Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie BSI TR-03109-2

Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases

Version 1.1 – 17.12.2014

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

1 Einleitung....4
1.1 Terminologie und Referenzen....4
1.2 Übersicht der Use Cases....4
1.3 Änderungshistorie....8
2 Vor-Personalisierung + Integration von Sicherheitsmodul und GW....9
2.1 Auswahl und Setzen des Security Environment....9
2.2 Allgemeine Use Cases....10
2.2.1 Sicherungsmechanismen des SMGW....10
2.2.2 Management der Applikationsebene des Sicherheitsmoduls....10
2.2.3 File-/Kartenmanagement....10
2.2.4 Schlüsselmanagement....11
2.2.5 Generierung von Schlüsselpaaren....13
2.2.6 Import von Public Keys....15
2.2.7 Signaturgenerierung und -verifikation....18
2.2.8 Zugriff auf Technische Datenfelder im Sicherheitsmodul....20
2.3 Vor-Personalisierung 1....22
2.4 Integration von Sicherheitsmodul und GW....29
2.5 Vor-Personalisierung 2....31
3 Installation + Vor-Ort-Inbetriebnahme des SMGW....36
4 Personalisierung, Normalbetrieb (End-Usage) und Außerbetriebnahme des SMGW....37
4.1 Auswahl und Setzen des Security Environment....37
4.2 Zugriff auf Technische Datenfelder im Sicherheitsmodul....38
4.3 Sicherungsmechanismen des SMGW....40
4.4 Administration des SMGW....44
4.4.1 Sicherung der Administrationstätigkeiten des GW-Administrators....45
4.4.2 Schlüsselmanagement....49
4.4.3 Management des SM-PKI-Root-Zertifikates....60
4.4.4 File-/Kartenmanagement....62
4.4.5 Management des Life Cycle-Status des Sicherheitsmoduls....67
4.4.6 Management der Applikationsebene des Sicherheitsmoduls....68
4.5 Krypto-Anwendungen....69
Literaturverzeichnis....82
Stichwort- und Abkürzungsverzeichnis....83

Tabellenverzeichnis

Tabelle 1: Übersicht der Use Cases....8
Tabelle 2: Änderungshistorie....8

1 Einleitung

Das vorliegende Dokument beinhaltet einen informativen Anhang zur Technischen Richtlinie BSI TR-03109-2 [TR-03109-2] und benennt Anwendungsfälle, die die Nutzung des Sicherheitsmoduls im SMGW beschreiben und das Zusammenspiel zwischen GW und Sicherheitsmodul in den verschiedenen Phasen des Lebenszyklus-Modells für das Sicherheitsmodul bzw. SMGW illustrieren.

Die folgenden Kapitel dieses Dokumentes beschreiben anhand von typischen Anwendungsfällen (Use Cases), wie das generelle Zusammenspiel von GW und Sicherheitsmodul vorgesehen ist und wie das Sicherheitsmodul adäquat und den Belangen des Smart Meter-Systems entsprechend im GW eingebunden werden kann.

Für jeden Anwendungsfall werden die erforderliche Sequenz von Kommandos für das Sicherheitsmodul und die durchzuführenden Aufgaben auf Seiten des GW – z.B. hinsichtlich der Datenvorbereitung für die Kommandos und der nachfolgenden Datennachbereitung der von den Kommandos ausgegebenen Daten – angegeben. Die Notation „ ⩤ “ in den Ablaufbeschreibungen der Use Cases bedeutet in diesem Zusammenhang das Absetzen eines Kommandos vom GW an das Sicherheitsmodul.

Die Kapitel des vorliegenden Dokumentes orientieren sich an den Phasen des Lebenszyklus-Modells für das SMGW wie in [TR-03109-1], [TR-03109-1A] und [TR-03109-2], Kap. 2 dargestellt. Relevant sind mithin folgende Phasen im Lebenszyklus-Modell:

- Vor-Personalisierung + Integration von Sicherheitsmodul und GW (siehe Kap. 2)
- Installation + Vor-Ort-Inbetriebnahme des SMGW (siehe Kap. 3)
- Personalisierung des SMGW (siehe Kap. 4)
- Normalbetrieb (End-Usage) des SMGW (siehe Kap. 4)
- Außerbetriebnahme des SMGW (siehe Kap. 4.4.5)

Die Use Cases für die Phasen „Personalisierung des SMGW“ und „Normalbetrieb des SMGW“ können zusammengefasst werden, da diese von den Abläufen her prinzipiell als gleich zu betrachten sind und je nach Phase ggf. lediglich unterschiedliches Schlüssel- und Zertifikatsmaterial benötigen.

1.1 Terminologie und Referenzen

Zur Terminologie und zu den verwendeten Abkürzungen sowie Bezeichnern für Kommandos, Ordner, Datenfelder und Key- und PIN-Objekte sei auf [TR-03109-2] verwiesen.

Ferner sind folgende Dokumentenreferenzen direkt im vorliegenden Dokument bzw. indirekt über [TR-03109-2] relevant:

[TR-03109], [TR-03109-1], [TR-03109-1A], [TR-03109-2], [TR-03109-3], [TR-03109-4], [ISO 7816-3], [ISO 7816-4], [ISO 7816-8], [ISO 7816-9], [ISO 14443-4], [TR-03111], [TR-03110-1], [TR-03110-2], [TR-03110-3], [TR-03116-3], [TR-03117], [EN 14890-1], [EN 14890-2].

1.2 Übersicht der Use Cases

Folgende Tabelle fasst die im vorliegenden Dokument betrachteten Use Cases zusammen:

Use Case ID	Titel des Use Case	Kapitel-referenz
Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“		
UC_VI_01_01	Use Case „Auswahl und Setzen des Security Environment (Vor-Personalisierung)“	2.1
---	Use Cases zu Sicherungsmechanismen des SMGW	2.2.1, 4.3
---	Use Case zum Management der Applikationsebene des Sicherheitsmoduls	2.2.2, 4.4.6
UC_VI_02_01	Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“	2.2.3
UC_VI_02_02	Use Case „Aktivieren eines DF/EF (Vor-Personalisierung)“	2.2.3
UC_VI_02_03	Use Case „Löschen eines Key-Objektes (Vor-Personalisierung)“	2.2.4
UC_VI_02_04	Use Case „Deaktivieren eines Key-Objektes (Vor-Personalisierung)“	2.2.4
UC_VI_02_05	Use Case „Generierung eines ECC-Schlüsselpaares (Vor-Personalisierung)“	2.2.5
UC_VI_02_06	Use Case „Export des Public Key eines ECC-Schlüsselpaares (Vor-Personalisierung)“	2.2.5
UC_VI_02_07	Use Case „Wechsel des Import-Schlüsselpaares“	2.2.6
UC_VI_02_08	Use Case „Import eines Public Key (Vor-Personalisierung)“	2.2.6
UC_VI_02_09	Use Case „Generieren einer Signatur / DST (Vor-Personalisierung)“	2.2.7
UC_VI_02_10	Use Case „Generieren einer Signatur / AT (Vor-Personalisierung)“	2.2.7
UC_VI_02_11	Use Case „Prüfen einer Signatur (Vor-Personalisierung)“	2.2.7
UC_VI_02_12	Use Case „Auslesen eines transparenten Technischen Datenfeldes“	2.2.8
UC_VI_02_13	Use Case „Auslesen eines Record-orientierten Technischen Datenfeldes“	2.2.8
UC_VI_02_14	Use Case „Update eines Record-orientierten Technischen Datenfeldes“	2.2.8
UC_VI_03_01	Use Case „Import des SM-PKI-Root-Zertifikates in das Sicherheitsmodul (Vor-Personalisierung)“	2.3
UC_VI_03_02	Use Case „Generierung eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“	2.3
UC_VI_03_03	Use Case „Export des Public Key eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“	2.3
UC_VI_03_04	Use Case „Erstellung des Zertifikatsrequest-Pakets für Gütesiegel-Zertifikate“	2.3
UC_VI_03_05	Use Case „Import eines Gütesiegel-Zertifikates in das Sicherheitsmodul“	2.3

Use Case ID	Titel des Use Case	Kapitel-referenz
UC_VI_04_01	Use Case „Initiales Hochfahren des SMGW“	2.4
UC_VI_04_02	Use Case „Generierung eines Keys für die Speicherverschlüsselung des GW und Import in das Sicherheitsmodul“	2.4
UC_VI_05_01	Use Case „Import der Public Keys des GW-Administrators (Vor-Personalisierung)“	2.5
UC_VI_05_02	Use Case „Prüfung einer Zertifikatskette (Vor-Personalisierung)“	2.5
UC_VI_05_03	Use Case „Prüfung der in der Initialen Konfigurationsdatei gelieferten Zertifikate des GW-Administrators (Vor-Personalisierung)“	2.5
UC_VI_05_04	Use Case „Prüfung der Signatur der Initialen Konfigurationsdatei (Vor-Personalisierung)“	2.5
UC_VI_05_05	Use Case „Löschen der Import-Schlüssel (Vor-Personalisierung)“	2.5
Phase „Installation + Vor-Ort-Inbetriebnahme des SMGW“		
---	---	3
Phasen „Personalisierung des SMGW“, „Normalbetrieb (End-Usage) des SMGW“, „Außerbetriebnahme des SMGW“		
UC_PN_01_01	Use Case „Auswahl und Setzen des Security Environment“	4.1
UC_PN_02_01	Use Case „Auslesen eines transparenten Technischen Datenfeldes“	4.2
UC_PN_02_02	Use Case „Auslesen eines Record-orientierten Technischen Datenfeldes“	4.2
UC_PN_02_03	Use Case „Update eines Record-orientierten Technischen Datenfeldes“	4.2
UC_PN_03_01	Use Case „PACE-Authentisierung“	4.3
UC_PN_03_02	Use Case „Wechsel der GW-System-PIN“	4.3
UC_PN_03_03	Use Case „Zurücksetzen des Sicherheitszustandes PACE“	4.3
UC_PN_03_04	Use Case „Auslesen eines symmetrischen GW-Keys“	4.3
UC_PN_03_05	Use Case „Update eines symmetrischen GW-Keys“	4.3
UC_PN_04_01	Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“	4.4.1
UC_PN_04_02	Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“	4.4.1
UC_PN_04_03	Use Case „Zurücksetzen des Sicherheitszustandes AUTH“	4.4.1
UC_PN_04_04	Use Case „Wechsel des GW-Administrators“	4.4.1
UC_PN_04_05	Use Case „Anlegen eines Key-Objektes“	4.4.2

Use Case ID	Titel des Use Case	Kapitel-referenz
UC_PN_04_06	Use Case „Löschen eines Key-Objektes“	4.4.2
UC_PN_04_07	Use Case „Aktivieren eines Key-Objektes“	4.4.2
UC_PN_04_08	Use Case „Deaktivieren eines Key-Objektes“	4.4.2
UC_PN_04_09	Use Case „Generierung eines ECC-Schlüsselpaares“	4.4.2
UC_PN_04_10	Use Case „Export des Public Key eines ECC-Schlüsselpaares“	4.4.2
UC_PN_04_11	Use Case „Import eines Public Key“	4.4.2
UC_PN_04_12	Use Case „Erstellung eines Zertifikatsrequest-Pakets (SM-PKI)“	4.4.2
UC_PN_04_13	Use Case „Prüfung einer Zertifikatskette (SM-PKI)“	4.4.2
UC_PN_04_14	Use Case „Update des SM-PKI-Root-Zertifikates“	4.4.3
UC_PN_04_15	Use Case „Auslesen des SM-PKI-Root-Zertifikates“	4.4.3
UC_PN_04_16	Use Case „Selektieren eines DF/EF“	4.4.4
UC_PN_04_17	Use Case „Anlegen eines DF/EF“	4.4.4
UC_PN_04_18	Use Case „Löschen eines DF/EF“	4.4.4
UC_PN_04_19	Use Case „Aktivieren eines DF/EF“	4.4.4
UC_PN_04_20	Use Case „Deaktivieren eines DF/EF“	4.4.4
UC_PN_04_21	Use Case „Terminieren eines DF/EF“	4.4.4
UC_PN_04_22	Use Case „Terminieren des Sicherheitsmoduls“	4.4.5
UC_PN_04_23	Use Case „Zurücksetzen der Applikationsebene des Sicherheitsmoduls“	4.4.6
UC_PN_05_01	Use Case „Erzeugen und Ausgeben einer Zufallszahl“	4.5
UC_PN_05_02	Use Case „Generieren einer Signatur / DST“	4.5
UC_PN_05_03	Use Case „Generieren einer Signatur / AT“	4.5
UC_PN_05_04	Use Case „Prüfen einer Signatur“	4.5
UC_PN_05_05	Use Case „Aufbau eines TLS-Kanals zwischen externer Welt und SMGW / SMGW in der Rolle TLS-Client“	4.5
UC_PN_05_06	Use Case „Aufbau eines TLS-Kanals zwischen externer Welt und SMGW / SMGW in der Rolle TLS-Server“	4.5
UC_PN_05_07	Use Case „Inhaltsdatenverschlüsselung mit SMGW/Sicherheitsmodul als Recipient“	4.5
UC_PN_05_08	Use Case „Inhaltsdatenverschlüsselung mit SMGW/Sicherheitsmodul als Initiator“	4.5
UC_PN_05_09	Use Case „Inhaltsdatensignatur / Signaturgenerierung“	4.5

Use Case ID	Titel des Use Case	Kapitel-referenz
UC_PN_05_10	Use Case „Inhaltsdatensignatur / Signaturprüfung“	4.5
UC_PN_05_11	Use Case „Generieren eines TLS-Schlüsselpaares für einen Zähler“	4.5

Tabelle 1: Übersicht der Use Cases

1.3 Änderungshistorie

Version	Datum	Änderung
V 1.0	18.03.2013	Erstausgabe
V 1.01	19.05.2014	Anpassungen an [TR-03109-2]
V1.0.2	15.08.2014	Anpassungen an [TR-03109-2] und [TR-03109-1]
V 1.1	17.12.2014	Anpassungen an [TR-03109-2], Ergänzung von Klarstellungen, kleine Fehlerbereinigungen, Aktualisierung des Literaturverzeichnisses

Tabelle 2: Änderungshistorie

2 Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Ausgangspunkt für die Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“ ist ein initialisiertes Sicherheitsmodul. Das Sicherheitsmodul beinhaltet das vordefinierte File- und Objektsystem wie in [TR-03109-2], Kap. 3.1, 3.2 und 3.3 beschrieben.

Es wird eine ausreichend gesicherte Umgebung des Integrators sowie die Vertrauenswürdigkeit des Integrators angenommen.

Relevantes Security Environment für die Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“: Siehe [TR-03109-2], Kap. 3.3.1, 3.3.3.1.

Die Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“ lässt sich mit dem vom Sicherheitsmodul angebotenen Kommando-Set realisieren.

2.1 Auswahl und Setzen des Security Environment

UC_VI_01_01:

Use Case „Auswahl und Setzen des Security Environment (Vor-Personalisierung)“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Beim Start bzw. Hochfahren des Sicherheitsmoduls ist defaultmäßig das SE mit SEID = 01 gesetzt. Für die Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“ ist explizit das zugehörige SE wie in [TR-03109-2], Kap. 3.3.1, 3.3.3.1 definiert zu setzen.

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.

Ablauf:

➢ MSE RESTORE (SEID für Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“)

Nachbedingungen:

- Es gelten die Zugriffsregeln wie für das zur Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“ zugeordnete Security Environment definiert. Siehe [TR-03109-2], Kap. 3.3.1, 3.3.3.1.

2.2 Allgemeine Use Cases

2.2.1 Sicherungsmechanismen des SMGW

Die Anwendungsfälle

- UC_PN_03_01: Use Case „PACE-Authentisierung“,
- UC_PN_03_02: Use Case „Wechsel der GW-System-PIN“ und
- UC_PN_03_03: Use Case „Zurücksetzen des Sicherheitszustandes PACE“

aus Kap. 4.3 gelten sinngemäß auch für die Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“ mit den Angaben zum Aspekt Secure Messaging in Kap. 2.3 und 2.5.

2.2.2 Management der Applikationsebene des Sicherheitsmoduls

Der Anwendungsfall

- UC_PN_04_23: Use Case „Zurücksetzen der Applikationsebene des Sicherheitsmoduls“

aus Kap. 4.4.6 gilt sinngemäß auch für die Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“.

2.2.3 File-/Kartenmanagement

UC_VI_02_01:

Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Die Selektion eines DF/EF per File-ID erfolgt innerhalb des aktuell selektierten DF. Um im Filesystem des Sicherheitsmoduls zu navigieren, ist ggf. eine sukzessive mehrfache Anwendung des Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“ erforderlich.

Das DF.SMGW kann auch direkt per AID selektiert werden.

Beim Hochfahren des Sicherheitsmoduls ist automatisch das MF selektiert.

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.

Ablauf:

Für die Selektion des MF:

➢ SELECT (leeres Kommando-Datenfeld)

Für die Selektion eines DF/EF via File-ID:

- SELECT (File-ID des zu selektierenden DF/EF)

Für die direkte Adressierung des DF.SMGW:

- SELECT (AID des DF.SMGW)

Nachbedingungen:

- ---

UC_VI_02_02:

Use Case „Aktivieren eines DF/EF (Vor-Personalisierung)“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Anwendung zur Aktivierung von Ordnern (DF) und Datenfeldern (EF), im vorliegenden Fall insbesondere für das DF.SMGW der SMGW-Applikation, für die transparenten Datenfelder EF.GSCert_TLS, EF.GSCert_SIG und EF.GSCert_ENC für die Gütesiegel-Zertifikate, für die transparenten Datenfelder EF.SMPKIRoot_x für das SM-PKI-Root-Zertifikat sowie für das Record-orientierte Datenfeld EF.GWKeys für die GW-Keys im DF.SMGW.

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- LCSI des DF, in dem das zu aktivierende DF/EF liegt, steht nicht auf „terminated“.

Ablauf:

Selektion des DF, in dem das zu aktivierende DF/EF liegt. (UC_VI_02_01: Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“)

- SELECT (File-ID des zu aktivierenden DF/EF)
- ACTIVATE FILE

Nachbedingungen:

- ---

2.2.4 Schlüsselmanagement

UC_VI_02_03:

Use Case „Löschen eines Key-Objektes (Vor-Personalisierung)“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Zu löschendes Key-Objekt ist deaktiviert. (UC_VI_02_04: Use Case „Deaktivieren eines Key-Objektes (Vor-Personalisierung)“)

Ablauf:

Selektion des DF, in dem das zu löschende Key-Objekt liegt. (UC_VI_02_01: Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“)

➢ DELETE KEY (Übergabe der Key Reference des zu löschenden Key-Objektes)

Nachbedingungen:

- ---

UC_VI_02_04:

Use Case „Deaktivieren eines Key-Objektes (Vor-Personalisierung)“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.

Ablauf:

Selektion des DF, in dem das zu deaktivierende Key-Objekt liegt. (UC_VI_02_01: Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“)

➢ DEACTIVATE KEY (Übergabe der Key Reference des zu deaktivierenden Key-Objektes)

Nachbedingungen:

- ---

2.2.5 Generierung von Schlüsselpaaren

UC_VI_02_05:

Use Case „Generierung eines ECC-Schlüsselpaares (Vor-Personalisierung)“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Anwendung für:

a) die Generierung der vorläufigen GW-Schlüsselpaare:

- Vorläufiges TLS-Key Pair (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE)
- Vorläufiges SIG-Key Pair (GW_WAN_SIG_PRV_PRE, GW_WAN_SIG_PUB_PRE)
- Vorläufiges ENC-Key Pair (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE)

b) die Generierung des Integrator-spezifischen Import-Schlüssels:

- Import-Key Pair (IMP_PRV, IMP_PUB)

Die Speicherung der in a) genannten vorläufigen GW-Schlüsselpaare erfolgt in den Key Pair-Objekten Key.WAN_TLS_PRE, Key.WAN_SIG_PRE bzw. Key.WAN_ENC_PRE des DF.SMGW. Die Speicherung des in b) genannten Import-Schlüsselpaares erfolgt im Key Pair-Objekt Key.IMP im MF.

