
C_12545_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	2
2 Änderung in gemSpec_PKI.....	3
2.1 Kapitel 5.12.3 <tsp>.HBA-qCA<n> - Aussteller-CA_QES.....	3
2.2 Kapitel 5.13.3.1 C.GEM.OCSP OCSP-Signer-Zertifikat.....	4
3 Änderungen in Steckbriefen.....	7
3.1 Änderungen in gemProdT_X509_TSP_QES.....	7
3.2 Änderungen in gemProdT_X509_TSP_nonQES_eGK, gemProdT_X509_TSP_nonQES_HBA, gemProdT_X509_TSP_nonQES_SMC-B und gemProdT_X509_TSP_nonQES_Komp.....	7

1 Änderungsbeschreibung

Das AIA-Feld in Zertifikatsprofilen dient zur Bereitstellung von Informationen, die bei der Validierung des zu prüfenden Zertifikates helfen können. Bisher wurde in Zertifikatsprofilen der TI lediglich OCSP als accessMethod vorgesehen. Hierzu wird dann die URL des OSCP-Responders als accessLocation aufgeführt.

Gemäß dem RFC 5280 ist allerdings auch die Hinterlegung von CAIssuers als accessMethod möglich, um andere CA-Dienste aufzuführen, die bei der Bildung des Vertrauenspfades und damit bei der Zertifikats-Validierung ebenfalls helfen können. Diese Methode wird nun ergänzend bei Profilen von QES-CA-Zertifikaten als auch bei OCSP-Signer-Zertifikaten erlaubt. Dieses ist in den Zertifikaten der TSPs auch schon erfolgreich in der Vergangenheit im Einsatz gewesen und wird nun auch spezifikatorisch als optionales Feld geregelt.

Hinweis: In den für die QES-Zertifikatsprüfung in der TI spezifizierten Prüfvorgaben ("TUC_PKI_030 - QES Zertifikatsprüfung") ist die Verarbeitung von CAIssuers bisher nicht vorgesehen. Für Prüfmechanismen außerhalb der TI kann die Nutzung von CAIssuers allerdings hilfreich sein.

2 Änderung in gemSpec_PKI

In der Profiltabelle im Kapitel 5.12.3 bzw. 5.13.3.1 wird die Extension "AuthorityInfoAccess" jeweils um die Zeile "CAIssuers | 0-1" ergänzt.

2.1 Kapitel 5.12.3 <tsp>.HBA-qCA<n> - Aussteller-CA_QES

GS-A_4948-01 -Umsetzung QES-CA-Zertifikate

Der TSP-X.509 QES MUSS für die Zertifikate der von ihm betriebenen CAs die Attributsbelegung der Felder gemäß Tab_PKI_215* umsetzen.

Tabelle 1: Tab_PKI_215* <tsp>.HBA-qCA<n> - Aussteller- CA_QES der TI

Element	Inhalt	Kar.	
certificate	C.<tsp>.HBA-qCA<n>		
tbsCertificate			
version	2 (v3)		
CertificateSerialNumber	gemäß [RFC5280#4.1.2.2]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4358-*]		
issuer	DN der ausstellenden CA		
validity	Gültigkeit des Zertifikats (von - bis)		
subject			
commonName	<tsp>.HBA-qCA <n> *)	1	
organizationalUnitName	Qualifizierter VDA der Telematikinfrastruktur	0-1	
organizationIdentifier	Vom VDA verwendeter organizationIdentifier gemäß [ETSI EN 319 412-2] und [X.520]	0-1	
organizationName	Name des VDA für QES	1	
countryName	DE	1	
andere Attribute		0	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4358-*] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
extensions			critical
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der CA, für die dieses Zertifikat ausgestellt wird	1	FALSE

