
C_12627_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	2
2 Änderung in gemSpec_PKI.....	3
2.1 in Kapitel 8.3.1.1 TUC_PKI_018 „Zertifikatsprüfung in der TI“.....	3
3 Änderungen in Steckbriefen.....	10
3.1 Änderungen in gemProdT_X509_TSP_nonQES_eGK/gemProdT_X509_TSP_nonQES_HBA/gemPro dT_X509_TSP_nonQES_Komp/gemProdT_X509_TSP_nonQES_SMC-B/ gemProdT_X509_TSP_QES.....	10

1 Änderungsbeschreibung

Die Störungsampel und Service Monitoring wurden abgekündigt. Im TUC_PKI_018 - Standardablauf 7. gemSpec_PKI, der TLS-Zertifikate der Störungsampe prüft, wird entsprechend angepasst. Der Ausdruck "Störungsampel" wird durch den "Betriebsdatenerfassung (BDE)" ersetzt. Des Weiteren fallen die Anforderungen aus der Spezifikation gemSpec_ServiceMon aufgrund der Abkündigung weg. Diese Anforderungen müssen daher aus den betroffenen Steckbriefen entfernt werden.

Die der Anforderung GS-A_4652-02 zugewiesenen Steckbriefe sind nicht betroffen, da die Änderung sich lediglich auf die Prüfung von TLS-Zertifikate der Störungsampel bezieht.

2 Änderung in gemSpec_PKI

2.1 in Kapitel 8.3.1.1 TUC_PKI_018 „Zertifikatsprüfung in der TI“

GS-A_4652-02 -TUC_PKI_018: Zertifikatsprüfung in der TI

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_018 zur Zertifikatsprüfung umsetzen

Tabelle 1: TUC_PKI_018 „Zertifikatsprüfung in der TI“

Element	Beschreibung
Name	TUC_PKI_018 „Zertifikatsprüfung“
Beschreibung	Dieser Use Case beschreibt die Prüfung nicht-qualifizierter Zertifikate und umfasst die Offline- wie Online-Prüfung.
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Eine zeitlich nicht abgelaufene TSL (innerhalb der TSL-Graceperiod) steht als valide Basis zur Prüfung von Zertifikaten zur Verfügung
Auslöser	Zertifikats-Check
Eingangsdaten	<ul style="list-style-type: none">• Das zu prüfende Zertifikat• Referenzzeitpunkt: Zeitpunkt, für den das Zertifikat geprüft werden soll (optional; bei Nichtangabe Verwendung der aktuellen Systemzeit): Zeitpunkt, für den das Zertifikat geprüft werden soll, s. a. Glossar aus Kap. 11.2• PolicyList Liste der im aktuellen Aufruf zulässigen Zertifikatstyp-OIDs. Die Liste muss mindestens eine OID enthalten.• Vorgesehene KeyUsage (intendedKeyUsage, mehrere Werte möglich)• Vorgesehene ExtendedKeyUsage (intendedExtendedKeyUsage, mehrere Werte möglich)• OCSP-Graceperiod (legt bei der Verwendung von (gecachten) OCSP-

	<p>Antworten den maximal zulässige Zeitraum fest, den die Systemzeit der prüfenden Komponente noch nach dem Zeitpunkt der OCSP- Antwort liegen darf (Default: 10 min)</p> <ul style="list-style-type: none"> • Offline-Modus (ja/nein) • Beigefügte OCSP-Response zum angefragten Zertifikat (optional; z. B. in der Signatur eingebettet) • Timeout-Parameter (Default: 10s) • TOLERATE_OCSP_FAILURE (true/false, Default: false) - Der Parameter definiert das Verhalten für den Fall, dass die OCSP-Prüfung nicht durchgeführt werden konnte, weil der OCSP-Responder beispielsweise technisch nicht erreichbar ist. • Prüfmodus (OCSP, CRL)
Komponenten	System, OCSP-Responder
Ausgangsdaten	Status der Prüfung, OCSP-Response, im Zertifikat enthaltene Rollen-OIDs
Referenzen	[RFC5280] Kap. 6.1, [X.509] Referenzierte Standards in den aufzurufenden TUCs
Standardablauf	<p>Die Zertifikatsprüfung setzt sich aus folgenden Schritten zusammen:</p> <ol style="list-style-type: none"> 1. [System] Die Gültigkeit des Zertifikats wird geprüft (TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats") . 2. [System] Prüfung der Extension KeyUsage auf Vorhandensein. Zudem wird die KeyUsage und ExtendedKeyUsage (falls vorhanden) auf die richtige Belegung entsprechend der vorgesehenen (intendedKeyUsage bzw. intendedExtendedKeyUsage) KeyUsage geprüft. Die intendedKeyUsage sowie die intendedExtendedKeyUsage können aus einer Liste mehrerer erlaubter Werte bestehen. Es wird geprüft, dass die im Parameter intendedKeyUsage bzw. intendedExtendedKeyUsage übergebenen Werte eine Teilmenge der Werte in der jeweiligen Extension KeyUsage bzw. ExtendedKeyUsage des

Zertifikats sind. Da die übergebenen Parameter die Verwendung des Zertifikats im Aufrufkontext widerspiegeln, ist es dabei nicht notwendig, dass diese zu den Werten in der Zertifikatsextension komplett identisch sind. Enthält ein übergebener Parameter keine Werte, so bedeutet dies, dass der Inhalt der Zertifikatsextension nicht relevant ist.