Je nach verwendeter Kommando-Variante des Kommandos GENERATE ASYMMETRIC KEY PAIR erfolgt eine Schlüsselgenerierung mit oder ohne Ausgabe des Public Key.

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Key Pair-Objekt, das befüllt werden soll, ist vorhanden. Für die vorläufigen GW-Schlüsselpaare sowie das Integrator-spezifische Import-Schlüsselpaar sind die entsprechenden Key Pair-Objekte bereits im Rahmen der Initialisierung des Sicherheitsmoduls (siehe [TR-03109-2], Kap. 3.1.2) angelegt worden, die dann in diesem Use Case über das Kommando GENERATE ASYMMETRIC KEY PAIR mit Schlüsseldaten gefüllt werden.
- Falls ein bereits gefülltes Key Pair-Objekt neu befüllt werden soll: Key-Attribut Key-LifeCycleStatus des Key Pair-Objektes besitzt den Wert „operational state – deactivated“. (UC_VI_02_04: Use Case „Deaktivieren eines Key-Objektes (Vor-Personalisierung)“)

Ablauf:

Selektion des DF, in dem das zu befüllende Key Pair-Objekt liegt. (UC_VI_02_01: Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“)

➢ GENERATE ASYMMETRIC KEY PAIR (Kommando-Variante für Schlüsselgenerierung mit / ohne Ausgabe des Public Key; Übergabe relevanter Informationen für die Schlüsselgenerierung gemäß Kommando-Spezifikation)

Nachbedingungen:

- Das Key-Attribut Key-LifeCycleStatus des Key Pair-Objektes besitzt nach der Schlüsselgenerierung den Wert „operational state – activated“, so dass das Key Pair-Objekt direkt zu seiner Nutzung für Krypto-Operationen bereitsteht.
- Sofern im Rahmen der Kommando-Ausführung des Kommandos GENERATE ASYMMETRIC KEY PAIR keine Ausgabe des Public Key-Parts des generierten Schlüsselpaares erfolgt, kann ein späterer Export des Public Key-Parts über UC_VI_02_06: Use Case „Export des Public Key eines ECC-Schlüsselpaares (Vor-Personalisierung)“ erfolgen.

UC_VI_02_06:

Use Case „Export des Public Key eines ECC-Schlüsselpaares (Vor-Personalisierung)“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Anwendung für:

a) den Export der vorläufigen GW-Schlüssel:

- Vorläufiger TLS-Public Key GW_WAN_TLS_PUB_PRE
- Vorläufiger SIG- Public Key GW_WAN_SIG_PUB_PRE
- Vorläufiger ENC-Public Key GW_WAN_ENC_PUB_PRE

b) den Export des Integrator-spezifischen Import-Schlüssels:

- Import-Public Key IMP_PUB

Die Speicherung der zugehörigen vorläufigen GW-Schlüsselpaare (siehe a)) erfolgt in den Key Pair-Objekten Key.WAN_TLS_PRE, Key.WAN_SIG_PRE bzw. Key.WAN_ENC_PRE des DF.SMGW. Die Speicherung des zugehörigen Import-Schlüsselpaares (siehe b)) erfolgt im Key Pair-Objekt Key.IMP im MF.

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Key Pair-Objekt, dessen Public Key ausgegeben werden soll, ist vorhanden und wurde mittels Schlüsselgenerierung über das Kommando GENERATE ASYMMETRIC KEY PAIR mit Schlüsseldaten befüllt. (UC_VI_02_05: Use Case „Generierung eines ECC-Schlüsselpaares (Vor-Personalisierung)“)

Ablauf:

Selektion des DF, in dem das Key Pair-Objekt liegt, dessen Public Key ausgegeben werden soll. (UC_VI_02_01: Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“)

- GENERATE ASYMMETRIC KEY PAIR (Kommando-Variante für die Ausgabe des Public Key ohne Schlüsselgenerierung; Übergabe der Key Reference des Key Pair-Objektes, dessen Public Key ausgegeben werden soll)

Nachbedingungen:

- ---

2.2.6 Import von Public Keys

UC_VI_02_07:

Use Case „Wechsel des Import-Schlüsselpaares“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Im Rahmen der Produktion des Sicherheitsmoduls generiert der Hersteller des Sicherheitsmoduls ein Schlüsselpaar (IMP_PRV_TRANS, IMP_PUB_TRANS), mit dem der Import von Public Keys in der Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“ realisiert wird. Je nach Hersteller kann das Schlüsselpaar kundenspezifisch gewählt sein. Das Schlüsselpaar hat den Charakter eines Transport-Schlüsselpaares (siehe unten).

Im Auslieferungszustand enthält das initialisierte Sicherheitsmodul das Schlüsselpaar (IMP_PRV_TRANS, IMP_PUB_TRANS) im Key Pair-Objekt Key.IMP_TRANS im MF sowie zusätzlich nochmal den Public Key IMP_PUB_TRANS im Public Key-Objekt Key.IMP_PUB_TRANS im MF. Hinweis: Grund für die doppelte Speicherung des Public Key ist das Set der verfügbaren Kommandos des Sicherheitsmoduls.

Über diesen Use Case kann das Transport-Import-Schlüsselpaar (IMP_PRV_TRANS, IMP_PUB_TRANS) gegen ein Integrator-eigenes Import-Schlüsselpaar (IMP_PRV, IMP_PUB) ausgetauscht werden. Die Speicherung des neuen Import-Schlüsselpaares (IMP_PRV, IMP_PUB) erfolgt dabei im Key Pair-Objekt Key.IMP im MF, die zusätzliche Speicherung des Public Key IMP_PUB erfolgt dabei im Public Key-Objekt Key.IMP_PUB im MF.

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Transport-Import-Schlüsselpaar (IMP_PRV_TRANS, IMP_PUB_TRANS) (im Key Pair-Objekt Key.IMP_TRANS) sowie zusätzlich der Public Key IMP_PUB_TRANS (im Public Key-Objekt Key.IMP_PUB_TRANS) liegen im Sicherheitsmodul vor und sind aktiviert.

  (Hinweis: Die Anlage und Befüllung der genannten Key-Objekte ist bereits im Rahmen der Initialisierung des Sicherheitsmoduls erfolgt.)
- Key Pair-Objekt Key.IMP zur Speicherung von (IMP_PRV, IMP_PUB) ist vorhanden und das Key-Attribut Key-LifeCycleStatus des Key Pair-Objektes besitzt den Wert „initialisation“ oder „operational state – deactivated“ (UC_VI_02_04: Use Case „Deaktivieren eines Key-Objektes (Vor-Personalisierung)“).

(Hinweis: Die Anlage des Key Pair-Objektes ist bereits im Rahmen der Initialisierung des Sicherheitsmoduls erfolgt.)

- Public Key-Objekt Key.IMP_PUB zur Speicherung von IMP_PUB ist vorhanden und das Key-Attribut Key-LifeCycleStatus des Public Key-Objektes besitzt den Wert „initialisation“ oder „operational state – deactivated“ (UC_VI_02_04: Use Case „Deaktivieren eines Key-Objektes (Vor-Personalisierung)“).

  (Hinweis: Die Anlage des Public Key-Objektes ist bereits im Rahmen der Initialisierung des Sicherheitsmoduls erfolgt.)

Ablauf:

1. Schritt: Generierung von (IMP_PRV, IMP_PUB)

Durchführung von UC_VI_02_05: Use Case „Generierung eines ECC-Schlüsselpaares (Vor-Personalisierung)“ und ggf. UC_VI_02_06: Use Case „Export des Public Key eines ECC-Schlüsselpaares (Vor-Personalisierung)“ für die Generierung des neuen Import-Schlüsselpaares mit Speicherung im Key Pair-Objekt Key.IMP sowie für den Export des Public Key-Parts.

2. Schritt: Erstellung des Import-Zertifikates IMP_PUB_CRT zu IMP_PUB

Erstellung des Inputs IMP_PUB_CRTBody für das Import-Zertifikat IMP_PUB_CRT zu IMP_PUB. Für das Import-Zertifikat ist darauf zu achten, dass die dort eingetragene Key Reference mit dem Key-Attribut Key-Name des zu befüllenden Public Key-Objektes Key.IMP_PUB übereinstimmt.

Durchführung von UC_VI_02_09: Use Case „Generieren einer Signatur / DST (Vor-Personalisierung)“ zur Generierung der Signatur über IMP_PUB_CRTBody unter Nutzung des Signaturschlüssels IMP_PRV_TRANS im Key Pair-Objekt Key.IMP_TRANS. Ergebnis ist die Signatur Sig_IMP_PUB_CRTBody.

Erstellung des Import-Zertifikates IMP_PUB_CRT zu IMP_PUB. Dies besteht aus IMP_PUB_CRTBody und Sig_IMP_PUB_CRTBody.

3. Schritt: Import von IMP_PUB

Selektion des DF, in dem das zu befüllende Public Key-Objekt Key.IMP_PUB liegt. (UC_VI_02_01: Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“)

- MSE SET (DST) (für PSO VERIFY CERTIFICATE vorgesehene Kommando-Variante 1.2; insbesondere Übergabe der Key Reference des Public Key-Objektes Key.IMP_PUB_TRANS mit dem Signaturprüfschlüssel IMP_PUB_TRANS und Übergabe des zu verwendenden Krypto-Algorithmus)
- PSO VERIFY CERTIFICATE (Übergabe des Import-Zertifikates IMP_PUB_CRT des zu importierenden Public Key IMP_PUB; das Import-Zertifikat enthält insbesondere Key-Zusatzinformationen sowie die Key Reference des zu befüllenden Public Key-Objektes Key.IMP_PUB)

Nachbedingungen:

- Das Key-Attribut Key-LifeCycleStatus des Key Pair-Objektes Key.IMP für (IMP_PRV, IMP_PUB) besitzt nach der Schlüsselgenerierung den Wert „operational state – activated“, so dass das Key Pair-Objekt direkt zu seiner Nutzung für Krypto-Operationen bereitsteht.

- Das Key-Attribut Key-LifeCycleStatus des Public Key-Objektes Key.IMP_PUB für IMP_PUB besitzt nach dem Schlüsselimport den Wert „operational state – activated“, so dass das Public Key-Objekt direkt zu seiner Nutzung für Krypto-Operationen bereitsteht.

UC_VI_02_08:

Use Case „Import eines Public Key (Vor-Personalisierung)“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Der Import eines Public Key KEY_PUB in dieser Phase wird über ein Import-Schlüsselpaar (IMP_PRV, IMP_PUB) realisiert. Die Speicherung des Import-Schlüsselpaares (IMP_PRV, IMP_PUB) erfolgt im Key Pair-Objekt Key.IMP im MF, die zusätzliche Speicherung des Public Key IMP_PUB erfolgt im Public Key-Objekt Key.IMP_PUB im MF.

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Import-Schlüsselpaar (IMP_PRV, IMP_PUB) (im Key Pair-Objekt Key.IMP) sowie zusätzlich der Public Key IMP_PUB (im Public Key-Objekt Key.IMP_PUB) liegen im Sicherheitsmodul vor und sind aktiviert.

  (Hinweis: Die Anlage dieser Key-Objekte ist bereits im Rahmen der Initialisierung des Sicherheitsmoduls erfolgt. Für die Befüllung der Key-Objekte mit Schlüsseldaten siehe UC_VI_02_07: Use Case „Wechsel des Import-Schlüsselpaares“.)
- Zu importierender Public Key KEY_PUB liegt vor.
- Public Key-Objekt zur Speicherung von KEY_PUB ist vorhanden und das Key-Attribut Key-LifeCycleStatus des Public Key-Objektes besitzt den Wert „initialisation“ oder „operational state – deactivated“ (UC_VI_02_04: Use Case „Deaktivieren eines Key-Objektes (Vor-Personalisierung)“).

  (Hinweis: Für die Anwendung des vorliegenden Use Case ist die Anlage entsprechender Public Key-Objekte bereits im Rahmen der Initialisierung des Sicherheitsmoduls erfolgt.)

Ablauf:

1. Schritt: Erstellung des Import-Zertifikates KEY_PUB_CRT zu KEY_PUB

Erstellung des Inputs KEY_PUB_CRTBody für das Import-Zertifikat KEY_PUB_CRT zu KEY_PUB. Für das Import-Zertifikat ist darauf zu achten, dass die dort eingetragene Key Reference mit dem Key-Attribut Key-Name des zu befüllenden Public Key-Objektes für KEY_PUB übereinstimmt.

Durchführung von UC_VI_02_09: Use Case „Generieren einer Signatur / DST (Vor-Personalisierung)“ zur Generierung der Signatur über KEY_PUB_CRTBody unter Nutzung des Signaturschlüssels IMP_PRV. Ergebnis ist die Signatur Sig_KEY_PUB_CRTBody.

Erstellung des Import-Zertifikates KEY_PUB_CRT zu KEY_PUB. Dies besteht aus KEY_PUB_CRTBody und Sig_KEY_PUB_CRTBody.

2. Schritt: Import von KEY_PUB

Selektion des DF, in dem das zu befüllende Public Key-Objekt für KEY_PUB liegt. (UC_VI_02_01: Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“)

- MSE SET (DST) (für PSO VERIFY CERTIFICATE vorgesehene Kommando-Variante 1.2; insbesondere Übergabe der Key Reference des Public Key-Objektes Key.IMP_PUB mit dem Signaturprüfschlüssel IMP_PUB und Übergabe des zu verwendenden Krypto-Algorithmus)
- PSO VERIFY CERTIFICATE (Übergabe des Import-Zertifikates KEY_PUB_CRT des zu importierenden Public Key KEY_PUB; das Import-Zertifikat enthält insbesondere Key-Zusatzinformationen sowie die Key Reference des zu befüllenden Public Key-Objektes für KEY_PUB)

Nachbedingungen:

- Das Key-Attribut Key-LifeCycleStatus des Public Key-Objektes für KEY_PUB besitzt nach dem Schlüsselimport den Wert „operational state – activated“, so dass das Public Key-Objekt direkt zu seiner Nutzung für Krypto-Operationen bereitsteht.

2.2.7 Signaturgenerierung und -verifikation

UC_VI_02_09:

Use Case „Generieren einer Signatur / DST (Vor-Personalisierung)“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Die Aufbereitung der zu signierenden Daten inkl. Hashen der Daten erfolgt durch das GW bzw. anderweitig außerhalb des Sicherheitsmoduls (Signaturdaten).

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Key Pair-Objekt mit dem Signaturschlüssel ist im Sicherheitsmodul vorhanden und ist aktiviert. (UC_VI_02_05: Use Case „Generierung eines ECC-Schlüsselpaares (Vor-Personalisierung)“)

Ablauf:

Aufbereitung der Signaturdaten inkl. Hashing (passend zur vorgesehenen Elliptischen Kurve / Schlüssellänge des Signaturschlüssels).

Bestimmung des Signaturschlüssels bzw. des zugehörigen Key Pair-Objektes (Speicherort im Filesystem, Key-ID). Selektion des DF, in dem das Key Pair-Objekt mit dem Signaturschlüssel gespeichert ist. (UC_VI_02_01: Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“)

- MSE SET (DST) (für Signaturgenerierung vorgesehene Kommando-Variante 1.1; insbesondere Übergabe der Key Reference des Key Pair-Objektes mit dem Signaturschlüssel und Übergabe des zu verwendenden Krypto-Algorithmus)

- PSO COMPUTE DIGITAL SIGNATURE (Signaturdaten)

Nachbedingungen:

- ---

UC_VI_02_10:

Use Case „Generieren einer Signatur / AT (Vor-Personalisierung)“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Die Aufbereitung der zu signierenden Daten inkl. Hashen der Daten erfolgt durch das GW bzw. anderweitig außerhalb des Sicherheitsmoduls (Signaturdaten). Diese Signaturdaten bilden das zu signierende Token.

Als Signaturschlüssel wird ein Authentisierungsschlüssel (Schlüssel der Anwendungsklasse AT) verwendet.

Anwendung des Use Case im Rahmen der Erstellung eines Zertifikatsrequests zu einem vorläufigen ENC-Schlüssel. (UC_VI_03_04: Use Case „Erstellung des Zertifikatsrequest-Pakets für Gütesiegel-Zertifikate“)

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Key Pair-Objekt mit dem Authentisierungsschlüssel ist im Sicherheitsmodul vorhanden und ist aktiviert. (UC_VI_02_05: Use Case „Generierung eines ECC-Schlüsselpaares (Vor-Personalisierung)“)

Ablauf:

Aufbereitung des Tokens, d.h. der Signaturdaten inkl. Hashing (passend zur vorgesehenen Elliptischen Kurve / Schlüssellänge des Authentisierungsschlüssels).

Bestimmung des Authentisierungsschlüssels bzw. des zugehörigen Key Pair-Objektes (Speicherort im Filesystem, Key-ID). Selektion des DF, in dem das Key Pair-Objekt mit dem Authentisierungsschlüssel gespeichert ist. (UC_VI_02_01: Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“)

- MSE SET (AT) (für interne Authentisierung vorgesehene Kommando-Variante 2.4; insbesondere Übergabe der Key Reference des Key Pair-Objektes mit dem Authentisierungsschlüssel und Übergabe des zu verwendenden Krypto-Algorithmus)
- INTERNAL AUTHENTICATE (Token, d.h. Signaturdaten)

Nachbedingungen:

- ---

UC_VI_02_11:

Use Case „Prüfen einer Signatur (Vor-Personalisierung)“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Die Aufbereitung der zu prüfenden Daten inkl. Hashen der Daten erfolgt durch das GW bzw. anderweitig außerhalb des Sicherheitsmoduls (Signaturprüfdaten).

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Für Variante 2 (s.u.): Public Key-Objekt mit dem Signaturprüfschlüssel ist im Sicherheitsmodul vorhanden und ist aktiviert. (UC_VI_02_08: Use Case „Import eines Public Key (Vor-Personalisierung)“)

Ablauf:

Variante 1: mit Übergabe des Public Key im Kommando

Zusammenstellung der Signaturprüfdaten mit ihrer Signatur.

Bestimmung des Signaturprüfschlüssels.

- PSO VERIFY DIGITAL SIGNATURE (Signaturprüfdaten, Signatur, Signaturprüfschlüssel)

Variante 2: ohne Übergabe des Public Key im Kommando

Zusammenstellung der Signaturprüfdaten mit ihrer Signatur.

Bestimmung des Signaturprüfschlüssels bzw. des zugehörigen Public Key-Objektes (Speicherort im Filesystem, Key-Name). Selektion des DF, in dem das Public Key-Objekt mit dem Signaturprüfschlüssel gespeichert ist. (UC_VI_02_01: Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“)

- MSE SET (DST) (für Signaturverifikation vorgesehene Kommando-Variante 1.2; insbesondere Übergabe der Key Reference des Public Key-Objektes mit dem Signaturprüfschlüssel und Übergabe des zu verwendenden Krypto-Algorithmus)
- PSO VERIFY DIGITAL SIGNATURE (Signaturprüfdaten, Signatur)

Nachbedingungen:

- ---

2.2.8 Zugriff auf Technische Datenfelder im Sicherheitsmodul

UC_VI_02_12:

Use Case „Auslesen eines transparenten Technischen Datenfeldes“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Anwendung auf die transparenten Technischen Datenfelder EF.SecModAccess und EF.SecModCrypto.