KeyUsage {2 5 29 15}	keyCertSign crlSign	1 0-1	TRUE
SubjectAltNames {2 5 29 17}		0	FALSE
BasicConstraints {2 5 29 19}	ca = TRUE pathLength = 0	1 1	TRUE
CertificatePolicies {2 5 29 32}	policyIdentifier = <id-etsi-qcp-natural-qscd> {0.4.0.194112.1.2} policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_policy_hba_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie Ggf. weitere policyIdentifier Ggf. weitere policyQualifierInfo	0-1 0-1 1 0-1 0-n 0-n	FALSE
CRLDistributionPoints {2 5 29 31}	CDP	0-1	FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst CAIssuers	0-1 0-1	FALSE
AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
Admission {1 3 36 8 3 3}		0	FALSE
ValidityModel {1 3 6 1 4 1 8301 3 5}	id-validity-Model-chain {1 3 6 1 4 1 8301 3 5 1}	1	FALSE
ExtendedKeyUsage {2 5 29 37}		0	FALSE
QCStatements {1.3.6.1.5.5.7.1.3}	<id-etsi-qcs-QcCompliance> {0.4.0.1862.1.1} Ggf. weitere Einträge	0-1 0-n	FALSE
andere Erweiterungen	Ggf. weitere Erweiterungen durch die BNetzA gesetzt, die hier jedoch nicht spezifiziert sind.		
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4358-*)]		
signature	Wert der Signatur		

*) Der Name kann mit oder ohne Leerzeichen vor der laufenden Nr. <n> geschrieben werden. [=<,TSP X.509 QES,funkt. Eignung: Test Produkt/FA]

2.2 Kapitel 5.13.3.1 C.GEM.OCSP OCSP-Signer-Zertifikat

GS-A_4741-01 -Umsetzung Zertifikatsprofil C.GEM.OCSP

Der TSP-X.509 nonQES, die gematik-Root-CA und der TSL-Dienst MÜSSEN C.GEM.OCSP gemäß Tab_PKI_253* umsetzen.

Tabelle 2: Tab_PKI_253* C.GEM.OCSP Zertifikatsprofil OCSP-Signer

Element	Inhalt	Kar.	
---------	--------	------	--

certificate		C.GEM.OCSP		
	tbsCertificate			
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357-*]		
	issuer	DN der ausstellenden CA		
	validity	Gültigkeit des Zertifikats (von - bis)		
	subject			
	commonName	Name des OCSP-Responders	1	
	serialNumber	Zur Unterscheidung gleichartiger Instanzen	0-1	
	organizationalUnitName	Name der Abteilung für den Betrieb des OCSP	0-1	
	organizationName	Name des OCSP-Diensteanbieters	1	
	countryName	Land der Anschrift des OCSP-Diensteanbieters	1	
	andere Attribute		0	
	subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4357-*] und individueller Wert des öffentlichen Schlüssels des Zertifikatsbesitzers		
	extensions			critical
	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des OCSP-Signers	1	FALSE
	KeyUsage {2 5 29 15}	nonRepudiation	1	TRUE
	SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
	BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie)	1 0-1	FALSE
	CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst CAIssuers	0-1 0-1	FALSE
	AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
	ExtendedKeyUsage {2 5 29 37}	KeyPurposeId = id-kp-OCSPSigning	1	FALSE
	id-pkix-ocsp-nocheck	OCSP-Nocheck = NULL	0-1	FALSE

		{1.3.6.1.5.5.7.48.1.5}		
		<i>andere Erweiterungen</i>		0
	signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357-*]		
	signature	Wert der Signatur		

【<=, TSP X.509 nonQES - HBA, TSP X.509 nonQES - eGK, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC, funkt. Eignung: Test Produkt/FA】

3 Änderungen in Steckbriefen

3.1 Änderungen in 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_QES_PTV]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 3: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4948-01	Umsetzung QES-CA-Zertifikate	gemSpec_PKI

3.2 Änderungen in gemProdT_X509_TSP_nonQES_eGK, gemProdT_X509_TSP_nonQES_HBA, gemProdT_X509_TSP_nonQES_SMC-B und gemProdT_X509_TSP_nonQES_Komp

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_X509_TSP_nonQES_eGK_PTV, gemProdT_X509_TSP_nonQES_HBA_PTV, gemProdT_X509_TSP_nonQES_SMC-B_PTV und gemProdT_X509_TSP_nonQES_Komp_PTV]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 4: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4741-01	Umsetzung Zertifikatsprofil C.GEM.OCSP	gemSpec_PKI