3.

[System] Das passende CA-Zertifikat wird in den TSL-Informationen gesucht (TUC_PKI_003 "CA-Zertifikat in TSL-Informationen finden")

4.

[System] Mathematische Prüfung der Signatur des Zertifikats (TUC_PKI_004 "Mathematische Prüfung der Zertifikatssignatur").

5.

[System] Der ServiceStatus (vgl. Tab_PKI_271) des CA-Zertifikats wird geprüft. Im Fall von „revoked“ wird der Zeitpunkt des Gültigkeitsbeginns (Feld "notBefore" gemäß [RFC5280]#4.1.2.5) des End-Entity-Zertifikats mit dem Datum des Statuswechsels (StatusStartingTime) verglichen.

Der Zeitpunkt des Gültigkeitsbeginns des End-Entity-Zertifikats liegt vor dem Zeitpunkt des Statuswechsels.

6.

[System, Prüfmodus Offline] Falls JA, weiter mit Schritt 8, sonst mit 7.

7.

[System, Prüfmodus OCSP]

Statusinformation zum Zertifikat durch Abfrage des zugeordneten OCSP-Dienstes ermitteln (TUC_PKI_006 "OCSP-Abfrage").

TUC_PKI_006 wird für TLS-Zertifikate der **StörungssampelBetriebsdatenerfassung (BDE)**(C.ZD.TLS-S mit technischer Rolle oid_stamp) und nonQES-Zertifikate einer eGK mit dem Parameter

ENFORCE_CERTHASH_CHECK=false aufgerufen. Für alle anderen Zertifikate wird TUC_PKI_006 mit dem Defaultwert ENFORCE_CERTHASH_CHECK=true aufgerufen.

Wenn der zuständige OCSP-Responder die Statusinformation des Zertifikats mit einem Wert „revoked“ oder „unknown“ gemäß GS-A 4690 zurückgibt – Meldungskürzel (CERT_REVOKED) bzw. (CERT_UNKNOWN) gemäß Tab_PKI_274 oder eine wegen ENFORCE_CERTHASH_CHECK=true

	<p>erforderliche certHash-Erweiterung fehlt (CERTHASH_EXTENSION_MISSING) bzw. falsch ist (CERTHASH_MISMATCH), darf das Zertifikat nicht als gültig bewertet werden.</p> <p>8. [System:] Ermittlung (TUC_PKI_009 "Rollenermittlung") der Rolle</p> <p>9. [System:] Prüfung, ob eine der übergebenen Zertifikatstyp-OIDs (aus der Parameter PolicyList) im Zertifikat enthalten ist (TUC_PKI_007 "Prüfung Zertifikatstyp"). Zur Prüfung muss die Liste (PolicyList s.o.) mindestens eine OID enthalten.</p> <p>10. [System:] Ende des Use Cases mit Rückgabe des/der im Zertifikat enthaltenen Rollen-OID(s).</p>
Varianten/Alternativen	<p>6a. [System:] Der Offline-Modus ist aktiviert. Es werden keine Statusinformationen zum Zertifikat eingeholt.</p> <p>7a. [System, Prüfmodus CRL] Prüfung der Sperrinformation des Zertifikates mittels CRL (TUC_PKI_021 "CRL-Prüfung"). Wenn das Zertifikat in der Sperrliste (CRL) enthalten ist – Meldungskürzel (CERT_REVOKED) gemäß Tab_PKI_274, darf das Zertifikat nicht als gültig bewertet werden.</p> <p>7b [System] Eine OCSP-Response zu dem zu prüfenden Zertifikat wurde im Aufruf mit übergeben. Falls diese zum Referenzzeitpunkt gültig ist, wird nicht der TUC_PKI_006 aufgerufen, sondern die beigefügte OCSP-Response zur weiteren Prüfung verwendet.</p>
Fehlerfälle	<p>2a. [System:] KeyUsage ist nicht vorhanden bzw. nicht alle Werte der intendedKeyUsage in der KeyUsage enthalten (WRONG_KEYUSAGE).</p> <p>2a1. [System:] intendedExtendedKeyUsage enthält Werte und nicht alle davon sind in der ExtendedKeyUsage enthalten (WRONG_EXTENDEKEYUSAGE).</p> <p>5a. [System:] Das Ausgabedatum des End-Entity-Zertifikats liegt nach dem Datum des</p>

