Signaturprüfbericht für qualifizierte Signaturen

Prüfprotokoll nach §17 Abs. 2 Signaturgesetz (SigG)

1. Zusammenfassung der Prüfergebnisse

Signaturprüfung:	Erfolgreich
Datei:	test_m_sig_2.pdf
Dateigröße:	9917
Hashwert (SHA-1):	556CA419C8B4EE1358DCC21BA5D9EECFE0DDFF5B
Prüfzeitpunkt:	16.01.2008, 15:41:25
Geprüfte Signaturen:	1
Signaturformat:	eingebettete PDF-Unterschrift
Signaturprofil:	ISIS-MTT SigG
geprüft durch:	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 1 2006:PN
Unterschriftszeitpunkt:	29.11.2007, 13:15:53 +01'00"
Attributzertifikat:	nicht vorhanden
Einsatzbeschränkung:	Nur für Massensignaturen im Rahmen des Signaturportals.
Signaturverfahren:	sha1withRSAEncryption
Schlüssellänge:	2048 bit
Begründung:	i.V. Max Mustermann, Freiberufler Mentana- Claimsoft AG
Ort:	signaturportal.de - Signatur/Postvollmacht

Inhaberzertifikat Unterschrift 1: signaturportal.de 2:PN

Name:	signaturportal.de 2:PN
Zertifikatstyp	qualifiziert nach §2 Nr. 3 SigG
Herausgeber:	D-TRUST Qualified CA 1 2006:PN
Seriennummer:	035A2E
gültig von:	22.06.2007, 12:31:23
gültig bis:	02.07.2009, 12:31:23

Zwischenzertifizierungstelle Unterschrift 1: signaturportal.de 2:PN

Name:	D-TRUST Qualified CA 1 2006:PN
Herausgeber:	D-TRUST Qualified Root CA 1 2006:PN
Seriennummer:	00B961
gültig von:	27.04.2006, 14:40:54
gültig bis:	27.04.2011, 14:40:54

Vertrauenswürdige Stammzertifizierungstelle Unterschrift 1: signaturportal.de 2:PN

Name:	D-TRUST Qualified Root CA 1 2006:PN
Herausgeber:	D-TRUST Qualified Root CA 1 2006:PN
Seriennummer:	00B95F
gültig von:	27.04.2006, 14:40:54
gültig bis:	27.04.2011, 14:40:54

3. Zertifikatsdaten

Unterzeichnerzertifikat Unterschrift 1

Seriennummer:	035A2E
Inhaber:	countryName=DE, organizationName=Mentana GmbH, commonName=signaturportal.de 2:PN, surname=signaturportal.de 2:PN, serialNumber=DTR11824221831790125, pseudonym=signaturportal.de 2:PN signaturportal.de 2:PN DE Mentana GmbH
Herausgeber:	countryName=DE, organizationName=D-Trust GmbH, commonName=D-TRUST Qualified CA 1 2006:PN D-TRUST Qualified CA 1 2006:PN DE D-Trust GmbH
Signaturalgorithmus:	sha1withRSAEncryption
Schlüssellänge:	2048 bit
qualifiziertes Zertifikat:	ja (ISIS-MTT QC-Statement)

Unterzeichnerzertifikat Unterschrift 1

gültig von:	22.06.2007, 12:31:23	
gültig bis:	02.07.2009, 12:31:23	
Erweiterungen	Beschreibung:	authorityKeyIdentifier
	OID:	2.5.29.35
	Wert:	8420887FC18F5345C03BB37FF4B5533B7359CC84
	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:	1.3.6.1.4.1.4788.2.30.1
	Beschreibung:	cRLDistributionPoints
	OID:	2.5.29.31
	Wert:	URI={ldap://directory.d-trust.net/CN=D-TRUST%20Qualified%20CA%201%202006% URI={http://www.d-trust.net/crl/d-trust_qualified_ca_1_2006.crl}
	Beschreibung:	subjectKeyIdentifier
	OID:	2.5.29.14
	Wert:	CB2A9430B3CAD268675967C533CEF2E3CD117AE2
	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:	00B961
Inhaber:	countryName=DE, organizationName=D-Trust GmbH, commonName=D-TRUST Qualified CA 1 2006:PN D-TRUST Qualified CA 1 2006:PN DE D-Trust GmbH
Herausgeber:	countryName=DE, organizationName=D-Trust GmbH, commonName=D-TRUST Qualified Root CA 1 2006:PN D-TRUST Qualified Root CA 1 2006:PN DE D-Trust GmbH
Signaturalgorithmus:	sha1withRSAEncryption
Schlüssellänge:	2048 bit
qualifiziertes Zertifikat:	ja (ISIS-MTT QC-Statement)

