Unterstützte Signaturkarten und Hardware-Token

Signaturkarten für eine qualifizierte elektronische Signatur (QES)

Mit dieser Anwendung können Sie die meisten von qualifizierten Vertrauensdiensteanbietern herausgegebenen Signaturkarten und Hardware-Token aus Deutschland verwenden. Die Listen mit den unterstützten Signaturkarten für eine qualifizierte elektronische Signatur sind den Tabellen Unterstützte Signaturkarten geeignet für eine qualifizierte Signatur (QES) (Tabellen 2a und 2b) zu entnehmen. Die Signaturkarten erlauben in der Regel die Erzeugung von qualifizierten und fortgeschrittenen Signaturen (ggf. auch Authentisierung). Außerdem können damit Daten ver- und entschlüsselt werden. Dieses gilt nur, wenn entsprechende Schlüssel/ Zertifikate auf der Signaturkarte vorhanden sind. Für die Anmeldung am beA-Postfach können Hardware-Token verwendet werden, welche die Schlüsselverwendung Authentisierung und Verschlüsselung besitzen. Bei Signaturkarten wird zwischen Einzel-, Stapel- und Multisignaturkarten unterschieden. Diese Anwendung unterstützt alle drei Kartenvarianten.

Qualifizierte Signaturkarten basieren auf sogenannten sicheren Signaturerstellungseinheiten (SSEE) bzw. Qualified Signature Creation Devices (QSCD). Für eine Signaturkarte werden von einem Vertrauensdiensteanbieter manchmal unterschiedliche SSEE bzw. QSCD verwendet. Es kann auch vorkommen, dass eine SSEE/ QSCD von mehreren Vertrauensdiensteanbietern genutzt wird. Unterstützt werden die in den Tabellen 2a und 2b angegebenen Kombinationen von Signaturkarte und SSEE.

Die unterstützten Signaturkarten müssen sich im Originalzustand befinden, d.h. so, wie sie durch den qVDA herausgegeben und zugestellt wurden. Es gibt eine Ausnahme: Wird von einem qVDA eine dezentrale Personalisierung einer Original-Signaturkarte angeboten, also das Nachladen von qualifizierten Zertifikaten, wird die Signaturkarte weiterhin unterstützt. Dieses ist zum Beispiel bei der beA-Karte möglich. Andere Modifizierungen der Signaturkarte, wie z.B. das lokale Aufspielen eigenen Schlüsselmaterials, könnten die Signaturkarte für diese Anwendung unbrauchbar machen oder sogar zerstören.

Tabelle 2a: Unterstützte Signaturkarten geeignet für eine qualifizierte Signatur mit Anbieterakkreditierung (QES)

Qualifizierte Vertrauensdiensteanbieter (BNetzA Gütezeichen)	Handelsname der Signaturkarte	Schlüsselverwendung	Name der SSEE in der Bestätigungsurkunde	Registrierungsnr. der Bestätigungsurkunde der SSEE
Deutsche Telekom AG c/o T-Systems International GmbH (Z0001)	TeleSec PKS-ECC-Signaturkarte (SignatureCard 2.0) 4)	Authentisierung Verschlüsselung 5) QES	Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 2.0 Release 1/SLE78CLX1440P	SRC.00016.TE.11.2012
	TeleSec PKS-ECC-Multisignatur (SignatureCard 2.0) 1) 4)			
Bundesnotarkammer, Zertifizierungsstelle (Z0003)	beA-Signatur 6)	Authentisierung Verschlüsselung QES	Signaturerstellungseinheit STARCOS 3.5 ID ECC C1	SRC.00013.TE.10.2012
Bundesnotarkammer, Zertifizierungsstelle (Z0003)	Bundesnotarkammer, Zertifizierungsstelle qualifizierte elektronische Signatur 2)	Authentisierung Verschlüsselung QES	Signaturerstellungseinheit STARCOS 3.5 ID ECC C1	SRC.00013.TE.10.2012
D-Trust GmbH (Z0017)	D-TRUST Card 3.0	Authentisierung Verschlüsselung QES	Sichere Signaturerstellungseinheit STARCOS 3.4 Health QES C1 Bestätigung wurde erweitert auf Nachfolgeversion STARCOS 3.4 Health QES C2 (siehe Nachtrag)	BSI.02120.TE.05.2009 Nachtrag 1 vom 15.11.2010 Nachtrag 2 vom 05.05.2015
	D-TRUST Card 3.0 Multicard 100 2)			
	D-TRUST Card 3.0 Multicard 1)			
	Personalausweis (PA), wenn mit einem QES-Zertifikat der D-Trust personalisiert 3) 7)	QES	Signaturerstellungseinheit „TCOS Identity Card Version 1.0 Release 1/P5CD128/145"	SRC.00007.TE.10.2010
			Signaturerstellungseinheit „TCOS Identity Card Version 1.0 R 1/SLE78CLX1440P"	SRC.00006.TE.11.2010
			Signaturerstellungseinheit „STARCOS 3.5 ID GCC C1"	SRC.00008.TE.12.2010 Nachtrag 1 vom 06.02.2013
			Signaturerstellungseinheit „STARCOS 3.5 ID GCC C1R"	SRC.00014.TE.02.2012 Nachtrag 1 vom 06.02.2013
dgnservice (Z0033)	sprintCard businessCard 2)	Authentisierung Verschlüsselung QES	Signaturerstellungseinheit STARCOS 3.5 ID ECC C1R	SRC.00021.TE.05.2013 Nachtrag 1 vom 14.11.2013