	<p>Statuswechsels. Abbruch mit Fehlermeldung (CA_CERTIFICATE_REVOKED_IN_TSL) 7c.</p> <p>[System] Eine OCSP-Response zu dem zu prüfenden Zertifikat wurde im Aufruf mit übergeben, ergab bei den weiteren Prüfschritten jedoch kein gültiges Ergebnis (Überprüfung und Auswertung der Gültigkeit der OCSP-Response in TUC_PKI_006 schlägt fehl). Eine erneute Prüfung wird in diesem Fall durch Aufruf des TUC_PKI_006 durchgeführt, als wäre keine OCSP-Response beigefügt. In den Rückgabewerten dieses TUC wird die Warnmeldung (PROVIDED_OCSP_RESPONSE_NOT_VALID) an die aufrufende Funktion übergeben.</p>
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	<p>Gültige Status zu Schritt 5 sind gemäß Tab_PKI_271 .</p> <p>Schritt 5 stellt eine Sperrprüfung des CA-Zertifikats (für nonQES-HBA- und SMC-B-Zertifikate) gemäß Ketten- bzw. Kompromissmodell dar. Vgl. Kap. 8.1.1 Initialisierung TI-Vertrauensraum.</p> <p>Eine Zertifikatsprüfung in der TI gemäß TUC_PKI_018 darf nach Ablauf der TSL-Graceperiod nicht positiv ausfallen (vgl. GS-A_5336).</p>
Zugehörige Diagramme	<p>Aktivitätsdiagramm TUC_PKI_018 "Zertifikatsprüfung".</p> <p>Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.</p>

33
 34 **【<=,TSP X.509 nonQES - HBA, Intermediär VSDM, TSP X.509 nonQES - eGK, Zentrales-**
 35 **Netz, KOM-LE FD, DiPag_FD, Konfigdienst, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES**
 36 **- gSMC, NCPeH_FD, gematik Root-CA, Konnektor Highspeed, Basis-Consumer, TSL-Dienst,**
 37 **SigD, VSDD, Zeitdienst, OCSP-Proxy, Aktensystem_ePA, Verzeichnisdienst, UFS,**
 38 **SG_BestNetze, TSP X.509 QES, IDP-D, CMS, Namensdienst, eRp_FD, Konnektor PTV5,**
 39 **Konnektor PTV5Plus, Konnektor PTV6, Zugangsdienst,funkt. Eignung: Herstellererklärung,**
 40 **Sich.techn. Eignung: Herstellererklärung, funkt. Eignung: Test Produkt/FA】**

3 Änderungen in Steckbriefen

3.1 Änderungen in gemProdT_X509_TSP_nonQES_eGK/gemProdT_X509_TSP_nonQES_H BA/gemProdT_X509_TSP_nonQES_Komp/ gemProdT_X509_TSP_nonQES_SMC-B/gemProdT_X509_TSP_QES

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments
[gemProdT_X509_TSP_nonQES_eGK/gemProdT_X509_TSP_nonQES_HBA/gemProdT_X509_TSP_nonQES_Komp/gemProdT_X509_TSP_nonQES_SMC-B/gemProdT_X509_TSP_QES]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 2: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_15166	Nutzer der Schnittstelle I_Monitoring_Update, Zertifikatsprüfung	gemSpec_ServiceMon
TIP1-A_7117	Service Monitoring und Client, I_Monitoring_Update, WebService	gemSpec_ServiceMon
TIP1-A_7118	Service Monitoring und Client, I_Monitoring_Update, eindeutige Zuordnung	gemSpec_ServiceMon
TIP1-A_7119	Service Monitoring und Client, I_Monitoring_Update, Servicepunkte und IP-Adressen	gemSpec_ServiceMon
TIP1-A_7120	Service Monitoring und Client, I_Monitoring_Update, maximale Zeitabweichung zwischen Berichtszeitraum und Nachrichtenübermittlung	gemSpec_ServiceMon
TIP1-A_7126	Nutzer des Service Monitorings I_Monitoring_Update, Zeitstempel bei Ausfall/Wiederherstellung	gemSpec_ServiceMon
TIP1-A_7127	Nutzer des Service Monitorings I_Monitoring_Update, eindeutige Zuordnung des Messwertes	gemSpec_ServiceMon
TIP1-A_7128	Nutzer des Service Monitorings I_Monitoring_Update, maximale HTTP-Nachrichtenlänge	gemSpec_ServiceMon

TIP1-A_7129	Nutzer des Service Monitorings I_Monitoring_Update, Selbstauskunft als Bestandteil jeder SOAP-Nachricht	gemSpec_ServiceMon
-------------	---	--------------------

58

59

60

61

62

63