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- MF ist selektiert. (UC_VI_02_01: Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“)

Ablauf:

Variante 1: Referenzierung des EF.SecModAccess bzw. EF.SecModCrypto via SELECT-Kommando

- SELECT (File-ID des EF.SecModAccess bzw. EF.SecModCrypto)
- READ BINARY

Variante 2: Referenzierung des EF.SecModAccess bzw. EF.SecModCrypto via SFI

- READ BINARY (SFI des EF.SecModAccess bzw. EF.SecModCrypto)

Nachbedingungen:

- ---

UC_VI_02_13:

Use Case „Auslesen eines Record-orientierten Technischen Datenfeldes“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Anwendung auf die Record-orientierten Technischen Datenfelder EF.SecModTRInfo und EF.SecModLifeCycle.

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- MF ist selektiert. (UC_VI_02_01: Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“)

Ablauf:

Variante 1: Referenzierung des EF.SecModTRInfo bzw. EF.SecModLifeCycle via SELECT-Kommando

- SELECT (File-ID des EF.SecModTRInfo bzw. EF.SecModLifeCycle)
- READ RECORD (Record-Nummer des auszulesenden Records)

Variante 2: Referenzierung des EF.SecModTRInfo bzw. EF.SecModLifeCycle via SFI

- READ RECORD (SFI des EF.SecModTRInfo bzw. EF.SecModLifeCycle, Record-Nummer des auszulesenden Records)

Nachbedingungen:

- ---

UC_VI_02_14:

Use Case „Update eines Record-orientierten Technischen Datenfeldes“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Anwendung auf das Record-orientierte Technische Datenfeld EF.SecModLifeCycle.

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- MF ist selektiert. (UC_VI_02_01: Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“)
- Update-Daten für das Technische Datenfeld liegen vor.

Ablauf:

Variante 1: Referenzierung des EF.SecModLifeCycle via SELECT-Kommando

- SELECT (File-ID des EF.SecModLifeCycle)
- UPDATE RECORD (Record-Nummer des zu schreibenden Records, Update-Daten)

Variante 2: Referenzierung des EF.SecModLifeCycle via SFI

- UPDATE RECORD (SFI des EF.SecModLifeCycle, Record-Nummer des zu schreibenden Records, Update-Daten)

Nachbedingungen:

- ---

2.3 Vor-Personalisierung 1

Findet die Teilphase „Vor-Personalisierung 1“ vor dem Setzen der GW-System-PIN als einem der Integrationsschritte in der Teilphase „Integration“ von Sicherheitsmodul und GW statt, so ist die GW-System-PIN noch nicht im Sicherheitsmodul gesetzt und es besteht noch keine PACE-gesicherte Kommunikationsverbindung zwischen Sicherheitsmodul und GW. Die für das Sicherheitsmodul für „Vor-Personalisierung 1“ auszuführenden Kommandos laufen – sofern der Sicherheitsmodul-Hersteller nichts anderes vorsieht – ggf. ohne Beteiligung des GW und ungesichert, d.h. ohne Secure Messaging ab.

Findet hingegen die Teilphase „Integration“ komplett vor der Teilphase „Vor-Personalisierung 1“ statt, so besteht zum Zeitpunkt der Teilphase „Vor-Personalisierung 1“ eine Kommunikationsverbindung zwischen GW und Sicherheitsmodul. Ferner ist in diesem Fall die GW-System-PIN im Sicherheitsmodul gesetzt, und für die Absicherung der Kommunikation zwischen GW und Sicherheitsmodul in der Teilphase „Vor-Personalisierung 1“ kann das PACE-Protokoll bzw. der PACE-Kanal zwischen GW und Sicherheitsmodul genutzt werden. Die Verwendung der PACE-Authentisierung und des PACE-Kanals zwischen GW und Sicherheitsmodul in der Teilphase „Vor-Personalisierung 1“ wird in diesem Fall empfohlen.

Soll in der Teilphase „Vor-Personalisierung 1“ der PACE-Kanal zwischen GW und Sicherheitsmodul genutzt werden, so ist für die im folgenden beschriebenen Use Cases in der Teilphase „Vor-Personalisierung 1“ zusätzlich folgender Punkt in die Vorbedingungen aufzunehmen:

- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)

Ferner erfolgen dann die in der Teilphase „Vor-Personalisierung 1“ auszuführenden Kommandos nunmehr mit Secure Messaging, soweit das betreffende Kommando dies seitens des Sicherheitsmoduls zulässt und die Nutzung von Secure Messaging im betreffenden Kommando angezeigt wird.

UC_VI_03_01:

Use Case „Import des SM-PKI-Root-Zertifikates in das Sicherheitsmodul (Vor-Personalisierung)“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Die Speicherung des SM-PKI-Root-Zertifikates erfolgt im transparenten Datenfeld EF.SMPKIRoot_x (sinnvollerweise x=1 für das initiale SM-PKI-Root-Zertifikat) im DF.SMGW. Ferner erfolgt zusätzlich die Speicherung des Root-Public Key aus dem SM-PKI-Root-Zertifikat im zugehörigen Public Key-Objekt Key.SMPKIRoot_x im DF.SMGW. Die zusätzliche Speicherung des Root-Public Key erfolgt aus dem Grund, als dass das Sicherheitsmodul bei Krypto-Operationen mit dem Root-Public Key mit diesem nur in Form eines Public Key-Objektes arbeiten und hierfür nicht auf den im Zertifikat enthaltenen Public Key zurückgreifen kann.

Hinsichtlich der Speicherung des Root-Public Key im Sicherheitsmodul hat der Integrator für die Übereinstimmung zwischen dem Root-Public Key im SM-PKI-Root-Zertifikat und dem importierten Public Key Sorge zu tragen.

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Zu schreibendes SM-PKI-Root-Zertifikat liegt vor.

Ablauf:

1.Schritt:

Selektion des DF.SMGW. (UC_VI_02_01: Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“)

2. Schritt: Import des SM-PKI-Root-Zertifikates

Variante 1: Referenzierung des EF.SMPKIRoot_x via SELECT-Kommando

- SELECT (File-ID des EF.SMPKIRoot_x)
- UPDATE BINARY (SM-PKI-Root-Zertifikat)

Variante 2: Referenzierung des EF.SMPKIRoot_x via SFI

- UPDATE BINARY (SFI des EF.SMPKIRoot_x, SM-PKI-Root-Zertifikat)

3. Schritt: Import des Root-Public Key (aus dem SM-PKI-Root-Zertifikat)

Extrahieren des Root-Public Key aus dem SM-PKI-Root-Zertifikat.

Durchführung von UC_VI_02_08: Use Case „Import eines Public Key (Vor-Personalisierung)“ für den Import des Root-Public Key in das Sicherheitsmodul und für die Speicherung des Root-Public Key im vorgesehenen Public Key-Objekt Key.SMPKIRoot_x.

4. Schritt: Aktivierung des EF.SMPKIRoot_x

Nach Abschluss des Schreibens des SM-PKI-Root-Zertifikates: Durchführung von UC_VI_02_02: Use Case „Aktivieren eines DF/EF (Vor-Personalisierung)“, angewandt auf EF.SMPKIRoot_x.

Nachbedingungen:

- ---

UC_VI_03_02:

Use Case „Generierung eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Anwendung für die onboard-Generierung der vorläufigen GW-Schlüsselpaare für die WAN-Kommunikation, d.h.

- (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE)
- (GW_WAN_SIG_PRV_PRE, GW_WAN_SIG_PUB_PRE)
- (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE)

Die Speicherung der vorgenannten vorläufigen GW-Schlüsselpaare erfolgt in den Key Pair-Objekten Key.WAN_TLS_PRE, Key.WAN_SIG_PRE bzw. Key.WAN_ENC_PRE im DF.SMGW.

Je nach verwendeter Kommando-Variante des Kommandos GENERATE ASYMMETRIC KEY PAIR erfolgt eine Schlüsselgenerierung mit oder ohne Ausgabe des Public Key.

Rollen:

Integrator, GW

Vorbedingungen:

- Siehe UC_VI_02_05: Use Case „Generierung eines ECC-Schlüsselpaares (Vor-Personalisierung)“, angewandt auf die vorläufigen GW-Schlüsselpaare und deren Key Pair-Objekte.

Ablauf:

Siehe UC_VI_02_05: Use Case „Generierung eines ECC-Schlüsselpaares (Vor-Personalisierung)“, angewandt auf die vorläufigen GW-Schlüsselpaare und deren Key Pair-Objekte.

Nachbedingungen:

- Siehe UC_VI_02_05: Use Case „Generierung eines ECC-Schlüsselpaares (Vor-Personalisierung)“, angewandt auf die vorläufigen GW-Schlüsselpaare und deren Key Pair-Objekte.

UC_VI_03_03:

Use Case „Export des Public Key eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Anwendung für den Export der vorläufigen GW-Public Keys

- GW_WAN_TLS_PUB_PRE
- GW_WAN_SIG_PUB_PRE
- GW_WAN_ENC_PUB_PRE

sofern der Export eines Public Keys eines zuvor onboard generierten vorläufigen GW-Schlüsselpaares nicht in UC_VI_03_02: Use Case „Generierung eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“ erfolgt.

Die Speicherung der vorläufigen GW-Schlüsselpaare erfolgt in den Key Pair-Objekten Key.WAN_TLS_PRE, Key.WAN_SIG_PRE bzw. Key.WAN_ENC_PRE im DF.SMGW. Siehe UC_VI_03_02: Use Case „Generierung eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“.

Rollen:

Integrator, GW

Vorbedingungen:

- Siehe UC_VI_02_06: Use Case „Export des Public Key eines ECC-Schlüsselpaares (Vor-Personalisierung)“, angewandt auf die vorläufigen GW-Schlüsselpaare und deren Key Pair-Objekte.

Ablauf:

Siehe UC_VI_02_06: Use Case „Export des Public Key eines ECC-Schlüsselpaares (Vor-Personalisierung)“, angewandt auf die vorläufigen GW-Schlüsselpaare und deren Key Pair-Objekte.

Nachbedingungen:

- Siehe UC_VI_02_06: Use Case „Export des Public Key eines ECC-Schlüsselpaares (Vor-Personalisierung)“, angewandt auf die vorläufigen GW-Schlüsselpaare und deren Key Pair-Objekte.

UC_VI_03_04:

Use Case „Erstellung des Zertifikatsrequest-Pakets für Gütesiegel-Zertifikate“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Anwendung für das Zertifikatsrequest-Paket mit den drei Zertifikatsrequests zu den vorläufigen GW-Schlüsselpaaren für die WAN-Kommunikation

- (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE)
- (GW_WAN_SIG_PRV_PRE, GW_WAN_SIG_PUB_PRE)
- (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE)

Für Details siehe [TR-03109-4].

Die Speicherung der vorläufigen GW-Schlüsselpaare erfolgt in den Key Pair-Objekten Key.WAN_TLS_PRE, Key.WAN_SIG_PRE bzw. Key.WAN_ENC_PRE im DF.SMGW. Siehe UC_VI_03_02: Use Case „Generierung eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“.

Die Generierung der Autorisierungssignatur zum Zertifikatsrequest-Paket liegt außerhalb des vorliegenden Use Case.

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Vorläufiges GW-Schlüsselpaar (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE), (GW_WAN_SIG_PRV_PRE, GW_WAN_SIG_PUB_PRE) bzw. (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE) wurde generiert und ist aktiviert. (UC_VI_03_02: Use Case „Generierung eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“).

Ablauf:

Zertifikatsrequest für das vorläufige TLS-Schlüsselpaar:

Sofern für das vorläufige Schlüsselpaar (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE) in UC_VI_03_02: Use Case „Generierung eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“ keine Ausgabe des Public Key-Parts erfolgt ist, Durchführung von

UC_VI_03_03: Use Case „Export des Public Key eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“ für den Export des Public Key GW_WAN_TLS_PUB_PRE.

Zusammenstellung des Zertifikatsrequests zum Public Key GW_WAN_TLS_PUB_PRE. Ergebnis: ZertRequest_TLS_PRE.

Für die innere Signatur des Zertifikatsrequests:

- Aufbereitung von ZertRequest_TLS_PRE für die innere Signatur (Hashing). Ergebnis: InputSig_ZertRequest_TLS_PRE.
- Durchführung von UC_VI_02_09: Use Case „Generieren einer Signatur / DST (Vor-Personalisierung)“ mit InputSig_ZertRequest_TLS_PRE als Signaturdaten und unter Nutzung von GW_WAN_TLS_PRV_PRE als Signaturschlüssel (→ „Selbst-Signatur des vorläufigen TLS-Schlüssels“). Ergebnis: Sig_ZertRequest_TLS_PRE.

Zusammenstellung des finalen Zertifikatsrequests zum vorläufigen TLS-Schlüsselpaar, bestehend aus ZertRequest_TLS_PRE und Sig_ZertRequest_TLS_PRE.

Zertifikatsrequest für das vorläufige SIG-Schlüsselpaar:

(analog zu „Zertifikatsrequest für das vorläufige TLS-Schlüsselpaar“)

Sofern für das vorläufige Schlüsselpaar (GW_WAN_SIG_PRV_PRE, GW_WAN_SIG_PUB_PRE) in UC_VI_03_02: Use Case „Generierung eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“ keine Ausgabe des Public Key-Parts erfolgt ist, Durchführung von UC_VI_03_03: Use Case „Export des Public Key eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“ für den Export des Public Key GW_WAN_SIG_PUB_PRE.

Zusammenstellung des Zertifikatsrequests zum Public Key GW_WAN_SIG_PUB_PRE. Ergebnis: ZertRequest_SIG_PRE.

Für die innere Signatur des Zertifikatsrequests:

- Aufbereitung von ZertRequest_SIG_PRE für die innere Signatur (Hashing). Ergebnis: InputSig_ZertRequest_SIG_PRE.
- Durchführung von UC_VI_02_09: Use Case „Generieren einer Signatur / DST (Vor-Personalisierung)“ mit InputSig_ZertRequest_SIG_PRE als Signaturdaten und unter Nutzung von GW_WAN_SIG_PRV_PRE als Signaturschlüssel (→ „Selbst-Signatur des vorläufigen SIG-Schlüssels“). Ergebnis: Sig_ZertRequest_SIG_PRE.

Zusammenstellung des finalen Zertifikatsrequests zum vorläufigen SIG-Schlüsselpaar, bestehend aus ZertRequest_SIG_PRE und Sig_ZertRequest_SIG_PRE.

Zertifikatsrequest für das vorläufige ENC-Schlüsselpaar:

(analog zu „Zertifikatsrequest für das vorläufige TLS-Schlüsselpaar“)

Sofern für das vorläufige Schlüsselpaar (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE) in UC_VI_03_02: Use Case „Generierung eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“ keine Ausgabe des Public Key-Parts erfolgt ist, Durchführung von UC_VI_03_03: Use Case „Export des Public Key eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“ für den Export des Public Key GW_WAN_ENC_PUB_PRE.

Zusammenstellung des Zertifikatsrequests zum Public Key GW_WAN_ENC_PUB_PRE. Ergebnis: ZertRequest_ENC_PRE.

Für die innere Signatur des Zertifikatsrequests:

- Aufbereitung von ZertRequest_ENC_PRE für die innere Signatur (Hashing). Ergebnis: InputSig_ZertRequest_ENC_PRE.
- Durchführung von UC_VI_02_10: Use Case „Generieren einer Signatur / AT (Vor-Personalisierung)“ mit InputSig_ZertRequest_ENC_PRE als Signaturdaten und unter Nutzung von GW_WAN_ENC_PRV_PRE als Signaturschlüssel (→ „Selbst-Signatur des vorläufigen ENC-Schlüssels“). Ergebnis: Sig_ZertRequest_ENC_PRE.

Zusammenstellung des finalen Zertifikatsrequests zum vorläufigen ENC-Schlüsselpaar, bestehend aus ZertRequest_ENC_PRE und Sig_ZertRequest_ENC_PRE.

Zertifikatsrequest-Paket:

Erstellung des Zertifikatsrequest-Pakets, bestehend aus

- ZertRequest_TLS_PRE und Sig_ZertRequest_TLS_PRE
- ZertRequest_SIG_PRE und Sig_ZertRequest_SIG_PRE
- ZertRequest_ENC_PRE und Sig_ZertRequest_ENC_PRE

Ergebnis: ZertRequestPaket_PRE.

Bei den vorläufigen GW-Schlüsselpaaren für die WAN-Kommunikation entfällt die äußere Signatur des Zertifikatsrequest-Pakets.

Nachbedingungen:

- ---

UC_VI_03_05:

Use Case „Import eines Gütesiegel-Zertifikates in das Sicherheitsmodul“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Anwendung für den Import der Gütesiegel-Zertifikate

- GW_WAN_TLS_CRT_PRE
- GW_WAN_SIG_CRT_PRE
- GW_WAN_ENC_CRT_PRE

zu den vorläufigen GW-Schlüsselpaaren

- (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE)
- (GW_WAN_SIG_PRV_PRE, GW_WAN_SIG_PUB_PRE)
- (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE)

in das Sicherheitsmodul und dortige Speicherung.

Die Speicherung der Gütesiegel-Zertifikate erfolgt in den transparenten Datenfeldern EF.GSCert_TLS, EF.GSCert_SIG bzw. EF.GSCert_ENC im DF.SMGW.

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Gütesiegel-Zertifikat GW_WAN_TLS_CRT_PRE, GW_WAN_SIG_CRT_PRE bzw. GW_WAN_ENC_CRT_PRE liegt im GW vor.

Ablauf:

Selektion des DF.SMGW. (UC_VI_02_01: Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“)

Für x=TLS, SIG bzw. ENC:

Variante 1: Referenzierung des EF.GSCert_x via SELECT-Kommando

- SELECT (File-ID des EF.GSCert_x)
- UPDATE BINARY (GW_WAN_x_CRT_PRE)

Variante 2: Referenzierung des EF.GSCert_x via SFI

- UPDATE BINARY (SFI des EF.GSCert_x, GW_WAN_x_CRT_PRE)

Nach Abschluss des Schreibens des Gütesiegel-Zertifikates: Durchführung von UC_VI_02_02: Use Case „Aktivieren eines DF/EF (Vor-Personalisierung)“, angewandt auf EF.GSCert_x.

Nachbedingungen:

- ---

2.4 Integration von Sicherheitsmodul und GW

UC_VI_04_01:

Use Case „Initiales Hochfahren des SMGW“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Beim Initialen Hochfahren des SMGW findet insbesondere das Pairing zwischen GW und Sicherheitsmodul statt. Die GW-System-PIN wird im Sicherheitsmodul gesetzt, genauer im PIN-Objekt PIN.GW im MF abgelegt.

Rollen:

GW

Vorbedingungen:

- Kommando-Kommunikation zwischen GW und Sicherheitsmodul ist möglich.
- PIN-Objekt zur Speicherung der GW-System-PIN ist vorhanden.

  (Hinweis: Die Anlage des PIN-Objektes PIN.GW für die GW-System-PIN ist im Rahmen der Initialisierung des Sicherheitsmoduls über das Initialisierungsfile bereits erfolgt.)

Ablauf:

GW-interne Generierung der GW-System-PIN. Alternativ externe Generierung der GW-System-PIN und Import in das GW.

- CHANGE REFERENCE DATA (Kommando-Variante Setzen einer PIN; insbesondere Übergabe der PIN Reference des PIN-Objektes PIN.GW sowie der GW-System-PIN selbst)

Nachbedingungen:

- Nach erfolgreicher Kommando-Ausführung ist die GW-System-PIN (als Referenzwert) im Sicherheitsmodul hinterlegt und steht nachfolgend für die Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul zur Verfügung.

UC_VI_04_02:

Use Case „Generierung eines Keys für die Speicherverschlüsselung des GW und Import in das Sicherheitsmodul“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Die Speicherung der symmetrischen GW-Keys erfolgt im Record-orientierten Datenfeld EF.GWKeys im DF.SMGW.

Rollen:

GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.

Ablauf:

Generierung des GW-Keys.