1) Multisignaturkarte. In Abhängigkeit von der Anwendung ist nach der PIN-Eingabe die Erzeugung von a) genau einer QES möglich, b) bis zu 500 QES im Batchverfahren möglich. Die Erzeugung von Signaturen innerhalb eines festgelegten Zeitfensters ist nicht möglich.
2) Stapelsignaturkarte. In Abhängigkeit von der Anwendung ist nach der PIN-Eingabe die Erzeugung von a) genau einer QES möglich, b) kartenabhängig die Erzeugung von bis zu 100 QES im Batchverfahren möglich.
3) Der mit einem qualifizierten Zertifikat personalisierte PA kann technisch bedingt nicht für eine fortgeschrittene Signatur, für Ver- und Entschlüsselung sowie für zertifikatsbasierte Authentisierung verwendet werden, da das notwendige Schlüsselmaterial nicht vorhanden ist.
4) Kein Signieren von XML-Daten möglich.
5) Gilt auch für Signaturkarte beA-Basis mit nachträglich aufgeladenem QES-Zertifikat.
6) Ver-/ und Entschlüsselung nur im CMS-Format möglich.
7) Der Vertrieb von nachladbaren QES-Zertifikaten mit dem Handelsnamen „sign.me" wurde von der D-TRUST GmbH eingestellt. Mehr Informationen auf der Webseite des Anbieters.

Tabelle 2b: Unterstützte Signaturkarten geeignet für eine qualifizierte Signatur (QES)

Qualifizierte Vertrauensdiensteanbieter (BNetzA Gütezeichen)	Handelsname der Signaturkarte	Schlüsselverwendung	Name der SSEE in der Bestätigungsurkunde	Registrierungsnr. der Bestätigungsurkunde der SSEE
D-Trust GmbH	D-TRUST Card 3.0 qualified	Authentisierung Verschlüsselung QES	Sichere Signaturerstellungseinheit STARCOS 3.4 Health QES C1 Bestätigung wurde erweitert auf Nachfolgeversion STARCOS 3.4 Health QES C2 (siehe Nachtrag)	BSI.02120.TE.05.2009 Nachtrag 1 vom 15.11.2010 Nachtrag 2 vom 05.05.2015
	D-TRUST Card 3.0 Multicard 100 qualified 2)			
	D-TRUST Card 3.0 Multicard qualified 1)			
	D-TRUST Card 3.1	Authentisierung Verschlüsselung QES	Sichere Signaturerstellungseinheit STARCOS 3.4 Health QES C1 Bestätigung wurde erweitert auf Nachfolgeversion STARCOS 3.4 Health QES C2 (siehe Nachtrag)	BSI.02120.TE.05.2009 Nachtrag 1 vom 15.11.2010 Nachtrag 2 vom 05.05.2015
	D-TRUST Card 3.1 Multi 100 2)			
	D-TRUST Card 3.1 Multi 1)			
D-Trust GmbH	D-TRUST Card 3.1 5)	QES	Digitale Signatur: Sichere Signaturerstellungseinheiten CardOS V5.0 with Application for QES, V1.0	BSI.02136.TE.07.2013
	D-TRUST Card 3.4 Multicard 100 2) 5)			
	D-TRUST Card 3.4 Multi 1) 5)			
S-TRUST 4)	S-TRUST Multisignaturkarte 1)	Authentisierung Verschlüsselung QES	Signaturerstellungseinheit ZKA-Signaturkarte, Version 6.32 M	TUVIT.93176.TU.05.2011
Deutsche Rentenversicherung Bund (DRV) 3)	Signaturkarte der Deutschen Rentenversicherung Bund (Einzelsignatur)	Verschlüsselung QES	Sichere Signaturerstellungseinheit CardOS V5.0 with Application for QES, V1.0	BSI.02136.TE.07.2013
	Multisignaturkarte der Deutschen Rentenversicherung Bund 1))	QES		
Bundesagentur für Arbeit 3)	Signaturkarte der Bundesagentur für Arbeit (BA)	Authentisierung Verschlüsselung QES	Sichere Signaturerstellungseinheit STARCOS 3.4 Health HBA C1 und C2	BSI.02120.TE.05.2009 Nachtrag vom 15.11.2010

1) Multisignaturkarte. In Abhängigkeit von der Anwendung ist nach der PIN-Eingabe die Erzeugung von a) genau einer QES möglich, b) von bis zu 500 QES im Batchverfahren möglich. Die Erzeugung von Signaturen innerhalb eines festgelegten Zeitfensters nicht möglich.
2) Stapelsignaturkarte. In Abhängigkeit von der Anwendung ist nach der PIN-Eingabe die Erzeugung von a) genau einer QES möglich, b) kartenabhängig die Erzeugung von bis zu 100 QES im Batchverfahren möglich.
3) Die Signaturkarte wird nur an Mitarbeiter der Behörde ausgegeben (geschlossene Nutzergruppe).
4) Der Vertrieb von S-TRUST-Signaturkarten wurde eingestellt. Mehr Informationen auf der Webseite des Anbieters.
5) Die Signaturkarte wird durch den qualifizierten Vertrauensdiensteanbieter nur in Projektlösungen ausgegeben.

