutzung im Rahmen der betreffenden Kommando-Ausführung gelöscht.
- Eine Auswertung des Key-Attributs Key-CryptoAlg eines Key Pair-Objektes erfolgt im Rahmen der Ausführung des auf das Key Pair-Objekt zugreifenden Krypto-Kommandos bzw. des vorhergehenden Kommandos zum Setzen der Schlüsselreferenz.
- Unterstützt werden die Krypto-Kommandos GENERATE ASYMMETRIC KEY PAIR, PSO COMPUTE DIGITAL SIGNATURE, GENERAL AUTHENTICATE und INTERNAL AUTHENTICATE.

3.2.4.2.2 Public Key-Objekte

Für die im Sicherheitsmodul gespeicherten und verwalteten Public Key-Objekte gilt Folgendes:

- Hinweis: Die Generierung von Key-Paaren, deren Public Key-Part in einem Public Key-Objekt im Sicherheitsmodul abgelegt wird, erfolgt ausschließlich extern.
- Public Key-Objekte werden persistent oder temporär im Sicherheitsmodul gespeichert.
- Im Public Key-Objekt gespeichert werden die Daten des Public Key:
  - Public Key-Daten (Kurvenpunkt)
- Für persistente Public Key-Objekte werden mindestens folgende Public Key-Zusatzinformationen (Key-Attribute) gespeichert:
  - Key-Name (4-8 Byte Länge): zur Identifikation des Public Key-Objektes, relevant für die Schlüsselsuche

    Für die Schlüsselnummer steht Key-Name komplett zur Verfügung. Wird in einem Kommando ein Public Key-Objekt referenziert, so wird im Sinne der [ISO 7816-4] nicht Key-Name, sondern die sog. Key Reference übergeben. Die Key Reference stimmt aber mit Key-Name überein.
  - Key-Type: hier „ECC Public Key“
  - Key-LifeCycleStatus: Public Key „initialisation“ / „operational state – activated“ / „operational state – deactivated“ (LCSI des Public Key-Objektes)
  - Key-Storage: persistente / temporäre Speicherung des Public Keys
  - Key-UsageCounterInit: Initialwert eines Bedienungszählers für den Public Key (optionales Attribut)
  - Key-UsageCounter: Aktueller Wert des Bedienungszählers für den Public Key (optionales Attribut)
  - Key-Curve: Informationen zu den zum Public Key zugehörigen Kurvenparametern (OID oder Hersteller-spezifische Codierung/Speicherung, siehe hierzu auch Kap. 3.2.4.4 und [TR-03109-2], Kap. 3.4.6.1)
  - Key-Usage: Informationen zum Verwendungszweck bzw. zur Anwendungsklasse des Key-Paares, hier AT = authentication bzw. DST = digital signature; ggf. relevant für die Schlüsselsuche (Hersteller-spezifische Implementierung der Schlüsselsuche)
  - Key-CryptoAlg: Informationen zum Krypto-Algorithmus (ohne Bezug zur Elliptischen Kurve bzw. Schlüssellänge, für den der Public Key eingesetzt werden darf; hier ECDSA ohne Hashing / ECDSA mit Hashing / ECKA-EG / ECKA-DH, siehe Kap. 3.2.4.3, insbesondere Tabelle 6, und Kap. 3.2.4.5, [TR-03109-3], [TR-03111] bzw. [EN 14890-1] (OID oder Hersteller-spezifische Codierung/Speicherung, siehe hierzu auch [TR-03109-2], Kap. 3.4.6.1)

    Für ein Public Key-Objekt müssen in Key-CryptoAlg mehrere Krypto-Algorithmen eingetragen werden können.
  - Key-SEID: Information, in welchem Security Environment (SE) der Public Key nutzbar ist

- Eine Auswertung des Key-Attributs Key-CryptoAlg eines Public Key-Objektes erfolgt im Rahmen der Ausführung des auf das Public Key-Objekt zugreifenden Krypto-Kommandos bzw. des vorhergehenden Kommandos zum Setzen der Schlüsselreferenz.
- Unterstützt werden die Krypto-Kommandos PSO VERIFY DIGITAL SIGNATURE, PSO VERIFY CERTIFICATE und GENERAL AUTHENTICATE.

3.2.4.2.3 Key-LifeCycleStatus

Mittels des Kommandos CREATE KEY wird ein persistentes Key-Objekt mit dem Wert „initialisation“ für das Key-Attribut Key-LifeCycleStatus angelegt; das Key-Objekt ist hierbei mit seinen Betriebssystem-internen Speicherstrukturen angelegt, aber noch nicht mit Schlüsseldaten gefüllt. Im Falle eines Key Pair-Objektes wird dieses über das Kommando GENERATE ASYMMETRIC KEY PAIR mit Schlüsseldaten gefüllt und in den Status „operational state – activated“ versetzt. Im Falle eines Public Key-Objektes wird dieses über das Kommando PSO VERIFY CERTIFICATE mit Schlüsseldaten gefüllt und in den Status „operational state – activated“ überführt. Über das Kommando DEACTIVATE KEY kann ein solches (gefülltes) Key-Objekt explizit deaktiviert werden.

Ein persistentes Key Pair-Objekt im Zustand „initialisation“ ist für die Verwendung in Krypto-Kommandos mit Ausnahme des Kommandos GENERATE ASYMMETRIC KEY PAIR (in der Variante Schlüsselgenerierung mit/ohne Ausgabe des Public Key) gesperrt. Ferner ist ein persistentes Key Pair-Objekt im Zustand „operational state – deactivated“ für die Verwendung in Krypto-Kommandos mit Ausnahme des Kommandos GENERATE ASYMMETRIC KEY PAIR (in der Variante Schlüsselgenerierung mit/ohne Ausgabe des Public Key sowie in der Variante Ausgabe des Public Key ohne Schlüsselgenerierung) gesperrt. Über ein GENERATE ASYMMETRIC KEY PAIR kann ein persistentes Key Pair-Objekt im Zustand „initialisation“ oder „operational state – deactivated“ mit (neuen) Schlüsseldaten gefüllt werden. Ein Befüllen eines persistenten Key Pair-Objektes im Zustand „operational state – activated“ ist nicht möglich.

Ein persistentes Public Key-Objekt im Zustand „initialisation“ oder „operational state – deactivated“ ist für die Verwendung in Krypto-Kommandos mit Ausnahme des Kommandos PSO VERIFY CERTIFICATE, sofern es sich um das zu befüllende Public Key-Objekt handelt, gesperrt. Über ein PSO VERIFY CERTIFICATE kann ein persistentes Public Key-Objekt im Zustand „initialisation“ oder „operational state – deactivated“ mit (neuen) Schlüsseldaten gefüllt werden. Ein Befüllen eines persistenten Public Key-Objektes im Zustand „operational state – activated“ ist nicht möglich.

Für temporäre Key Pair-Objekte wird nach Kap. 3.2.4.2.1 nur der Key-LifeCycleStatus „operational state – activated“ genutzt, so dass diese Key Pair-Objekte stets über das Kommando GENERATE ASYMMETRIC KEY PAIR mit (neuen) Schlüsseldaten gefüllt werden können.

Von den Zuständen „operational state – activated“ und „operational state – deactivated“ gibt es keinen Schritt zurück auf den Wert „initialisation“.

3.2.4.3 Klassifikation der Schlüssel

Folgende Schlüsselarten werden im Smart Meter-System bzgl. ihrer Verwendung unterschieden:

TLS-Keys: Schlüssel für TLS

SIG-Keys: Schlüssel für Inhaltsdatensignatur und sonstige Signaturen (z.B. der PKI-Root-CA oder von Sub-CAs der PKI)

ENC-Keys: Schlüssel für Inhaltsdatenverschlüsselung (ElGamal Key Agreement)

AUT-Keys: Schlüssel für (externe) Authentisierung

DH-Keys: Schlüssel für Diffie-Hellman Key Agreement

Hinweis: Für die Verwendung von AUT-Keys siehe die Angaben in Kap. 3.1.2.

Folgende Tabelle 6 gibt eine detaillierte Übersicht über die im Sicherheitsmodul des Smart Meter Mini-HSM verwendeten Schlüsselarten, deren Klassifikation und diesbzgl. relevanten Key-Attribute:

Schlüsselart	**Schlüsseltyp (Key-Attribut Key-Type)**	**Speicherart (Key-Attribut Key-Storage)**	**Anwendungsklasse (Key-Attribut Key-Usage)**	**Krypto-Algorithmus (Key-Attribut Key-CryptoAlg) (siehe Tabelle 7)**
Schlüssel des Mini-HSM Users				
TLS-Key	Key Pair-Objekt	persistent	DST	ECDSA ohne Hashing: id-ecdsa-plain-signatures
SIG-Key	Key Pair-Objekt	persistent	DST	ECDSA ohne Hashing: id-ecdsa-plain-signatures
SIG-Key[1]	Public Key-Objekt	persistent	DST	ECDSA mit Hashing: id-ecdsa-plain-SHA
ENC-Key	Key Pair-Objekt	persistent	AT	ECKA-EG: id-ecka-eg und ECDSA ohne Hashing: id-ecdsa-plain-signatures
AUT-Key (nur für GW-Administrator relevant)	Key Pair-Objekt	persistent	AT	ECDSA ohne Hashing: id-ecdsa-plain-signatures
DH-Key	Key Pair-Objekt	temporär Hinweis: Verwendung nur für die Kommandos GENERATE ASYMMETRIC KEY PAIR und GENERAL AUTHENTICATE / ECKA-DH	AT	ECKA-DH: id-ecka-dh
Schlüssel der externen Welt				
TLS-Key	Public Key-Objekt	persistent oder Übergabe im Kommando	DST	ECDSA ohne Hashing: id-ecdsa-plain-signatures
SIG-Key	Public Key-Objekt	persistent oder Übergabe	DST	ECDSA ohne Hashing:

1 Falls ein Import von öffentlichen Schlüsseln unter Verwendung des SIG-Keys des Mini-HSM Users erfolgen soll, so ist zum Key Pair-Objekt bzgl. SIG ein entsprechendes Public Key-Objekt bzgl. SIG mit den öffentlichen Schlüsseldaten des im Key Pair-Objekt hinterlegten Schlüsselpaars zu betreiben.

Schlüsselart	Schlüsseltyp (Key-Attribut Key-Type)	Speicherart (Key-Attribut Key-Storage)	Anwendungsklasse (Key-Attribut Key-Usage)	Krypto-Algorithmus (Key-Attribut Key-CryptoAlg) (siehe Tabelle 7)
		im Kommando		id-ecdsa-plain-signatures
ENC-Key	Public Key-Objekt	persistent oder Übergabe im Kommando	AT	ECKA-EG: id-ecka-eg
DH-Key	Public Key-Objekt	Übergabe im Kommando GENERAL AUTHENTICATE / ECKA-DH	AT	ECKA-DH: id-ecka-dh
PKI-Schlüssel (Root-CA, Sub-CAs)				
SIG-Key	Public Key-Objekt	persistent oder Übergabe im Kommando	DST	ECDSA ohne Hashing: id-ecdsa-plain-signatures
Import-Schlüssel				
SIG-Key	Key Pair-Objekt	persistent	DST	ECDSA ohne Hashing: id-ecdsa-plain-signatures
SIG-Key	Public Key-Objekt	persistent	DST	ECDSA mit Hashing: id-ecdsa-plain-SHA

Tabelle 6: Klassifikation der Schlüssel

Zur Notation in vorstehender Tabelle 6:

In der Spalte „Krypto-Algorithmus“ ist für das Key-Attribut Key-CryptoAlg nur der jeweils relevante OID aus Tabelle 7 vermerkt. Wie in den Kap. 3.2.4.2.1 und 3.2.4.2.2 angegeben, kann der Eintrag im Key-Attribut Key-CryptoAlg aber auch durch eine entsprechende Hersteller-spezifische Codierung realisiert werden.

Hinweis: Für die Erstellung der Zertifikatsrequests zu TLS- und SIG-Keys des Mini-HSM Users wird für die Erzeugung der inneren Signatur das Kommando PSO COMPUTE DIGITAL SIGNATURE verwendet. Für die Erstellung der Zertifikatsrequests zu ENC- und AUT-Keys des Mini-HSM Users wird für die Erzeugung der inneren Signatur das Kommando INTERNAL AUTHENTICATE verwendet. Die Erstellung der Zertifikatsrequests zu TLS-, SIG- und ENC-Keys der externen Welt liegt außerhalb des Bereichs des Smart Meter Mini-HSM und seines Sicherheitsmoduls.

3.2.4.4 Domain Parameter Elliptischer Kurven

Für die im Sicherheitsmodul verwendeten Elliptischen Kurven gilt:

- Implementiert werden im Sicherheitsmodul alle Elliptischen Kurven wie in [TR-03109-3] bzw. [TR-03116-3] vorgesehen.
- Die Domain Parameter einer Elliptischen Kurve umfassen: Primzahl, erster Koeffizient, zweiter Koeffizient, Basispunkt, Ordnung des Basispunktes, Cofaktor.
- Es erfolgt Sicherheitsmodul-intern eine Betriebssystem-spezifische Ablage der Domain Parameter (Hersteller-abhängige Codierung und Speicherung).

- Für eine *gesicherte* Ablage der Domain Parameter im Sicherheitsmodul ist von Seiten des Betriebssystems zu sorgen (insbesondere Integritätsschutz).
- In Krypto-Kommandos erfolgt eine Referenzierung der Elliptischen Kurven ausschließlich über ihre OID für sog. Standardized Domain Parameter, siehe [TR-03111], Kap. 6 und [RFC 5114]. Ausnahme bildet das MSE-Kommando (SET-Variante mit AT-Template) zum Setzen der Elliptischen Kurve für das Kommando GENERAL AUTHENTICATE / Variante PACE; hier wird im MSE-Kommando die Elliptische Kurve über ihre ID wie in [TR-03110-3], Abschnitt A.2.1.1 angegeben referenziert.

