Signaturprüfbericht für qualifizierte Signaturen

Prüfprotokoll nach §17 Abs. 2 Signaturgesetz (SigG)

1. Zusammenfassung der Prüfergebnisse

Signaturprüfung:	Erfolgreich
Datei:	muster-rechnung_signiert.pdf
Dateigröße:	68527
Datei erzeugt:	28.11.2008, 09:58:31
Datei verändert:	28.11.2008, 09:58:31
Hashwert (SHA-1):	76FB6D3DFDFE413AC54F269B9F03829B6EA667BA
Prüfzeitpunkt:	28.11.2008, 09:58:34
Geprüfte Signaturen:	1
Signaturformat:	eingebettete PDF-Unterschrift
Signaturprofil:	ISIS-MTT SigG
Signaturkomponente:	M-Doc Autoverifier
Prüfmodell:	Kettenmodell
Sperrungsprüfung:	Abfrage des OCSP-Responders

1.1. Darstellung der Prüfschritte

Integritätsprüfung:	Durchgeführt	Die Integritätsprüfung verifiziert die Unversehrtheit des Dokumentes und des Unterzeichnerzertifikates. Die Prüfung stellt sicher, daß die empfangenen Daten nicht verändert wurden und dem Urheber eindeutig zugeordnet werden können. Diese Prüfung erfolgt offline.
Zertifikatskettenprüfung:	Durchgeführt	Die Zertifikatskettenprüfung verifiziert die Identität des Unterzeichners. Hierbei wird die Zertifikatshierarchie bis zu einem qualifizierten ZDA (Trustcenter) aufgebaut und die Gültigkeit der Zertifikatssignaturen geprüft. Diese Prüfung erfolgt offline.
Sperrungsprüfung:	Durchgeführt	Die Sperrungsprüfung ermittelt, ob das Unterzeichnerzertifikat zum Signaturzeitpunkt noch gültig war. Hierbei wird auch überprüft, ob das Zertifikat beim Herausgeber gesperrt wurde. Diese Prüfung erfolgt durch Auswertung der Sperrliste des Trustcenters (CRL) und durch Online-Abfrage der Sperrungsdatenbank (OCSP). Diese Prüfung erfolgt online.

2. Prüfergebnisse

2.1. Prüfung der Unterschriften

Details Unterschrift 1: signaturportal.de 2:PN

Prüfergebnis:	Unterschrift wurde erfolgreich verifiziert
qualifizierte Signatur:	ja
Unterzeichner:	signaturportal.de 2:PN
Zertifikatsaussteller:	D-TRUST Qualified CA 3 2007:PN
Unterschriftszeitpunkt:	26.11.2008, 13:44:19 +01'00"
Attributzertifikat:	nicht vorhanden
Einsatzbeschränkung:	Nur für Massensignaturen im Rahmen des Signaturportals.

Details Unterschrift 1: signaturportal.de 2:PN

Signaturverfahren:	sha256withRSAEncryption
Schlüssellänge:	2048 bit
Begründung:	i.V.Max Mustermann Hier-steht-Ihre-Firma
Ort:	Signaturportal.de - Signatur-/Postvollmacht
Eignung Hash-Wert:	SHA256 Sicherheitsgeeignet bis: 31.12.2013
Eignung Schlüssellänge:	RSA2048 Sicherheitsgeeignet bis: 31.12.2013

Inhaberzertifikat Unterschrift 1: signaturportal.de 2:PN

Name:	signaturportal.de 2:PN
Zertifikatstyp	qualifiziert nach §2 Nr. 3 SigG
Herausgeber:	D-TRUST Qualified CA 3 2007:PN
Seriennummer:	075165
gültig von:	29.04.2008, 22:59:59
gültig bis:	05.07.2009, 22:59:59
Widerrufzeitpunkt:	

Zwischenzertifizierungstelle Unterschrift 1: signaturportal.de 2:PN

Name:	D-TRUST Qualified CA 3 2007:PN
Herausgeber:	D-TRUST Qualified Root CA 3 2007:PN
Seriennummer:	04386E
gültig von:	31.10.2007, 06:47:39
gültig bis:	31.10.2012, 06:42:31
Widerrufzeitpunkt:	