Selektion des DF.SMGW. (UC_VI_02_01: Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“)

Variante 1: Referenzierung des EF.GWKeys via SELECT-Kommando

- SELECT (File-ID des EF.GWKeys)
- UPDATE RECORD (Record-Nummer des Records für den zu schreibenden Key, GW-Key)

Variante 2: Referenzierung des EF.GWKeys via SFI

- UPDATE RECORD (SFI des EF.GWKeys, Record-Nummer des Records für den zu schreibenden Key, GW-Key)

Nach Abschluss des Schreibens des GW-Keys: Durchführung von UC_VI_02_02: Use Case „Aktivieren eines DF/EF (Vor-Personalisierung)“, angewandt auf EF.GWKeys (sofern EF.GWKeys nicht schon aktiviert ist).

Nachbedingungen:

- ---

2.5 Vor-Personalisierung 2

Für die nachfolgenden Use Cases wird davon ausgegangen, dass die Teilphasen „Vor-Personalisierung 1“ und „Integration“ von Sicherheitsmodul und GW abgeschlossen sind. So besteht zum Zeitpunkt der Teilphase „Vor-Personalisierung 2“ eine Kommunikationsverbindung zwischen GW und Sicherheitsmodul. Ferner ist die GW-System-PIN im Sicherheitsmodul gesetzt, und für die Absicherung der Kommunikation zwischen GW und Sicherheitsmodul in der Teilphase „Vor-Personalisierung 2“ kann das PACE-Protokoll bzw. der PACE-Kanal zwischen GW und Sicherheitsmodul genutzt werden. Die Verwendung der PACE-Authentisierung und des PACE-Kanals zwischen GW und Sicherheitsmodul in der Teilphase „Vor-Personalisierung 2“ wird empfohlen.

Soll in der Teilphase „Vor-Personalisierung 2“ der PACE-Kanal zwischen GW und Sicherheitsmodul genutzt werden, so ist für die im folgenden beschriebenen Use Cases in der Teilphase „Vor-Personalisierung 2“ zusätzlich folgender Punkt in die Vorbedingungen aufzunehmen:

- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)

Ferner erfolgen dann die in der Teilphase „Vor-Personalisierung 2“ auszuführenden Kommandos nunmehr mit Secure Messaging, soweit das betreffende Kommando dies seitens des Sicherheitsmoduls zulässt und die Nutzung von Secure Messaging im betreffenden Kommando angezeigt wird.

UC_VI_05_01:

Use Case „Import der Public Keys des GW-Administrators (Vor-Personalisierung)“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Anwendung für den Import des folgenden initialen Schlüsselmaterials des GW-Administrators, das in der „Initialen Konfigurationsdatei“ geliefert wird:

- GWADM_TLS_PUB
- GWADM_SIG_PUB
- GWADM_ENC_PUB
- GWADM_AUT_PUB

Die Speicherung der vorgenannten Administrationsschlüssel des GW-Administrators erfolgt in den Public Key-Objekten Key.GWA_TLS_x, Key.GWA_SIG_x, Key.GWA_ENC_x bzw. Key.GWA_AUT_x (sinnvollerweise x=1 für das initiale Schlüsselmaterial) im MF.

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Siehe UC_VI_02_08: Use Case „Import eines Public Key (Vor-Personalisierung)“, angewandt auf den Import der Administrator-Schlüssel GWADM_TLS_PUB, GWADM_SIG_PUB, GWADM_ENC_PUB und GWADM_AUT_PUB und deren Public Key-Objekte.
- „Initiale Konfigurationsdatei“ liegt vor.

Ablauf:

Extrahieren der Administrator-Schlüssel GWADM_TLS_PUB, GWADM_SIG_PUB, GWADM_ENC_PUB bzw. GWADM_AUT_PUB aus den in der „Initialen Konfigurationsdatei“ gelieferten Zertifikaten GWADM_TLS_CRT, GWADM_SIG_CRT, GWADM_ENC_CRT bzw. GWADM_AUT_CRT aus der SM-PKI.

Durchführung von UC_VI_02_08: Use Case „Import eines Public Key (Vor-Personalisierung)“, angewandt auf den Import der Administrator-Schlüssel GWADM_TLS_PUB, GWADM_SIG_PUB, GWADM_ENC_PUB bzw. GWADM_AUT_PUB und deren Public Key-Objekte.

Nachbedingungen:

- Siehe UC_VI_02_08: Use Case „Import eines Public Key (Vor-Personalisierung)“, angewandt auf den Import der Administrator-Schlüssel GWADM_TLS_PUB, GWADM_SIG_PUB, GWADM_ENC_PUB und GWADM_AUT_PUB und deren Public Key-Objekte.

UC_VI_05_02:

Use Case „Prüfung einer Zertifikatskette (Vor-Personalisierung)“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Betrachtet wird hier die Prüfung einer Kette von X.509-Zertifikaten bis zur SM-PKI-Root im Rahmen der SM-PKI. Für Details siehe [TR-03109-4].

Die Prüfung einer Zertifikatskette baut auf der Prüfung einzelner (Zertifikats-) Signaturen auf. Für das Parsen der beteiligten X.509-Zertifikate ist das GW zuständig.

Für den Use Case wird angenommen, dass das SM-PKI-Root-Zertifikat im transparenten Datenfeld EF.SMPKIRoot_x im DF.SMGW und der Root-Public Key des Zertifikates im zugehörigen Public Key-Objekt Key.SMPKIRoot_x im DF.SMGW gespeichert ist.

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.

- Kette der zu prüfenden Zertifikate (bis ggf. auf das SM-PKI-Root-Zertifikat) liegt im GW vor.
- Der Root-Public Key der SM-PKI liegt im Sicherheitsmodul vor und ist aktiviert. Der im Sicherheitsmodul im Public Key-Objekt Key.SMPKIRoot_x gespeicherte Root-Public Key stimmt mit dem Public Key des SM-PKI-Root-Zertifikates, das im zum Root-Public Key zugehörigen Datenfeld EF.SMPKIRoot_x im Sicherheitsmodul abgelegt ist, überein. (UC_VI_03_01: Use Case „Import des SM-PKI-Root-Zertifikates in das Sicherheitsmodul (Vor-Personalisierung)“)

Ablauf:

Fortlaufende Anwendung von UC_VI_02_11: Use Case „Prüfen einer Signatur (Vor-Personalisierung)“. Für die einzelnen zu prüfenden Zertifikate ist jeweils der Zertifikatsbody und die Signatur des Zertifikates aus dem Zertifikat zu extrahieren sowie der relevante Signaturprüfschlüssel zu bestimmen und ggf. dieser Signaturprüfschlüssel in das Sicherheitsmodul zu importieren (Übergabe des Signaturprüfschlüssels im Kommando PSO VERIFY DIGITAL SIGNATURE oder Anwendung von UC_VI_02_08: Use Case „Import eines Public Key (Vor-Personalisierung)“), falls der Signaturprüfschlüssel nicht anderweitig schon im Sicherheitsmodul vorliegt.

Für die Prüfung gegen das SM-PKI-Root-Zertifikat:

Signaturprüfschlüssel ist der im Sicherheitsmodul im Public Key-Objekt Key.SMPKIRoot_x hinterlegte Root-Public Key (der mit dem Public Key des SM-PKI-Root-Zertifikates, das im zugehörigen Datenfeld EF.SMPKIRoot_x abgelegt ist, übereinstimmt).

Nachbedingungen:

- ---

UC_VI_05_03:

Use Case „Prüfung der in der Initialen Konfigurationsdatei gelieferten Zertifikate des GW-Administrators (Vor-Personalisierung)“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- „Initiale Konfigurationsdatei“ liegt vor.

Ablauf:

Aufbereitung der „Initialen Konfigurationsdatei“, insbesondere Extrahieren der Zertifikate des GW-Administrators sowie der Zertifikate in den jeweils zugehörigen Zertifikatsketten.

Bestimmen der Signaturprüfschlüssel für die Prüfung der einzelnen Zertifikate.

Für jedes der Zertifikate des GW-Administrators:

Durchführung von UC_VI_05_02: Use Case „Prüfung einer Zertifikatskette (Vor-Personalisierung)“.

Nachbedingungen:

- ---

UC_VI_05_04:

Use Case „Prüfung der Signatur der Initialen Konfigurationsdatei (Vor-Personalisierung)“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Die „Initiale Konfigurationsdatei“ ist mit dem Signaturschlüssel GWADM_SIG_PRV des GW-Administrators signiert. Diese Signatur ist unter Verwendung des zugehörigen Signaturprüfschlüssels GWADM_SIG_PUB zu prüfen.

Auch wenn der Signaturprüfschlüssel GWADM_SIG_PUB ggf. schon im Public Key-Objekt Key.GWA_SIG_x im MF gespeichert sein sollte, kann dieses Public Key-Objekt nicht zur Signaturprüfung benutzt werden, da die Zugriffsregeln des Sicherheitsmoduls für die Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“ eine Verwendung der Schlüssel des GW-Administrators nicht zulassen.

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- „Initiale Konfigurationsdatei“ liegt vor. In dieser Datei ist insbesondere der Signaturprüfschlüssel GWADM_SIG_PUB des GW-Administrators enthalten.

Ablauf:

Extrahieren des Signaturprüfschlüssels GWADM_SIG_PUB des GW-Administrators aus dem zugehörigen Zertifikat in der „Initialen Konfigurationsdatei“.

Extrahieren der zu prüfenden Signatur der „Initialen Konfigurationsdatei“ aus derselbigen.

Durchführung von UC_VI_02_11: Use Case „Prüfen einer Signatur (Vor-Personalisierung)“ für die Prüfung der Signatur der „Initialen Konfigurationsdatei“ unter Nutzung des Signaturprüfschlüssels GWADM_SIG_PUB. Hierzu Nutzung des vorgenannten Use Case in der Variante 1 mit dem Kommando PSO VERIFY DIGITAL SIGNATURE „mit Übergabe des Public Key im Kommando“ zur Übergabe des Signaturprüfschlüssels GWADM_SIG_PUB an das Sicherheitsmodul.

Nachbedingungen:

- ---

UC_VI_05_05:

Use Case „Löschen der Import-Schlüssel (Vor-Personalisierung)“

Phase:

Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Hinweise:

Anwendung zum Abschluss der Teilphase „Vor-Personalisierung 2“.

Mit dem Löschen aller Key-Objekte, die Import-Schlüssel für den Import von Public Keys speichern, wird die Vor-Personalisierung des Sicherheitsmoduls abgeschlossen. Ein nachfolgender Import von Public Keys und insbesondere ein nachfolgendes Update von SM-PKI-Root-Zertifikaten ist nur unter Beteiligung des GW-Administrators möglich, siehe Kap. 4.4.

Die Speicherung der Import-Schlüssel erfolgt in den Key Pair-Objekten Key.IMP_TRANS und Key.IMP sowie in den Public Key-Objekten Key.IMP_PUB_TRANS und Key.IMP_PUB im MF.

Rollen:

Integrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Siehe UC_VI_02_03: Use Case „Löschen eines Key-Objektes (Vor-Personalisierung)“, angewandt auf das Löschen von allen Import-Keys und deren Key-Objekten.

Ablauf:

Durchführung von UC_VI_02_03: Use Case „Löschen eines Key-Objektes (Vor-Personalisierung)“ für das Löschen von allen Import-Keys und deren Key-Objekten.

Nachbedingungen:

- Siehe UC_VI_02_03: Use Case „Löschen eines Key-Objektes (Vor-Personalisierung)“, angewandt auf das Löschen von allen Import-Keys und deren Key-Objekten.
- Ein nachfolgender Import von Public Keys und insbesondere ein nachfolgendes Update von SM-PKI-Root-Zertifikaten ist nur unter Beteiligung des GW-Administrators möglich, siehe Kap. 4.4.

3 Installation + Vor-Ort-Inbetriebnahme des SMGW

In der Phase „Installation + Vor-Ort-Inbetriebnahme des SMGW“ erfolgen keine Arbeiten am SMGW, die das Sicherheitsmodul betreffen. Aus diesem Grund werden im vorliegenden Dokument für diese Phase keine Use Cases definiert.

4 Personalisierung, Normalbetrieb (End-Usage) und Außerbetriebnahme des SMGW

Relevantes Security Environment für die Phase „Personalisierung des SMGW“: Siehe [TR-03109-2], Kap. 3.3.1, 3.3.3.3.

Relevantes Security Environment für die Phase „Normalbetrieb des SMGW“ sowie für die Phase „Außerbetriebnahme des Sicherheitsmoduls“: Siehe [TR-03109-2], Kap. 3.3.1, 3.3.3.3.

4.1 Auswahl und Setzen des Security Environment

Im vorliegenden Kapitel ist beim Use Case bei Beteiligung des GW-Administrators der Vollständigkeit halber in den Vorbedingungen der TLS-Kanal zwischen GW-Administrator und GW aufgenommen, da die Administrationstätigkeiten des GW-Administrators über diesen TLS-Kanal laufen. Der TLS-Kanal zwischen GW-Administrator und GW nimmt jedoch keinen direkten Einfluss auf die Administration des Sicherheitsmoduls, da dieser Kanal im GW endet und nicht bis zum Sicherheitsmodul reicht.

UC_PN_01_01:

Use Case „Auswahl und Setzen des Security Environment“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Das Auswählen und Setzen des SE wird erforderlich, sofern nicht schon bereits das für diese Phasen relevante SE gesetzt ist. Beim Start bzw. Hochfahren des Sicherheitsmoduls ist defaultmäßig das SE mit SEID = 01 gesetzt.

Ausführung ohne Secure Messaging.

Rollen:

GW, GW-Administrator

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Falls der GW-Administrator beteiligt ist: TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)

Ablauf:

➢ MSE RESTORE (SEID für Phase „Personalisierung des SMGW“ bzw. „Normalbetrieb des SMGW“)

Nachbedingungen:

- Es gelten die Zugriffsregeln wie für das zur Phase „Personalisierung des SMGW“ bzw. „Normalbetrieb des SMGW“ zugeordnete Security Environment definiert. Siehe [TR-03109-2], Kap. 3.3.1, 3.3.3.3.

4.2 Zugriff auf Technische Datenfelder im Sicherheitsmodul

Im vorliegenden Kapitel ist bei den Use Cases bei Beteiligung des GW-Administrators der Vollständigkeit halber in den Vorbedingungen der TLS-Kanal zwischen GW-Administrator und GW aufgenommen, da die Administrationstätigkeiten des GW-Administrators über diesen TLS-Kanal laufen. Der TLS-Kanal zwischen GW-Administrator und GW nimmt jedoch keinen direkten Einfluss auf die Administration des Sicherheitsmoduls, da dieser Kanal im GW endet und nicht bis zum Sicherheitsmodul reicht.

UC_PN_02_01:

Use Case „Auslesen eines transparenten Technischen Datenfeldes“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Anwendung auf die transparenten Technischen Datenfelder EF.SecModAccess und EF.SecModCrypto.

Ausführung ohne Secure Messaging.

Rollen:

GW, GW-Administrator

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Falls der GW-Administrator beteiligt ist: TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- MF ist selektiert. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

Ablauf:

Variante 1: Referenzierung des EF.SecModAccess bzw. EF.SecModCrypto via SELECT-Kommando

- SELECT (File-ID des EF.SecModAccess bzw. EF.SecModCrypto)
- READ BINARY

Variante 2: Referenzierung des EF.SecModAccess bzw. EF.SecModCrypto via SFI

- READ BINARY (SFI des EF.SecModAccess bzw. EF.SecModCrypto)

Nachbedingungen:

- ---

UC_PN_02_02:

Use Case „Auslesen eines Record-orientierten Technischen Datenfeldes“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Anwendung auf die Record-orientierten Technischen Datenfelder EF.SecModTRInfo und EF.SecModLifeCycle.

Für das Technische Datenfeld EF.SecModTRInfo erfolgt die Ausführung der Kommandos ohne Secure Messaging, für das Technische Datenfeld EF.SecModLifeCycle mit Secure Messaging.

Rollen:

GW, GW-Administrator

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Für das Technische Datenfeld EF.SecModLifeCycle: Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- Falls der GW-Administrator beteiligt ist: TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- MF ist selektiert. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

Ablauf:

Variante 1: Referenzierung des EF.SecModTRInfo bzw. EF.SecModLifeCycle via SELECT-Kommando

- SELECT (File-ID des EF.SecModTRInfo bzw. EF.SecModLifeCycle)
- READ RECORD (Record-Nummer des auszulesenden Records)

Variante 2: Referenzierung des EF.SecModTRInfo bzw. EF.SecModLifeCycle via SFI

- READ RECORD (SFI des EF.SecModTRInfo bzw. EF.SecModLifeCycle, Record-Nummer des auszulesenden Records)

Nachbedingungen:

- ---

UC_PN_02_03:

Use Case „Update eines Record-orientierten Technischen Datenfeldes“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Anwendung auf das Record-orientierte Technische Datenfeld EF.SecModLifeCycle.

Ausführung mit Secure Messaging.

Rollen:

GW, GW-Administrator

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- Falls der GW-Administrator beteiligt ist: TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- MF ist selektiert. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)
- Update-Daten für das Technische Datenfeld liegen vor.

Ablauf:

Variante 1: Referenzierung des EF.SecModLifeCycle via SELECT-Kommando

- SELECT (File-ID des EF.SecModLifeCycle)
- UPDATE RECORD (Record-Nummer des zu schreibenden Records, Update-Daten)

Variante 2: Referenzierung des EF.SecModLifeCycle via SFI

- UPDATE RECORD (SFI des EF.SecModLifeCycle, Record-Nummer des zu schreibenden Records, Update-Daten)

Nachbedingungen:

- ---

4.3 Sicherungsmechanismen des SMGW

Im vorliegenden Kapitel ist bei den Use Cases bei Beteiligung des GW-Administrators der Vollständigkeit halber in den Vorbedingungen der TLS-Kanal zwischen GW-Administrator und GW aufgenommen, da die Administrationstätigkeiten des GW-Administrators über diesen TLS-Kanal laufen. Der TLS-Kanal zwischen GW-Administrator und GW nimmt jedoch keinen direkten Einfluss auf die Administration des Sicherheitsmoduls, da dieser Kanal im GW endet und nicht bis zum Sicherheitsmodul reicht.

UC_PN_03_01:

Use Case „PACE-Authentisierung“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Die Speicherung der GW-System-PIN erfolgt im PIN-Objekt PIN.GW im MF.

Ausführung ohne Secure Messaging.

Rollen:

GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- MF ist selektiert. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)
- GW-System-PIN ist im Sicherheitsmodul im PIN-Objekt PIN.GW als Referenzwert vorhanden.

Ablauf:

- MSE SET (AT) (für PACE vorgesehene Kommando-Variante 2.2; insbesondere Übergabe der PIN Reference des PIN-Objektes PIN.GW)
- GENERAL AUTHENTICATE / PACE (Kommando-Sequenz aus mehreren Kommandos)

Nachbedingungen:

- Die erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul setzt im Sicherheitsmodul den Sicherheitszustand PACE. Ferner besteht ein sicherer Kanal zwischen GW und Sicherheitsmodul für den nachfolgenden Datenverkehr.

UC_PN_03_02:

Use Case „Wechsel der GW-System-PIN“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Betrachtet wird der Wechsel der GW-System-PIN, die im Rahmen des PACE-Protokolls zwischen GW und Sicherheitsmodul Verwendung findet und im Sicherheitsmodul im PIN-Objekt PIN.GW abgelegt ist.

Ausführung mit Secure Messaging.

Rollen:

GW, GW-Administrator

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. Das PACE-Protokoll wird unter Verwendung der alten GW-System-PIN, die im GW vorliegt sowie im Sicherheitsmodul im PIN-Objekt PIN.GW als Referenzwert hinterlegt ist, durchgeführt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- Falls der GW-Administrator beteiligt ist: TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- MF ist selektiert. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)
- Neue GW-System-PIN liegt im GW vor.