3.2.4.5 Object Identifier (OID)

Im Zusammenhang mit Krypto-Funktionalität werden im Sicherheitsmodul folgende Object Identifier (OIDs) verwendet:

Elliptische Kurven / Krypto-Algorithmen / Krypto-Protokolle	**OID**
Elliptische Kurven	
Domain Parameter für Elliptische Kurven: Parameter wie in [TR-03116-3], Kap. 2.2 vorgegeben.	Siehe [TR-03111], Kap. 6 für Brainpool-Kurven bzw. [RFC 5114] für NIST-Kurven.
Krypto-Algorithmen	
ECDSA ohne Hashing: ECDSA-Parameter wie für die Implementierung der Signaturerzeugung und -verifikation vom Applikationsserver benötigt (Inhaltsdatensignatur, TLS, sonstige Signaturen) und in [TR-03116-3], Kap. 2, 3, 4, 5 und 6 vorgegeben.	id-ecdsa-plain-signatures (0.4.0.127.0.7.1.1.4.1) Siehe [TR-03111], Kap. 5.2.1.1.
ECDSA mit Hashing: ECDSA- und Hash-Parameter wie in [TR-03116-3], Kap. 2 vorgegeben.	id-ecdsa-plain-SHA (0.4.0.127.0.7.1.1.4.1.7) id-ecdsa-plain-SHA256 (0.4.0.127.0.7.1.1.4.1.3) id-ecdsa-plain-SHA384 (0.4.0.127.0.7.1.1.4.1.4) id-ecdsa-plain-SHA512 (0.4.0.127.0.7.1.1.4.1.5) Siehe [TR-03111], Kap. 5.2.1.1. id-ecdsa-plain-SHA wird nur im Key-Attribut Key-CryptoAlg verwendet, um anzuzeigen, dass bei Verwendung des Key-Objektes (hier: im Kommando PSO VERIFY CERTIFICATE) Sicherheitsmodul-intern ein Hashing stattfindet. Der zu verwendende Hash-Algorithmus wird über ein dem betreffenden Krypto-Kommando vorhergehendes MSE SET-Kommando ausgewählt, wozu id-ecdsa-plain-SHA256, id-ecdsa-plain-SHA384 bzw. id-ecdsa-plain-SHA512 zur Anzeige von SHA-256, SHA-384 bzw. SHA-512 zur Verfügung steht.
ECKA-EG (ohne KDF): Parameter wie für die Implementierung der Inhaltsdatenverschlüsselung vom Applikationsserver	id-ecka-eg (0.4.0.127.0.7.1.1.5.1) Siehe [TR-03111], Kap. 5.3.1.

Elliptische Kurven / Krypto-Algorithmen / Krypto-Protokolle	**OID**
benötigt und in [TR-03116-3], Kap. 2 und 8 vorgegeben.	
ECKA-DH (ohne KDF): Parameter wie für die Implementierung von TLS vom Applikationsserver benötigt (TLS Handshake) und in [TR-03116-3], Kap. 2, 3, 4, 5 und 6 vorgegeben.	id-ecka-dh (0.4.0.127.0.7.1.1.5.2) Siehe [TR-03111], Kap. 5.3.1.
Krypto-Protokolle	
PACE: Protokoll-Parameter wie für die Implementierung von PACE vom Applikationsserver benötigt und in [TR-03116-3], Kap. 9 vorgegeben.	id-PACE-ECDH-GM-AES-CBC-CMAC-128 (0.4.0.127.0.7.2.2.4.2.2) id-PACE-ECDH-GM-AES-CBC-CMAC-192 (0.4.0.127.0.7.2.2.4.2.3) id-PACE-ECDH-GM-AES-CBC-CMAC-256 (0.4.0.127.0.7.2.2.4.2.4) Siehe [TR-03110-3] und [TR-03111], Kap. 5.4.1.
ECKA-EG (ohne KDF): • Protokoll-Variante [TR-03111], Kap. 4.3.2.2 mit Smart Meter Mini-HSM/Sicherheitsmodul als Recipient (Protokoll-Variante 1.1 in Kap. 4.5.5 a)) • Protokoll-Variante [TR-03111], Kap. 4.3.2.2 mit Smart Meter Mini-HSM/Sicherheitsmodul als Initiator (Protokoll-Variante 1.2 in Kap. 4.5.5 a)) Protokoll-Parameter wie für die Implementierung der Inhaltsdatenverschlüsselung vom Applikationsserver benötigt und in [TR-03116-3], Kap. 2 und 8 vorgegeben.	 id-ECKA-EG-REC-woKDF (0.4.0.127.0.7.2.2.9.1.1) id-ECKA-EG-INI-woKDF (0.4.0.127.0.7.2.2.9.2.1)
ECKA-DH (ohne KDF): • Protokoll-Variante [TR-03111], Kap. 4.3.2.1 mit Smart Meter Mini-HSM/Sicherheitsmodul als Initiator oder Recipient (TLS-Client, Protokoll-Variante 2.1 in Kap. 4.5.5 a)) • Protokoll-Variante [TR-03111], Kap. 4.3.2.1 mit Smart Meter Mini-HSM/Sicherheitsmodul als Initiator oder Recipient (TLS-Server, Protokoll-Variante 2.2 in Kap. 4.5.5 a)) Protokoll-Parameter wie für die TLS-Implementierung vom Applikationsserver benötigt und in [TR-03116-3], Kap. 2, 4, 5 und 6 vorgegeben.	 id-ECKA-DH-CLT-woKDF (0.4.0.127.0.7.2.2.10.1.1) id-ECKA-DH-SRV-woKDF (0.4.0.127.0.7.2.2.10.2.1)

Tabelle 7: Object Identifier (OID)

OIDs für Krypto-Algorithmen werden im Key-Attribut Key-CryptoAlg der Key-Objekte sowie in Kommandos zum Setzen relevanter Krypto-Informationen (z.B. zur Auswahl der zu verwendenden Hash-Funktion) für ein nachfolgendes Krypto-Kommando verwendet. OIDs für Krypto-Protokolle hingegen werden für die Auswahl der Protokoll-Variante eines Krypto-Kommandos (hier: Variante des Kommandos GENERAL AUTHENTICATE) eingesetzt.

3.2.5 Sicherheitsmodul als Speicher und Nutzer von PINs

3.2.5.1 Generelles

Im Rahmen des PACE-Protokolls verwendet das Sicherheitsmodul des Smart Meter Mini-HSM eine System-PIN (im Folgenden als HSM-System-PIN bezeichnet).

Die HSM-System-PIN (bzw. deren Referenzwert) wird in einem sog. PIN-Objekt im MF des Sicherheitsmoduls gespeichert. Das für die HSM-System-PIN erforderliche PIN-Objekt wird im Initialisierungsfile für das Sicherheitsmodul bereits (als leeres Objekt) angelegt und mit spezifischen Werten für die PIN-Zusatzinformationen vorbelegt.

Die HSM-System-PIN wird initial in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ gesetzt und in der Phase „Installation + Vor-Ort-Inbetriebnahme des Smart Meter Mini-HSM“ durch den Mini-HSM User bzw. den Applikationsserver gewechselt.

3.2.5.2 PIN-Objekte

Für im Sicherheitsmodul gespeicherte und verwaltete PIN-Objekte gilt Folgendes:

- Die Referenzierung erfolgt über eine PIN-ID von 1 Byte Länge bzw. in Kommandos über die sog PIN Reference (siehe unten).
- Die PIN-Suche im Sicherheitsmodul erfolgt anhand der PIN Reference und ist Betriebssystem-spezifisch implementiert.
- Das Betriebssystem erkennt und lehnt die mehrfache Vergabe von PIN-IDs innerhalb desselben Ordners für die im Sicherheitsmodul gespeicherten PIN-Objekte ab.
- Gespeichert werden die PIN-Daten:
  - sog. PIN-Referenzwert
- Gespeichert werden mindestens folgende PIN-Zusatzinformationen (PIN-Attribute):
  - PIN-ID (zur Identifikation der PIN, relevant für die PIN-Suche)

    Für die eigentliche PIN-Nummer stehen nur die untersten 5 Bit in der PIN-ID zur Verfügung. Wird in einem Kommando ein PIN-Objekt referenziert, so wird im Sinne der [ISO 7816-4] nicht die PIN-ID, sondern die sog. PIN Reference übergeben. Die PIN Reference stimmt in ihren untersten 5 Bit mit den untersten 5 Bit der PIN-ID überein, während über das MSBit der PIN Reference die Steuerung der PIN-Suche (1 für lokale Suche, 0 für globale Suche) erfolgt.
  - PIN-LifeCycleStatus: PIN „initialisation“ / „operational state – activated“ (LCSI des PIN-Objektes)
  - PIN-Mindestlänge

Für die HSM-System-PIN ist eine Mindestlänge von 10 Dezimalziffern vorgegeben. Siehe hierzu die Vorbelegung des PIN-Objektes für die HSM-System-PIN im Initialisierungsfile in Kap. 3.1.2.

Aufgrund der vorgegebenen Mindestlänge der HSM-System-PIN von 10 Dezimalziffern kann auf einen Fehlbedienungszähler für die PIN verzichtet werden. Das Sicherheitsmodul hat ausreichende Sicherheitsmechanismen zu implementieren derart, dass ein Brute Force-Angriff auf die HSM-System-PIN bei der Verwendung der PIN im Rahmen der Ausführung des PACE-Protokolls bzw. bei der (indirekten) PIN-Prüfung bei einem Wechsel der PIN über das Kommando CHANGE

REFERENCE DATA bzgl. der für das Sicherheitsmodul angenommenen Resistenz gegen hohes Angriffspotenzial nicht möglich ist.

Die Codierung der HW-System-PIN erfolgt als Character String (ASCII-Codierung) wie in [TR-03110-3], Kap. D.2.1.4 definiert.

3.2.5.3 PIN-LifeCycleStatus

Ein PIN-Objekt im Zustand „initialisation“ ist vor seiner Nutzung für Operationen (wie z.B. GENERAL AUTHENTICATE / Variante PACE) mit PIN-Daten zu füllen. Dies wird über das Kommando CHANGE REFERENCE DATA in der Variante Setzen einer PIN ermöglicht.

3.3 Zugriffsregeln im Sicherheitsmodul

3.3.1 Zugriffsregel-Mechanismus und Sicherheitszustände

Das Betriebssystem des Sicherheitsmoduls stellt einen Zugriffsregel-Mechanismus bereit, der den Zugriff auf im Sicherheitsmodul gespeicherte bzw. verarbeitete Daten und Objekte sowie auf die im Betriebssystem verfügbaren Kommandos kontrolliert. Der Zugriffsregel-Mechanismus berücksichtigt den Life Cycle-Status des Sicherheitsmoduls, den Life Cycle-Status (LCSI) der im Sicherheitsmodul verwalteten Ordner (DFs), Datenfelder (EFs), Key- und PIN-Objekte, das Security Environment (SE) sowie die vom Sicherheitsmodul verwalteten Sicherheitszustände, d.h. wertet diese Informationen jeweils aus und schaltet entsprechend der gesetzten Zugriffsregeln den Zugriff auf Daten, Objekte bzw. Kommandos des Sicherheitsmoduls frei.

Zugriffsregeln werden Betriebssystem-intern Hersteller-spezifisch codiert. Es erfolgen diesbzgl. keine weiteren technischen Vorgaben von Seiten des vorliegenden Dokuments.

Das Sicherheitsmodul verwaltet folgenden Sicherheitszustand:

- PACE := PIN-bezogener Sicherheitszustand, der über ein erfolgreiches GENERAL AUTHENTICATE / Variante PACE gesetzt wird

  Genutzt wird dies im Rahmen des PACE-Protokolls zwischen Applikationsserver und Sicherheitsmodul.

  Hinweis: Die erfolgreiche Ausführung des PACE-Protokolls ist mit dem Aufbau eines sicheren Kanals zwischen Applikationsserver und Sicherheitsmodul verbunden, der für nachfolgende Kommandos zur Verfügung steht (Secure Messaging). Siehe hierzu auch Kap. 3.5.

Ein Zurücksetzen des zuvor genannten Sicherheitszustands des Sicherheitsmoduls ist über einen Aufruf des Kommandos MANAGE CHANNEL möglich.

Für die gegenseitige PACE-basierte Authentisierung zwischen Applikationsserver und Sicherheitsmodul und damit zum Setzen des Sicherheitszustandes PACE wird das PIN-Objekt PIN.HSM (siehe Kap. 3.1.2, Tabelle 5) herangezogen und in den Zugriffsregeln für DFs, EFs, Key- und PIN-Objekte entsprechend hinterlegt.

Das Sicherheitsmodul verwendet zur Differenzierung der Zugriffsregeln für die Ordner (DFs), Datenfelder (EFs), Key- und PIN-Objekte in den verschiedenen Phasen des Lebenszyklus-Modells für Sicherheitsmodul und Mini-HSM entsprechende Security Environments (SE). Folgende SEs sind den einzelnen Phasen des Lebenszyklus-Modells zugeordnet:

Phase des Lebenszyklus-Modells	SEID
Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM	02
Installation + Vor-Ort-Inbetriebnahme des Smart Meter Mini-HSM	01
Personalisierung des Smart Meter Mini-HSM	01
Normalbetrieb des Smart Meter Mini-HSM	01

Tabelle 8: Security Environments (SE)

Für die Ausprägung der für das Sicherheitsmodul relevanten SEs mit den ihnen jeweils zugeordneten Zugriffsregeln siehe Kap. 3.3.3 mit seinen den einzelnen Phasen des Lebenszyklus-Modells des Smart Meter Mini-HSM zugeordneten Unterkapiteln 3.3.3.1, 3.3.3.2 und 3.3.3.3.