Andere Signaturkarten

Diese Anwendung unterstützt auch Signaturkarten, mit der eine fortgeschrittene Signatur erzeugt werden kann. Die Liste ist der Tabelle andere unterstützte Signaturkarten (Tabelle 2c) zu entnehmen.

Tabelle 2c: Andere unterstützte Signaturkarten

Vertrauensdiensteanbieter (BNetzA Gütezeichen)	Handelsname der Signaturkarte	Schlüsselverwendung	Name der SEE	Bemerkungen
Bundesnotarkammer, Zertifizierungsstelle (Z0003)	beA-Karte Basis	Authentisierung Verschlüsselung	Signaturerstellungseinheit STARCOS 3.5 ID ECC C1	SRC.00013.TE.10.2012
Bundesnotarkammer, Zertifizierungsstelle (Z0003)	beA-Karte Mitarbeiter	Authentisierung Verschlüsselung	Java Card Open Platform (JCOP)	-
Deutschland-Online Infrastruktur (DOI) CA 1)	Signaturkarte der TeleSec ECC-Signaturkarte (SignatureCard 2.0) 2)	Authentisierung Fortgeschrittene Signatur	Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 2.0 Release 1/SLE78CLX1440P	SRC.00016.TE.11.2012
Europäisches Patentamt – European Patent Office (EPO)	Online Services Smart Card Epoline	Fortgeschrittene Signatur	-	-
Landeshauptstadt Hannover (LHH) 1)	TeleSec ECC-Signaturkarte (SignatureCard 2.0) mit DOI-Zertifikat	Authentisierung Verschlüsselung Fortgeschrittene Signatur	Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 2.0 Release 1/SLE78CLX1440P	SRC.00016.TE.11.2012
VR Bank	VR-BankCard VR-NetworldCard	Authentisierung Verschlüsselung Fortgeschrittene Signatur	-	-

1) Die Signaturkarte wird nur an Mitarbeiter der Behörde ausgegeben.
2) Kein Signieren von XML-Daten möglich

PIN-Management der unterstützten Signaturkarten

Diese Anwendung unterstützt technisch die Eingabe einer 6 bis 12-stelligen numerischen PIN auf dem Chipkartenleser. Abweichend davon kann es technisch bedingte

Einschränkungen geben. Im Anwendungsfall ist stets die gemeinsame Schnittmenge der unterstützten PIN-Längen von Signaturkarte, Chipkartenleser und dieser Anwendung maßgeblich. Beispiel:

Komponente	unterstützte PIN-Länge
diese Anwendung	6 bis 12-stellig
Ihre Signaturkarte (Signatur-PIN)	6 bis 10-stellig
Ihr Chipkartenleser für QES	4 bis 16-stellig
gemeinsame Schnittmenge	**6 bis 10-stellig**

Wichtig: Bei einer Signaturkarte kann die unterstützte PIN-Länge je nach Funktion der PIN (z.B. Signatur-PIN, Entschlüsselungs-PIN, Authentisierungs-PIN) unterschiedlich sein. Bitte informieren Sie sich anhand der Dokumentation Ihrer Signaturkarte und Ihres Chipkartenleser. Oder fragen Sie den Herausgeber Ihrer Signaturkarte oder den Hersteller Ihres Chipkartenleser, welche PIN-Längen unterstützt werden. Falls Sie dies nicht beachten, besteht die Gefahr, dass Ihre Signaturkarte unbrauchbar wird.

Sollten Sie beabsichtigen, Ihre PIN zu ändern, achten Sie bitte darauf, tatsächlich nur die alte PIN einzugeben und keinesfalls eine weitere Ziffer. Sonst kann es bei einigen Signaturkarten passieren, dass die neue PIN nicht so ist, wie sie es erwarten.

Beispiel

Die richtige alte PIN ist 123456. Der Benutzer gibt aber versehentlich für die alte PIN 12345666 ein, weil die Tastatur des Chipkartenleser prellt (mechanisch ausgelöster Störeffekt, der bei Betätigung des Tastaturknopfs kurzzeitig ein mehrfaches Schließen und Öffnen des Kontakts hervorruft). Verwendet der Benutzer für die neue PIN 654321 und wiederholt diese korrekt, so wird die PIN-Änderung bei einigen Signaturkarten trotzdem durchgeführt. Bei diesen Signaturkarten ist die PIN dann 66654321. Die Ursache für dieses Verhalten ist die Anfälligkeit eines bestimmten verwendeten PIN-Verfahrens im Zusammenhang mit der für diesen Fall unzureichenden Spezifikation ISO 7816-4. Für die PIN-Änderung kann es daher sicherer sein, die PC-Tastatur zu verwenden.