

Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

Änderungsbedarf:

Bei der Common-Criteria-Zertifizierung ist aufgefallen, dass der Konnektor im Fehlerzustand EC_FIREWALL_NOT_RELIABLE theoretisch alle Ports schließen muss. Dies stellt einen Widerspruch zu Tabelle 5: TAB_KON_504 dar, nach der noch einige Operationen (insbesondere die Administration des Konnektors) möglich sind. Die Administrierbarkeit des Konnektors über die Managementschnittstelle im Fehlerzustand EC_FIREWALL_NOT_RELIABLE ist aus betrieblichen Gründen gewünscht, aus Sicherheitsgründen aber nur bei besonderen organisatorischen Maßnahmen möglich. Diese Maßnahmen und deren Umsetzung muss der Hersteller im Rahmen der CC-Evaluierung mit Prüfstelle und BSI abstimmen.

TAB_KON_504 muss so angepasst werden, dass nur noch die elementaren Operationen für eine Administrierbarkeit des Konnektors erlaubt sind. Zudem muss eine Anforderung eingefügt werden, dass die Administrierbarkeit mit Prüfstelle und BSI abzustimmen ist und das Security Target entsprechend zu erweitern ist.

Achtung! Die ursprünglich vorgesehenen Änderungen an der Tabelle TAB_KON_504 wurden zugunsten einer gedoppelten Afo TIP1-A_4510-02 aufgegeben, weil diese kompliziert aufgebaute Tabelle sonst für PTV4 gedoppelt werden müsste.

Änderungen in [gemSpec_Kon]

3.3 Betriebszustand

[...]

TIP1-A_4510-02 – ab PTV4: Sicherheitskritische Fehlerzustände

Der Konnektor MUSS bei eingetretenem Fehlerzustand aus Tabelle Tab_Kon_503 Betriebszustand_Fehlerzustandsliste mit Severity=Fatal dafür sorgen, dass von den Operationen der Basisdienste und Technische Use Cases (TUCs) der Basisdienste, die relevant für Fachanwendungen sind, nur erlaubte Operationen und TUCs gestartet und ausgeführt werden.

Welche Operationen und TUCs je eingetretenem Fehlerzustand ausgeführt werden dürfen, legt Tabelle „TAB_KON_504 Ausführungserlaubnis für Dienste in kritischen Fehlerzuständen“ fest: Jede Erlaubnis ist dort durch ein „x“ definiert.

Abweichend zu Angaben in der Tabelle TAB_KON_504 DÜRFEN folgende Operationen und TUCs NICHT im Zustand EC_Firewall_Not_Reliable ausgeführt werden:

- TUC_KON_000 PrüfeAufrufkontext
- TUC_KON_041 Einbringen der Endpunktinformationen während der Bootup-Phase
- GetCardTerminals
- GetCards
- GetResourceInformation

- Subscribe
- RenewSubscription
- Unsubscribe
- GetSubscription
- ReadCardCertificate
- CheckCertificateExpiration
- VerifyCertificate

Sind mehrere Fehlerzustände gleichzeitig eingetreten, dürfen nur die Operationen und TUCs ausgeführt werden, die für alle eingetretenen Fehlerzustände erlaubt sind. Der Konnektor muss Anfragen, die auf Grund eines kritischen Fehlerzustandes nicht ausgeführt oder abgebrochen werden, mit einem Fehler (Fehlercode 4002) beantworten.

Tabelle : TAB_KON_502 Fehlercodes „Betriebszustand“

Fehlercode	ErrorType	Severity	Fehlertext
4002	Security	Fatal	Der Konnektor befindet sich in einem kritischen Betriebszustand

<==

Tabelle : TAB_KON_504 Ausführungserlaubnis für Dienste in kritischen Fehlerzuständen