Darüber hinaus hängt der Zugriff auf Ordner (DFs), Datenfelder (EFs), Key- und PIN-Objekte durch Kommandos des Sicherheitsmoduls von ihrem jeweiligen Life Cycle-Status (LCSI) ab. Siehe hierzu Kap. 3.3.2.

Zusammengenommen gelten die in den folgenden Kapiteln 3.3.2 und 3.3.3 genannten Zugriffsbedingungen für die im Sicherheitsmodul gespeicherten bzw. verarbeiteten Daten und Objekte sowie Kommandos in Abhängigkeit vom Life Cycle-Status des Sicherheitsmoduls, vom Life Cycle-Status (LCSI) der Ordner (DFs), Datenfelder (EFs), Key- und PIN-Objekte und vom jeweiligen SE.

Die Zugriffsregeln für das Sicherheitsmodul werden bereits im Rahmen der Produktion bzw. Initialisierung des Sicherheitsmoduls in diesem hinterlegt. Die Zugriffsregeln sind Gegenstand der CC-Zertifizierung des Sicherheitsmoduls und nach Auslieferung des Sicherheitsmoduls als initialisiertes Modul nicht mehr veränderbar.

Im Sicherheitsmodul können im Rahmen der Initialisierung des Sicherheitsmoduls weitere Ordner (DFs), Datenfelder (EFs) sowie Key- und PIN-Objekte, die über die für das initiale Initialisierungsfile in Kap. 3.1.2 vordefinierten Ordner, Datenfelder, Key- und PIN-Objekte hinausgehen, angelegt werden. Hierzu kann das initiale Initialisierungsfile aus Kap. 3.1.2 entsprechend um die zusätzlichen Ordner, Datenfelder, Key- und PIN-Objekte erweitert werden. Diese zusätzlichen Ordner, Datenfelder, Key- und PIN-Objekte und deren Inhalte liegen außerhalb der vorliegenden Spezifikation des Sicherheitsmoduls wie dieses für seinen Einsatz im Smart Meter Mini-HSM vorgesehen ist. Es muss aber sichergestellt und im Rahmen der CC-Zertifizierung des Sicherheitsmoduls geprüft werden, dass diese zusätzlichen Ordner, Datenfelder, Key- und PIN-Objekte sowie die zugehörigen Management- und Krypto-Kommandos nicht die für das Sicherheitsmodul und seinen Einsatz im Smart Meter Mini-HSM vorgesehenen Sicherheitsstrukturen verändern, umgehen oder außer Kraft setzen. Siehe hierzu auch Kap. 5.

Auch können in den nachfolgenden Phasen des Lebenszyklus-Modells – je nach Zugriffsregelpolitik des im Smart Meter Mini-HSM integrierten Sicherheitsmoduls – unter Einhaltung der Zugriffsregeln wie in Kap. 3.3.3.1 und 3.3.3.3 angegeben weitere Ordner, Datenfelder, Key- und PIN-Objekte im Sicherheitsmodul angelegt werden.

3.3.2 Kommando-Verhalten in Abhängigkeit vom LCSI der Ordner, Datenfelder, Key- und PIN-Objekte

Betrachtet werden im Folgenden die folgenden Objekttypen, die durch das Sicherheitsmodul und sein Betriebssystem bereitgestellt, verwaltet und verwendet werden:

MF / DF / EF / Key-Objekt (Key Pair-Objekt bzw. Public Key-Objekt) / PIN-Objekt.

Objekte der vorgenannten Objekttypen tragen jeweils einen LCSI. Für die vom Betriebssystem des Sicherheitsmoduls mindestens bereitzustellenden und zu verarbeitenden LCSI-Werte siehe Kap. 3.2.2, 3.2.4.2.1, 3.2.4.2.2 und 3.2.5.2.

Die folgenden Tabellen 9, 10, 11, 12, 13 und 14 geben für die verschiedenen Objekttypen jeweils an, ob bei einem Kommando-Zugriff auf ein Objekt des betreffenden Objekttyps in Abhängigkeit von seinem LCSI das betreffende Kommando prinzipiell ausgeführt werden kann (Notation: 'JA') oder das betreffende Kommando mit einer Fehlermeldung abbricht, da der gewünschte Objekt-Zugriff vom Betriebssystem des Sicherheitsmoduls prinzipiell abgelehnt wird (Notation: 'NEIN'). Die Angabe '---' in den Tabellen zeigt an, dass das betreffende Kommando für den in der jeweiligen Tabelle betrachteten Objekttyp nicht relevant ist.

Hierbei geht es nur um den *grundsätzlichen* Zugriff auf ein Objekt durch ein Kommando hinsichtlich der Auswertung des LCSI des Objektes. Etwaig weitere für ein Objekt bestehende Zugriffsbedingungen wie in Kap. 3.3.3.1 und 3.3.3.3 genannt werden in diesem Kapitel im Folgenden nicht betrachtet.

Für einen Zugriff auf ein konkretes Objekt ergibt sich im Endeffekt eine UND-Verknüpfung, bestehend zum einen aus der betreffenden LCSI-abhängigen grundsätzlichen Zugriffsbedingung (wie im Folgenden für die verschiedenen Objekttypen ausgeführt) und zum anderen aus der weiteren betreffenden Phasen-, Objekttyp- und Objekt-abhängigen spezifischen Zugriffsbedingung wie in Kap. 3.3.3.1 und 3.3.3.3, Tabellen 15, 16, 17, 18 und 19 angegeben.

Für die in den Tabellen 9, 10, 11, 12, 13 und 14 aufgeführten Kommandos siehe die Übersichtstabelle 18 in [TR-03109-2], Kap. 3.4.1 sowie die Kommandobeschreibungen in Kap. 3.4 und 4.

a) MF

MF				
Kommando	**LCSI**			
	initialisation[1]	**operational state - activated**	**operational state - deactivated**[2]	**terminated**[3]
SELECT[4]	JA	JA	JA	JA
CREATE FILE	NEIN	JA	NEIN	NEIN
DELETE FILE	NEIN	NEIN	JA	JA
ACTIVATE FILE	NEIN	JA[5]	JA	NEIN
DEACTIVATE FILE	NEIN	NEIN	JA	NEIN
TERMINATE DF	NEIN	NEIN	JA	JA

MF				
Kommando	**LCSI**			
	initialisation[1]	**operational state - activated**	**operational state - deactivated**[2]	**terminated**[3]
CREATE KEY	NEIN	JA	NEIN	NEIN

Tabelle 9: Zugriff auf MF

Anmerkungen zu den nummerierten Tabelleneinträgen in Tabelle 9:

1 Im vorliegenden Fall für das MF nicht relevant, da der LCSI des MF im Initialisierungsfile mit „operational state – activated“ vorbelegt ist und ein Rückschritt auf LCSI „initialisation“ nicht möglich ist.

2 Im vorliegenden Fall für das MF nicht relevant, da der LCSI des MF im Initialisierungsfile mit „operational state – activated“ vorbelegt ist und für das MF mit diesem LCSI-Wert das Kommando DEACTIVATE FILE nicht möglich ist. Die Belegung in dieser Spalte erfolgt nur aus Gründen der Konsistenz zu den Festlegungen für DFs (siehe Tabelle 10).

3 Im vorliegenden Fall für das MF nicht relevant, da der LCSI des MF im Initialisierungsfile mit „operational state – activated“ vorbelegt ist und für das MF mit diesem LCSI-Wert das Kommando TERMINATE DF nicht möglich ist. Die Belegung in dieser Spalte erfolgt nur aus Gründen der Konsistenz zu den Festlegungen für DFs (siehe Tabelle 10).

4 Das Kommando ist (üblicherweise) nicht mit einer Auswertung von Zugriffsregeln verbunden.

5 Erfolgreiche Kommando-Ausführung ändert am LCSI des MF nichts.

b) DFs

DF				
Kommando	**LCSI**			
	initialisation	**operational state - activated**	**operational state - deactivated**	**terminated**
SELECT[1]	JA	JA	JA	JA
CREATE FILE	JA	JA	NEIN	NEIN
DELETE FILE	JA	JA	JA	JA
ACTIVATE FILE	JA	JA[2]	JA	NEIN
DEACTIVATE FILE	JA	JA	JA[3]	NEIN
TERMINATE DF	JA	JA	JA	JA[4]
CREATE KEY	JA	JA	NEIN	NEIN

Tabelle 10: Zugriff auf DFs

Anmerkungen zu den nummerierten Tabelleneinträgen in Tabelle 10:

1 Das Kommando ist (üblicherweise) nicht mit einer Auswertung von Zugriffsregeln verbunden.

2 Erfolgreiche Kommando-Ausführung ändert am LCSI des DF nichts.

3 Erfolgreiche Kommando-Ausführung ändert am LCSI des DF nichts.

4 Erfolgreiche Kommando-Ausführung ändert am LCSI des DF nichts.

c) EFs

EF				
Kommando	**LCSI**			
	initialisation	**operational state - activated**	**operational state - deactivated**	**terminated**
SELECT[1]	JA	JA	JA	JA
DELETE FILE	JA	JA	JA	JA
ACTIVATE FILE	JA	JA[2]	JA	NEIN
DEACTIVATE FILE	JA	JA	JA[3]	NEIN
TERMINATE EF	JA	JA	JA	JA[4]
READ BINARY	JA[5]	JA	NEIN	NEIN
UPDATE BINARY	JA	JA	NEIN	NEIN
READ RECORD	JA[6]	JA	NEIN	NEIN
UPDATE RECORD	JA	JA	NEIN	NEIN
APPEND RECORD (sofern implementiert)	JA	JA	NEIN	NEIN

Tabelle 11: Zugriff auf EFs

Anmerkungen zu den nummerierten Tabelleneinträgen in Tabelle 11:

1 Das Kommando ist (üblicherweise) nicht mit einer Auswertung von Zugriffsregeln verbunden.

2 Erfolgreiche Kommando-Ausführung ändert am LCSI des EF nichts.

3 Erfolgreiche Kommando-Ausführung ändert am LCSI des EF nichts.

4 Erfolgreiche Kommando-Ausführung ändert am LCSI des EF nichts.

5 Evtl. EF noch leer (Nutzdaten noch nicht vorhanden).

6 Evtl. EF noch leer (Nutzdaten noch nicht vorhanden).

d) Key-Objekte

d1) Key Pair-Objekte

Key Pair-Objekt (persistent)			
Kommando	**LCSI (Key-LifeCycleStatus)**		
	initialisation	**operational state - activated**	**operational state - deactivated**
DELETE KEY	JA	JA	JA
ACTIVATE KEY	NEIN[1]	JA[2]	JA
DEACTIVATE KEY	NEIN	JA	JA[3]
MSE SET[4]	JA	JA	JA
GENERATE ASYMMETRIC KEY PAIR / KeyGen	JA	NEIN	JA
GENERATE ASYMMETRIC KEY PAIR / Export Public Key	NEIN[5]	JA	JA[6]
PSO COMPUTE DIGITAL SIGNATURE	NEIN	JA	NEIN
GENERAL AUTHENTICATE / ECKA-EG[7]	NEIN	JA	NEIN
GENERAL AUTHENTICATE / ECKA-DH[8]	---	---	---
INTERNAL AUTHENTICATE	NEIN	JA	NEIN

Tabelle 12: Zugriff auf Key Pair-Objekte

Anmerkungen zu den nummerierten Tabelleneinträgen in Tabelle 12:

1 Key Pair-Objekt noch leer (Schlüsseldaten noch nicht vorhanden).

2 Erfolgreiche Kommando-Ausführung ändert am LCSI des Key Pair-Objektes nichts.

3 Erfolgreiche Kommando-Ausführung ändert am LCSI des Key Pair-Objektes nichts.

4 Das Kommando ist nicht mit einer Auswertung von Zugriffsregeln verbunden.

5 Da das Key Pair-Objekt noch leer ist (Schlüsseldaten noch nicht vorhanden), macht diese Kommando-Variante im LCSI „initialisation“ keinen Sinn.

6 Das Key Pair-Objekt ist noch mit alten Schlüsseldaten gefüllt, und es erfolgt eine Ausgabe dieser alten Schlüsseldaten.

7 Relevant ist hier nur GENERAL AUTHENTICATE in der Protokoll-Variante 1.1.

8 Nicht relevant, da nur ephemerale, also temporäre Schlüssel beteiligt sind.

Für temporäre Key Pair-Objekte wird im Sicherheitsmodul nur der Key-LifeCycleStatus „operational state – activated“ verwendet, siehe Kap. 3.2.4.2.1. Ein Zugriff auf temporäre Key Pair-Objekte findet über die Kommandos GENERATE ASYMMETRIC KEY PAIR in der Variante Schlüsselgenerierung mit Ausgabe des Public Key, GENERAL AUTHENTICATE / ECKA-EG (nur Protokoll-Variante 1.2) und GENERAL AUTHENTICATE / ECKA-DH (beide Protokoll-Varianten

2.1 und 2.2) statt und ist im Key-LifeCycleStatus „operational state – activated“ möglich. Weitere Kommandos, insbesondere Key Management-Kommandos wie z.B. DELETE KEY, DEACTIVATE KEY, usw. werden für temporäre Key Pair-Objekte nicht benötigt.

d2) Public Key-Objekte

Public Key-Objekt (persistent)				
Kommando		**LCSI (Key-LifeCycleStatus)**		
		initialisation	**operational state - activated**	**operational state - deactivated**
DELETE KEY		JA	JA	JA
ACTIVATE KEY		NEIN[1]	JA[2]	JA
DEACTIVATE KEY		NEIN	JA	JA[3]
MSE SET[4]		JA	JA	JA
PSO VERIFY CERTIFICATE				
	zu befüllendes Public Key-Objekt	JA	NEIN	JA
	Signaturprüfschlüssel	NEIN	JA	NEIN
PSO VERIFY DIGITAL SIGNATURE		NEIN	JA	NEIN
GENERAL AUTHENTICATE / ECKA-EG[5]		NEIN	JA	NEIN
GENERAL AUTHENTICATE / ECKA-DH[6]		---	---	---

Tabelle 13: Zugriff auf Public Key-Objekte

Anmerkungen zu den nummerierten Tabelleneinträgen in Tabelle 13:

1 Public Key-Objekt noch leer (Schlüsseldaten noch nicht vorhanden).

2 Erfolgreiche Kommando-Ausführung ändert am LCSI des Public Key-Objektes nichts.

3 Erfolgreiche Kommando-Ausführung ändert am LCSI des Public Key-Objektes nichts.

4 Das Kommando ist nicht mit einer Auswertung von Zugriffsregeln verbunden.

5 Relevant ist hier nur GENERAL AUTHENTICATE in der Protokoll-Variante 1.2.

6 Nicht relevant, da nur ephemerale, also temporäre Schlüssel beteiligt sind.

Temporäre Public Key-Objekte sind nur bei der Übergabe von Public Keys in einzelnen Krypto-Kommandos relevant und tragen keinen Key-LifeCycleStatus, siehe Kap. 3.2.4.2.2. Daher werden temporäre Public Key-Objekte hier nicht weiter betrachtet.

e) PIN-Objekte

PIN-Objekt		
Kommando	**LCSI (PIN-LifeCycleStatus)**	
	initialisation	**operational state - activated**
CHANGE REFERENCE DATA / Variante Setzen einer PIN	JA	NEIN
CHANGE REFERENCE DATA / Variante Wechseln einer PIN	NEIN	JA
GENERAL AUTHENTICATE / PACE	NEIN	JA

Tabelle 14: Zugriff auf PIN-Objekte

3.3.3 Phasen- bzw. SE-abhängige spezifische Zugriffsbedingungen

In den folgenden Unterkapiteln werden die Phasen- bzw. SE-abhängigen spezifischen Zugriffsbedingungen für die vom Betriebssystem des Sicherheitsmoduls verwalteten und verwendeten Objekttypen und Objekte betrachtet.