Ablauf:

- CHANGE REFERENCE DATA (Kommando-Variante Wechseln einer PIN; insbesondere Übergabe der PIN Reference des PIN-Objektes PIN.GW sowie von alter und neuer GW-System-PIN)

Nachbedingungen:

- Ein Wechsel der GW-System-PIN über das Kommando CHANGE REFERENCE DATA bedingt nicht notwendig ein Zurücksetzen des Sicherheitszustandes PACE oder ein Schließen des bestehenden sicheren Kanals zwischen GW und Sicherheitsmodul, der zuvor über das PACE-Protokoll mit der alten GW-System-PIN aufgebaut wurde. Es wird daher empfohlen, über den Aufruf des Kommandos MANAGE CHANNEL explizit ein Zurücksetzen des Sicherheitszustandes PACE (inklusive Schließen des sicheren Kanals und Löschen der zugehörigen Session Keys) herbeizuführen (UC_PN_03_03: Use Case „Zurücksetzen des Sicherheitszustandes PACE“). Für nachfolgende Zugriffe auf das Sicherheitsmodul, die einen gesetzten Sicherheitszustand PACE bzw. einen sicheren Kanal zwischen GW und Sicherheitsmodul erfordern, ist bei Umsetzung der Empfehlung dann das PACE-Protokoll erneut - nun mit der neuen GW-System-PIN - erfolgreich auszuführen (UC_PN_03_01: Use Case „PACE-Authentisierung“).

UC_PN_03_03:

Use Case „Zurücksetzen des Sicherheitszustandes PACE“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Anwendung zum gezielten Zurücksetzen eines gesetzten Sicherheitszustandes PACE im Sicherheitsmodul in Verbindung mit dem Schließen des bestehenden sicheren Kanals zwischen GW und Sicherheitsmodul, der zuvor über das PACE-Protokoll mit der GW-System-PIN aufgebaut wurde, sowie in Verbindung mit dem Löschen zugehöriger Session Keys.

Ausführung ohne Secure Messaging.

Rollen:

GW, GW-Administrator

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- Falls der GW-Administrator beteiligt ist: TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)

Ablauf:

Durchführung von UC_PN_04_23: Use Case „Zurücksetzen der Applikationsebene des Sicherheitsmoduls“.

Nachbedingungen:

- Siehe Nachbedingungen in UC_PN_04_23: Use Case „Zurücksetzen der Applikationsebene des Sicherheitsmoduls“. Die erfolgreiche Ausführung des Kommandos MANAGE CHANNEL führt insbesondere zum Zurücksetzen des Sicherheitszustandes PACE, der die gegenseitige Authentisierung und den sicheren Kanal zwischen GW und Sicherheitsmodul anzeigt. Für nachfolgende Zugriffe auf das Sicherheitsmodul, die einen gesetzten Sicherheitszustand PACE bzw. einen sicheren Kanal zwischen GW und Sicherheitsmodul erfordern, ist das PACE-Protokoll erneut erfolgreich auszuführen (UC_PN_03_01: Use Case „PACE-Authentisierung“).

UC_PN_03_04:

Use Case „Auslesen eines symmetrischen GW-Keys“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Die Speicherung der symmetrischen GW-Keys erfolgt im Record-orientierten Datenfeld EF.GWKeys im DF.SMGW.

Ausführung mit Secure Messaging.

Rollen:

GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- DF.SMGW ist selektiert. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

Ablauf:

Variante 1: Referenzierung des EF.GWKeys via SELECT-Kommando

- SELECT (File-ID des EF.GWKeys)
- READ RECORD (Record-Nummer des Records mit dem auszulesenden Key)

Variante 2: Referenzierung des EF.GWKeys via SFI

- READ RECORD (SFI des EF.GWKeys, Record-Nummer des Records mit dem auszulesenden Key)

Nachbedingungen:

- ---

UC_PN_03_05:

Use Case „Update eines symmetrischen GW-Keys“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Die Speicherung der symmetrischen GW-Keys erfolgt im Record-orientierten Datenfeld EF.GWKeys im DF.SMGW.

Ausführung mit Secure Messaging.

Rollen:

GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- DF.SMGW ist selektiert. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)
- Zu schreibender GW-Key liegt vor.

Ablauf:

Variante 1: Referenzierung des EF.GWKeys via SELECT-Kommando

- SELECT (File-ID des EF.GWKeys)
- UPDATE RECORD (Record-Nummer des Records für den zu schreibenden Key, GW-Key)

Variante 2: Referenzierung des EF.GWKeys via SFI

- UPDATE RECORD (SFI des EF.GWKeys, Record-Nummer des Records für den zu schreibenden Key, GW-Key)

Nachbedingungen:

- ---

4.4 Administration des SMGW

In den folgenden Unterkapiteln ist bei den Use Cases, soweit sinnvoll, der Vollständigkeit halber in den Vorbedingungen der TLS-Kanal zwischen GW-Administrator und GW aufgenommen, da die Administrationstätigkeiten des GW-Administrators über diesen TLS-Kanal laufen. Der TLS-Kanal zwischen GW-Administrator und GW nimmt jedoch keinen direkten Einfluss auf die Administration des Sicherheitsmoduls, da dieser Kanal im GW endet und nicht bis zum Sicherheitsmodul reicht.

4.4.1 Sicherung der Administrationstätigkeiten des GW-Administrators

UC_PN_04_01:

Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Siehe die Ausführungen zum allgemeinen Anwendungsfall UC_PN_05_05: Use Case „Aufbau eines TLS-Kanals zwischen externer Welt und SMGW / SMGW in der Rolle TLS-Client“.

Relevante Keys in der Phase Personalisierung:

- Vorläufiges TLS-Key Pair (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE) des GW im Sicherheitsmodul
- TLS-Key Pair (GWADM_TLS_PRV, GWADM_TLS_PUB) des GW-Administrators

Relevante Keys in der Phase Normalbetrieb:

- Betriebs-TLS-Key Pair (GW_WAN_TLS_PRV, GW_WAN_TLS_PUB) des GW im Sicherheitsmodul
- TLS-Key Pair (GWADM_TLS_PRV, GWADM_TLS_PUB) des GW-Administrators

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Siehe UC_PN_05_05: Use Case „Aufbau eines TLS-Kanals zwischen externer Welt und SMGW / SMGW in der Rolle TLS-Client“ unter Verwendung des o.g. Schlüsselmaterials.

Ablauf:

Siehe UC_PN_05_05: Use Case „Aufbau eines TLS-Kanals zwischen externer Welt und SMGW / SMGW in der Rolle TLS-Client“ unter Verwendung des o.g. Schlüsselmaterials.

Nachbedingungen:

- Siehe UC_PN_05_05: Use Case „Aufbau eines TLS-Kanals zwischen externer Welt und SMGW / SMGW in der Rolle TLS-Client“ unter Verwendung des o.g. Schlüsselmaterials.

UC_PN_04_02:

Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Relevantes Schlüsselmaterial:

- AUT-Key Pair (GWADM_AUT_PRV, GWADM_AUT_PUB) des GW-Administrators

Das Public Key-Objekt für den Public Key GWADM_AUT_PUB ist durch Key.GWA_AUT_x (x=1 oder 2) im MF gegeben.

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- AUT-Key Pair (GWADM_AUT_PRV, GWADM_AUT_PUB) des GW-Administrators existiert.
- Public Key GWADM_AUT_PUB des GW-Administrators liegt im Sicherheitsmodul vor und ist aktiviert. (Aus der Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“ ist das Schlüsselmaterial bereits im Sicherheitsmodul vorhanden, bzw. für Schlüsselwechsel siehe UC_PN_04_11: Use Case „Import eines Public Key“, ggf. UC_PN_04_07: Use Case „Aktivieren eines Key-Objektes“.) Der Public Key GWADM_AUT_PUB ist im Public Key-Objekt Key.GWA_AUT_x (x=1 oder 2) im MF gespeichert.

Ablauf:

Hinweis: Das Public Key-Objekt Key.GWA_AUT_x (x=1 oder 2) für den Public Key GWADM_AUT_PUB des GW-Administrators ist im MF angesiedelt und wird bei der Schlüsselsuche stets gefunden, so dass eine Selektion des MF nicht erforderlich ist.

- MSE SET (AT) (für EXTERNAL AUTHENTICATE vorgesehene Kommando-Variante 2.3; insbesondere Übergabe der Key Reference des Public Key-Objektes für GWADM_AUT_PUB als Authentisierungsschlüssel und Übergabe des zu verwendenden Krypto-Algorithmus)
- GET CHALLENGE (16 Byte Challenge wie für das folgende Kommando EXTERNAL AUTHENTICATE benötigt)

Übermittlung der Challenge an den GW-Administrator (im bestehenden TLS-Kanal zwischen GW-Administrator und GW).

Generierung des Authentisierungstokens durch den GW-Administrator unter Verwendung von GWADM_AUT_PRV.

Übermittlung des Authentisierungstokens vom GW-Administrator an das GW (im bestehenden TLS-Kanal zwischen GW-Administrator und GW).

- EXTERNAL AUTHENTICATE (Authentisierungstoken des GW-Administrators)

Nachbedingungen:

- Erfolgreiche Ausführung der Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul setzt im Sicherheitsmodul den Sicherheitszustand AUTH.

UC_PN_04_03:

Use Case „Zurücksetzen des Sicherheitszustandes AUTH“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Anwendung zum gezielten Zurücksetzen eines gesetzten Sicherheitszustandes AUTH im Sicherheitsmodul zum Abschluss der Administrationstätigkeiten des GW-Administrators.

Ausführung ohne Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (UC_PN_04_02: Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“)

Ablauf:

Durchführung von UC_PN_04_23: Use Case „Zurücksetzen der Applikationsebene des Sicherheitsmoduls“.

Nachbedingungen:

- Siehe Nachbedingungen in UC_PN_04_23: Use Case „Zurücksetzen der Applikationsebene des Sicherheitsmoduls“. Die erfolgreiche Ausführung des Kommandos MANAGE CHANNEL führt insbesondere zum Zurücksetzen des Sicherheitszustandes AUTH, der die Administrationstätigkeiten am Sicherheitsmodul absichert. Nachfolgende Administrationstätigkeiten des GW-Administrators erfordern eine erneute Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul (UC_PN_04_02: Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“).

UC_PN_04_04:

Use Case „Wechsel des GW-Administrators“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Der Wechsel des GW-Administrators ist mit dem Wechsel der Administrationsschlüssel des GW-Administrators verbunden.

Über das Initialisierungsfile des Sicherheitsmoduls sind bereits zwei Sätze von Public Key-Objekten für die Administrationsschlüssel des GW-Administrators angelegt (x=1 bzw. 2):

- Public Key-Objekt Key.GWA_TLS_x für die Ablage des TLS-Public Key des GW-Administrators

- Public Key-Objekt Key.GWA_SIG_x für die Ablage des SIG-Public Key des GW-Administrators
- Public Key-Objekt Key.GWA_ENC_x für die Ablage des ENC-Public Key des GW-Administrators
- Public Key-Objekt Key.GWA_AUT_x für die Ablage des AUT-Public Key des GW-Administrators

Der Use Case betrachtet den Fall, dass die Administrationsschlüssel des alten GW-Administrators in den o.g. Public Key-Objekten für x=1 abgelegt sind und die Administrationsschlüssel des neuen GW-Administrators in den o.g. Public Key-Objekten für x=2 abgelegt werden sollen, um ein direktes Überschreiben der alten Administrationsschlüssel zu vermeiden.

Der Import der neuen Administrationsschlüssel erfordert die Mitwirkung des alten GW-Administrators.

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- Erfolgreiche Authentisierung des alten GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (UC_PN_04_02: Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“)
- Public Key-Objekt Key.GWA_SIG_1 ist vorhanden, ist mit Schlüsseldaten gefüllt und ist aktiviert. (ggf. UC_PN_04_07: Use Case „Aktivieren eines Key-Objektes“)

Ablauf:

Wiederholte Durchführung von UC_PN_04_13: Use Case „Prüfung einer Zertifikatskette (SM-PKI)“ für die Prüfung der Zertifikate zu den Public Keys des neuen GW-Administrators.

Wiederholte Durchführung von UC_PN_04_11: Use Case „Import eines Public Key“ für den Import der Public Keys des neuen GW-Administrators. Die für den Import der Public Keys erforderlichen Import-Zertifikate werden dabei durch den alten GW-Administrator erstellt und mit seinem privaten Signaturschlüssel (passend zum in Key.GWA_SIG_1 gespeicherten Public Key) signiert. Ferner werden in den Import-Zertifikaten die mit den Public Keys des neuen GW-Administrators zu befüllenden Public Key-Objekte entsprechend referenziert, derart dass der neue TLS-Public Key im Public Key-Objekt Key.GWA_TLS_2, der neue SIG-Public Key im Public Key-Objekt Key.GWA_SIG_2, der neue ENC-Public Key im Public Key-Objekt Key.GWA_ENC_2 und der neue AUT-Public Key im Public Key-Objekt Key.GWA_AUT_2 gespeichert werden.

Sollen die Public Keys des neuen GW-Administrators zunächst noch nicht aktiv sein, so Anwendung von UC_PN_04_08: Use Case „Deaktivieren eines Key-Objektes“ zur Deaktivierung der entsprechenden Public Key-Objekte, hier also Key.GWA_TLS_2, Key.GWA_SIG_2,

Key.GWA_ENC_2 und Key.GWA_AUT_2. Sollen anschließend zu gegebener Zeit die Public Keys des neuen GW-Administrators aktiv geschaltet werden, so Anwendung von UC_PN_04_07: Use Case „Aktivieren eines Key-Objektes“ zur Aktivierung der entsprechenden Public Key-Objekte, hier also Key.GWA_TLS_2, Key.GWA_SIG_2, Key.GWA_ENC_2 und Key.GWA_AUT_2.

Nachbedingungen:

- Sofern durch den alten GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (UC_PN_04_03: Use Case „Zurücksetzen des Sicherheitszustandes AUTH“)
- Sobald die Administrationsschlüssel des alten GW-Administrators nicht mehr benötigt werden und nur noch der neue GW-Administrator Administrationstätigkeiten am Sicherheitsmodul vornehmen (können) soll, wird empfohlen, die entsprechenden Public Key-Objekte, hier also Key.GWA_TLS_1, Key.GWA_SIG_1, Key.GWA_ENC_1 und Key.GWA_AUT_1 zu deaktivieren (UC_PN_04_08: Use Case „Deaktivieren eines Key-Objektes“). Bei einer Deaktivierung der Public Keys des alten GW-Administrators sollte aber dafür Sorge getragen werden, dass zuvor die Public Keys des neuen GW-Administrators (hier: Public Key-Objekte Key.GWA_TLS_2, Key.GWA_SIG_2, Key.GWA_ENC_2 und Key.GWA_AUT_2) aktiviert wurden (UC_PN_04_07: Use Case „Aktivieren eines Key-Objektes“), damit der neue GW-Administrator die weiteren Administrationstätigkeiten vornehmen kann.

4.4.2 Schlüsselmanagement

UC_PN_04_05:

Use Case „Anlegen eines Key-Objektes“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (UC_PN_04_02: Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“)

Ablauf:

Selektion des DF, in dem das neue Key-Objekt angelegt werden soll. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

- CREATE KEY (Übergabe der Key Reference des anzulegenden Key-Objektes inkl. weiterer Informationen zum Key-Objekt)

Nachbedingungen:

- Bei der Anlage eines Key-Objektes über das Kommando CREATE KEY besitzt das Key-Attribut Key-LifeCycleStatus den Wert „initialisation“. Vor Nutzung des Key-Objektes z.B. für Krypto-Operationen ist dieses mit Schlüsseldaten zu füllen. Für ein Key Pair-Objekt erfolgt dies mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR, siehe UC_PN_04_09: Use Case „Generierung eines ECC-Schlüsselpaares“; für ein Public Key-Objekt erfolgt dies mittels des Kommandos PSO VERIFY CERTIFICATE, siehe UC_PN_04_11: Use Case „Import eines Public Key“).
- Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (UC_PN_04_03: Use Case „Zurücksetzen des Sicherheitszustandes AUTH“)

UC_PN_04_06:

Use Case „Löschen eines Key-Objektes“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (UC_PN_04_02: Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“)
- Zu löschendes Key-Objekt ist deaktiviert. (UC_PN_04_08: Use Case „Deaktivieren eines Key-Objektes“)

Ablauf:

Selektion des DF, in dem das zu löschende Key-Objekt liegt. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

- DELETE KEY (Übergabe der Key Reference des zu löschenden Key-Objektes)

Nachbedingungen:

- Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (UC_PN_04_03: Use Case „Zurücksetzen des Sicherheitszustandes AUTH“)

UC_PN_04_07:

Use Case „Aktivieren eines Key-Objektes“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (UC_PN_04_02: Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“)

Ablauf:

Selektion des DF, in dem das zu aktivierende Key-Objekt liegt. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“

- ACTIVATE KEY (Übergabe der Key Reference des zu aktivierenden Key-Objektes)

Nachbedingungen:

- Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (UC_PN_04_03: Use Case „Zurücksetzen des Sicherheitszustandes AUTH“)

UC_PN_04_08:

Use Case „Deaktivieren eines Key-Objektes“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (UC_PN_04_02: Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“)

Ablauf:

Selektion des DF, in dem das zu deaktivierende Key-Objekt liegt. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

➢ DEACTIVATE KEY (Übergabe der Key Reference des zu deaktivierenden Key-Objektes)

Nachbedingungen:

- Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (UC_PN_04_03: Use Case „Zurücksetzen des Sicherheitszustandes AUTH“)

UC_PN_04_09:

Use Case „Generierung eines ECC-Schlüsselpaares“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Anwendung insbesondere für die Generierung der GW-Betriebsschlüsselpaare:

- Betriebs-TLS-Key Pair (GW_WAN_TLS_PRV, GW_WAN_TLS_PUB)
- Betriebs-SIG-Key Pair (GW_WAN_SIG_PRV, GW_WAN_SIG_PUB)
- Betriebs-ENC-Key Pair (GW_WAN_ENC_PRV, GW_WAN_ENC_PUB)

Je nach verwendeter Kommando-Variante des Kommandos GENERATE ASYMMETRIC KEY PAIR erfolgt eine Schlüsselgenerierung mit oder ohne Ausgabe des Public Key.

Bei der Schlüsselgenerierung ist im Hinblick auf UC_PN_04_12: Use Case „Erstellung eines Zertifikatsrequest-Pakets (SM-PKI)“ darauf zu achten, dass für die äußere Signatur des Zertifikatsrequest-Pakets der alte Signaturschlüssel GW_WAN_SIG_PRV benötigt wird und dieser daher bei der Schlüsselgenerierung nicht überschrieben werden darf.

