Governikus KG

Governikus Communicator

Unterstützte Betriebssysteme – Chipkartenlesegeräte - Signaturkarten

Governikus Communicator, Release 3.6.4

Karten-Leser-Ansteuerung (MCard) Version 1.25.0.2 vom 14.09.2016

Dokumentenversion: 3.6.4_0

Inhaltsverzeichnis

1 Einleitung

Mit dem Governikus Communicator können Dokumente qualifiziert elektronisch signiert werden. Dafür werden eine geeignete Signaturkarte und ein geeignetes Chipkartenlesegerät benötigt. Es können fast alle

- Chipkartenlesegeräte verwendet werden, die in Deutschland für die Erzeugung einer qualifizierten elektronischen Signatur (QES) zugelassen sind und
- Signaturkarten verwendet werden, die durch deutsche Zertifizierungsdiensteanbieter (ZDA) herausgegeben werden und mit denen man eine QES erzeugen kann.

Im Folgenden sind die unterstützten Chipkartenlesegeräte, die unterstützten Signaturkarten sowie die unterstützten Kombinationen von Betriebssystem, Chipkartenlesegerät und Signaturkarten aufgeführt. Diese Unterstützung wird durch eine Komponente der Governikus KG erbracht, die Kartenansteuerung ("MCard").

1.1 Aktuelle Hinweise

Bugfixing für Nutzung TeleSec-Signaturkarte

Das Fehlerhandling wurde für die Nutzung von Kartenleser der Sicherheitsklasse 1 und RFID verbessert.

Unterstützung Signaturkarte beA-Signatur

Die Signaturkarte beA-Signatur, die durch die Bundesnotarkammer im Auftrag der Bundesrechtsanwaltskammer herausgegeben wird und auf dem Kartenbetriebssystem STARCOS 3.5 basiert, wird für die Erzeugung einer qualifizierten Signatur (QES) sowie für die Schlüsselverwendung Authentisierung und Ver-/Entschlüsselung unterstützt. Hiervon betroffen ist auch die Signaturkarte beA-Basis mit nachträglich aufgetragenen Signaturzertifikat (QES).

Unterstützung beA-Karte Mitarbeiter

Die beA-Karte Mitarbeiter, die durch die Bundesnotarkammer im Auftrag der Bundesrechtsanwaltskammer herausgegeben wird und auf dem Kartenbetriebssystem Java Card Open Plattform (JCOP) basiert, wird für die Schlüsselverwendung Authentisierung sowie Ver-/Entschlüsselung unterstützt.

Multisignaturkarte der Bundesagentur für Arbeit (BA)

Die Multisignaturkarte der Bundesagentur für Arbeit (BA) wird in der MCard für die Erzeugung von Stapelsignaturen, die über einen geeigneten Client erzeugt werden können, unterstützt.

Einsatzumgebung Terminalserver

Mit dieser MCard-Version wird der Terminalserver Citrix XenApp 7.6 nur in Kombination mit Windows Server 2008 R2 SP1 und ausgewählten Chipkartenlesern sowie der Signaturkarte

der Bundesnotarkammer unterstützt (Tabelle 5b). Die Unterstützung der Einsatzumgebung unter Windows Server 2012 bleibt weiterhin erhalten (Tabelle 5a).

1.2 Hinweis zu Änderungen getesteter Produkte

Alle in diesem Dokument gelisteten Karten und Kartenleser wurden durch die Governikus GmbH & Co. KG funktional positiv getestet. Es kann dennoch nicht ausgeschlossen werden, dass einzelne Hersteller technisch veränderte Produkte unter gleichem Produktnamen in den Verkehr bringen. Dies kann aufgrund der technischen Änderung zu funktionalen Einschränkungen und Fehlern bis hin zur mangelnden Nutzbarkeit des Produkte führen kann. Die Governikus GmbH & Co. KG kann für derartige Funktionseinschränkungen, Fehler und dadurch verursachte Schadensverläufe nicht verantwortlich gemacht werden.