Es werden grundsätzlich die folgenden beiden Optionen für die Zugriffsregelpolitik des Sicherheitsmoduls des Smart Meter Mini-HSM spezifiziert:

Option 1:

Diese Option sieht eine Administration des File- und Objektsystems im Sicherheitsmodul des Smart Meter Mini-HSM nicht nur im Rahmen der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ durch den Integrator des Smart Meter Mini-HSM vor, sondern auch eine Administration im Rahmen der Phasen „Personalisierung des Smart Meter Mini-HSM“ und „Normalbetrieb des Smart Meter Mini-HSM“ durch den Mini-HSM User selbst und ermöglicht damit mehr Flexibilität und Administrationsmöglichkeit für den Mini-HSM User als die nachfolgend beschriebene Option 2.

Option 2:

Diese Option sieht eine Administration des File- und Objektsystems im Sicherheitsmodul des Smart Meter Mini-HSM ausschließlich im Rahmen der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ durch den Integrator vor.

3.3.3.1 Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM

Im Rahmen der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ werden bestimmte Datenfelder und Key- und PIN-Objekte, die mit der Initialisierung des Sicherheitsmoduls über das Initialisierungsfile mit seinen spezifischen Ordnern, Datenfeldern, Key- und PIN-Objekten (siehe Kap. 3.1.2) auf das Sicherheitsmodul aufgebracht wurden, mit Inhalt gefüllt.

In der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ wird initial die HSM-System-PIN generiert und im Sicherheitsmodul als Referenzwert hinterlegt (Kommando CHANGE REFERENCE DATA / Variante Setzen einer PIN).

Ferner werden in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ auf die Belange des jeweiligen Mini-HSM Users zugeschnitten weitere Ordner, Datenfelder und Key-Objekte im Sicherheitsmodul angelegt.

Relevant für die Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ ist das SE mit der SEID = 02.

Für die Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“, d.h. im SE mit SEID = 02, stehen prinzipiell alle im vorliegenden Dokument in Kap. 3.4 und 4 für das Sicherheitsmodul spezifizierten Kommandos zur Verfügung. Jedoch bestehen über spezielle, dem SE mit SEID = 02 zugeordnete Zugriffsregeln Beschränkungen bzgl. der Ausführbarkeit der Kommandos des Sicherheitsmoduls. Diese Beschränkungen ergeben sich spezifisch für Ordner, Datenfelder sowie Key- und PIN-Objekte wie in den folgenden Tabellen 15 und 16 dargestellt.

Für die Zugriffsregeln in den beiden Tabellen 15 und 16 gilt für die Einträge 'PACE' folgende Interpretation: Im Einzelfall kann in der Phase der Vor-Personalisierung von der Erzwingung von PACE durch das Sicherheitsmodul selbst abgesehen werden, sofern das Sicherheitsmodul eine Verwendung von PACE zulässt und eine entsprechende Auflage in der Benutzerdokumentation zum Sicherheitsmodul formuliert wird, die die Verwendung von PACE durch den Nutzer des Sicherheitsmoduls anfordert.

Option 1:

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
MF	• SELECT: ALWAYS • DELETE FILE: NEVER (MF nicht löschbar) • DEACTIVATE FILE: NEVER (MF nicht deaktivierbar) • TERMINATE DF: NEVER (MF nicht terminierbar) • CREATE FILE: PACE • CREATE KEY: PACE
	Über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner sind im SE 01 und SE 02 verwendbar und dort mit folgenden Zugriffsregeln belegt: SE 01: • SELECT DF: ALWAYS • CREATE FILE: PACE • DELETE FILE: PACE • ACTIVATE FILE: PACE • DEACTIVATE FILE: PACE • TERMINATE DF: PACE • CREATE KEY: PACE SE 02: • SELECT DF: ALWAYS • CREATE FILE: PACE • DELETE FILE: PACE

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
	• ACTIVATE FILE: PACE • DEACTIVATE FILE: PACE • TERMINATE DF: PACE • CREATE KEY: PACE Über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs sind im SE 01 und SE 02 verwendbar und dort mit folgenden Zugriffsregeln belegt: SE 01: • SELECT EF: ALWAYS • READ BINARY / READ RECORD: PACE • UPDATE BINARY / UPDATE RECORD: PACE • APPEND RECORD: PACE (sofern das Kommando im Sicherheitsmodul implementiert ist) • DELETE FILE: PACE • ACTIVATE FILE: PACE • DEACTIVATE FILE: PACE • TERMINATE EF: PACE SE 02: • SELECT EF: ALWAYS • READ BINARY / READ RECORD: PACE • UPDATE BINARY / UPDATE RECORD: PACE • APPEND RECORD: PACE (sofern das Kommando im Sicherheitsmodul implementiert ist) • DELETE FILE: PACE • ACTIVATE FILE: PACE • DEACTIVATE FILE: PACE • TERMINATE EF: PACE Zu den Zugriffsregeln für über CREATE KEY angelegte Key-Objekte siehe untenstehende Angaben in den Tabellenzeilen zu Key Pair-Objekten und Public Key-Objekten.
EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation)	• SELECT EF: ALWAYS • READ RECORD: ALWAYS • UPDATE RECORD: NEVER, ausgenommen das Sicherheitsmodul bietet die Funktionalität des Sicherheitsmodul-Firmware-Updates (in diesem Fall gelten die Zugriffsregeln für ein Update des Datenfeldes wie im Rahmen des Firmware-Updates vorgesehen) • APPEND RECORD: PACE (sofern das Kommando im Sicherheitsmodul implementiert ist) • DELETE FILE: NEVER • ACTIVATE FILE: NEVER • DEACTIVATE FILE: NEVER • TERMINATE EF: NEVER

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität)	• SELECT EF: ALWAYS • READ BINARY: ALWAYS • UPDATE BINARY: NEVER, ausgenommen das Sicherheitsmodul bietet die Funktionalität des Sicherheitsmodul-Firmware-Updates (in diesem Fall gelten die Zugriffsregeln für ein Update des Datenfeldes wie im Rahmen des Firmware-Updates vorgesehen) • DELETE FILE: NEVER • ACTIVATE FILE: NEVER • DEACTIVATE FILE: NEVER • TERMINATE EF: NEVER
EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität)	• SELECT EF: ALWAYS • READ BINARY: ALWAYS • UPDATE BINARY: NEVER, ausgenommen das Sicherheitsmodul bietet die Funktionalität des Sicherheitsmodul-Firmware-Updates (in diesem Fall gelten die Zugriffsregeln für ein Update des Datenfeldes wie im Rahmen des Firmware-Updates vorgesehen) • DELETE FILE: NEVER • ACTIVATE FILE: NEVER • DEACTIVATE FILE: NEVER • TERMINATE EF: NEVER
EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls)	• SELECT EF: ALWAYS • READ RECORD: PACE • UPDATE RECORD: PACE • APPEND RECORD: PACE (sofern das Kommando im Sicherheitsmodul implementiert ist) • DELETE FILE: PACE • ACTIVATE FILE: PACE • DEACTIVATE FILE: PACE • TERMINATE EF: PACE
PIN-Objekte (PIN.HSM zur Speicherung der HSM-System-PIN)	PIN.HSM: • CHANGE REFERENCE DATA / Variante Setzen einer PIN: ALWAYS • CHANGE REFERENCE DATA / Variante Wechseln einer PIN: PACE • GENERAL AUTHENTICATE / PACE: ALWAYS Hinweis: Das Kommando CHANGE REFERENCE DATA in der Variante „Setzen einer PIN“ ist für das PIN-Objekt PIN.HSM für die HSM-System-PIN in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ genau einmal ausführbar. Dies wird über das Kommando-Verhalten des Kommandos CHANGE REFERENCE DATA in der Variante „Setzen einer PIN“ sowie über das PIN-Attribut PIN-LifeCycleStatus des PIN-Objektes erreicht, das im

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
	Initialisierungsfile mit dem Wert „initialisation“ vorbelegt ist.
Key Pair-Objekte	Speziell gelten für die für das Initialisierungsfile in Kap. 3.1.2 vordefinierten Key Pair-Objekte folgende Zugriffsregeln: *Key.USR_TLS_x, Key.USR_SIG_x, Key.USR_ENC_x, Key.USR_AUT_x:* Diese Key Pair-Objekte tragen das Key-Attribut Key-SEID mit Wert 01 und sind in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ nicht weiter von Interesse. Key.IMP_TRANS: • PSO COMPUTE DIGITAL SIGNATURE: PACE • DELETE KEY: PACE • DEACTIVATE KEY: PACE Key.IMP: • GENERATE ASYMMETRIC KEY PAIR (alle 3 Varianten): PACE • PSO COMPUTE DIGITAL SIGNATURE: PACE Key.EPH_x: Diese Key Pair-Objekte tragen das Key-Attribut Key-SEID mit Wert 01 und sind in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ nicht weiter von Interesse. Für alle zuvor genannten Key Pair-Objekte sind jeweils alle weiteren Kommandos zum Key Management sowie alle weiteren Krypto-Kommandos nicht zulässig (Zugriffsregel NEVER).
	Über das Kommando CREATE KEY (persistent) angelegte Key Pair-Objekte sind im SE 01 und SE 02 verwendbar. Über das Kommando CREATE KEY (persistent) angelegte Key Pair-Objekte werden automatisch mit folgenden Zugriffsregeln belegt: <u>SE 01:</u> Generell: • DELETE KEY: PACE • ACTIVATE KEY: PACE • DEACTIVATE KEY: PACE Ferner: 1) für Key Pair-Objekte der AT-Anwendungsklasse: falls Key-CryptoAlg = id-ecka-eg: • GENERATE ASYMMETRIC KEY PAIR / Export Public Key: PACE • GENERATE ASYMMETRIC KEY PAIR / KeyGen: PACE • GENERAL AUTHENTICATE / ECKA-EG: PACE falls Key-CryptoAlg = id-ecdsa-plain-signatures: • GENERATE ASYMMETRIC KEY PAIR / Export Public Key: PACE • GENERATE ASYMMETRIC KEY PAIR / KeyGen: PACE

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
	• INTERNAL AUTHENTICATE: PACE falls Key-CryptoAlg = id-ecdsa-plain-SHA: nicht relevant 2) für Key Pair-Objekte der DST-Anwendungsklasse: falls Key-CryptoAlg = id-ecdsa-plain-signatures: • GENERATE ASYMMETRIC KEY PAIR / Export Public Key: PACE • GENERATE ASYMMETRIC KEY PAIR / KeyGen: PACE • PSO COMPUTE DIGITAL SIGNATURE: PACE falls Key-CryptoAlg = id-ecdsa-plain-SHA: nicht relevant <u>SE 02:</u> Generell: • DELETE KEY: PACE • ACTIVATE KEY: PACE • DEACTIVATE KEY: PACE Die zuvor verwendete Angabe 'nicht relevant' bei einzelnen Angaben zu Key-CryptoAlg bedeutet, dass es im Smart Meter-System derzeit nicht zwingend erforderlich ist, entsprechende Key-Objekte mit dem betreffenden Wert für das Key-Attribut Key-CryptoAlg anlegen zu können, da es keine entsprechenden Anwendungsfälle gibt und solche Key-Objekte daher später im Betrieb nicht genutzt werden würden. Für die Implementierung des Kommandos CREATE KEY siehe auch Kap. [TR-03109-2], Kap. 4.4.1. Alle weiteren Kommandos zum Key Management sowie alle weiteren Krypto-Kommandos sind nicht zulässig (Zugriffsregel NEVER). Neue Key Pair-Objekte können in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ im Sicherheitsmodul angelegt werden.
Public Key-Objekte	Speziell gelten für die für das Initialisierungsfile in Kap. 3.1.2 vordefinierten Public Key-Objekte folgende Zugriffsregeln: *Key.USR_SIG_PUB_x:* Diese Public Key-Objekte tragen das Key-Attribut Key-SEID mit Wert 01 und sind in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ nicht weiter von Interesse. Key.IMP_PUB_TRANS: • PSO VERIFY CERTIFICATE: PACE • DELETE KEY: PACE • DEACTIVATE KEY: PACE Key.IMP_PUB: • PSO VERIFY CERTIFICATE: PACE Für alle zuvor genannten Public Key-Objekte sind jeweils alle weiteren Kommandos zum Key Management sowie alle weiteren Krypto-Kommandos nicht zulässig (Zugriffsregel NEVER).
	Über das Kommando CREATE KEY (persistent) angelegte Public Key-Objekte sind im SE 01 und SE 02 verwendbar.