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (UC_PN_04_02: Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“)
- Key Pair-Objekt, das mit Schlüsseldaten befüllt werden soll, ist im Sicherheitsmodul vorhanden. (ggf. UC_PN_04_05: Use Case „Anlegen eines Key-Objektes“)
- Falls ein bereits gefülltes Key Pair-Objekt mit neuen Schlüsseldaten befüllt werden soll: Key-Attribut Key-LifeCycleStatus des Key Pair-Objektes besitzt den Wert „operational state – deactivated“. (ggf. UC_PN_04_08: Use Case „Deaktivieren eines Key-Objektes“)

Ablauf:

Selektion des DF, in dem das zu befüllende Key Pair-Objekt liegt. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

➢ GENERATE ASYMMETRIC KEY PAIR (Kommando-Variante für Schlüsselgenerierung mit / ohne Ausgabe des Public Key; Übergabe relevanter Informationen für die Schlüsselgenerierung gemäß Kommando-Spezifikation)

Nachbedingungen:

- Das Key-Attribut Key-LifeCycleStatus des Key Pair-Objektes besitzt nach der Schlüsselgenerierung den Wert „operational state – activated“, so dass das Key Pair-Objekt direkt zu seiner Nutzung für Krypto-Operationen bereitsteht.
- Sofern im Rahmen der Kommando-Ausführung des Kommandos GENERATE ASYMMETRIC KEY PAIR keine Ausgabe des Public Key-Parts des generierten Schlüsselpaares erfolgt, kann ein späterer Export des Public Key-Parts über UC_PN_04_10: Use Case „Export des Public Key eines ECC-Schlüsselpaares“ erfolgen.
- Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (UC_PN_04_03: Use Case „Zurücksetzen des Sicherheitszustandes AUTH“)

UC_PN_04_10:

Use Case „Export des Public Key eines ECC-Schlüsselpaares“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Anwendung insbesondere für den Export der GW-Betriebsschlüssel (nur Public Key):

- Betriebs-TLS-Public Key GW_WAN_TLS_PUB
- Betriebs-SIG-Public Key GW_WAN_SIG_PUB
- Betriebs-ENC-Public Key GW_WAN_ENC_PUB

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- Falls der GW-Administrator beteiligt ist: TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- Key Pair-Objekt, dessen Public Key ausgegeben werden soll, ist im Sicherheitsmodul vorhanden und wurde mittels Schlüsselgenerierung über das Kommando GENERATE ASYMMETRIC KEY PAIR mit Schlüsseldaten befüllt. (UC_PN_04_09: Use Case „Generierung eines ECC-Schlüsselpaares“)

Ablauf:

Selektion des DF, in dem das Key Pair-Objekt liegt, dessen Public Key ausgegeben werden soll. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

➢ GENERATE ASYMMETRIC KEY PAIR (Kommando-Variante für die Ausgabe des Public Key ohne Schlüsselgenerierung; Übergabe der Key Reference des Key Pair-Objektes, dessen Public Key ausgegeben werden soll)

Nachbedingungen:

- ---

UC_PN_04_11:

Use Case „Import eines Public Key“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Besteht für den Use Case zusätzlich der Wunsch nach einer Prüfung des Zertifikates zum zu importierenden Public Key inklusive einer Prüfung seiner Zertifikatskette (im Rahmen der SM-PKI), so ist UC_PN_04_13: Use Case „Prüfung einer Zertifikatskette (SM-PKI)“ hinzuzuziehen.

Relevantes Schlüsselmaterial:

- SIG-Key Pair (GWADM_SIG_PRV, GWADM_SIG_PUB) des GW-Administrators
- Zu importierender Public Key KEY_PUB

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (UC_PN_04_02: Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“)
- SIG-Key Pair (GWADM_SIG_PRV, GWADM_SIG_PUB) des GW-Administrators existiert, und der Signaturprüfschlüssel GWADM_SIG_PUB liegt im Sicherheitsmodul vor und ist aktiviert (ggf. UC_PN_04_07: Use Case „Aktivieren eines Key-Objektes“). (Der initiale Import des GWADM_SIG_PUB erfolgt über die „Initiale Konfigurationsdatei“ im Rahmen der Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“, siehe Kap. 2.5. Für das spätere Einbringen neuer Public Keys GWADM_SIG_PUB_neu in den Phasen „Personalisierung des SMGW“ und „Normalbetrieb des SMGW“ erfolgt eine Nutzung des vorliegenden Use Case „Import eines Public Key“. In letzterem Fall wird als Schlüsselpaar des GW-Administrators zur Sicherung des Schlüsselimports das alte Schlüsselpaar (GWADM_SIG_PRV_alt, GWADM_SIG_PUB_alt) verwendet.)
- Zu importierender Public Key KEY_PUB liegt vor. Import-Zertifikat KEY_PUB_CRT zu KEY_PUB liegt vor. Das Import-Zertifikat beinhaltet KEY_PUB (und weitere Key-Zusatzinformationen) und ist vom GW-Administrator mit seinem Signaturschlüssel GWADM_SIG_PRV signiert. Im Falle eines KEY_PUB, der in der SM-PKI zertifiziert ist, entnimmt der GW-Administrator KEY_PUB aus dem zugehörigen Zertifikat der SM-PKI und generiert zu diesem Public Key das vorgenannte Import-Zertifikat. Für die Übereinstimmung der Schlüsseldaten zwischen dem Zertifikat der SM-PKI und dem Import-Zertifikat ist dabei Sorge zu tragen.
- Public Key-Objekt zur Speicherung von KEY_PUB ist im Sicherheitsmodul vorhanden. Hierzu Anwendung von UC_PN_04_05: Use Case „Anlegen eines Key-Objektes“ für die Anlage eines Public Key-Objektes für den zu importierenden Public Key, sofern nicht ein bereits vorhandenes Public Key-Objekt mit dem zu importierenden Public Key (neu) befüllt werden soll; bei Neu-Befüllung eines bereits vorhandenen Public Key-Objektes besitzt dabei das Key-Attribut Key-LifeCycleStatus des Public Key-Objektes den Wert „initialisation“ oder „operational state – deactivated“ (UC_PN_04_08: Use Case „Deaktivieren eines Key-Objektes“). Der im Key-Attribut Key-Name des Public Key-Objektes eingetragene Key-Name stimmt mit der Key Reference im Import-Zertifikat zu KEY_PUB überein.

Ablauf:

Selektion des DF, in dem das zu befüllende Public Key-Objekt liegt. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

- MSE SET (DST) (für PSO VERIFY CERTIFICATE vorgesehene Kommando-Variante 1.2; insbesondere Übergabe der Key Reference des Public Key-Objektes mit dem Signaturprüfschlüssel GWADM_SIG_PUB und Übergabe des zu verwendenden Krypto-Algorithmus)
- PSO VERIFY CERTIFICATE (Übergabe des Import-Zertifikates KEY_PUB_CRT des zu importierenden Public Key KEY_PUB; das Import-Zertifikat enthält insbesondere Key-Zusatzinformationen sowie die Key Reference des zu befüllenden Public Key-Objektes)

Nachbedingungen:

- Das Key-Attribut Key-LifeCycleStatus des Public Key-Objektes für KEY_PUB besitzt nach dem Schlüsselimport den Wert „operational state – activated“, so dass das Public Key-Objekt direkt zu seiner Nutzung für Krypto-Operationen bereitsteht.
- Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (UC_PN_04_03: Use Case „Zurücksetzen des Sicherheitszustandes AUTH“)

UC_PN_04_12:

Use Case „Erstellung eines Zertifikatsrequest-Pakets (SM-PKI)“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Betrachtet wird hier nur die Erstellung eines Zertifikatsrequest-Pakets für das GW im Rahmen der SM-PKI. Für Details siehe [TR-03109-4].

Anwendung für das Zertifikatsrequest-Paket mit seinen drei Zertifikatsrequests zu neu generierten GW-Betriebsschlüsselpaaren:

- Betriebs-TLS-Key Pair (GW_WAN_TLS_PRV_neu, GW_WAN_TLS_PUB_neu)
- Betriebs-SIG-Key Pair (GW_WAN_SIG_PRV_neu, GW_WAN_SIG_PUB_neu)
- Betriebs-ENC-Key Pair (GW_WAN_ENC_PRV_neu, GW_WAN_ENC_PUB_neu)

Für die äußere Signatur des Zertifikatsrequest-Pakets wird das alte Signaturschlüsselpaar (GW_WAN_SIG_PRV_alt, GW_WAN_SIG_PUB_alt) des GW herangezogen. Beim Wechsel von den vorläufigen GW-Schlüsselpaaren zu den GW-Betriebsschlüsselpaaren im Rahmen der Teilphase „Personalisierung des SMGW“ bedeutet dies die Verwendung des vorläufigen GW-Signaturschlüsselpaares für die äußere Signatur des Zertifikatsrequest-Pakets.

Die Generierung der Autorisierungssignatur zum Zertifikatsrequest-Paket liegt außerhalb des vorliegenden Use Case.

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- Altes SIG-Schlüsselpaar (GW_WAN_SIG_PRV_alt, GW_WAN_SIG_PUB_alt) des GW liegt im Sicherheitsmodul vor und ist aktiviert. (UC_VI_03_02: Use Case „Generierung eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“, UC_PN_04_09: Use Case „Generierung eines ECC-Schlüsselpaares“, ggf. UC_PN_04_07: Use Case „Aktivieren eines Key-Objektes“)
- Neue GW-Schlüsselpaare (GW_WAN_TLS_PRV_neu, GW_WAN_TLS_PUB_neu), (GW_WAN_SIG_PRV_neu, GW_WAN_SIG_PUB_neu) bzw. (GW_WAN_ENC_PRV_neu, GW_WAN_ENC_PUB_neu) wurden generiert und sind aktiviert (UC_PN_04_09: Use Case „Generierung eines ECC-Schlüsselpaares“, ggf. UC_PN_04_07: Use Case „Aktivieren eines Key-Objektes“).

Ablauf:

Zertifikatsrequest für das neue TLS-Schlüsselpaar:

Sofern für das neue Schlüsselpaar (GW_WAN_TLS_PRV_neu, GW_WAN_TLS_PUB_neu) in UC_PN_04_09: Use Case „Generierung eines ECC-Schlüsselpaares“ keine Ausgabe des Public Key-Parts erfolgt ist, Durchführung von UC_PN_04_10: Use Case „Export des Public Key eines ECC-Schlüsselpaares“ für den Export des Public Key GW_WAN_TLS_PUB_neu.

Zusammenstellung des Zertifikatsrequests zum Public Key GW_WAN_TLS_PUB_neu. Ergebnis: ZertRequest_TLS.

Für die innere Signatur des Zertifikatsrequests:

- Aufbereitung von ZertRequest_TLS für die innere Signatur (Hashing). Ergebnis: InputSig_ZertRequest_TLS.
- Durchführung von UC_PN_05_02: Use Case „Generieren einer Signatur / DST“ mit InputSig_ZertRequest_TLS als Signaturdaten und unter Nutzung von GW_WAN_TLS_PRV_neu als Signaturschlüssel (→ „Selbst-Signatur des neuen TLS-Schlüssels“). Ergebnis: Sig_ZertRequest_TLS.

Zusammenstellung des finalen Zertifikatsrequests zum TLS-Schlüsselpaar, bestehend aus ZertRequest_TLS und Sig_ZertRequest_TLS.

Zertifikatsrequest für das neue SIG-Schlüsselpaar:

(analog zu „Zertifikatsrequest für das neue TLS-Schlüsselpaar“)

Sofern für das neue Schlüsselpaar (GW_WAN_SIG_PRV_neu, GW_WAN_SIG_PUB_neu) in UC_PN_04_09: Use Case „Generierung eines ECC-Schlüsselpaares“ keine Ausgabe des Public

Key-Parts erfolgt ist, Durchführung von UC_PN_04_10: Use Case „Export des Public Key eines ECC-Schlüsselpaares“ für den Export des Public Key GW_WAN_SIG_PUB_neu.

Zusammenstellung des Zertifikatsrequests zum Public Key GW_WAN_SIG_PUB_neu. Ergebnis: ZertRequest_SIG.

Für die innere Signatur des Zertifikatsrequests:

- Aufbereitung von ZertRequest_SIG für die innere Signatur (Hashing). Ergebnis: InputSig_ZertRequest_SIG.
- Durchführung von UC_PN_05_02: Use Case „Generieren einer Signatur / DST“ mit InputSig_ZertRequest_SIG als Signaturdaten und unter Nutzung von GW_WAN_SIG_PRV_neu als Signaturschlüssel (→ „Selbst-Signatur des neuen SIG-Schlüssels“). Ergebnis: Sig_ZertRequest_SIG.

Zusammenstellung des finalen Zertifikatsrequests zum SIG-Schlüsselpaar, bestehend aus ZertRequest_SIG und Sig_ZertRequest_SIG.

Zertifikatsrequest für das neue ENC-Schlüsselpaar:

(analog zu „Zertifikatsrequest für das neue TLS-Schlüsselpaar“)

Sofern für das neue Schlüsselpaar (GW_WAN_ENC_PRV_neu, GW_WAN_ENC_PUB_neu) in UC_PN_04_09: Use Case „Generierung eines ECC-Schlüsselpaares“ keine Ausgabe des Public Key-Parts erfolgt ist, Durchführung von UC_PN_04_10: Use Case „Export des Public Key eines ECC-Schlüsselpaares“ für den Export des Public Key GW_WAN_ENC_PUB_neu.

Zusammenstellung des Zertifikatsrequests zum Public Key GW_WAN_ENC_PUB_neu. Ergebnis: ZertRequest_ENC.

Für die innere Signatur des Zertifikatsrequests:

- Aufbereitung von ZertRequest_ENC für die innere Signatur (Hashing). Ergebnis: InputSig_ZertRequest_ENC.
- Durchführung von UC_PN_05_03: Use Case „Generieren einer Signatur / AT“ mit InputSig_ZertRequest_ENC als Signaturdaten und unter Nutzung von GW_WAN_ENC_PRV_neu als Signaturschlüssel (→ „Selbst-Signatur des neuen ENC-Schlüssels“). Ergebnis: Sig_ZertRequest_ENC.

Zusammenstellung des finalen Zertifikatsrequests zum ENC-Schlüsselpaar, bestehend aus ZertRequest_ENC und Sig_ZertRequest_ENC.

Zertifikatsrequest-Paket:

Erstellung des Zertifikatsrequest-Pakets, bestehend aus

- ZertRequest_TLS und Sig_ZertRequest_TLS
- ZertRequest_SIG und Sig_ZertRequest_SIG
- ZertRequest_ENC und Sig_ZertRequest_ENC

Ergebnis: ZertRequestPaket.

Für die äußere Signatur des Zertifikatsrequest-Pakets:

- Aufbereitung von ZertRequestPaket für die äußere Signatur (Hashing). Ergebnis: InputSig_ZertRequestPaket.

- Durchführung von UC_PN_05_02: Use Case „Generieren einer Signatur / DST“ mit InputSig_ZertRequestPaket als Signaturdaten und unter Nutzung von GW_WAN_SIG_PRV_alt als Signaturschlüssel. Ergebnis: Sig_ZertRequestPaket.

Zusammenstellung des finalen Zertifikatsrequest-Pakets zu den drei neuen Schlüsselpaaren, bestehend aus ZertRequestPaket und Sig_ZertRequestPaket.

Nachbedingungen:

- ---

UC_PN_04_13:

Use Case „Prüfung einer Zertifikatskette (SM-PKI)“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Betrachtet wird hier nur die Prüfung einer Kette von X.509-Zertifikaten bis zur SM-PKI-Root im Rahmen der SM-PKI. Für Details siehe [TR-03109-4].

Die Prüfung einer Zertifikatskette baut auf der Prüfung einzelner (Zertifikats-) Signaturen auf. Für das Parsen der beteiligten X.509-Zertifikate ist das GW zuständig.

Für den Use Case wird angenommen, dass das SM-PKI-Root-Zertifikat im transparenten Datenfeld EF.SMPKIRoot_x im DF.SMGW und der Root-Public Key des Zertifikates im zugehörigen Public Key-Objekt Key.SMPKIRoot_x im DF.SMGW gespeichert ist.

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- Falls der GW-Administrator beteiligt ist: TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- Kette der zu prüfenden Zertifikate (bis ggf. auf das SM-PKI-Root-Zertifikat) liegt im GW vor.
- Der Root-Public Key der SM-PKI liegt im Sicherheitsmodul vor und ist aktiviert. Der im Sicherheitsmodul im Public Key-Objekt Key.SMPKIRoot_x gespeicherte Root-Public Key stimmt mit dem Public Key des SM-PKI-Root-Zertifikates, das im zum Root-Public Key zugehörigen Datenfeld EF.SMPKIRoot_x im Sicherheitsmodul abgelegt ist, überein.

Ablauf:

Fortlaufende Anwendung von UC_PN_05_02: Use Case „Prüfen einer Signatur / DST“. Für die einzelnen zu prüfenden Zertifikate ist jeweils der Zertifikatsbody und die Signatur des Zertifikates

aus dem Zertifikat zu extrahieren sowie der relevante Signaturprüfschlüssel zu bestimmen und ggf. dieser Signaturprüfschlüssel in das Sicherheitsmodul zu importieren (Übergabe des Signaturprüfschlüssels im Kommando PSO VERIFY DIGITAL SIGNATURE oder Anwendung von UC_PN_04_11: Use Case „Import eines Public Key“), falls der Signaturprüfschlüssel nicht anderweitig schon im Sicherheitsmodul vorliegt.

Für die Prüfung gegen das SM-PKI-Root-Zertifikat:

Signaturprüfschlüssel ist der im Sicherheitsmodul im Public Key-Objekt Key.SMPKIRoot_x hinterlegte Root-Public Key (der mit dem Public Key des SM-PKI-Root-Zertifikates, das im zugehörigen Datenfeld EF.SMPKIRoot_x abgelegt ist, übereinstimmt).

Nachbedingungen:

- ---

4.4.3 Management des SM-PKI-Root-Zertifikates

UC_PN_04_14:

Use Case „Update des SM-PKI-Root-Zertifikates“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Die Speicherung des neuen SM-PKI-Root-Zertifikates erfolgt im transparenten Datenfeld EF.SMPKIRoot_x im DF.SMGW. Ferner erfolgt die Speicherung des neuen Root-Public Key aus dem neuen SM-PKI-Root-Zertifikat im vorgesehenen zugehörigen Public Key-Objekt Key.SMPKIRoot_x im DF.SMGW. Die zusätzliche Speicherung des Root-Public Key aus dem Zertifikat erfolgt aus dem Grund, als dass das Sicherheitsmodul bei Krypto-Operationen mit dem Root-Public Key mit diesem nur in Form eines Public Key-Objektes arbeiten und hierfür nicht auf den im Zertifikat enthaltenen Public Key zurückgreifen kann.

Bzgl. der Speicherung des neuen Root-Public Key im Sicherheitsmodul hat der GW-Administrator für die Übereinstimmung zwischen dem Public Key im Zertifikat und dem importierten Public Key Sorge zu tragen.

Beim Update des SM-PKI-Root-Zertifikates ist zu beachten, dass ein Überschreiben des aktuell gespeicherten alten SM-PKI-Root-Zertifikates aus Anwendungssicht evtl. nicht erwünscht ist. Entsprechendes gilt für das Update des zugehörigen Root-Public Key aus dem Zertifikat bzw. das zugehörige Public Key-Objekt mit den Schlüsseldaten des alten Root-Public Key.

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)

- TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (UC_PN_04_02: Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“)
- Zu schreibendes neues SM-PKI-Root-Zertifikat inkl. des zugehörigen Link-Zertifikates liegt vor.

Ablauf:

1. Schritt: Prüfung des Link-Zertifikates

Prüfung des Link-Zertifikates unter Nutzung von UC_PN_05_04: Use Cases „Prüfen einer Signatur / DST“. Aus dem Link-Zertifikat ist der Zertifikatsbody und die Signatur des Zertifikates zu extrahieren; ferner ist der relevante Signaturprüfschlüssel (hier: der alte Root-Public Key) zu bestimmen. Zu prüfen ist die Signatur über den Zertifikatsbody des Link-Zertifikates unter Nutzung dieses Signaturprüfschlüssels.

2. Schritt: Import des neuen SM-PKI-Root-Zertifikates

Selektion des DF.SMGW. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

Variante 1: Referenzierung des EF.SMPKIRoot_x via SELECT-Kommando

- SELECT (File-ID des EF.SMPKIRoot_x)
- UPDATE BINARY (SM-PKI-Root-Zertifikat)

Variante 2: Referenzierung des EF.SMPKIRoot_x via SFI

- UPDATE BINARY (SFI des EF.SMPKIRoot_x, SM-PKI-Root-Zertifikat)

3. Schritt: Import des neuen Root-Public Key (aus dem neuen SM-PKI-Root-Zertifikat)

Extrahieren des Root-Public Key aus dem SM-PKI-Root-Zertifikat.

Durchführung von UC_PN_04_11: Use Case „Import eines Public Key“ für den Import des neuen Root-Public Key in das Sicherheitsmodul und die Speicherung des neuen Root-Public Key im dafür vorgesehenen Public Key-Objekt Key.SMPKIRoot_x.