Vertrauenswürdige Stammzertifizierungstelle Unterschrift 1: signaturportal.de 2:PN

Name:	D-TRUST Qualified Root CA 3 2007:PN
Herausgeber:	D-TRUST Qualified Root CA 3 2007:PN
Seriennummer:	04386D
gültig von:	31.10.2007, 06:42:31
gültig bis:	31.10.2012, 06:42:31
Widerrufzeitpunkt:	

3. Zertifikatsdaten

Unterzeichnerzertifikat Unterschrift 1

.

Seriennummer:	075165
Inhaber:	countryName=DE, organizationName=Mentana GmbH, commonName=signaturportal.de 2:PN, surname=signaturportal.de 2:PN, serialNumber=DTRWS945248092570225, pseudonym=signaturportal.de 2:PN signaturportal.de 2:PN DE Mentana GmbH
Herausgeber:	countryName=DE, organizationName=D-Trust GmbH, commonName=D-TRUST Qualified CA 3 2007:PN D-TRUST Qualified CA 3 2007:PN DE D-Trust GmbH
Signaturalgorithmus:	sha256withRSAEncryption
Schlüssellänge:	2048 bit
qualifiziertes Zertifikat:	ja (ISIS-MTT QC-Statement)

Unterzeichnerzertifikat Unterschrift 1

gültig von:	29.04.2008, 22:59:59	
gültig bis:	05.07.2009, 22:59:59	
Widerrufzeitpunkt:		
Erweiterungen	Beschreibung:	authorityKeyIdentifier
	OID:	2.5.29.35
	Wert:	B289CC15BCF6CCD1117F624EE0E854F31C0CB172
	Beschreibung:	qcStatements
	OID:	1.3.6.1.5.5.7.1.3
	Wert:	0.4.0.1862.1.1, 0.4.0.1862.1.3
	Beschreibung:	authorityInfoAccess
	OID:	1.3.6.1.5.5.7.1.1
	Wert:	URI={1.3.6.1.5.5.7.48.1=http://qual.ocsp.d-trust.net}
	Beschreibung:	certificatePolicies
	OID:	2.5.29.32
	Wert:	1.3.6.1.4.1.4788.2.31.1
	Beschreibung:	cRLDistributionPoints
	OID:	2.5.29.31
	Wert:	URI={ldap://directory.d-trust.net/CN=D-TRUST%20Qualified%20CA%203%202007%3APN,O=D-Trust%20GmbH,C=DE?certificaterevocationlist}, URI={http://www.d-trust.net/crl/d-trust_qualified_ca_3_2007.crl}
	Beschreibung:	subjectKeyIdentifier
	OID:	2.5.29.14
	Wert:	69521B444FF7A2EF14B40B82D2E9722C3E4F9D53
	Beschreibung:	keyUsage
	OID:	2.5.29.15
	Wert:	Rechtsverbindliche Willenserklärung (40)
	Beschreibung:	id-isismtt-at-restriction
	OID:	1.3.36.8.3.8
	Wert:	Nur für Massensignaturen im Rahmen des Signaturportals.

Stammzertifikate Unterschrift 1

.

Seriennummer:	04386E
Inhaber:	countryName=DE, organizationName=D-Trust GmbH, commonName=D-TRUST Qualified CA 3 2007:PN D-TRUST Qualified CA 3 2007:PN DE D-Trust GmbH
Herausgeber:	countryName=DE, organizationName=D-Trust GmbH, commonName=D-TRUST Qualified Root CA 3 2007:PN D-TRUST Qualified Root CA 3 2007:PN DE D-Trust GmbH
Signaturalgorithmus:	sha256withRSAEncryption
Schlüssellänge:	2048 bit
qualifiziertes Zertifikat:	ja (ISIS-MTT QC-Statement)