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
	Über das Kommando CREATE KEY (persistent) angelegte Public Key-Objekte werden automatisch mit folgenden Zugriffsregeln belegt: SE 01: Generell: • DELETE KEY: PACE • ACTIVATE KEY: PACE • DEACTIVATE KEY: PACE Ferner: 1) für Public Key-Objekte der AT-Anwendungsklasse: falls Key-CryptoAlg = id-ecka-eg: • GENERAL AUTHENTICATE / ECKA-EG: PACE falls Key-CryptoAlg = id-ecdsa-plain-signatures: nicht relevant falls Key-CryptoAlg = id-ecdsa-plain-SHA: nicht relevant 2) für Public Key-Objekte der DST-Anwendungsklasse: falls Key-CryptoAlg = id-ecdsa-plain-signatures: • PSO VERIFY DIGITAL SIGNATURE: PACE falls Key-CryptoAlg = id-ecdsa-plain-SHA: • PSO VERIFY CERTIFICATE: PACE SE 02: Generell: • DELETE KEY: PACE • ACTIVATE KEY: PACE • DEACTIVATE KEY: PACE Die zuvor verwendete Angabe 'nicht relevant' bei einzelnen Angaben zu Key-CryptoAlg bedeutet, dass es im Smart Meter-System derzeit nicht zwingend erforderlich ist, entsprechende Key-Objekte mit dem betreffenden Wert für das Key-Attribut Key-CryptoAlg anlegen zu können, da es keine entsprechenden Anwendungsfälle gibt und solche Key-Objekte daher später im Betrieb nicht genutzt werden würden. Für die Implementierung des Kommandos CREATE KEY siehe auch [TR-03109-2], Kap. 4.4.1. Alle weiteren Kommandos zum Key Management sowie alle weiteren Krypto-Kommandos sind nicht zulässig (Zugriffsregel NEVER). Neue Public Key-Objekte können in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ im Sicherheitsmodul angelegt werden.

Tabelle 15: Option 1: Zugriffsregeln für MF/DFs/EFs/Key-Objekte/PIN-Objekte in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ (SEID = 02)

Option 2:

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
MF	• SELECT: ALWAYS • DELETE FILE: NEVER (MF nicht löschbar) • ACTIVATE FILE: NEVER (MF nicht aktivierbar) • DEACTIVATE FILE: NEVER (MF nicht deaktivierbar) • TERMINATE DF: NEVER (MF nicht terminierbar) • CREATE FILE: PACE • CREATE KEY: PACE
	Über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner sind im SE 01 und SE 02 verwendbar und dort mit folgenden Zugriffsregeln belegt: SE 01: • SELECT DF: ALWAYS • CREATE FILE: NEVER • DELETE FILE: NEVER • ACTIVATE FILE: NEVER • DEACTIVATE FILE: NEVER • TERMINATE DF: NEVER • CREATE KEY: NEVER SE 02: • SELECT DF: ALWAYS • CREATE FILE: PACE • DELETE FILE: PACE • ACTIVATE FILE: NEVER • DEACTIVATE FILE: NEVER • TERMINATE DF: NEVER • CREATE KEY: PACE Über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs sind im SE 01 und SE 02 verwendbar und dort mit folgenden Zugriffsregeln belegt: SE 01: • SELECT EF: ALWAYS • READ BINARY / READ RECORD: PACE • UPDATE BINARY / UPDATE RECORD: PACE • APPEND RECORD: PACE (sofern das Kommando im Sicherheitsmodul implementiert ist) • DELETE FILE: NEVER • ACTIVATE FILE: NEVER • DEACTIVATE FILE: NEVER • TERMINATE EF: NEVER SE 02: • SELECT EF: ALWAYS

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
	• READ BINARY / READ RECORD: NEVER • UPDATE BINARY / UPDATE RECORD: NEVER • APPEND RECORD: NEVER (sofern das Kommando im Sicherheitsmodul implementiert ist) • DELETE FILE: PACE • ACTIVATE FILE: NEVER • DEACTIVATE FILE: NEVER • TERMINATE EF: NEVER Zu den Zugriffsregeln für über CREATE KEY angelegte Key-Objekte siehe untenstehende Angaben in den Tabellenzeilen zu Key Pair-Objekten und Public Key-Objekten.
EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation)	• SELECT EF: ALWAYS • READ RECORD: ALWAYS • UPDATE RECORD: NEVER, ausgenommen das Sicherheitsmodul bietet die Funktionalität des Sicherheitsmodul-Firmware-Updates (in diesem Fall gelten die Zugriffsregeln für ein Update des Datenfeldes wie im Rahmen des Firmware-Updates vorgesehen) • APPEND RECORD: PACE (sofern das Kommando im Sicherheitsmodul implementiert ist) • DELETE FILE: NEVER • ACTIVATE FILE: NEVER • DEACTIVATE FILE: NEVER • TERMINATE EF: NEVER
EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität)	• SELECT EF: ALWAYS • READ BINARY: ALWAYS • UPDATE BINARY: NEVER, ausgenommen das Sicherheitsmodul bietet die Funktionalität des Sicherheitsmodul-Firmware-Updates (in diesem Fall gelten die Zugriffsregeln für ein Update des Datenfeldes wie im Rahmen des Firmware-Updates vorgesehen) • DELETE FILE: NEVER • ACTIVATE FILE: NEVER • DEACTIVATE FILE: NEVER • TERMINATE EF: NEVER
EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität)	• SELECT EF: ALWAYS • READ BINARY: ALWAYS • UPDATE BINARY: NEVER, ausgenommen das Sicherheitsmodul bietet die Funktionalität des Sicherheitsmodul-Firmware-Updates (in diesem Fall gelten die Zugriffsregeln für ein Update des Datenfeldes wie im Rahmen des Firmware-Updates vorgesehen) • DELETE FILE: NEVER • ACTIVATE FILE: NEVER • DEACTIVATE FILE: NEVER

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
	• TERMINATE EF: NEVER
EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls)	• SELECT EF: ALWAYS • READ RECORD: PACE • UPDATE RECORD: PACE • APPEND RECORD: PACE (sofern das Kommando im Sicherheitsmodul implementiert ist) • DELETE FILE: PACE oder alternativ NEVER • ACTIVATE FILE: PACE oder alternativ NEVER • DEACTIVATE FILE: PACE oder alternativ NEVER • TERMINATE EF: PACE oder alternativ NEVER
PIN-Objekte (PIN.HSM zur Speicherung der HSM-System-PIN)	PIN.HSM: • CHANGE REFERENCE DATA / Variante Setzen einer PIN: ALWAYS • CHANGE REFERENCE DATA / Variante Wechseln einer PIN: PACE • GENERAL AUTHENTICATE / PACE: ALWAYS Hinweis: Das Kommando CHANGE REFERENCE DATA in der Variante „Setzen einer PIN“ ist für das PIN-Objekt PIN.HSM für die HSM-System-PIN in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ genau einmal ausführbar. Dies wird über das Kommando-Verhalten des Kommandos CHANGE REFERENCE DATA in der Variante „Setzen einer PIN“ sowie über das PIN-Attribut PIN-LifeCycleStatus des PIN-Objektes erreicht, das im Initialisierungsfile mit dem Wert „initialisation“ vorbelegt ist.
Key Pair-Objekte	Speziell gelten für die für das Initialisierungsfile in Kap. 3.1.2 vordefinierten Key Pair-Objekte folgende Zugriffsregeln: Key.IMP_TRANS: • PSO COMPUTE DIGITAL SIGNATURE: PACE • DELETE KEY: PACE • DEACTIVATE KEY: PACE Key.IMP: • GENERATE ASYMMETRIC KEY PAIR (alle 3 Varianten): PACE • PSO COMPUTE DIGITAL SIGNATURE: PACE Key.EPH_x: Diese Key Pair-Objekte tragen das Key-Attribut Key-SEID mit Wert 01 und sind in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ nicht weiter von Interesse. Für alle zuvor genannten Key Pair-Objekte sind jeweils alle weiteren Kommandos zum Key Management sowie alle weiteren Krypto-Kommandos nicht zulässig (Zugriffsregel NEVER).
	Über das Kommando CREATE KEY (persistent) angelegte Key Pair-

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
	Objekte sind im SE 01 und SE 02 verwendbar. Über das Kommando CREATE KEY (persistent) angelegte Key Pair-Objekte werden automatisch mit folgenden Zugriffsregeln belegt: SE 01: Generell: • ACTIVATE KEY: PACE • DEACTIVATE KEY: PACE Ferner: 1) für Key Pair-Objekte der AT-Anwendungsklasse: falls Key-CryptoAlg = id-ecka-eg: • GENERATE ASYMMETRIC KEY PAIR / Export Public Key: PACE • GENERATE ASYMMETRIC KEY PAIR / KeyGen: PACE • GENERAL AUTHENTICATE / ECKA-EG: PACE falls Key-CryptoAlg = id-ecdsa-plain-signatures: • GENERATE ASYMMETRIC KEY PAIR / Export Public Key: PACE • GENERATE ASYMMETRIC KEY PAIR / KeyGen: PACE • INTERNAL AUTHENTICATE: PACE falls Key-CryptoAlg = id-ecdsa-plain-SHA: nicht relevant 2) für Key Pair-Objekte der DST-Anwendungsklasse: falls Key-CryptoAlg = id-ecdsa-plain-signatures: • GENERATE ASYMMETRIC KEY PAIR / Export Public Key: PACE • GENERATE ASYMMETRIC KEY PAIR / KeyGen: PACE • PSO COMPUTE DIGITAL SIGNATURE: PACE falls Key-CryptoAlg = id-ecdsa-plain-SHA: nicht relevant SE 02: Generell: • DELETE KEY: PACE Die zuvor verwendete Angabe 'nicht relevant' bei einzelnen Angaben zu Key-CryptoAlg bedeutet, dass es im Smart Meter-System derzeit nicht zwingend erforderlich ist, entsprechende Key-Objekte mit dem betreffenden Wert für das Key-Attribut Key-CryptoAlg anlegen zu können, da es keine entsprechenden Anwendungsfälle gibt und solche Key-Objekte daher später im Betrieb nicht genutzt werden würden. Für die Implementierung des Kommandos CREATE KEY siehe auch [TR-03109-2], Kap. 4.4.1. Alle weiteren Kommandos zum Key Management sowie alle weiteren Krypto-Kommandos sind nicht zulässig (Zugriffsregel NEVER). Neue Key Pair-Objekte können in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ im Sicherheitsmodul angelegt werden.
Public Key-Objekte	Speziell gelten für die für das Initialisierungsfile in Kap. 3.1.2

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
	vordefinierten Public Key-Objekte folgende Zugriffsregeln: Key.IMP_PUB_TRANS: • PSO VERIFY CERTIFICATE: PACE • DELETE KEY: PACE • DEACTIVATE KEY: PACE Key.IMP_PUB: • PSO VERIFY CERTIFICATE: PACE Für alle zuvor genannten Public Key-Objekte sind jeweils alle weiteren Kommandos zum Key Management sowie alle weiteren Krypto-Kommandos nicht zulässig (Zugriffsregel NEVER).
	Über das Kommando CREATE KEY (persistent) angelegte Public Key-Objekte sind im SE 01 und SE 02 verwendbar. Über das Kommando CREATE KEY (persistent) angelegte Public Key-Objekte werden automatisch mit folgenden Zugriffsregeln belegt: SE 01: Generell: • ACTIVATE KEY: PACE • DEACTIVATE KEY: PACE Ferner: 1) für Public Key-Objekte der AT-Anwendungsklasse: falls Key-CryptoAlg = id-ecka-eg: • GENERAL AUTHENTICATE / ECKA-EG: PACE falls Key-CryptoAlg = id-ecdsa-plain-signatures: nicht relevant falls Key-CryptoAlg = id-ecdsa-plain-SHA: nicht relevant 2) für Public Key-Objekte der DST-Anwendungsklasse: falls Key-CryptoAlg = id-ecdsa-plain-signatures: • PSO VERIFY DIGITAL SIGNATURE: PACE optional: falls Key-CryptoAlg = id-ecdsa-plain-SHA: • PSO VERIFY CERTIFICATE: PACE SE 02: Generell: • DELETE KEY: PACE Die zuvor verwendete Angabe 'nicht relevant' bei einzelnen Angaben zu Key-CryptoAlg bedeutet, dass es im Smart Meter-System derzeit nicht zwingend erforderlich ist, entsprechende Key-Objekte mit dem betreffenden Wert für das Key-Attribut Key-CryptoAlg anlegen zu können, da es keine entsprechenden Anwendungsfälle gibt und solche Key-Objekte daher später im Betrieb nicht genutzt werden würden. Für die Implementierung des Kommandos CREATE KEY siehe auch [TR-03109-2], Kap. 4.4.1. Alle weiteren Kommandos zum Key Management sowie alle weiteren Krypto-Kommandos sind nicht zulässig (Zugriffsregel NEVER).

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
	Neue Public Key-Objekte können in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ im Sicherheitsmodul angelegt werden.

Tabelle 16: Option 2: Zugriffsregeln für MF/DFs/EFs/Key-Objekte/PIN-Objekte in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ (SEID = 02)

Zulässig sind in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ Hersteller-spezifische zusätzliche technische Sicherungsmechanismen auf Seiten des Sicherheitsmoduls, z.B. zur Freischaltung des Sicherheitsmoduls für seine Integration und Vor-Personalisierung (Umschalten auf das Security Environment mit SEID = 02) oder für die Absicherung des Datentransports der Vor-Personalisierungsdaten zum Sicherheitsmodul.