Nachbedingungen:

- Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (UC_PN_04_03: Use Case „Zurücksetzen des Sicherheitszustandes AUTH“)

UC_PN_04_15:

Use Case „Auslesen des SM-PKI-Root-Zertifikates“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Die Speicherung des SM-PKI-Root-Zertifikates erfolgt im transparenten Datenfeld EF.SMPKIRoot_x im DF.SMGW.

Für das Parsen des X.509-Zertifikates ist das GW zuständig.

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- Falls der GW-Administrator beteiligt ist: TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)

Ablauf:

Selektion des DF.SMGW. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

Variante 1: Referenzierung des EF.SMPKIRoot_x via SELECT-Kommando

- SELECT (File-ID des EF.SMPKIRoot_x)
- READ BINARY

Variante 2: Referenzierung des EF.SMPKIRoot_x via SFI

- READ BINARY (SFI des EF.SMPKIRoot_x)

Nachbedingungen:

- ---

4.4.4 File-/Kartenmanagement

UC_PN_04_16:

Use Case „Selektieren eines DF/EF“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Die Selektion eines DF/EF per File-ID erfolgt innerhalb des aktuell selektierten DF. Um im Filesystem des Sicherheitsmoduls zu navigieren, ist ggf. eine sukzessive mehrfache Anwendung des Use Cases „Selektieren eines DF/EF“ erforderlich.

Das DF.SMGW kann auch direkt per AID selektiert werden.

Beim Hochfahren des Sicherheitsmoduls ist automatisch das MF selektiert.

Ausführung ohne Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.

Ablauf:

Für die Selektion des MF:

➢ SELECT (leeres Kommando-Datenfeld)

Für die Selektion eines DF/EF via File-ID:

➢ SELECT (File-ID des zu selektierenden DF/EF)

Für die direkte Adressierung des DF.SMGW:

➢ SELECT (AID des DF.SMGW)

Nachbedingungen:

- ---

UC_PN_04_17:

Use Case „Anlegen eines DF/EF“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (UC_PN_04_02: Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“)
- LCSI des DF, in dem das neue DF/EF angelegt werden soll, steht nicht auf „terminated“.

Ablauf:

Selektion des DF, in dem das neue DF/EF angelegt werden soll. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

➢ CREATE FILE (Übergabeparameter gemäß Kommando-Spezifikation)

Nachbedingungen:

- Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (UC_PN_04_03: Use Case „Zurücksetzen des Sicherheitszustandes AUTH“)

UC_PN_04_18:

Use Case „Löschen eines DF/EF“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (UC_PN_04_02: Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“)
- LCSI des DF, in dem das zu löschende DF/EF liegt, steht nicht auf „terminated“.

Ablauf:

Selektion des DF, in dem das zu löschende DF/EF liegt. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

- SELECT (File-ID des zu löschenden DF/EF)
- DELETE FILE

Nachbedingungen:

- Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (UC_PN_04_03: Use Case „Zurücksetzen des Sicherheitszustandes AUTH“)

UC_PN_04_19:

Use Case „Aktivieren eines DF/EF“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (UC_PN_04_02: Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“)
- LCSI des DF, in dem das zu aktivierende DF/EF liegt, steht nicht auf „terminated“.

Ablauf:

Selektion des DF, in dem das zu aktivierende DF/EF liegt. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

- SELECT (File-ID des zu aktivierenden DF/EF)
- ACTIVATE FILE

Nachbedingungen:

- Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (UC_PN_04_03: Use Case „Zurücksetzen des Sicherheitszustandes AUTH“)

UC_PN_04_20:

Use Case „Deaktivieren eines DF/EF“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (UC_PN_04_02: Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“)
- LCSI des DF, in dem das zu deaktivierende DF/EF liegt, steht nicht auf „terminated“.

Ablauf:

Selektion des DF, in dem das zu deaktivierende DF/EF liegt. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

- SELECT (File-ID des zu deaktivierenden DF/EF)
- DEACTIVATE FILE

Nachbedingungen:

- Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (UC_PN_04_03: Use Case „Zurücksetzen des Sicherheitszustandes AUTH“)

UC_PN_04_21:

Use Case „Terminieren eines DF/EF“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)

- Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (UC_PN_04_02: Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“)
- LCSI des DF, in dem das zu terminierende DF/EF liegt, steht nicht auf „terminated“.

Ablauf:

Selektion des DF, in dem das zu terminierende DF/EF liegt. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

- SELECT (File-ID des zu terminierenden DF/EF)
- TERMINATE DF/EF

Nachbedingungen:

- Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (UC_PN_04_03: Use Case „Zurücksetzen des Sicherheitszustandes AUTH“)

4.4.5 Management des Life Cycle-Status des Sicherheitsmoduls

UC_PN_04_22:

Use Case „Terminieren des Sicherheitsmoduls“

Phase:

Außerbetriebnahme des SMGW

Hinweise:

Ausführung mit Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)
- Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (UC_PN_04_02: Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“)

Ablauf:

- TERMINATE CARD USAGE

Nachbedingungen:

- Erfolgreiche Kommando-Ausführung nimmt das Sicherheitsmodul irreversibel außer Betrieb. Für die nachfolgend noch ausführbaren Kommandos siehe [TR-03109-2], Kap. 3.4.10.1, 4.9.1.

Das Sicherheitsmodul bietet dem GW darüber hinaus die Möglichkeit, weitere eigendefinierte Life Cycle-Stati im Sicherheitsmodul zu hinterlegen, z.B. im Datenfeld EF.SecModLifeCycle. Siehe hierzu auch UC_PN_02_02: Use Case „Auslesen eines Record-orientierten Technischen Datenfeldes“ und UC_PN_02_03: Use Case „Update eines Record-orientierten Technischen Datenfeldes“. Auf Seiten des Sicherheitsmoduls erfolgt aber keine Auswertung dieser eigendefinierten, im Sicherheitsmodul hinterlegten Life Cycle-Stati.

4.4.6 Management der Applikationsebene des Sicherheitsmoduls

UC_PN_04_23:

Use Case „Zurücksetzen der Applikationsebene des Sicherheitsmoduls“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Anwendung zum gezielten Zurücksetzen der Applikationsebene des Sicherheitsmoduls.

Ausführung ohne Secure Messaging.

Rollen:

GW-Administrator, GW

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Falls der GW-Administrator beteiligt ist: TLS-Kanal zwischen GW-Administrator und GW besteht. (UC_PN_04_01: Use Case „Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW“)

Ablauf:

➢ MANAGE CHANNEL

Nachbedingungen:

- Das Zurücksetzen der Applikationsebene des Sicherheitsmoduls beinhaltet eine Re-Initialisierung des Sicherheitsmoduls mit Werten, wie diese nach einem Cold- bzw. Warm-Reset des Sicherheitsmoduls gesetzt sind, und ist insbesondere mit dem Zurücksetzen aller Sicherheitszustände (hier: PACE, AUTH), dem Schließen sicherer Kanäle, dem Löschen von Session Keys und der Selektion des MF verbunden. Für nachfolgende Zugriffe auf das Sicherheitsmodul, die einen gesetzten Sicherheitszustand PACE und / oder AUTH erfordern, ist das PACE-Protokoll bzw. die externe Authentisierung des GW-Administrators erneut erfolgreich auszuführen (UC_PN_03_01: Use Case „PACE-Authentisierung“, UC_PN_04_02: Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“).

4.5 Krypto-Anwendungen

Im folgenden Kapitel bedeutet in den Use Cases die Angabe EXT in „Rolle“ einen Teilnehmer aus dem WAN, HAN, LMN bzw. den GW-Administrator (sofern nichts anderes angegeben).

Die Use Cases laufen ggf. im Rahmen von TLS-Kanälen ab, z.B. die Use Cases bzgl. der Inhaltsdatenverschlüsselung und -signatur. Um die Use Cases an dieser Stelle übersichtlich zu halten, wurde darauf verzichtet, TLS-Kanäle in den Vorbedingungen aufzunehmen. Bestehende TLS-Kanäle nehmen keinen direkten Einfluss auf die Nutzung des Sicherheitsmoduls, da diese Kanäle im GW enden und nicht bis zum Sicherheitsmodul reichen.

UC_PN_05_01:

Use Case „Erzeugen und Ausgeben einer Zufallszahl“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Ausführung des Kommandos GET CHALLENGE mit oder ohne Secure Messaging. Die das Kommando GET CHALLENGE aufrufende Stelle zeigt über das CLA-Byte im Kommando-Header an, ob das Kommando mit oder ohne Secure Messaging ausgeführt werden soll.

Rollen:

GW, EXT

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Sofern das Kommando GET CHALLENGE mit Secure Messaging ausgeführt werden soll: Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)

Ablauf:

➢ GET CHALLENGE (Anzeige der gewünschten Länge der Zufallszahl im Kommando)

Nachbedingungen:

- Im Fall der Variante P1='00' steht die generierte Zufallszahl auch Sicherheitsmodul-intern weiterhin zur Verfügung (z.B. für ein nachfolgendes Kommando EXTERNAL AUTHENTICATE); im Fall der Variante P1='01' wird die Zufallszahl nur nach extern ausgegeben.

UC_PN_05_02:

Use Case „Generieren einer Signatur / DST“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Die Aufbereitung der zu signierenden Daten inkl. Hashen der Daten erfolgt durch das GW bzw. anderweitig außerhalb des Sicherheitsmoduls (Signaturdaten).

Ausführung mit Secure Messaging.

Rollen:

GW, EXT

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- Key Pair-Objekt mit dem Signaturschlüssel ist im Sicherheitsmodul vorhanden und ist aktiviert. (UC_PN_04_09: Use Case „Generierung eines ECC-Schlüsselpaares“, ggf. UC_PN_04_07: Use Case „Aktivieren eines Key-Objektes“)

Ablauf:

Aufbereitung der Signaturdaten inkl. Hashing (passend zur vorgesehenen Elliptischen Kurve / Schlüssellänge des Signaturschlüssels).

Bestimmung des Signaturschlüssels bzw. des zugehörigen Key Pair-Objektes im Sicherheitsmodul (Speicherort im Filesystem, Key-ID). Selektion des DF, in dem der Signaturschlüssel bzw. das zugehörige Key Pair-Objekt liegt. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

- MSE SET (DST) (für Signaturgenerierung vorgesehene Kommando-Variante 1.1; insbesondere Übergabe der Key Reference des Key Pair-Objektes mit dem Signaturschlüssel und Übergabe des zu verwendenden Krypto-Algorithmus)
- PSO COMPUTE DIGITAL SIGNATURE (Signaturdaten)

Nachbedingungen:

- ---

UC_PN_05_03:

Use Case „Generieren einer Signatur / AT“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Die Aufbereitung der zu signierenden Daten inkl. Hashen der Daten erfolgt durch das GW bzw. anderweitig außerhalb des Sicherheitsmoduls (Signaturdaten). Diese Signaturdaten bilden das zu signierende Token.

Als Signaturschlüssel wird ein Authentisierungsschlüssel (Schlüssel der Anwendungsklasse AT) verwendet.

Anwendung des Use Case im Rahmen der Erstellung eines Zertifikatsrequests zu einem ENC-Schlüssel. (UC_PN_04_12: Use Case „Erstellung eines Zertifikatsrequest-Pakets (SM-PKI)“)

Ausführung mit Secure Messaging.

Rollen:

GW, EXT

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- Key Pair-Objekt mit dem Authentisierungsschlüssel ist im Sicherheitsmodul vorhanden und ist aktiviert. (UC_PN_04_09: Use Case „Generierung eines ECC-Schlüsselpaares“, ggf. UC_PN_04_07: Use Case „Aktivieren eines Key-Objektes“)

Ablauf:

Aufbereitung des Tokens, d.h. der Signaturdaten inkl. Hashing (passend zur vorgesehenen Elliptischen Kurve / Schlüssellänge des Authentisierungsschlüssels).

Bestimmung des Authentisierungsschlüssels bzw. des zugehörigen Key Pair-Objektes im Sicherheitsmodul (Speicherort im Filesystem, Key-ID). Selektion des DF, in dem der Authentisierungsschlüssel bzw. das zugehörige Key Pair-Objekt liegt. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

- MSE SET (AT) (für interne Authentisierung vorgesehene Kommando-Variante 2.4; insbesondere Übergabe der Key Reference des Key Pair-Objektes mit dem Authentisierungsschlüssel und Übergabe des zu verwendenden Krypto-Algorithmus)
- INTERNAL AUTHENTICATE (Token, d.h. Signaturdaten)

Nachbedingungen:

- ---

UC_PN_05_04:

Use Case „Prüfen einer Signatur“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Die Aufbereitung der zu prüfenden Daten inkl. Hashen der Daten erfolgt durch das GW bzw. anderweitig außerhalb des Sicherheitsmoduls (Signaturprüfdaten).

Die Ausführung des Kommandos PSO VERIFY DIGITAL SIGNATURE in der Variante „ohne Übergabe des Public Key im Kommando“ erfolgt stets mit Secure Messaging. Das Kommando PSO VERIFY DIGITAL SIGNATURE in der Variante „mit Übergabe des Public Key im Kommando“ kann mit oder ohne Secure Messaging ausgeführt werden; die das Kommando PSO VERIFY DIGITAL SIGNATURE aufrufende Stelle zeigt über das CLA-Byte im Kommando-Header an, ob das Kommando mit oder ohne Secure Messaging ausgeführt werden soll.

Rollen:

GW, EXT

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Für das Kommando PSO VERIFY DIGITAL SIGNATURE in der Variante „ohne Übergabe des Public Key im Kommando“ (siehe untenstehende Variante 2) sowie für den Fall, dass das Kommando PSO VERIFY DIGITAL SIGNATURE in der Variante „mit Übergabe des Public Key im Kommando“ (siehe untenstehende Variante 1) mit Secure Messaging ausgeführt werden soll: Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- Für Variante 2: Public Key-Objekt mit dem Signaturprüfschlüssel ist im Sicherheitsmodul vorhanden und ist aktiviert. (UC_PN_04_11: Use Case „Import eines Public Key“, ggf. UC_PN_04_07: Use Case „Aktivieren eines Key-Objektes“)

Ablauf:

Variante 1: mit Übergabe des Public Key im Kommando

Zusammenstellung der Signaturprüfdaten mit ihrer Signatur.

Bestimmung des Signaturprüfschlüssels.

- PSO VERIFY DIGITAL SIGNATURE (Signaturprüfdaten, Signatur, Signaturprüfschlüssel)

Variante 2: ohne Übergabe des Public Key im Kommando

Zusammenstellung der Signaturprüfdaten mit ihrer Signatur.

Bestimmung des Signaturprüfschlüssels bzw. des zugehörigen Public Key-Objektes im Sicherheitsmodul (Speicherort im Filesystem, Key-Name). Selektion des DF, in dem der Signaturprüfschlüssel bzw. das zugehörige Public Key-Objekt liegt. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

- MSE SET (DST) (für Signaturverifikation vorgesehene Kommando-Variante 1.2; insbesondere Übergabe der Key Reference des Public Key-Objektes mit dem Signaturprüfschlüssel und Übergabe des zu verwendenden Krypto-Algorithmus)
- PSO VERIFY DIGITAL SIGNATURE (Signaturprüfdaten, Signatur)

Nachbedingungen:

- ---

UC_PN_05_05:

Use Case „Aufbau eines TLS-Kanals zwischen externer Welt und SMGW / SMGW in der Rolle TLS-Client“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Relevantes statisches TLS-Schlüsselmaterial:

- TLS-Key Pair (GW_EXT_TLS_PRV, GW_EXT_TLS_PUB) des GW im Sicherheitsmodul
- TLS-Key Pair (EXT_TLS_PRV, EXT_TLS_PUB) der externen Welt

wobei EXT = Teilnehmer im WAN, LMN, HAN, … Beim Wechsel der vorläufigen GW-Schlüsselpaare zu den GW-Betriebsschlüsselpaaren in der Teilphase „Personalisierung des SMGW“ bedeutet dies die Verwendung des vorläufigen TLS-Schlüsselpaares des GW und des TLS-Schlüsselpaares des GW-Administrators.

Relevantes ephemerales DH-Schlüsselmaterial:

- DH-Key Pair (GW_PRV_EPH, GW_PUB_EPH) des GW im Sicherheitsmodul
- DH-Key Pair (EXT_PRV_EPH, EXT_PUB_EPH) der externen Welt

Siehe auch die Beschreibungen zu ECKA-DH Protokoll-Variante 2.1 in [TR-03109-2], Kap. 4.5.5 a).

Ausführung mit Secure Messaging.

Rollen:

GW, EXT

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- TLS-Schlüsselpaar (GW_EXT_TLS_PRV, GW_EXT_TLS_PUB) des GW liegt im Sicherheitsmodul vor und ist aktiviert. (UC_VI_03_02: Use Case „Generierung eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“, UC_PN_04_09: Use Case „Generierung eines ECC-Schlüsselpaares“, ggf. UC_PN_04_07: Use Case „Aktivieren eines Key-Objektes“)
- TLS-Public Key GW_EXT_TLS_PUB des GW steht der externen Welt zur Verfügung. (ggf. UC_VI_03_03: Use Case „Export des Public Key eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“, UC_PN_04_10: Use Case „Export des Public Key eines ECC-Schlüsselpaares“)
- TLS-Schlüsselpaar (EXT_TLS_PRV, EXT_TLS_PUB) der externen Welt wurde durch diese generiert.
- TLS-Public Key EXT_TLS_PUB der externen Welt liegt im GW vor.

Ablauf:

Implementierung des TLS-Verbindungsaufbaus gemäß der Vorgaben in [TR-03109-3] bzw. [TR-03116-3], Kap. 4, 5 bzw. 6. Für die Spezifikation von TLS siehe auch RFC 5246 und RFC 5289. Aufgrund der Vielzahl an Optionen für die Implementierung wird an dieser Stelle auf eine detaillierte Beschreibung des TLS-Verbindungsaufbaus und der diesbzgl. Teilaufgaben auf Seiten des GW verzichtet, und es werden nachfolgend nur die Use Cases benannt, die für den TLS-Verbindungsaufbau im Zusammenhang mit der Nutzung des Sicherheitsmoduls durch das GW relevant sind. Ferner wird die Kommando-Abfolge für die Aushandlung des Shared Secret Value angegeben.

a) Für den TLS-Verbindungsaufbau relevante Use Cases unter Nutzung der o.g. statischen TLS-Schlüsselpaare (GW_EXT_TLS_PRV, GW_EXT_TLS_PUB) des GW im Sicherheitsmodul und (EXT_TLS_PRV, EXT_TLS_PUB) der externen Welt:

UC_PN_05_01: Use Case „Erzeugen und Ausgeben einer Zufallszahl“

UC_PN_05_02: Use Case „Generieren einer Signatur / DST“

UC_PN_05_04: Use Case „Prüfen einer Signatur“

UC_PN_04_11: Use Case „Import eines Public Key“

Ggf. Prüfung von Zertifikatsketten:

- Für TLS-Schlüssel im WAN, d.h. mit Zertifikaten aus der SM-PKI: Durchführung von UC_PN_04_13: Use Case „Prüfung einer Zertifikatskette (SM-PKI)“.
- Für TLS-Schlüssel außerhalb der SM-PKI: Prüfung einer Zertifikatskette auf analogem Weg unter Nutzung des Sicherheitsmoduls wie in UC_PN_04_13: Use Case „Prüfung einer Zertifikatskette (SM-PKI)“ beschrieben.

b) Kommando-Abfolge für die Aushandlung des Shared Secret Value Z_{AB}:

Externe Welt hat ephemerales DH-Key Pair (EXT_PRV_EPH, EXT_PUB_EPH) generiert und den Public Key EXT_PUB_EPH dem GW zugeliefert.