1.3 Notwendige Schutzvorkehrungen für diese Anwendung

Diese Anwendung unterliegt, wird sie für die Erzeugung oder Prüfung von QES verwendet, als Signaturanbringungskomponente (SAK) den Anforderungen des deutschen Signaturgesetzes. Potenziellen Bedrohungen muss dann durch einen unterschiedlichen "Mix" von Sicherheitsvorkehrungen in der SAK selbst und durch die Einsatzumgebung begegnet werden. Diese organisatorischen und technischen Maßnahmen sollen sicherstellen, dass den Ergebnissen der Signaturanwendungskomponente auch tatsächlich vertraut werden kann. Damit wird das komplette System, auf dem die SAK ausgeführt wird, vertrauenswürdig. Diese Anwendung ist für die Einsatzumgebung "Geschützter Einsatzbereich" entwickelt worden. Das ist typischerweise ein Einzelplatz-PC, der privat oder in Büros im täglichen Einsatz ist. Neben der technischen Absicherung gegen Bedrohungen in der Anwendung selbst (siehe dazu die bei der Bundesnetzagentur veröffentlichte Herstellererklärung), hat der Anwender für diese Einsatzumgebung noch zusätzliche Sicherheitsvorkehrungen zu treffen:

- Wenn ein Internetzugang besteht, ist die Verwendung einer Firewall notwendig, um einen entfernten Zugriff auszuschließen.
- Um Trojaner und Viren weitestgehend ausschließen zu können, ist die Installation eines aktuellen Anti-Virenprogramms (automatisches Update möglichst aktiviert) erforderlich. Dieses gilt auch für das Einspielen von Daten über Datenträger.
- Grundsätzlich darf nur vertrauenswürdige Software installiert und verwendet werden. Das gilt besonders für das Betriebssystem. Es muss sichergestellt werden, dass das Betriebssystem und das Java Runtime Environment (JRE) bezüglich der Sicherheitspatches und Updates auf dem aktuellen Stand ist (Windows: automatisches Update ist zu aktivieren, etwaige Service Packs müssen installiert sein).
- Ebenfalls ist dafür Sorge zu tragen, dass niemand einen manuellen, unbefugten Zugriff auf das System erlangen kann. Dies kann z. B. durch Aufstellung in einem abschließbaren Raum geschehen. Außerdem ist immer die Bildschirm-Sperr-Funktion des Betriebssystems zu aktivieren. Wird das System von mehreren Personen genutzt, ist für jeden Nutzer ein eigenes Benutzerkonto anzulegen.
- Es ist zu kontrollieren, dass der verwendete Chipkartenleser nicht böswillig manipuliert wurde, um Daten (z. B. PIN, Hashwerte etc.) auszuforschen oder zu verändern. Das Ausforschen der PIN auf dem PC oder Notebook kann nur dann mit Sicherheit ausgeschlossen werden, wenn ein Chipkartenleser mit sicherer PIN-Eingabe eingesetzt wird.
- Zum Schutz vor Fehlern bei der Nutzung dieser Anwendung ist zu beachten:

- Soll eine Anzeige der zu signierenden Daten erfolgen, ist eine geeignete Anwendung zu nutzen, d. h. eine Anwendung, die Dateien des entsprechenden Dateityps öffnen und die zu signierenden oder signierten Daten zuverlässig darstellen kann.
- Es ist eine vertrauenswürdige Eingabe der PIN sicherzustellen. Das bedeutet: die Eingabe der Signatur-PIN darf weder beobachtet noch die PIN anderen Personen bekannt gemacht werden. Die PIN ist zu ändern, wenn der Verdacht oder die Gewissheit besteht, die PIN könnte nicht mehr geheim sein.
- Nur beim Betrieb mit einem bestätigten Chipkartenlesegerät mit PIN-Pad ist sichergestellt, dass die PIN nur zur Signaturkarte übertragen wird. Das bedeutet, dass die Signatur-PIN nur am PIN-Pad des Chipkartenlesers eingegeben werden darf.

Die Hinweise des ZDA zum Umgang mit der persönlichen, geheimen Signatur-PIN sind ebenso zu beachten.

2 Unterstützte Betriebssysteme und JRE

Diese Anwendung ist auf vielen Client-Betriebssystemen lauffähig. Die Liste mit den unterstützten Betriebssystemen ist der Tabelle „unterstützte Betriebssysteme“ (Tabelle 1) zu entnehmen.

Betriebssysteme werden in der Regel solange unterstützt, wie der Hersteller dafür Sicherheitspatches herausgibt. Erreicht ein Betriebssystem seinen „End-of-Life-Zeitpunkt“ (EOL), erfolgt eine Abkündigung in dieser Tabelle. Das dort angegebene Datum bedeutet, dass eine nach diesem Datum bereitgestellte neue Version dieser Anwendung das angegebene Betriebssystem nicht mehr unterstützen wird.

Spätestens ab dem EOL sollte ein Betriebssystem nicht mehr verwendet werden, da dann keine Sicherheitspatches mehr bereitgestellt werden. Dieser Umstand kann die für eine SAK geforderte hohe Sicherheit gegen potenzielle Bedrohungen beeinträchtigen.