3.3.3.2 Installation + Vor-Ort-Inbetriebnahme des Smart Meter Mini-HSM

In der Phase „Installation + Vor-Ort-Inbetriebnahme des Smart Meter Mini-HSM“ erfolgt durch den Applikationsserver bzw. Mini-HSM User ein Wechsel der initial in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ gesetzten HSM-System-PIN (Kommando CHANGE REFERENCE DATA / Variante Wechseln einer PIN).

Relevant für die Phase „Installation + Vor-Ort-Inbetriebnahme des Smart Meter Mini-HSM“ ist das SE mit der SEID = 01.

Für das PIN-Management gelten folgende Zugriffsregeln:

PIN.HSM:

- CHANGE REFERENCE DATA / Variante Setzen einer PIN: NEVER
- CHANGE REFERENCE DATA / Variante Wechseln einer PIN: PACE
- GENERAL AUTHENTICATE / PACE: ALWAYS

Hinweis:

Das Kommando CHANGE REFERENCE DATA in der Variante „Setzen einer PIN“ ist für das PIN-Objekt PIN.HSM für die HSM-System-PIN in der Phase „Installation + Vor-Ort-Inbetriebnahme des Smart Meter Mini-HSM“ nicht mehr ausführbar.

Dies wird über das Kommando-Verhalten des Kommandos CHANGE REFERENCE DATA in der Variante „Setzen einer PIN“ sowie über das PIN-Attribut PIN-LifeCycleStatus des PIN-Objektes PIN.HSM erreicht, das im Initialisierungsfile mit dem Wert „initialisation“ vorbelegt ist und über den Aufruf des Kommandos CHANGE REFERENCE DATA in der Variante „Setzen einer PIN“ in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ irreversibel auf den Wert „operational state – activated“ umgesetzt wird.

3.3.3.3 Personalisierung und Normalbetrieb des Smart Meter Mini-HSM

In den Phasen „Personalisierung des Smart Meter Mini-HSM“ und „Normalbetrieb des Smart Meter Mini-HSM“ setzt eine Verwendung des Sicherheitsmoduls in der Regel (d.h. bis auf wenige Ausnahmen) eine erfolgreiche PACE-Authentisierung zwischen Applikationsserver und Sicherheitsmodul voraus, d.h. nur ein erfolgreich zwischen Applikationsserver und

Sicherheitsmodul ausgeführtes PACE-Protokoll schaltet das Sicherheitsmodul zu seiner weiteren Nutzung in den Phasen „Personalisierung des Smart Meter Mini-HSM“ und „Normalbetrieb des Smart Meter Mini-HSM“ frei.

Administrationstätigkeiten des Mini-HSM Users am Sicherheitsmodul im Smart Meter Mini-HSM setzen derzeit keine weitere Authentisierung des Mini-HSM Users gegenüber dem Sicherheitsmodul im Smart Meter Mini-HSM voraus.

Relevant für die Phasen „Personalisierung des Smart Meter Mini-HSM“ und „Normalbetrieb des Smart Meter Mini-HSM“ ist das SE mit der SEID = 01.

Für die Phasen „Personalisierung des Smart Meter Mini-HSM“ und „Normalbetrieb des Smart Meter Mini-HSM“ stehen (im SE mit SEID = 01) die in der folgenden Tabelle 17 gelisteten Kommandos des Sicherheitsmoduls wie im vorliegenden Dokument in Kap. 3.4 und 4 spezifiziert zur Verfügung.

Zur Notation in Tabelle 17:

In der folgenden Tabelle 17 bedeutet die Angabe 'X', dass für das jeweilige Kommando der betreffende Sicherheitszustand im Sicherheitsmodul gesetzt sein muss. Findet sich kein Eintrag wie 'X' oder anderes, so bestehen keine Nutzungsbeschränkungen für das jeweilige Kommando. Die Angabe '…' kennzeichnet, dass je nach Situation ein 'X' zu setzen ist oder nicht und die Zugriffsbedingung durch das Sicherheitsmodul entsprechend durchgesetzt wird, siehe dazu jeweils die zugehörigen Angaben in der Spalte „Bemerkung“. Mit der Angabe (X) wird gekennzeichnet, dass die aufrufende Stelle bei Aufruf des Kommandos entscheidet, ob der betreffende Sicherheitszustand ausgenutzt werden soll oder nicht; die Anzeige der aufrufenden Stelle erfolgt bzgl. des Sicherheitszustandes PACE über das CLA-Byte des betreffenden Kommandos. Die Angabe '---' schließlich bedeutet 'keine Zugriffsbedingung, da nicht relevant'.

Ferner ist die Notation 'X' in Tabelle 17 in der Spalte 'PACE' dahingehend zu verstehen, dass das betreffende Kommando in dem mittels des PACE-Protokolls aufgebauten sicheren Kanal zwischen Mini-HSM und Sicherheitsmodul, also mit Secure Messaging gemäß Kap. 3.5 ausgeführt wird. Für die Bedeutung der Notation '(X)' in der Spalte 'PACE' siehe die zugehörigen Angaben in der Spalte 'Bemerkung'.

Kommando	**PACE**	**Bemerkung**
Key Management		
CREATE KEY	X	
DELETE KEY	X	Weitere Zugriffsbeschränkungen je nach Key-Objekt, siehe Tabellen 18 und 19.
ACTIVATE KEY	X	Weitere Zugriffsbeschränkungen je nach Key-Objekt, siehe Tabellen 18 und 19.
DEACTIVATE KEY	X	Weitere Zugriffsbeschränkungen je nach Key-Objekt, siehe Tabellen 18 und 19.
Krypto-Kommandos (asymmetrische Kryptographie)		
GENERATE ASYMMETRIC KEY PAIR / KeyGen (Schlüsselgenerierung mit/ohne Export des Public Key)	X	Weitere Zugriffsbeschränkungen je nach Key-Objekt, siehe Tabellen 18 und 19.
GENERATE ASYMMETRIC KEY PAIR / Export Public Key (nur Schlüsselexport, ohne Schlüsselgenerierung)	X	

Kommando	PACE	Bemerkung
PSO COMPUTE DIGITAL SIGNATURE	X	
PSO VERIFY DIGITAL SIGNATURE / Variante ohne Übergabe des Public Key im Kommando	X	
PSO VERIFY DIGITAL SIGNATURE / Variante mit Übergabe des Public Key im Kommando	(X)	Das Kommando kann auf Seiten des Sicherheitsmoduls prinzipiell mit und ohne Secure Messaging ausgeführt werden und verlangt damit nicht notwendig einen gesetzten Sicherheitszustand PACE. Die das Kommando aufrufende Stelle zeigt im CLA-Byte entsprechend an, ob das Kommando mit oder ohne Secure Messaging ausgeführt werden soll.
PSO VERIFY CERTIFICATE	X	
GENERAL AUTHENTICATE / ECKA (-EG, -DH)	X	
GENERAL AUTHENTICATE / PACE		
INTERNAL AUTHENTICATE	X	
Management des Security Environments (SE)		
MSE SET		
MSE RESTORE		
Zufallszahlengenerierung		
GET CHALLENGE	(X)	Das Kommando kann auf Seiten des Sicherheitsmoduls prinzipiell mit und ohne Secure Messaging ausgeführt werden und verlangt damit nicht notwendig einen gesetzten Sicherheitszustand PACE. Die das Kommando aufrufende Stelle zeigt im CLA-Byte entsprechend an, ob das Kommando mit oder ohne Secure Messaging ausgeführt werden soll.
PIN-Management		
CHANGE REFERENCE DATA / Variante Wechseln einer PIN	X	Weitere Zugriffsbeschränkungen je nach PIN; für die HSM-System-PIN siehe Tabellen 18 und 19.
CHANGE REFERENCE DATA / Variante Setzen einer PIN	---	Diese Kommando-Variante ist in den Phasen „Personalisierung des Smart Meter Mini-HSM“ und „Normalbetrieb des Smart Meter Mini-HSM“ nicht relevant. Siehe hierzu auch die diesbzgl. Angaben in Tabellen 18 und 19 zum PIN-Objekt für die HSM-System-PIN.
Zugriff auf transparente EF		
READ BINARY	...	Zugriffsbeschränkungen je nach EF, siehe Tabellen 18 und 19.
UPDATE BINARY	...	Zugriffsbeschränkungen je nach EF, siehe Tabellen 18 und 19.

Kommando	PACE	Bemerkung
Zugriff auf Record-orientierte EF		
READ RECORD	...	Zugriffsbeschränkungen je nach EF, siehe Tabellen 18 und 19.
UPDATE RECORD	...	Zugriffsbeschränkungen je nach EF, siehe Tabellen 18 und 19.
APPEND RECORD (optional)	...	Zugriffsbeschränkungen je nach EF, siehe Tabellen 18 und 19.
Kartenmanagement / Management des Filesystems		
SELECT (MF/DF/EF)		
CREATE FILE	X	Weitere Zugriffsbeschränkungen je nach File möglich.
DELETE FILE	X	Weitere Zugriffsbeschränkungen je nach File möglich.
ACTIVATE FILE	X	Weitere Zugriffsbeschränkungen je nach File möglich.
DEACTIVATE FILE	X	Weitere Zugriffsbeschränkungen je nach File möglich.
TERMINATE DF	X	Weitere Zugriffsbeschränkungen je nach File möglich.
TERMINATE EF	X	Weitere Zugriffsbeschränkungen je nach File möglich.
Management des Life Cycle-Status		
TERMINATE CARD USAGE	X	
Management der Applikationsebene		
MANAGE CHANNEL		

Tabelle 17: Zugriffsregeln für Kommandos in den Phasen „Personalisierung des Smart Meter Mini-HSM“ und „Normalbetrieb des Smart Meter Mini-HSM“ (SEID = 01)

Ferner gelten für Ordner, Datenfelder sowie Key- und PIN-Objekte (für die Bezeichner siehe auch Kap. 3.1.2) folgende Festlegungen:

Zur Notation in den Tabellen 18 und 19:

Die Notation 'PACE' in den Tabellen 18 und 19 ist dahingehend zu verstehen, dass für den Fall des gesetzten Sicherheitszustandes PACE das betreffende Kommando in dem mittels des PACE-Protokolls aufgebauten sicheren Kanal zwischen Applikationsserver und Sicherheitsmodul, also mit Secure Messaging gemäß Kap. 3.5 ausgeführt wird.

Option 1:

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
MF	MF: • SELECT: ALWAYS • DELETE FILE: NEVER (MF nicht löschbar) • DEACTIVATE FILE: NEVER (MF nicht deaktivierbar) • TERMINATE DF: NEVER (MF nicht terminierbar) • CREATE FILE: PACE • CREATE KEY: PACE
	Über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner sind nur im SE 01 verwendbar und dort mit folgenden Zugriffsregeln belegt: • SELECT DF: ALWAYS • CREATE FILE: PACE • DELETE FILE: PACE • ACTIVATE FILE: PACE • DEACTIVATE FILE: PACE • TERMINATE DF: PACE • CREATE KEY: PACE Über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs sind nur im SE 01 verwendbar und dort mit folgenden Zugriffsregeln belegt: • SELECT EF: ALWAYS • READ BINARY / READ RECORD: PACE • UPDATE BINARY / UPDATE RECORD: PACE • APPEND RECORD: PACE (sofern das Kommando im Sicherheitsmodul implementiert ist) • DELETE FILE: PACE • ACTIVATE FILE: PACE • DEACTIVATE FILE: PACE • TERMINATE EF: PACE Zu den Zugriffsregeln für über CREATE KEY angelegte Key-Objekte siehe untenstehende Angaben in den Tabellenzeilen zu Key Pair-Objekten und Public Key-Objekten.
EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation)	• SELECT EF: ALWAYS • READ RECORD: ALWAYS • UPDATE RECORD: NEVER, ausgenommen das Sicherheitsmodul bietet die Funktionalität des Sicherheitsmodul-Firmware-Updates (in diesem Fall gelten die Zugriffsregeln für ein Update des Datenfeldes wie im Rahmen des Firmware-Updates vorgesehen) • APPEND RECORD: PACE (sofern das Kommando im Sicherheitsmodul implementiert ist) • DELETE FILE: NEVER

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
	• ACTIVATE FILE: NEVER • DEACTIVATE FILE: NEVER • TERMINATE EF: NEVER
EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität)	• SELECT EF: ALWAYS • READ BINARY: ALWAYS • UPDATE BINARY: NEVER, ausgenommen das Sicherheitsmodul bietet die Funktionalität des Sicherheitsmodul-Firmware-Updates (in diesem Fall gelten die Zugriffsregeln für ein Update des Datenfeldes wie im Rahmen des Firmware-Updates vorgesehen) • DELETE FILE: NEVER • ACTIVATE FILE: NEVER • DEACTIVATE FILE: NEVER • TERMINATE EF: NEVER
EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität)	• SELECT EF: ALWAYS • READ BINARY: ALWAYS • UPDATE BINARY: NEVER, ausgenommen das Sicherheitsmodul bietet die Funktionalität des Sicherheitsmodul-Firmware-Updates (in diesem Fall gelten die Zugriffsregeln für ein Update des Datenfeldes wie im Rahmen des Firmware-Updates vorgesehen) • DELETE FILE: NEVER • ACTIVATE FILE: NEVER • DEACTIVATE FILE: NEVER • TERMINATE EF: NEVER
EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls)	• SELECT EF: ALWAYS • READ RECORD: PACE • UPDATE RECORD: PACE • APPEND RECORD: PACE (sofern das Kommando im Sicherheitsmodul implementiert ist) • DELETE FILE: PACE • ACTIVATE FILE: PACE • DEACTIVATE FILE: PACE • TERMINATE EF: PACE
PIN-Objekte (PIN.HSM zur Speicherung der HSM-System-PIN)	Generell: • PINs können nicht ausgelesen werden • Zugriff über PIN-Management-Kommandos bzw. Krypto-Kommandos wie in oben stehender Tabelle 17 angegeben, mit untenstehenden Ausnahmen für PIN.HSM • zusätzlich zu den Angaben in Tabelle 17 bestehen je nach PIN-Management-Kommando ggf. weitere Zugriffsbeschränkungen in Abhängigkeit vom PIN-LifeCycleStatus des betreffenden PIN-Objektes: für Details siehe die Kommando-Spezifikation in [TR-03109-2], Kap. 4.8