Stammzertifikate Unterschrift 1

gültig von:	27.04.2006, 14:40:54	
gültig bis:	27.04.2011, 14:40:54	
Erweiterungen	Beschreibung:	authorityKeyIdentifier
	OID:	2.5.29.35
	Wert:	9AFE73A602367A2127A3377E14B3C304EAD82916
	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://ocsp.d-trust.net}
	Beschreibung:	certificatePolicies
	OID:	2.5.29.32
	Wert:	1.3.6.1.4.1.4788.2.30.1
	Beschreibung:	cRLDistributionPoints
	OID:	2.5.29.31
	Wert:	URI={ldap://directory.d-trust.net/CN=D-TRUST%20Qualified%20Root%20CA%201%2 URI={http://www.d-trust.net/crl/d-trust_qualified_root_ca_1_2006.crl}
	Beschreibung:	subjectKeyIdentifier
	OID:	2.5.29.14
	Wert:	8420887FC18F5345C03BB37FF4B5533B7359CC84
	Beschreibung:	keyUsage
	OID:	2.5.29.15
	Wert:	Sperrliste signieren, Zertifikat signieren (06)
	Beschreibung:	basicConstraints
	OID:	2.5.29.19
	Wert:	
Seriennummer:	00B95F	
Inhaber:	countryName=DE, organizationName=D-Trust GmbH, commonName=D-TRUST Qualified Root CA 1 2006:PN D-TRUST Qualified Root CA 1 2006:PN DE D-Trust GmbH	
Herausgeber:	countryName=DE, organizationName=D-Trust GmbH, commonName=D-TRUST Qualified Root CA 1 2006:PN D-TRUST Qualified Root CA 1 2006:PN DE D-Trust GmbH	
Signaturalgorithmus:	sha1withRSAEncryption	
Schlüssellänge:	2048 bit	
qualifiziertes Zertifikat:	ja (ISIS-MTT QC-Statement)	

Stammzertifikate Unterschrift 1

gültig von:	27.04.2006, 14:40:54	
gültig bis:	27.04.2011, 14:40:54	
Erweiterungen	Beschreibung:	basicConstraints
	OID:	2.5.29.19
	Wert:	
	Beschreibung:	subjectKeyIdentifier
	OID:	2.5.29.14
	Wert:	9AFE73A602367A2127A3377E14B3C304EAD82916
	Beschreibung:	authorityInfoAccess
	OID:	1.3.6.1.5.5.7.1.1
	Wert:	URI={1.3.6.1.5.5.7.48.1=http://ocsp.d-trust.net}
	Beschreibung:	certificatePolicies
	OID:	2.5.29.32
	Wert:	1.3.6.1.4.1.4788.2.30.1
	Beschreibung:	qcStatements
	OID:	1.3.6.1.5.5.7.1.3
	Wert:	0.4.0.1862.1.1
	Beschreibung:	keyUsage
	OID:	2.5.29.15
	Wert:	Sperrliste signieren, Zertifikat signieren (06)
	Beschreibung:	cRLDistributionPoints
	OID:	2.5.29.31
	Wert:	URI={ldap://directory.d-trust.net/CN=D-TRUST%20Qualified%20Root%20CA%201%2 URI={http://www.d-trust.net/crl/d-trust_qualified_root_ca_1_2006_pn.crl}

Signaturvollmacht

Sie finden die Signaturvollmacht auf unserer Webseite unter www.signaturportal.de.
Bei Problemen wenden Sie sich bitte per E-Mail an support@signaturportal.de.