	EC_ Soft ware_ Inte grity_ Check Failed	EC_ Ran dom_ Gene rator_ Not_ Reli able	EC_ Secu rity_ Log Not_ Writ able	EC_ Time_ Sync Pen ding_ Citi cal	EC_ Time_ Diffe rence_ Intole rable	EC_ CRL_ Out_ Of_ Date	EC_ TSL_ Out_ Of_ Date_ Bey ond_ Grace Period	EC_ TSL_ Trust_ An chor_ Out_ Of_ Date	EC_ Fire wall_ Not_ Reli able	EC_ Sec ure_ Key Store_ Not_ Avail able	EC_ FW_ Not_ Valid_ Sta tus_ Ble cked
Technische Use Cases (TUCs) der Basisdienste relevant für Fachanwendung und die Kommunikation mit Weiteren Anwendungen und SIS											
Zugriffsberechtigungsdienst											
TUC_ KON_000	PrüfeAufruf kontext	-	*	*	*	*	*	*	*	*	*
Dienstverzeichnisdienst											
TUC_ KON_041	Einbringen der Endpunkt informationen während der Bootup-Phase	-	-	-	*	*	*	*	*	*	*
Kartenterminaldienst											
TUC_ KON_051	Mit Anwender über Kartenterminal interagieren	-	-	-	-	-	*	*	*	-	-
Kartendienst											
TUC_ KON_005	Card-to-Card authentisieren	-	-	-	-	-	*	*	*	-	-
TUC_ KON_006	Datenzu griffsaudit eGK schreiben	-	-	-	-	-	*	*	*	-	-
TUC_ KON_007	eGK-Sperrung	-	-	-	-	-	*	*	*	-	-

		EC_Software_Integrity_Check_Failed	EC_Random_Generator_Not_Reliable	EC_Security_Log_Not_Writable	EC_Time_Sync_Pending_Critical	EC_Time_Difference_Intolerable	EC_CRL_Out_Of_Date	EC_TSL_Out_Of_Date_Beyond_Grace_Period	EC_TSL_Trust_Anchor_Out_Of_Date	EC_Firewall_Not_Reliable	EC_Security_Key_Store_Not_Available	EC_FW_Not_Valid_Status_Blocked
KON_018	prüfen											
TUC_KON_024	Karte zurücksetzen	-	-	-	-	-	*	*	*	-	-	*
TUC_KON_026	Liefere CardSession	-	-	-	-	-	*	-	*	-	-	-
TUC_KON_200	SendeAPDU	-	-	-	-	-	*	*	*	-	-	*
TUC_KON_202	LeseDatei	-	-	-	-	-	*	*	*	-	-	*
TUC_KON_203	SchreibeDatei	-	-	-	-	-	*	*	*	-	-	*
TUC_KON_209	LeseRecord	-	-	-	-	-	*	*	*	-	-	*
Systeminformationsdienst												
TUC_KON_256	System ereignis absetzen	-	*	*	*	*	*	*	*	*	*	*
Verschlüsselungsdienst												
TUC_KON_072	Daten symmetrisch verschlüsseln	-	-	-	*	*	*	*	*	-	-	*
TUC_KON_073	Daten symmetrisch entschlüsseln	-	-	-	*	*	*	*	*	-	-	*
Zertifikatsdienst												
TUC_KON_034	Zertifikats informationen extrahieren	-	-	-	*	*	*	*	*	-	-	*
Protokollierungsdienst												
TUC_KON_271	Schreibe Protokoll eintrag	-	*	*	*	*	*	*	*	*	*	*
TLS-Dienst												
TUC_KON_110	Kartenbasierte TLS-Verbindung aufbauen	-	-	-	-	-	-	-	-	-	-	-
Verbindung zum VPN-Konzentrator												
TUC_VPN-ZD_0001	„IPsec Tunnel TI aufbauen“	-	-	-	-	-	-	-	-	-	-	-
TUC_VPN-ZD_0002	„IPsec Tunnel SIS aufbauen“	-	-	-	-	-	-	-	-	-	-	-
Operationen der Basisdienste												
Kartendienst												
VerifyPin		-	-	-	-	-	*	*	*	-	-	*

