
C_12188_Anlage

Inhaltsverzeichnis

1 Änderung in gemSpec_Kon.....	2
---------------------------------------	----------

1 Änderung in gemSpec_Kon

Anforderung A_23536-02 wird neu erhoben.

A_23536-02 - TUC KON_159 - "Signaturdatenelemente nachbereiten"

Der Konnektor MUSS den technischen Use Case TUC_KON_159 "Signaturdatenelemente nachbereiten" umsetzen.

Tabelle 1: TAB_KON_892 - TUC_KON_159 „Signaturdatenelemente nachbereiten“

Element	Beschreibung
Name	TUC_KON_159 „Signaturdatenelemente nachbereiten“
Beschreibung	Es wird für das verwendete Signaturzertifikat die Statusauskunft eingeholt, überprüft und falls gefordert, in die vorab erstellte Signatur eingebettet.
Auslöser	TUC_KON_150 „Dokumente QES signieren“, TUC_KON_170 Dokumente mit Komfort signieren“, TUC_KON_160 „Dokumente nonQES signieren“
Vorbedingungen	keine
Eingangsdaten	<ul style="list-style-type: none"> signatureMode (Signaturart: QES nonQES) Signierte Dokumente / signiertes Dokument <ul style="list-style-type: none"> signatureType (URI für den Signaturtyp XML-, CMS-, S/MIME- oder PDF-Signatur) Zertifikatsreferenz (zu verwendende Signatur-Identität) includeRevocationInfo [Boolean] - optional; Default: true (Dieser Parameter steuert die Einbettung von OCSP-Responses in die Signatur. true: Die Sperrinformationen werden in die Signatur eingebettet.)
Komponenten	Konnektor, Kartenterminal, Signaturkarte
Ausgangsdaten	<ul style="list-style-type: none"> Prüfergebnis für das Zertifikat Signiertes Dokument/ Dokumente mit eingebetteter OCSP-Antwort optional/nur wenn includeRevocationInfo = true
Standardablauf	<ol style="list-style-type: none"> Ermitteln des Signaturzeitpunktes aus dem Signierten Dokument Einholen einer OCSP-Response zur Zertifikatsreferenz mit TUC_PKI_006 mit Referenzzeitpunkt=Signaturzeitpunkt OCSP-Graceperiod=0 Timeout-Parameter=2s und extrahieren der OCSP_creation_Time

	<p>3. Wenn includeRevocationInfo=true und signatureMode=QES: Ermitteln der Zeitdifferenz $dT = \text{Signaturzeitpunkt} - \text{OCSP_Creation_Time}$ Wenn $0 < dT < 2s$, dann führe nach dT erneut TUC_PKI_006 aus</p> <p>4. Signaturprüfung</p> <p>a) Wenn signatureMode=QES und/oder includeRevocationInfo=true wird das Signaturzertifikat durch Aufruf von TUC_KON_037 „Zertifikat prüfen“ {</p> <pre> certificate = Zertifikatsreferenz; qualifiedCheck = if_QC_present; offlineAllowNoCheck = true; gracePeriod=0; validationMode = OCSP; ocspResponse = OCSP-Response aus (2) oder (3) </pre> <p>geprüft. Die OCSP-Auskunft muss ausgewertet werden. Andere Zertifikatsprüfergebnisse können aus dem Cache genommen werden.</p> <p>b) sonst</p> <pre> Aufruf von TUC_KON_037 „Zertifikat prüfen“ { certificate = Zertifikatsreferenz; qualifiedCheck = if_QC_present; offlineAllowNoCheck = true; validationMode = OCSP} Zertifikatsprüfergebnisse können aus dem Cache genommen werden. </pre> <p>5. Falls includeRevocationInfo== true wird die OCSP-Antwort gemäß des signatureType in die Signatur für jedes Dokument eingebettet.</p> <p>signatureType = XMLDSig (XAdES) Einbettung der OCSP-Response im Sinne vom AdES-X-L; die base-64 kodierte OCSP-Response wird im Feld QualifyingProperties/UnsignedProperties /UnsignedSignatureProperties/RevocationValues /OCSPValues/EncapsulatedOCSPValue (selbst DER-kodiert) gespeichert.</p> <p>signatureType = CMS (CAdES) Ist die Einbettung von OCSP-Responses gefordert, wird die für die Offline-Prüfung notwendige OCSP-Antwort des EE-Zertifikats im Attribut SignedData.crls.other abgelegt.</p> <p>signatureType = PDF/A (PAdES) OCSP-Responses werden bei PAdES nicht eingebettet.</p>
	keine

Fehlerfälle	(->2) Für MGM_LU_ONLINE=Enabled gilt: Liefert die Zertifikatsprüfung (OCSP-Abfrage) die Warnung CERT_REVOKED oder CERT_UNKNOWN gemäß [gemSpec_PKI#Tab_PKI_274], dann wird der TUC mit Fehler 4123 abgebrochen.
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

Tabelle 2: TAB_KON_893 Fehlercodes TUC_KON_159 „Signaturdatenelemente nachbereiten

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4123	Security	Error	Fehler bei Signaturerstellung

Festlegen, welche Parameter sind in Schritt 3 an TUC_PKI_006 zu übergeben sind, insbes. Referenzzeitpunkt. [≤, Konnektor Highspeed, Konnektor PTV5Plus, Konnektor PTV6, Sich.techn. Eignung: CC-Evaluierung, funkt. Eignung: Test Produkt/FA, Sich.techn. Eignung: Prüfung durch CC-Prüfstelle]

Anforderung A_23536-01 entfällt.