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
	PIN.HSM: • CHANGE REFERENCE DATA / Variante Setzen einer PIN: NEVER • CHANGE REFERENCE DATA / Variante Wechseln einer PIN: PACE • GENERAL AUTHENTICATE / PACE: ALWAYS Hinweis: Das Kommando CHANGE REFERENCE DATA in der Variante „Setzen einer PIN“ ist für das PIN-Objekt PIN.HSM für die HSM-System-PIN in den Phasen „Personalisierung des Smart Meter Mini-HSM“ und „Normalbetrieb des Smart Meter Mini-HSM“ nicht mehr ausführbar. Dies wird über das Kommando-Verhalten des Kommandos CHANGE REFERENCE DATA in der Variante „Setzen einer PIN“ sowie über das PIN-Attribut PIN-LifeCycleStatus des PIN-Objektes PIN.HSM erreicht, das im Initialisierungsfile mit dem Wert „initialisation“ vorbelegt ist und über den Aufruf des Kommandos CHANGE REFERENCE DATA in der Variante „Setzen einer PIN“ in der Phase „Integration + Vor-Personalisierung von Sicherheitsmodul und Mini-HSM“ irreversibel auf den Wert „operational state – activated“ umgesetzt wird.
Key Pair-Objekte	Generell: • Schlüsselpaare werden ausschließlich onboard generiert (persistente / temporäre Speicherung im Sicherheitsmodul) • Private Keys verbleiben grundsätzlich im Sicherheitsmodul und können nicht ausgelesen werden • zugehörige Public Keys können ausgelesen werden • zusätzlich zu den Angaben in Tabelle 17 bestehen je nach Key Management- bzw. Krypto-Kommando ggf. weitere Zugriffsbeschränkungen in Abhängigkeit vom Key Pair-Objekt und seinem Key-LifeCycleStatus: für Details siehe die folgenden Angaben und die jeweilige Kommando-Spezifikation in [TR-03109-2], Kap. 3.4.5, 3.4.6, 4.4 und 4.5 sowie Kap. 3.2.4.2.3 und 3.3.2 d1)
	Speziell gelten für die für das Initialisierungsfile in Kap. 3.1.2 vordefinierten Key Pair-Objekte folgende Zugriffsregeln: *Key.USR_TLS_x, Key.USR_SIG_x:* • GENERATE ASYMMETRIC KEY PAIR / Export Public Key: PACE • GENERATE ASYMMETRIC KEY PAIR / KeyGen: PACE • PSO COMPUTE DIGITAL SIGNATURE: PACE • DELETE KEY: PACE • ACTIVATE KEY: PACE • DEACTIVATE KEY: PACE *Key.USR_ENC_x:* • GENERATE ASYMMETRIC KEY PAIR / Export Public Key: PACE • GENERATE ASYMMETRIC KEY PAIR / KeyGen: PACE • INTERNAL AUTHENTICATE: PACE

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
	• GENERAL AUTHENTICATE / ECKA-EG: PACE • DELETE KEY: PACE • ACTIVATE KEY: PACE • DEACTIVATE KEY: PACE *Key.USR_AUT_x:* • GENERATE ASYMMETRIC KEY PAIR / Export Public Key: PACE • GENERATE ASYMMETRIC KEY PAIR / KeyGen: PACE • INTERNAL AUTHENTICATE: PACE • DELETE KEY: PACE • ACTIVATE KEY: PACE • DEACTIVATE KEY: PACE Key.IMP_TRANS: Dieses Key Pair-Objekt ist in den Phasen „Personalisierung des Smart Meter Mini-HSM“ und „Normalbetrieb des Smart Meter Mini-HSM“ nicht mehr im Sicherheitsmodul vorhanden. Key.IMP: • GENERATE ASYMMETRIC KEY PAIR (alle 3 Varianten): PACE • PSO COMPUTE DIGITAL SIGNATURE: PACE • DELETE KEY: PACE • ACTIVATE KEY: PACE • DEACTIVATE KEY: PACE Key.EPH_x: • GENERATE ASYMMETRIC KEY PAIR / KeyGen mit Ausgabe des Public Key: PACE • GENERAL AUTHENTICATE / ECKA-DH: PACE Für alle zuvor genannten Key Pair-Objekte des Initialisierungsfiles wie in Kap. 3.1.2 definiert sind jeweils alle weiteren Kommandos zum Key Management sowie alle weiteren Krypto-Kommandos nicht zulässig (Zugriffsregel NEVER).
	Über das Kommando CREATE KEY (persistent) angelegte Key Pair-Objekte sind nur im SE 01 verwendbar. Über das Kommando CREATE KEY (persistent) angelegte Key Pair-Objekte werden automatisch mit folgenden Zugriffsregeln belegt: Generell: • DELETE KEY: PACE • ACTIVATE KEY: PACE • DEACTIVATE KEY: PACE Ferner: 1) für Key Pair-Objekte der AT-Anwendungsklasse: falls Key-CryptoAlg = id-ecka-eg:

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
	• GENERATE ASYMMETRIC KEY PAIR / Export Public Key: PACE • GENERATE ASYMMETRIC KEY PAIR / KeyGen: PACE • GENERAL AUTHENTICATE / ECKA-EG: PACE falls Key-CryptoAlg = id-ecdsa-plain-signatures: • GENERATE ASYMMETRIC KEY PAIR / Export Public Key: PACE • GENERATE ASYMMETRIC KEY PAIR / KeyGen: PACE • INTERNAL AUTHENTICATE: PACE falls Key-CryptoAlg = id-ecdsa-plain-SHA: nicht relevant 2) für Key Pair-Objekte der DST-Anwendungsklasse: falls Key-CryptoAlg = id-ecdsa-plain-signatures: • GENERATE ASYMMETRIC KEY PAIR / Export Public Key: PACE • GENERATE ASYMMETRIC KEY PAIR / KeyGen: PACE • PSO COMPUTE DIGITAL SIGNATURE: PACE falls Key-CryptoAlg = id-ecdsa-plain-SHA: nicht relevant Die zuvor verwendete Angabe 'nicht relevant' bei einzelnen Angaben zu Key-CryptoAlg bedeutet, dass es im Smart Meter-System derzeit nicht zwingend erforderlich ist, entsprechende Key-Objekte mit dem betreffenden Wert für das Key-Attribut Key-CryptoAlg anlegen zu können, da es keine entsprechenden Anwendungsfälle gibt und solche Key-Objekte daher später im Betrieb nicht genutzt werden würden. Für die Implementierung des Kommandos CREATE KEY siehe auch [TR-03109-2], Kap. 4.4.1. Alle weiteren Kommandos zum Key Management sowie alle weiteren Krypto-Kommandos sind nicht zulässig (Zugriffsregel NEVER). Neue Key Pair-Objekte können in den Phasen „Personalisierung des Smart Meter Mini-HSM“ und „Normalbetrieb des Smart Meter Mini-HSM“ im Sicherheitsmodul angelegt werden.
Public Key-Objekte	Generell: • Public Keys können importiert werden (temporäre / persistente Speicherung im Sicherheitsmodul) • zusätzlich zu den Angaben in Tabelle 17 bestehen je nach Key Management- bzw. Krypto-Kommando ggf. weitere Zugriffsbeschränkungen in Abhängigkeit vom Public Key-Objekt und seinem Key-LifeCycleStatus: für Details siehe die folgenden Angaben und die jeweilige Kommando-Spezifikation in [TR-03109-2], Kap. 3.4.5, 3.4.6, 4.4 und 4.5 sowie Kap. 3.2.4.2.3 und 3.3.2 d2)
	Speziell gelten für die für das Initialisierungsfile in Kap. 3.1.2 vordefinierten Public Key-Objekte folgende Zugriffsregeln: *Key.USR_SIG_PUB_x:* • PSO VERIFY CERTIFICATE: PACE • DELETE KEY: PACE • ACTIVATE KEY: PACE

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
	• DEACTIVATE KEY: PACE Key.IMP_PUB_TRANS: Dieses Public Key-Objekt ist in den Phasen „Personalisierung des Smart Meter Mini-HSM“ und „Normalbetrieb des Smart Meter Mini-HSM“ nicht mehr im Sicherheitsmodul vorhanden. Key.IMP_PUB: • PSO VERIFY CERTIFICATE: PACE • DELETE KEY: PACE • ACTIVATE KEY: PACE • DEACTIVATE KEY: PACE Für alle zuvor genannten Public Key-Objekte des Initialisierungsfiles wie in Kap. 3.1.2 definiert sind jeweils alle weiteren Kommandos zum Key Management sowie alle weiteren Krypto-Kommandos nicht zulässig (Zugriffsregel NEVER).
	Über das Kommando CREATE KEY (persistent) angelegte Public Key-Objekte sind nur im SE 01 verwendbar. Über das Kommando CREATE KEY (persistent) angelegte Public Key-Objekte werden automatisch mit folgenden Zugriffsregeln belegt: Generell: • DELETE KEY: PACE • ACTIVATE KEY: PACE • DEACTIVATE KEY: PACE Ferner: 1) für Public Key-Objekte der AT-Anwendungsklasse: falls Key-CryptoAlg = id-ecka-eg: • GENERAL AUTHENTICATE / ECKA-EG: PACE falls Key-CryptoAlg = id-ecdsa-plain-signatures: nicht relevant falls Key-CryptoAlg = id-ecdsa-plain-SHA: nicht relevant 2) für Public Key-Objekte der DST-Anwendungsklasse: falls Key-CryptoAlg = id-ecdsa-plain-signatures: • PSO VERIFY DIGITAL SIGNATURE: PACE falls Key-CryptoAlg = id-ecdsa-plain-SHA: • PSO VERIFY CERTIFICATE: PACE Die zuvor verwendete Angabe 'nicht relevant' bei einzelnen Angaben zu Key-CryptoAlg bedeutet, dass es im Smart Meter-System derzeit nicht zwingend erforderlich ist, entsprechende Key-Objekte mit dem betreffenden Wert für das Key-Attribut Key-CryptoAlg anlegen zu können, da es keine entsprechenden Anwendungsfälle gibt und solche Key-Objekte daher später im Betrieb nicht genutzt werden würden. Für die Implementierung des Kommandos CREATE KEY siehe auch [TR-03109-2], Kap. 4.4.1. Alle weiteren Kommandos zum Key Management sowie alle weiteren Krypto-Kommandos sind nicht zulässig (Zugriffsregel NEVER).

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
	Neue Public Key-Objekte können in den Phasen „Personalisierung des Smart Meter Mini-HSM“ und „Normalbetrieb des Smart Meter Mini-HSM“ im Sicherheitsmodul angelegt werden.

Tabelle 18: Option 1: Zugriffsregeln für MF/DFs/EFs/Key-Objekte/PIN-Objekte in den Phasen „Personalisierung des Smart Meter Mini-HSM“ und „Normalbetrieb des Smart Meter Mini-HSM“ (SEID = 01)

Option 2:

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
MF	MF: • SELECT: ALWAYS • DELETE FILE: NEVER (MF nicht löschbar) • ACTIVATE FILE: NEVER (MF nicht aktivierbar) • DEACTIVATE FILE: NEVER (MF nicht deaktivierbar) • TERMINATE DF: NEVER (MF nicht terminierbar) • CREATE FILE: NEVER • CREATE KEY: NEVER
EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation)	• SELECT EF: ALWAYS • READ RECORD: ALWAYS • UPDATE RECORD: NEVER, ausgenommen das Sicherheitsmodul bietet die Funktionalität des Sicherheitsmodul-Firmware-Updates (in diesem Fall gelten die Zugriffsregeln für ein Update des Datenfeldes wie im Rahmen des Firmware-Updates vorgesehen) • APPEND RECORD: PACE (sofern das Kommando im Sicherheitsmodul implementiert ist) • DELETE FILE: NEVER • ACTIVATE FILE: NEVER • DEACTIVATE FILE: NEVER • TERMINATE EF: NEVER
EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität)	• SELECT EF: ALWAYS • READ BINARY: ALWAYS • UPDATE BINARY: NEVER, ausgenommen das Sicherheitsmodul bietet die Funktionalität des Sicherheitsmodul-Firmware-Updates (in diesem Fall gelten die Zugriffsregeln für ein Update des Datenfeldes wie im Rahmen des Firmware-Updates vorgesehen) • DELETE FILE: NEVER • ACTIVATE FILE: NEVER • DEACTIVATE FILE: NEVER • TERMINATE EF: NEVER
EF.SecModCrypto	• SELECT EF: ALWAYS