	EC_Software_Integrity_Check_Failed	EC_Random_Generator_Not_Reliable	EC_Security_Log_Not_Writable	EC_Time_Sync_Pending_Critical	EC_Time_Difference_Intolerable	EC_CRL_Out_Of_Date	EC_TSL_Out_Of_Date_Beyond_Grace_Period	EC_TSL_Trust_Anchor_Out_Of_Date	EC_Firewall_Not_Reliable	EC_Security_Key_Store_Not_Available	EC_FW_Not_Valid_Status_Blocked
- UnblockPin	-	-	-	-	-	*	*	*	-	-	*
- ChangePin	-	-	-	-	-	*	*	*	-	-	*
- GetPinStatus	-	-	-	-	-	*	*	*	-	-	*
Systeminformationsdienst											
- Schnittstelle der Ereignissenke	-	*	*	*	*	*	*	*	*	*	*
- GetCardTerminals	-	*	*	*	*	*	*	*	*	*	*
- GetCards	-	*	*	*	*	*	*	*	*	*	*
- GetResourceInformation	-	*	*	*	*	*	*	*	*	*	*
- Subscribe	-	*	*	*	*	*	*	*	*	*	*
- RenewSubscription	-	*	*	*	*	*	*	*	*	*	*
- Unsubscribe	-	*	*	*	*	*	*	*	*	*	*
- GetSubscription	-	*	*	*	*	*	*	*	*	*	*
Verschlüsselungsdienst											
- EncryptDocument	-	-	-	-	-	*	*	*	-	-	*
- DecryptDocument	-	-	-	-	-	*	*	*	-	-	*
Signaturdienst											
- SignDocument	-	-	-	-	-	*	*	*	-	-	*
- VerifyDocument	-	-	-	-	-	*	*	*	-	-	*
- GetJobNumber	-	-	-	-	-	*	*	*	-	-	*
- StopSignature	-	-	-	-	-	*	*	*	-	-	*
Authentifizierungsdienst											
- ExternalAuthenticate	-	-	-	-	-	*	*	*	-	-	*
Zertifikatsdienst											
- ReadCardCertificate	-	-	-	-	-	*	*	*	*	*	*
- CheckCertificate Expiration	-	-	-	-	-	*	*	*	*	*	*
- VerifyCertificate	-	-	-	-	-	*	*	*	*	*	*
Zeitdienst											
- I_NTP_Time_Information	-	-	-	-	-	*	*	*	-	*	-
Konnektormanagement											
- Softwareaktualisierung	*	*	*	*	*	*	*	*	*	*	*
- Protokolleinsicht	*	*	*	*	*	*	*	*	*	*	*
- Werksreset	-	*	*	*	*	*	*	*	*	*	*
- Sonstiges	-	*	*	*	*	*	*	*	*	*	*

In den kritischen Fehlerzuständen, in denen keine TLS-Verbindung ins LAN aufgebaut werden (EC_Random_Generator_Not_Reliable, EC_Software_Integrity_Check_Failed, EC_Security_Log_Not_Writable, EC_Time_Sync_Pending_Critical,

EC_Time_Difference_Intolerable), kann keine Verbindung zu den Kartenterminals aufgebaut werden. Infolge sind hier keine Kartenoperationen zugelassen.

Wenn keine Verbindung zum VPN-Konzentrator des SIS aufgebaut werden kann, ist infolge das Internet nicht über den Konnektor erreichbar. Wenn keine Verbindung zum VPN-Konzentrator der TI aufgebaut werden kann, sind Bestandsnetze nicht erreichbar.

Bezüglich der Administration des Konnektors im Zustand EC_FIREWALL_NOT_RELIABLE ist eine Abstimmung mit der Prüfstelle und der Zertifizierungsstelle notwendig.

A_16203 Administration im Zustand EC_FIREWALL_NOT_RELIABLE

Der Hersteller des Konnektors MUSS Maßnahmen, die eine sichere Administration auch im Fehlerzustand EC_FIREWALL_NOT_RELIABLE ermöglichen, im Security Target verankern und der gematik zur Prüfung vorlegen. <== {Prüfverfahren: sich.tech.Eig.:CC-Evaluierung}

Die Architektur der TI ist so angelegt, dass die Fehlerzustände mit Severity=Fatal in den Tabellen TAB_KON_504 und TAB_KON_503 mit vernachlässigbarer Wahrscheinlichkeit von externen Einflüssen abhängen. Die SLAs für Dienste der zentralen TI-Plattform sind so gefasst, dass diese schwerwiegend verletzt werden müssten, um dadurch einen Konnektor in einen solchen kritischen Zustand zu bringen (externer Fehler aus Sicht des Konnektors). Dass beispielsweise der TSL-Dienst über den Zeitraum der Grace-Period-TSL (typisch: 7 Tage) nicht erreichbar ist (ErrorCondition EC_TSL_Out_Of_Date_Beyond_Grace_Period), kann nur bei massiver Verletzung der für zentrale Dienste festgelegten SLAs eintreten.