A_23536-01 - TUC_KON_159 - "Signaturdatenelemente nachbereiten"

Der Konnektor MUSS den technischen Use Case TUC_KON_159 "Signaturdatenelemente nachbereiten" umsetzen.

Tabelle 3: TAB_KON_892 - TUC_KON_159 „Signaturdatenelemente nachbereiten"

Element	Beschreibung
Name	TUC_KON_159 „Signaturdatenelemente nachbereiten"
Beschreibung	Es wird für das verwendete Signaturzertifikat die Statusauskunft eingeholt, überprüft und falls gefordert, in die vorab erstellte Signatur eingebettet.
Auslöser	TUC_KON_150 „Dokumente QES signieren", TUC_KON_170 Dokumente mit Komfort signieren", TUC_KON_160 „Dokumente nonQES signieren"
Vorbedingungen	keine
Eingangsdaten	<ul style="list-style-type: none"> signatureMode (Signaturart: QES nonQES) Signierte Dokumente / signiertes Dokument <ul style="list-style-type: none"> signatureType (URI für den Signaturtyp XML-, CMS-, S/MIME- oder PDF-Signatur) Zertifikatsreferenz (zu verwendende Signatur-Identität)

	<ul style="list-style-type: none"> includeRevocationInfo [Boolean] - optional; Default: true (Dieser Parameter steuert die Einbettung von OCSP-Responses in die Signatur. true: Die Sperrinformationen werden in die Signatur eingebettet.)
Komponenten	Konnektor, Kartenterminal, Signaturkarte
Ausgangsdaten	<ul style="list-style-type: none"> Prüfergebnis für das Zertifikat Signiertes Dokument/ Dokumente mit eingebetteter OCSP-Antwort optional/nur wenn includeRevocationInfo = true
Standardablauf	<p>1. Signaturprüfung</p> <p>a) Wenn signatureMode=QES und/oder includeRevocationInfo=true wird das Signaturzertifikat durch Aufruf von TUC_KON_037 „Zertifikat prüfen“ {</p> <pre> certificate = Zertifikatsreferenz; qualifiedCheck = if_QC_present; offlineAllowNoCheck = true; gracePeriod=0; validationMode = OCSP; getOCSPResponses = includeRevocationInfo} </pre> <p>geprüft. Eine OCSP-Auskunft muss eingeholt werden. Andere Zertifikatsprüfergebnisse können aus dem Cache genommen werden.</p> <p>b) sonst</p> <pre> Aufruf von TUC_KON_037 „Zertifikat prüfen“ { certificate = Zertifikatsreferenz; qualifiedCheck = if_QC_present; offlineAllowNoCheck = true; validationMode = OCSP} </pre> <p>Zertifikatsprüfergebnisse können aus dem Cache genommen werden.</p> <p>2. Falls includeRevocationInfo== true wird die OCSP-Antwort gemäß des signatureType in die Signatur für jedes Dokument eingebettet.</p> <p>signatureType = XMLDSig (XAdES) Einbettung der OCSP-Response im Sinne vom AdES-X-L; die base-64 kodierte OCSP-Response wird im Feld QualifyingProperties/UnsignedProperties/UnsignedSignatureProperties/RevocationValues/OCSPValues/EncapsulatedOCSPValue (selbst DER-kodiert) gespeichert.</p> <p>signatureType = CMS (CAAdES) Ist die Einbettung von OCSP-Responses gefordert, wird die für die Offline-Prüfung notwendige OCSP-Antwort des EE-Zertifikats im Attribut SignedData.crls.other abgelegt.</p> <p>signatureType = PDF/A (PAdES)</p>

	OCSP-Responses werden bei PAdES nicht eingebettet.
Varianten/Alternativen	keine
Fehlerfälle	(->1) Für MGM_LU_ONLINE=Enabled gilt: Liefert die Zertifikatsprüfung (OCSP-Abfrage) die Warnung CERT_REVOKED oder CERT_UNKNOWN gemäß [gemSpec_PKI#Tab_PKI_274], dann wird der TUC mit Fehler 4123 abgebrochen.
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

Tabelle 4: TAB_KON_893 Fehlercodes TUC_KON_159 „Signaturdatenelemente nachbereiten

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4123	Security	Error	Fehler bei Signaturerstellung

【<=, Konnektor Highspeed, Konnektor PTV5Plus, Konnektor PTV6, Sich.techn. Eignung: CC-Evaluierung, funkt. Eignung: Test Produkt/FA, Sich.techn. Eignung: Prüfung durch CC-Prüfstelle】