- MSE SET (AT) (für GENERAL AUTHENTICATE / ECKA-DH Protokoll-Variante 2.1 vorgesehene Kommando-Variante 2.1; Übergabe der Referenz auf die Protokoll-Variante 2.1)
- GENERAL AUTHENTICATE / ECKA-DH (Protokoll-Variante 2.1 mit Protokoll-Daten wie spezifiziert, insbesondere Übergabe von EXT_PUB_EPH)

Die Schlüsselableitung (KDF) der Session Keys (für Verschlüsselung und MAC-Sicherung des TLS-Kanals) aus dem von GENERAL AUTHENTICATE ausgegebenen Shared Secret Value Z_{AB} erfolgt durch das GW.

Nachbedingungen:

- Ephemerales Schlüsselmaterial ist im Sicherheitsmodul nicht mehr vorhanden.

UC_PN_05_06:

Use Case „Aufbau eines TLS-Kanals zwischen externer Welt und SMGW / SMGW in der Rolle TLS-Server“

Phase:

Normalbetrieb des SMGW

Hinweise:

Relevantes statisches TLS-Schlüsselmaterial:

- TLS-Key Pair (GW_EXT_TLS_PRV, GW_EXT_TLS_PUB) des GW im Sicherheitsmodul
- TLS-Key Pair (EXT_TLS_PRV, EXT_TLS_PUB) der externen Welt

wobei EXT = Teilnehmer im LMN oder HAN.

Relevantes ephemerales DH-Schlüsselmaterial:

- DH-Key Pair (GW_PRV_EPH, GW_PUB_EPH) des GW im Sicherheitsmodul
- DH-Key Pair (EXT_PRV_EPH, EXT_PUB_EPH) der externen Welt

Siehe auch die Beschreibungen zu ECKA-DH Protokoll-Variante 2.2 in [TR-03109-2], Kap. 4.5.5 a). Die temporäre Speicherung des DH-Key Pair (GW_PRV_EPH, GW_PUB_EPH) des GW erfolgt im Sicherheitsmodul im Key Pair-Objekt Key.EPH_x im MF.

Ausführung mit Secure Messaging.

Rollen:

GW, EXT (hier: LMN, HAN)

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- TLS-Schlüsselpaar (GW_EXT_TLS_PRV, GW_EXT_TLS_PUB) des GW liegt im Sicherheitsmodul vor und ist aktiviert. (UC_PN_04_09: Use Case „Generierung eines ECC-Schlüsselpaares“, ggf. UC_PN_04_07: Use Case „Aktivieren eines Key-Objektes“)
- TLS-Public Key GW_EXT_TLS_PUB des GW steht der externen Welt zur Verfügung. (ggf. UC_PN_04_10: Use Case „Export des Public Key eines ECC-Schlüsselpaares“)
- TLS-Schlüsselpaar (EXT_TLS_PRV, EXT_TLS_PUB) der externen Welt wurde durch diese generiert.
- TLS-Public Key EXT_TLS_PUB der externen Welt liegt im GW vor.
- Temporäres Key Pair-Objekt Key.EPH_x für das ephemerale Schlüsselmaterial des GW ist im Sicherheitsmodul angelegt.

  (Hinweis: Die Anlage dieses Key Pair-Objektes ist bereits im Rahmen der Initialisierung des Sicherheitsmoduls über das Initialisierungsfile erfolgt.)

Ablauf:

Implementierung des TLS-Verbindungsaufbaus gemäß der Vorgaben in [TR-03109-3] bzw. [TR-03116-3], Kap. 4, 5 bzw. 6. Für die Spezifikation von TLS siehe auch RFC 5246 und RFC 5289. Aufgrund der Vielzahl an Optionen für die Implementierung wird an dieser Stelle auf eine detaillierte Beschreibung des TLS-Verbindungsaufbaus und der diesbzgl. Teilaufgaben auf Seiten des GW verzichtet, und es werden nachfolgend nur die Use Cases benannt, die für den TLS-Verbindungsaufbau im Zusammenhang mit der Nutzung des Sicherheitsmoduls durch das GW relevant sind. Ferner wird die Kommando-Abfolge für die Aushandlung des Shared Secret Value angegeben.

a) Für den TLS-Verbindungsaufbau relevante Use Cases unter Nutzung der o.g. statischen TLS-Schlüsselpaare (GW_EXT_TLS_PRV, GW_EXT_TLS_PUB) des GW im Sicherheitsmodul und (EXT_TLS_PRV, EXT_TLS_PUB) der externen Welt:

UC_PN_05_01: Use Case „Erzeugen und Ausgeben einer Zufallszahl“

UC_PN_05_02: Use Case „Generieren einer Signatur / DST“

UC_PN_05_04: Use Case „Prüfen einer Signatur“

UC_PN_04_11: Use Case „Import eines Public Key“

Ggf. Prüfung von Zertifikatsketten:

Prüfung einer Zertifikatskette auf analogem Weg unter Nutzung des Sicherheitsmoduls wie in UC_PN_04_13: Use Case „Prüfung einer Zertifikatskette (SM-PKI)“ beschrieben. (Hinweis: Die TLS-Schlüssel der externen Welt im LMN liegen außerhalb der SM-PKI.)

b) Kommando-Abfolge für die Aushandlung des Shared Secret Value Z_{AB}:

Selektion des DF, in dem das Key Pair-Objekt Key.EPH_x für das ephemerale Schlüsselmaterial des GW liegt. (UC_PN_04_16: Use Case „Selektieren eines DF/EF“)

- GENERATE ASYMMETRIC KEY PAIR in der Variante 2 („Schlüsselgenerierung mit Ausgabe des Public Key“, als AT-Template Übergabe der Key Reference des Key Pair-Objektes Key.EPH_x sowie der OID für die vorgesehene Elliptische Kurve für die Generierung des ephemeralen Schlüsselmaterials des GW mit Ablage im Key Pair-Objekt Key.EPH_x und Ausgabe des ephemeralen Public Key an das GW)

Aufbereitung der Server Key Exchange Message durch das GW.

Durchführung von UC_PN_05_02: Use Case „Generieren einer Signatur / DST“ zur Signatur der Server Key Exchange Message des GW unter Nutzung des Schlüssels GW_EXT_TLS_PRV.

Externe Welt generiert ephemerales DH-Key Pair (EXT_PRV_EPH, EXT_PUB_EPH) und liefert den Public Key EXT_PUB_EPH dem GW zu.

- MSE SET (AT) (für GENERAL AUTHENTICATE / ECKA-DH Protokoll-Variante 2.2 vorgesehene Kommando-Variante 2.1; Übergabe der Referenz auf die Protokoll-Variante 2.2 und Übergabe der Key Reference (mit Anzeige globaler Suche) des Key Pair-Objektes Key.EPH_x)
- GENERAL AUTHENTICATE / ECKA-DH (Protokoll-Variante 2.2 mit Protokoll-Daten wie spezifiziert, insbesondere Übergabe von EXT_PUB_EPH)

Die Schlüsselableitung (KDF) der Session Keys (für Verschlüsselung und MAC-Sicherung des TLS-Kanals) aus dem von GENERAL AUTHENTICATE ausgegebenen Shared Secret Value Z_{AB} erfolgt durch das GW.

Nachbedingungen:

- Ephemerales Schlüsselmaterial ist im Sicherheitsmodul nicht mehr vorhanden.

UC_PN_05_07:

Use Case „Inhaltsdatenverschlüsselung mit SMGW/Sicherheitsmodul als Recipient“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Relevantes statisches ENC-Schlüsselmaterial:

- ENC-Key Pair (GW_PRV_STAT, GW_PUB_STAT) des GW im Sicherheitsmodul

Relevantes ephemerales ENC-Schlüsselmaterial:

- ENC-Key Pair (EXT_PRV_EPH, EXT_PUB_EPH) der externen Welt

Siehe auch die Beschreibungen zu ECKA-EG Protokoll-Variante 1.1 in [TR-03109-2], Kap. 4.5.5 a).

Ausführung mit Secure Messaging.

Rollen:

GW, EXT

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- Statisches ENC-Key Pair (GW_PRV_STAT, GW_PUB_STAT) des GW liegt im Sicherheitsmodul vor und ist aktiviert. (UC_PN_04_09: Use Case „Generierung eines ECC-Schlüsselpaares“, ggf. UC_PN_04_07: Use Case „Aktivieren eines Key-Objektes“)
- Der externen Welt (EXT = Teilnehmer im WAN, LMN, HAN, …) steht GW_PUB_STAT zur Verfügung. (ggf. UC_PN_04_10: Use Case „Export des Public Key eines ECC-Schlüsselpaares“)
- Ephemerales ENC-Key Pair (EXT_PRV_EPH, EXT_PUB_EPH) der externen Welt wurde durch diese generiert.
- Ephemeraler ENC-Public Key EXT_PUB_EPH der externen Welt liegt im GW vor.

Ablauf:

- MSE SET (AT) (für GENERAL AUTHENTICATE / ECKA-EG Protokoll-Variante 1.1 vorgesehene Kommando-Variante 2.1; Übergabe der Referenz auf die Protokoll-Variante 1.1 und Übergabe der Key Reference des Key Pair-Objektes für GW_PRV_STAT)
- GENERAL AUTHENTICATE / ECKA-EG (Protokoll-Variante 1.1 mit Protokoll-Daten wie spezifiziert, insbesondere Übergabe von EXT_PUB_EPH)

Die Schlüsselableitung (KDF) der Session Keys (für Verschlüsselung und MAC-Sicherung der Inhaltsdaten) aus dem von GENERAL AUTHENTICATE ausgegebenen Shared Secret Value Z_{AB} erfolgt durch das GW.

Die Inhaltsdatenverschlüsselung der mit der externen Welt ausgetauschten Daten erfolgt mit den zuvor abgeleiteten Session Keys durch das GW.

Nachbedingungen:

- ---

UC_PN_05_08:

Use Case „Inhaltsdatenverschlüsselung mit SMGW/Sicherheitsmodul als Initiator“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Relevantes ephemerales ENC-Schlüsselmaterial:

- ENC-Key Pair (GW_PRV_EPH, GW_PUB_EPH) des GW im Sicherheitsmodul

Relevantes statisches ENC-Schlüsselmaterial:

- ENC-Key Pair (EXT_PRV_STAT, EXT_PUB_STAT) der externen Welt

Siehe auch die Beschreibungen zu ECKA-EG Protokoll-Variante 1.2 in [TR-03109-2], Kap. 4.5.5 a).

Ausführung mit Secure Messaging.

Rollen:

GW, EXT

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- Statisches ENC-Key Pair (EXT_PRV_STAT, EXT_PUB_STAT) der externen Welt wurde durch diese generiert. (EXT = Teilnehmer im WAN, LMN, HAN, …)
- Statischer ENC-Public Key EXT_PUB_STAT steht dem GW zur Verfügung.

Ablauf:

Variante 1: ohne Übergabe von EXT_PUB_STAT im Kommando

Import von EXT_PUB_STAT (UC_PN_04_11: Use Case „Import eines Public Key“), sofern der Schlüssel nicht schon im Sicherheitsmodul vorliegt.

- MSE SET (AT) (für GENERAL AUTHENTICATE / ECKA-EG Protokoll-Variante 1.2 vorgesehene Kommando-Variante 2.1; Übergabe der Referenz auf die Protokoll-Variante 1.2 und Übergabe der Key Reference des Public Key-Objektes für EXT_PUB_STAT)
- GENERAL AUTHENTICATE / ECKA-EG (Protokoll-Variante 1.2 mit Protokoll-Daten wie spezifiziert, keine Übergabe von EXT_PUB_STAT)

Übermittlung von GW_PUB_EPH (ausgegeben von GENERAL AUTHENTICATE) an die externe Welt.

Die Schlüsselableitung (KDF) der Session Keys (für Verschlüsselung und MAC-Sicherung der Inhaltsdaten) aus dem von GENERAL AUTHENTICATE ausgegebenen Shared Secret Value Z_{AB} erfolgt durch das GW.

Die Inhaltsdatenverschlüsselung der mit der externen Welt ausgetauschten Daten mit den zuvor abgeleiteten Session Keys erfolgt durch das GW.

Variante 2: mit Übergabe von EXT_PUB_STAT im Kommando

- MSE SET (AT) (für GENERAL AUTHENTICATE / ECKA-EG Protokoll-Variante 1.2 vorgesehene Kommando-Variante 2.1; Übergabe der Referenz auf die Protokoll-Variante 1.2)
- GENERAL AUTHENTICATE / ECKA-EG (Protokoll-Variante 1.2 mit Protokoll-Daten wie spezifiziert, insbesondere Übergabe von EXT_PUB_STAT)

Übermittlung von GW_PUB_EPH (ausgegeben von GENERAL AUTHENTICATE) an die externe Welt.

Die Schlüsselableitung (KDF) der Session Keys (für Verschlüsselung und MAC-Sicherung der Inhaltsdaten) aus dem von GENERAL AUTHENTICATE ausgegebenen Shared Secret Value Z_{AB} erfolgt durch das GW.

Die Inhaltsdatenverschlüsselung der mit der externen Welt ausgetauschten Daten mit den zuvor abgeleiteten Session Keys erfolgt durch das GW.

Nachbedingungen:

- ---

UC_PN_05_09:

Use Case „Inhaltsdatensignatur / Signaturgenerierung“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Die Aufbereitung der zu signierenden Inhaltsdaten inkl. Hashen der Daten erfolgt durch das GW bzw. anderweitig außerhalb des Sicherheitsmoduls (Signaturdaten).

Relevantes Signaturschlüsselmaterial:

- SIG-Key Pair (GW_WAN_SIG_PRV, GW_WAN_SIG_PUB) des GW im Sicherheitsmodul

Ausführung mit Secure Messaging.

Rollen:

GW, EXT

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- SIG-Key Pair (GW_WAN_SIG_PRV, GW_WAN_SIG_PUB) des GW liegt im Sicherheitsmodul vor und ist aktiviert. (UC_PN_04_09: Use Case „Generierung eines ECC-Schlüsselpaares“, ggf. UC_PN_04_07: Use Case „Aktivieren eines Key-Objektes“)
- Signaturdaten (Inhaltsdaten in geeignet aufbereiteter Form) liegen im GW vor.

Ablauf:

Durchführung von UC_PN_05_02: Use Case „Generieren einer Signatur / DST“ mit GW_WAN_SIG_PRV als Signaturschlüssel zur Signatur der Signaturdaten.

Nachbedingungen:

- ---

UC_PN_05_10:

Use Case „Inhaltsdatensignatur / Signaturprüfung“

Phase:

Personalisierung des SMGW, Normalbetrieb des SMGW

Hinweise:

Die Aufbereitung der zu prüfenden Inhaltsdaten inkl. Hashen der Daten erfolgt durch das GW bzw. anderweitig außerhalb des Sicherheitsmoduls (Signaturprüfdaten).

Relevantes Signaturschlüsselmaterial:

- SIG-Key Pair (EXT_SIG_PRV, EXT_SIG_PUB) der externen Welt

Ausführung mit Secure Messaging.

Rollen:

GW, EXT

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)
- SIG-Key Pair (EXT_SIG_PRV, EXT_SIG_PUB) der externen Welt wurde durch diese generiert. (EXT = Teilnehmer im WAN, LMN, HAN, …)
- EXT_SIG_PUB steht dem GW zur Verfügung.
- Signaturprüfdaten (Inhaltsdaten in geeignet aufbereiteter Form) mit zu prüfender Signatur liegen im GW vor.

Ablauf:

Ggf. UC_PN_04_11: Use Case „Import eines Public Key“ für den Import von EXT_SIG_PUB, sofern der Signaturprüfschlüssel EXT_SIG_PUB noch nicht im Sicherheitsmodul vorliegt.

Durchführung von UC_PN_05_04: Use Case „Prüfen einer Signatur“ in der Variante 2 („ohne Übergabe des Public Key im Kommando“) mit EXT_SIG_PUB als Signaturprüfschlüssel zur Prüfung der Signatur über die Signaturprüfdaten.

Nachbedingungen:

- ---

UC_PN_05_11:

Use Case „Generieren eines TLS-Schlüsselpaares für einen Zähler“

Phase:

Normalbetrieb des SMGW

Hinweise:

Da für im Sicherheitsmodul generierte Schlüsselpaare ein Export des kompletten Schlüsselpaares (genauer ein Export des privaten Schlüsselteils) nicht möglich ist, wird das Sicherheitsmodul für die Schlüsselgenerierung von TLS-Schlüsselpaaren der Zähler auf folgende Weise eingebunden. Das Sicherheitsmodul liefert über seine Zufallszahlengenerierung eine hochwertige Zufallszahl, die das GW als privaten ECC-Schlüssel interpretiert und weiterverwendet. Das GW übernimmt die Aufgabe der Berechnung des zugehörigen öffentlichen ECC-Schlüssels aus dem privaten Schlüssel (d.h. aus der vom Sicherheitsmodul gelieferten Zufallszahl).

Ausführung mit Secure Messaging.

Rollen:

GW, EXT (hier: LMN)

Vorbedingungen:

- Life Cycle-Status des Sicherheitsmoduls steht nicht auf „terminiert“.
- Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (UC_PN_03_01: Use Case „PACE-Authentisierung“)

Ablauf:

Bestimmung der Elliptischen Kurve, zu der das Schlüsselpaar generiert werden soll.

➢ GET CHALLENGE (Anzeige der gewünschten Länge der Zufallszahl im Kommando)

Die vom Sicherheitsmodul ausgegebene Zufallszahl wird vom GW als privater ECC-Schlüssel interpretiert und weiterverwendet. Das GW berechnet aus dem privaten ECC-Schlüssel den zugehörigen öffentlichen ECC-Schlüssel (ECC-Punktmultiplikation unter Verwendung der Zufallszahl und der vorgesehenen Elliptischen Kurve).

Nachbedingungen:

- ---

Literaturverzeichnis

[TR-03109] BSI TR-03109 (Dachdokument), BSI, aktuelle Fassung

[TR-03109-1] BSI TR-03109-1 Smart Meter Gateway - Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, BSI, aktuelle Fassung

[TR-03109-1A] BSI TR-03109-1 Anhang: Betriebsprozesse, BSI, aktuelle Fassung

[TR-03109-2] 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

[TR-03109-4] BSI TR-03109-4 Public Key Infrastruktur für Smart Meter Gateways, BSI, aktuelle Fassung

[ISO 7816-3] ISO/IEC 7816-3: Identification cards - Integrated circuit cards with contacts - Part 3: Electrical interface and transmission protocols, ISO/IEC, IS 2006

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

[ISO 7816-8] ISO/IEC 7816-8: Identification cards - Integrated circuit cards - Part 8: Commands for security operations, ISO/IEC, IS 2004

[ISO 7816-9] ISO/IEC 7816-9: Identification cards - Integrated circuit cards - Part 9: Commands for card management, ISO/IEC, IS 2004

[ISO 14443-4] ISO/IEC 14443-4: Identification cards - Contactless integrated circuit cards - Proximity cards - Part 4: Transmission protocol, ISO/IEC, IS 2008

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

[TR-03110-1] BSI TR-03110-1 Advanced Security Mechanisms for Machine Readable Travel Documents - Part 1 - eMRTDs with BAC/PACEv2 and EACv1, BSI, Version 2.10, 2012

[TR-03110-2] BSI TR-03110-2 Advanced Security Mechanisms for Machine Readable Travel Documents - Part 2 - Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), BSI, Version 2.10, 2012

[TR-03110-3] BSI TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents - Part 3 - Common Specifications, BSI, Version 2.11, 2013

[TR-03116-3] BSI TR-03116-3 eCard-Projekte der Bundesregierung - Kryptographische Vorgaben für die Infrastruktur von Messsystemen, BSI, 2014

[TR-03117] BSI TR-03117 eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit, BSI, Version 1.0, 2009

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

[EN 14890-2] EN 14890-2: Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services, EN, 2011

Stichwort- und Abkürzungsverzeichnis

Siehe [TR-03109-2].