Diese Anwendung ist auf den in der Tabelle „unterstützte Betriebssysteme“ aufgeführten JRE-Versionen und angegebenen Updates (ORACLE Java Standard Edition Runtime Environment) lauffähig. Dieses sind in der Regel immer die aktuelle JRE-Version und die Vorversion. Über die Freigabe einer neuen Version oder aktuellerer Updates bereits unterstützter Versionen wird gesondert informiert.

JRE-Versionen werden in der Regel solange unterstützt, wie der Hersteller dafür Sicherheitspatches herausgibt. Erreicht ein JRE seinen „End-of-Life-Zeitpunkt“ (EOL), erfolgt eine Abkündigung in dieser Tabelle. Das dort angegebene Datum bedeutet, dass eine nach diesem Datum bereitgestellte neue Version dieser Anwendung das angegebene JRE nicht mehr unterstützen wird.

Unterstützte Kombinationen: Betriebssystem - Chipkartenlesegerät - Signaturkarte

Bitte beachten Sie bei der Auswahl des Betriebssystems: Die Funktionsfähigkeit der unterstützten Chipkartenlesegeräte (siehe Tabellen 3a bis 3c) mit den in der Tabelle „unterstützte Betriebssysteme“ (Tabelle 1) aufgeführten Betriebssystemen wurde getestet. Technisch bedingt kann es in seltenen Fällen allerdings zu Ausnahmen kommen, die nicht im Verantwortungsbereich dieser Anwendung liegen. Prüfen Sie daher bitte, ob Ihr Chipkartenlesegerät mit Ihrer Signaturkarte in Kombination mit Ihrem Betriebssystem unterstützt wird. Entsprechende Listen finden Sie in den Tabellen „Unterstützte Kombinationen Betriebssystem-Leser-Karten“ (Tabellen 4a bis d).

3 Unterstützte Signaturkarten

Signaturkarten für eine qualifizierte elektronische Signatur (QES)

Mit dieser Anwendung können Sie die meisten von deutschen Zertifizierungsdiensteanbietern herausgegebenen qualifizierten Signaturkarten verwenden. Die Listen mit den unterstützten Signaturkarten für eine qualifizierte elektronische Signatur sind den Tabellen „Unterstützte Signaturkarten deutscher Zertifizierungsdiensteanbieter für eine 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.

Bei Signaturkarten wird zwischen Einzel-, Stapel- und Multisignaturkarten unterschieden. Diese Anwendung unterstützt alle drei Kartenvarianten und erlaubt - unabhängig von der Kartenvariante - nach der PIN-Eingabe die Erzeugung von genau einer QES.

Qualifizierte Signaturkarten basieren auf sogenannten sicheren Signaturerstellungseinheiten (SSEE). Für eine Signaturkarte werden von einem ZDA manchmal unterschiedliche SSEE verwendet. Es kann auch vorkommen, dass eine SSEE von mehreren ZDA genutzt wird. Unterstützt werden nur die in den Tabellen „Unterstützte Signaturkarten deutscher Zertifizierungsdiensteanbieter für eine QES“ (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 ZDA herausgegeben und zugestellt wurden. Es gibt eine Ausnahme: Wird von einem ZDA eine dezentrale Personalisierung einer Original-Signaturkarte angeboten, also das Nachladen von qualifizierten Zertifikaten, wird die Signaturkarte weiterhin unterstützt. Dieses ist zum Beispiel beim neuen Personalausweis möglich. Andere Modifizierungen der Signaturkarte, wie z.B. das lokale Aufspielen eigenen Schlüsselmaterials, könnten die Signaturkarte für diese Anwendung unbrauchbar machen oder sogar zerstören.

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.

Unterstützte Kombinationen: Betriebssystem - Chipkartenlesegerät - Signaturkarte

Die Funktionsfähigkeit der in den Tabellen aufgeführten Signaturkarten mit dieser Anwendung wurde für die in den Tabellen „Unterstützte Chipkartenlesegeräte“ aufgeführten Chipkartenlesegeräte getestet. Technisch bedingt kann es in seltenen Fällen allerdings zu Ausnahmen kommen, die nicht im Verantwortungsbereich dieser Anwendung liegen. Prüfen Sie daher bitte, ob Ihr Chipkartenlesegerät mit Ihrer Signaturkarte in Kombination mit Ihrem Betriebssystem unterstützt wird. Entsprechende Listen finden Sie in den Tabellen „Unterstützte Kombinationen Betriebssystem-Leser-Karten“ (Tabellen 4a bis b).