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
(Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität)	• READ BINARY: ALWAYS • UPDATE BINARY: NEVER, ausgenommen das Sicherheitsmodul bietet die Funktionalität des Sicherheitsmodul-Firmware-Updates (in diesem Fall gelten die Zugriffsregeln für ein Update des Datenfeldes wie im Rahmen des Firmware-Updates vorgesehen) • DELETE FILE: NEVER • ACTIVATE FILE: NEVER • DEACTIVATE FILE: NEVER • TERMINATE EF: NEVER
EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls)	• SELECT EF: ALWAYS • READ RECORD: PACE • UPDATE RECORD: PACE • APPEND RECORD: PACE (sofern das Kommando im Sicherheitsmodul implementiert ist) • DELETE FILE: PACE oder alternativ NEVER • ACTIVATE FILE: PACE oder alternativ NEVER • DEACTIVATE FILE: PACE oder alternativ NEVER • TERMINATE EF: PACE oder alternativ NEVER
PIN-Objekte (PIN.HSM zur Speicherung der HSM-System-PIN)	Generell: • PINs können nicht ausgelesen werden • Zugriff über PIN-Management-Kommandos bzw. Krypto-Kommandos wie in oben stehender Tabelle 17 angegeben, mit untenstehenden Ausnahmen für PIN.HSM • zusätzlich zu den Angaben in Tabelle 17 bestehen je nach PIN-Management-Kommando ggf. weitere Zugriffsbeschränkungen in Abhängigkeit vom PIN-LifeCycleStatus des betreffenden PIN-Objektes: für Details siehe die Kommando-Spezifikation in [TR-03109-2], Kap. 4.8
	PIN.HSM: • CHANGE REFERENCE DATA / Variante Setzen einer PIN: NEVER • CHANGE REFERENCE DATA / Variante Wechseln einer PIN: PACE • GENERAL AUTHENTICATE / PACE: ALWAYS Hinweis: Das Kommando CHANGE REFERENCE DATA in der Variante „Setzen einer PIN“ ist für das PIN-Objekt PIN.HSM für die HSM-System-PIN in den Phasen „Personalisierung des Smart Meter Mini-HSM“ und „Normalbetrieb des Smart Meter Mini-HSM“ nicht mehr ausführbar. Dies wird über das Kommando-Verhalten des Kommandos CHANGE REFERENCE DATA in der Variante „Setzen einer PIN“ sowie über das PIN-Attribut PIN-LifeCycleStatus des PIN-Objektes PIN.HSM erreicht, das im Initialisierungsfile mit dem Wert „initialisation“ vorbelegt ist und über den Aufruf des Kommandos CHANGE REFERENCE DATA in der Variante „Setzen einer PIN“ in der Phase „Integration + Vor-

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
	Personalisierung von Sicherheitsmodul und Mini-HSM“ irreversibel auf den Wert „operational state – activated“ umgesetzt wird.
Key Pair-Objekte	Generell: • Schlüsselpaare werden ausschließlich onboard generiert (persistente / temporäre Speicherung im Sicherheitsmodul) • Private Keys verbleiben grundsätzlich im Sicherheitsmodul und können nicht ausgelesen werden • zugehörige Public Keys können ausgelesen werden • zusätzlich zu den Angaben in Tabelle 17 bestehen je nach Key Management- bzw. Krypto-Kommando ggf. weitere Zugriffsbeschränkungen in Abhängigkeit vom Key Pair-Objekt und seinem Key-LifeCycleStatus: für Details siehe die folgenden Angaben und die jeweilige Kommando-Spezifikation in [TR-03109-2], Kap. 3.4.5, 3.4.6, 4.4 und 4.5 sowie Kap. 3.2.4.2.3 und 3.3.2 d1)
	Speziell gelten für die für das Initialisierungsfile in Kap. 3.1.2 vordefinierten Key Pair-Objekte folgende Zugriffsregeln: Key.IMP_TRANS: Dieses Key Pair-Objekt ist in den Phasen „Personalisierung des Smart Meter Mini-HSM“ und „Normalbetrieb des Smart Meter Mini-HSM“ nicht mehr im Sicherheitsmodul vorhanden. Key.IMP: • GENERATE ASYMMETRIC KEY PAIR / Export Public Key: PACE • PSO COMPUTE DIGITAL SIGNATURE: PACE Key.EPH_x: • GENERATE ASYMMETRIC KEY PAIR / KeyGen mit Ausgabe des Public Key: PACE • GENERAL AUTHENTICATE / ECKA-DH: PACE Für alle zuvor genannten Key Pair-Objekte des Initialisierungsfiles wie in Kap. 3.1.2 definiert sind jeweils alle weiteren Kommandos zum Key Management sowie alle weiteren Krypto-Kommandos nicht zulässig (Zugriffsregel NEVER).
Public Key-Objekte	Generell: • Public Keys können importiert werden (temporäre / persistente Speicherung im Sicherheitsmodul) • zusätzlich zu den Angaben in Tabelle 17 bestehen je nach Key Management- bzw. Krypto-Kommando ggf. weitere Zugriffsbeschränkungen in Abhängigkeit vom Public Key-Objekt und seinem Key-LifeCycleStatus: für Details siehe die folgenden Angaben und die jeweilige Kommando-Spezifikation in [TR-03109-2], Kap. 3.4.5, 3.4.6, 4.4 und 4.5 sowie Kap. 3.2.4.2.3 und 3.3.2 d2)
	Speziell gelten für die für das Initialisierungsfile in Kap. 3.1.2 vordefinierten Public Key-Objekte folgende Zugriffsregeln: Key.IMP_PUB_TRANS:

MF/DFs/EFs/Key-Objekte/PIN-Objekte	Zugriffsregel
	Dieses Public Key-Objekt ist in den Phasen „Personalisierung des Smart Meter Mini-HSM“ und „Normalbetrieb des Smart Meter Mini-HSM“ nicht mehr im Sicherheitsmodul vorhanden. Key.IMP_PUB: • PSO VERIFY CERTIFICATE: PACE Für alle zuvor genannten Public Key-Objekte des Initialisierungsfiles wie in Kap. 3.1.2 definiert sind jeweils alle weiteren Kommandos zum Key Management sowie alle weiteren Krypto-Kommandos nicht zulässig (Zugriffsregel NEVER).

Tabelle 19: Option 2: Zugriffsregeln für MF/DFs/EFs/Key-Objekte/PIN-Objekte in den Phasen „Personalisierung des Smart Meter Mini-HSM“ und „Normalbetrieb des Smart Meter Mini-HSM“ (SEID = 01)

3.4 Kommandoset des Sicherheitsmoduls

Siehe BSI TR-03109-2 ([TR-03109-2]), Kap. 3.4 mit seinen Unterkapiteln. Die dortigen Ausführungen zum SMGW-Sicherheitsmodul und seinem Kommandoset gelten entsprechend für das Sicherheitsmodul im Smart Meter Mini-HSM mit folgenden Abweichungen:

- In [TR-03109-2], Kap. 3.4.1 entfällt in Tabelle 18 die Zeile für das Kommando EXTERNAL AUTHENTICATE.
- In [TR-03109-2], Kap. 3.4.6.1 entfällt im Text der Eintrag zum Kommando EXTERNAL AUTHENTICATE.
- Es entfällt [TR-03109-2], Kap. 3.4.6.7 zum Kommando EXTERNAL AUTHENTICATE.
- In [TR-03109-2], Kap. 3.4.7.1 zum Kommando MSE SET entfällt entsprechend die Unterstützung für das Kommando EXTERNAL AUTHENTICATE.
- In [TR-03109-2], Kap. 3.4.8.1 zum Kommando GET CHALLENGE entfällt entsprechend die Unterstützung für das Kommando EXTERNAL AUTHENTICATE.

3.5 Secure Messaging

Die im Rahmen des PACE-Protokolls zwischen Applikationsserver und Sicherheitsmodul ausgehandelten Session Keys werden nachfolgend für einen gesicherten Datentransfer zwischen Applikationsserver und Sicherheitsmodul verwendet. Für die gesicherte Kommunikation zwischen Applikationsserver und Sicherheitsmodul gelten die Ausführungen zum Secure Messaging in BSI TR-03109-2 ([TR-03109-2]), Kap. 3.5 entsprechend wie für ein Sicherheitsmodul im SMGW.

3.6 Weitere Funktionalitäten des Sicherheitsmoduls

Siehe BSI TR-03109-2 ([TR-03109-2]), 3.6 mit seinen Unterkapiteln. Die dortigen Ausführungen zum SMGW-Sicherheitsmodul und seinen weiteren Funktionalitäten gelten entsprechend für ein Sicherheitsmodul im Smart Meter Mini-HSM.

4 Feinspezifikation des Sicherheitsmoduls

Siehe BSI TR-03109-2 ([TR-03109-2]), Kap. 4 mit seinen Unterkapiteln. Die dortigen Ausführungen zum SMGW-Sicherheitsmodul und seinem Kommandoset gelten entsprechend für das Sicherheitsmodul im Smart Meter Mini-HSM mit folgenden Abweichungen:

- Es entfällt [TR-03109-2], Kap. 4.5.6 zum Kommando EXTERNAL AUTHENTICATE.
- In [TR-03109-2], Kap. 4.6.1 zum Kommando MSE SET entfällt entsprechend die Unterstützung für das Kommando EXTERNAL AUTHENTICATE. Siehe dortigen Abschnitt zu Variante 2.3.
- In [TR-03109-2], Kap. 4.7.1 zum Kommando GET CHALLENGE entfällt entsprechend die Unterstützung für das Kommando EXTERNAL AUTHENTICATE mit der internen Speicherung der generierten Zufallszahl. Es muss nur die Variante P1='01' unterstützt werden.
- Für Option 2 des File- und Objektsystems (siehe Kap. 3.3.3):

  Bei den Kartenmanagement-Kommandos kann bei Ablehnung des betreffenden Kommandos dieses statt mit dem Return Code '69 82' (SecurityStatusNotSatisfied) alternativ auch mit dem Return Code '6D 00' (InstructionNotSupported) oder '6A 86' (IncorrectParametersP1-P2) enden.

5 Sicherheitszertifizierung des Sicherheitsmoduls

Das Sicherheitsmodul für das Smart Meter Mini-HSM unterliegt einer Sicherheitszertifizierung nach Common Criteria (CC) auf Basis des Protection Profiles [PP 0095].

Die Implementierung des Sicherheitsmoduls erfolgt auf der Basis der im vorliegenden Dokument enthaltenen technischen Spezifikation für das Sicherheitsmodul. Für die Implementierung des Sicherheitsmoduls ist mindestens eine der beiden in Kap. 3.3.3 genannten Optionen (Option 1 / Option 2) der Zugriffsregelpolitik umzusetzen. Ferner gelten entsprechende Krypto-Anforderungen, wie diese für ein Sicherheitsmodul im SMGW in [TR-03109-3] formuliert sind, auch für das Sicherheitsmodul im Smart Meter Mini-HSM. Im Rahmen der Sicherheitszertifizierung des Sicherheitsmoduls wird nachgeprüft, dass die Implementierung des Sicherheitsmoduls die Vorgaben des vorliegenden Dokuments sowie der [TR-03109-3] erfüllt.

Im Rahmen seiner Initialisierung zusätzlich im Sicherheitsmodul aufgebrachte Ordner (DFs), Datenfelder (EFs) sowie Key- und PIN-Objekte, die über die für das initiale Initialisierungsfile in Kap. 3.1.2 vordefinierten Ordner, Datenfelder, Key- und PIN-Objekte hinausgehen, sowie alle weiteren Funktionalitäten des Betriebssystems des Sicherheitsmoduls, die über die nach dem vorliegenden Dokument verpflichtend zu implementierenden Funktionalitäten hinausgehen (wie z.B. zusätzliche Kommandos oder Kommando-Varianten, weitere Werte für den Life Cycle-Status des Sicherheitsmoduls und die zugehörigen Kommandos zum Weiterschalten des Life Cycle-Status, usw.), liegen außerhalb der vorliegenden Spezifikation des Sicherheitsmoduls, wie dieses für seinen Einsatz im Smart Meter Mini-HSM vorgesehen ist. Es muss aber sichergestellt und im Rahmen der CC-Zertifizierung des Sicherheitsmoduls geprüft werden, dass diese zusätzlichen Ordner, Datenfelder, Key- und PIN-Objekte mit ihren zugehörigen Management- und Krypto-Kommandos sowie diese zusätzlichen Funktionalitäten des Betriebssystems des Sicherheitsmoduls *nicht* die für das Sicherheitsmodul und seinen Einsatz im Smart Meter Mini-HSM vorgesehenen Sicherheitsstrukturen verändern, umgehen oder außer Kraft setzen. Insbesondere sind hierbei die in den Kap. 3.3.1 und 3.6 (bzw. [TR-03109-2], Kap. 3.6.3 und 3.6.4) stehenden Anforderungen bzgl. der CC-Zertifizierung des Sicherheitsmoduls zu berücksichtigen.

Die Benutzerdokumentation zu einem CC-zertifizierten Sicherheitsmodul beinhaltet insbesondere Informationen, Nutzungshinweise und Auflagen für den Nutzer des Sicherheitsmoduls bzgl. der Hersteller-spezifischen Implementierung der Schlüsselsuche im Sicherheitsmodul. Dies betrifft insbesondere den Aspekt, inwieweit deaktivierte und terminierte DFs in die Schlüsselsuche einbezogen oder in dieser Suche übersprungen werden.

Literaturverzeichnis

[TR-03109-2] Technische Richtlinie BSI TR-03109-2: Smart Meter Gateway - Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls, BSI, Version 1.1, 2014

[TR-03109-3] BSI TR-03109-3 Kryptographische Vorgaben, BSI, aktuelle Fassung

[PP 0095] BSI-CC-PP-0095 „Protection Profile for the Security Module of a Smart Meter Mini-HSM (Mini-HSM Security Module PP)“, BSI, Version 1.0, 2017

[ISO 7816-4] ISO/IEC 7816-4: Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange, ISO/IEC, IS 2013

[TR-03111] BSI TR-03111 Elliptic Curve Cryptography, BSI, Version 2.0, 2012

[TR-03110-3] BSI TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 3 - Common Specifications, BSI, Version 2.20, 2015

[TR-03116-3] BSI TR-03116-3 Kryptographische Vorgaben für Projekte der Bundesregierung - Teil 3: Intelligente Messsysteme, BSI, aktuelle Fassung

[EN 14890-1] EN 14890-1: Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic Services, EN, 2011

[RFC 5114] RFC 5114 - Additional Diffie-Hellman Groups for Use with IETF Standards, M. Lepinski, S. Kent, 2008

Stichwort- und Abkürzungsverzeichnis

Siehe Kap. 1.3.