Stammzertifikate Unterschrift 1

gültig von:	31.10.2007, 06:47:39	
gültig bis:	31.10.2012, 06:42:31	
Widerrufzeitpunkt:		
Erweiterungen	Beschreibung:	authorityKeyIdentifier
	OID:	2.5.29.35
	Wert:	3CEE42AA8CC297E2911313E8F464EBEFDAAEF08C
	Beschreibung:	qcStatements
	OID:	1.3.6.1.5.5.7.1.3
	Wert:	0.4.0.1862.1.1
	Beschreibung:	authorityInfoAccess
	OID:	1.3.6.1.5.5.7.1.1
	Wert:	URI={1.3.6.1.5.5.7.48.1=http://qual.ocsp.d-trust.net}
	Beschreibung:	certificatePolicies
	OID:	2.5.29.32
	Wert:	1.3.6.1.4.1.4788.2.31.1
	Beschreibung:	cRLDistributionPoints
	OID:	2.5.29.31
	Wert:	URI={ldap://directory.d-trust.net/CN=D-TRUST%20Qualified%20Root%20CA%203%202007%3APN,O=D-Trust%20GmbH,C=DE?certificaterevocationlist}, URI={http://www.d-trust.net/crl/d-trust_qualified_root_ca_3_2007_pn.crl}
	Beschreibung:	subjectKeyIdentifier
	OID:	2.5.29.14
	Wert:	B289CC15BCF6CCD1117F624EE0E854F31C0CB172
	Beschreibung:	keyUsage
	OID:	2.5.29.15
	Wert:	Sperrliste signieren, Zertifikat signieren (06)
	Beschreibung:	basicConstraints
	OID:	2.5.29.19
	Wert:	
Seriennummer:	04386D	
Inhaber:	countryName=DE, organizationName=D-Trust GmbH, commonName=D-TRUST Qualified Root CA 3 2007:PN D-TRUST Qualified Root CA 3 2007:PN DE D-Trust GmbH	
Herausgeber:	countryName=DE, organizationName=D-Trust GmbH, commonName=D-TRUST Qualified Root CA 3 2007:PN D-TRUST Qualified Root CA 3 2007:PN DE D-Trust GmbH	
Signaturalgorithmus:	sha256withRSAEncryption	
Schlüssellänge:	2048 bit	
qualifiziertes Zertifikat:	ja (ISIS-MTT QC-Statement)	

Stammzertifikate Unterschrift 1

gültig von:	31.10.2007, 06:42:31	
gültig bis:	31.10.2012, 06:42:31	
Widerrufzeitpunkt:		
Erweiterungen	Beschreibung:	qcStatements
	OID:	1.3.6.1.5.5.7.1.3
	Wert:	0.4.0.1862.1.1
	Beschreibung:	authorityInfoAccess
	OID:	1.3.6.1.5.5.7.1.1
	Wert:	URI={1.3.6.1.5.5.7.48.1=http://qual.ocsp.d-trust.net}
	Beschreibung:	certificatePolicies
	OID:	2.5.29.32
	Wert:	1.3.6.1.4.1.4788.2.31.1
	Beschreibung:	cRLDistributionPoints
	OID:	2.5.29.31
	Wert:	URI={ldap://directory.d-trust.net/CN=D-TRUST%20Qualified%20Root%20CA%203%202007%3APN,O=D-Trust%20GmbH,C=DE?certificaterevocationlist}, URI={http://www.d-trust.net/crl/d-trust_qualified_root_ca_3_2007_pn.crl}
	Beschreibung:	subjectKeyIdentifier
	OID:	2.5.29.14
	Wert:	3CEE42AA8CC297E2911313E8F464EBEFDAAEF08C
	Beschreibung:	keyUsage
	OID:	2.5.29.15
	Wert:	Sperrliste signieren, Zertifikat signieren (06)
	Beschreibung:	basicConstraints
	OID:	2.5.29.19
	Wert:	

Signaturvollmacht

Bei Signaturen im Intermediärmodell befindet sich die Signaturvollmacht einschl. eines Identitätsnachweises nach § 4 GWG in der Anlage des Hauptdokuments. Öffnen Sie den Kartenreiter 'Anlagen' im Adobe Acrobat Reader.
Bei Problemen wenden Sie sich bitte per E-Mail an support@sigmail.de.