PIN-Management der unterstützten Signaturkarten

Diese Anwendung unterstützt technisch die Eingabe einer 6 bis 12-stelligen numerischen PIN auf dem Chipkartenlesegerät. Abweichend davon kann es technisch bedingte Einschränkungen geben. Im Anwendungsfall ist stets die gemeinsame Schnittmenge der unterstützten PIN-Längen von Signaturkarte, Chipkartenlesegerät und dieser Anwendung maßgeblich.

Beispiel:

Komponente	*unterstützte PIN-Länge*
diese Anwendung	6 bis 12-stellig
Ihre Signaturkarte (Signatur-PIN)	6 bis 10-stellig
Ihr Chipkartenlesegerät 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 Chipkartenlesegeräts. Oder fragen Sie den ZDA Ihrer Signaturkarte oder den Hersteller Ihres Chipkartenlesegeräts, 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 123456**66** ein, weil die Tastatur des Chipkartenlesegeräts 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 **66**654321. 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.

4 Unterstützte Chipkartenlesegeräte

Mit dieser Anwendung können fast alle Chipkartenlesegeräte mit Tastatur (PIN-Pad) und ausgewählte Chipkartenlesegeräte ohne PIN-Pad verwendet werden, die in Deutschland für die Erzeugung einer QES zugelassen sind.

Für eine QES zugelassene Chipkartenlesegeräte

Alle für die Erzeugung einer QES zugelassenen Chipkartenlesegeräte werden über ihre eigene USB-Schnittstelle an den PC angeschlossen. Die Verbindung vom PC zum Chipkartenlesegerät wird über einen PC/SC-Treiber hergestellt, der zu installieren ist. Bitte informieren Sie sich beim Hersteller des Chipkartenlesegeräts, wie der Treiber zu installieren ist.

Die Listen mit den für eine QES geeigneten Chipkartenlesegeräten sind den Tabellen „unterstützte Chipkartenlesegeräte“ (Tabellen 3a und 3b) zu entnehmen. Für eine QES dürfen nur die dort aufgeführten Chipkartenlesegeräte verwendet werden. Es handelt sich ausschließlich um Geräte mit einer zum Zeitpunkt des Inverkehrbringens dieser Anwendung gültigen Bestätigung oder Herstellererklärung. Diese wurde von der zuständigen Aufsichtsbehörde Bundesnetzagentur (BNetzA) veröffentlicht.

Bitte beachten Sie, dass Bestätigungen oder Herstellererklärungen für Chipkartenlesegeräte zeitlich befristet sind. Bei Sicherheitsmängeln können Bestätigungen oder Herstellererklärungen von der Bundesnetzagentur für ungültig erklärt oder widerrufen werden. Dieses passiert allerdings nur äußerst selten. Trotzdem sollten Sie sich informieren, ob Ihr Chipkartenlesegerät immer noch den Anforderungen genügt. Aktuelle Informationen hierzu finden Sie in den Übersichten bei der Bundesnetzagentur.

Es kann darüber hinaus keine Gewährleistung dafür übernommen werden, dass

- die unterstützten Chipkartenlesegeräte auch mit älteren Treiberversionen oder anderen als den aufgeführten Betriebssystemen funktionieren und
- andere als die explizit aufgeführten Chipkartenlesegeräte verwendet werden können.

Chipkartenlesegeräte nicht für QES geeignet

Diese Anwendung unterstützt auch Chipkartenlesegeräte, die keine sichere PIN-Eingabe erlauben (HBCI-Klasse 1) und daher nicht für eine QES verwendet werden dürfen. Es handelt sich ausschließlich um Geräte mit USB-Schnittstelle, die über einen PC/SC-Treiber angesprochen werden. Die Liste der unterstützten Chipkartenlesegeräte ohne PIN-Pad ist der Tabelle „Unterstützte Chipkartenlesegeräte ohne PIN-Pad und für eine QES in Deutschland nicht geeignet“ (Tabelle 3c) zu entnehmen.

Neben diesen Geräten können auch viele weitere Chipkartenlesegeräte mit USB-Schnittstelle ohne PIN-Pad oder interne Chipkartenlesegeräte in Notebooks verwendet werden. Natürlich muss der Hersteller für das verwendete Betriebssystem einen Treiber zur Verfügung stellen. Eine Gewährleistung für die Funktionsfähigkeit kann gleichwohl nicht übernommen werden. Für eine QES dürfen diese Geräte selbstverständlich nicht verwendet werden.

Unterstützte Kombinationen: Betriebssystem - Chipkartenlesegerät - Signaturkarte

Die Funktionsfähigkeit der aufgeführten Chipkartenlesegeräte mit dieser Anwendung wurde für die in der Tabelle „unterstützte Betriebssysteme“ aufgeführten Betriebssysteme mit den bei den Herstellern der Chipkartenlesegeräte verfügbaren aktuellen PC/SC-Treibern getestet. Technisch bedingt kann es in seltenen Fällen allerdings zu Ausnahmen kommen, die nicht im Verantwortungsbereich dieser Anwendung liegen. Prüfen Sie daher bitte, ob Ihr Chipkartenlesegerät mit Ihrer Signaturkarte in Kombination mit Ihrem Betriebssystem unterstützt wird. Entsprechende Listen finden Sie in den Tabellen „Unterstützte Kombinationen Betriebssystem-Leser-Karten“ (Tabellen 4a bis b).

5 Unterstützte Kombinationen: Betriebssystem - Chipkartenlesegerät - Signaturkarte

In der Regel werden alle Kombinationen der in den Listen benannten Betriebssysteme, Chipkartenlesegeräte und Signaturkarten unterstützt. Aus technischen Gründen kann es in Ausnahmefällen allerdings vorkommen, dass die Signaturanbringung, Ver- und Entschlüsselung oder Authentisierung mit einer elektronischen Signaturkarte/SSEE in Kombination mit einem bestimmten Chipkartenlesegerät und einem bestimmten Betriebssystem nur eingeschränkt oder nicht funktioniert. Dieses kann unterschiedliche Gründe haben: Auf der Signaturkarte ist kein Verschlüsselungszertifikat vorhanden. Für eine neue Signaturkarte wurde noch kein geeigneter PC/SC-Treiber durch den Hersteller des Chipkartenlesegeräts für ein bestimmtes Betriebssystem bereitgestellt. Oder es liegt eine technische Inkompatibilität von Chipkartenlesegerät und Signaturkarte vor.

Prüfen Sie daher bitte, ob Ihre Signaturkarte in Kombination mit Ihrem Chipartenlesegerät und Ihrem Betriebssystem unterstützt wird. Entsprechende Listen finden Sie in den Tabellen „Unterstützte Kombinationen Betriebssystem-Leser-Karten“ (Tabellen 4a bis b).

6 Tabellen

Tabelle 1: Unterstützte Betriebssysteme und JRE

Betriebssysteme	**JRE Versionen und Updates**	**Abkündigung**
Windows 7 Convenience Update (SP2) – Home Basic, Home Premium, Professional, Ultimate, Enterprise – jeweils 32 Bit und 64 Bit	8 Update 101 (32 Bit)	
Windows 8 und 8.1: – Standard, Professional, Enterprise – 32 Bit	8 Update 101 (32 Bit)	
Windows 8 und 8.1: – Standard, Professional, Enterprise – 64 Bit	8 Update 101 (64 Bit)	
Windows 10 (Build 1607): – Professional, Enterprise – 64 Bit	8 Update 101 (64 Bit)	
openSUSE 13.2 64 Bit	8 Update 101 (64 Bit)	
Ubuntu 14.04 LTS 64 Bit	8 Update 101 (64 Bit)	

Tabelle 2a: Unterstützte Signaturkarten deutscher Zertifizierungsdiensteanbieter für eine QES mit Anbieterakkreditierung

Zertifizierungs-diensteanbieter (akkreditiert mit Gütezeichen BNetzA)	**Handelsname der Signaturkarte**	**Schlüsselver-wendung**	**Name der SSEE in der Bestätigungsur-kunde**	**Registrierungsnr. der Bestä-tigungsurkunde der SSEE**
Produktzentrum TeleSec der Deut-schen Telekom AG (Z0001)	TeleSec PKS-ECC-Signaturkarte (SignatureCard 2.0) 5)	Authentisierung Verschlüsselung 6) 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) 5)			
Bundesnotarkam-mer, Zertifizie-rungsstelle (Z0003)	beA-Signatur 7)	Authentisierung Verschlüsselung QES	Signaturerstellungseinheit STARCOS 3.5 ID ECC C1	SRC.00013.TE.10.2012
Bundesnotarkam-mer, Zertifizie-rungsstelle (Z0003)	Bundesnotarkammer, Zertifizierungs-stelle qualifizierte elektronische Sig-natur 2)	Authentisierung Verschlüsselung QES	Signaturerstellungseinheit STARCOS 3.5 ID ECC C1	SRC.00013.TE.10.2012
D-Trust GmbH (Z0017) 3)	D-TRUST Card 3.0	Authentisierung Verschlüsselung QES	Sichere Signaturerstellungseinheit STARCOS 3.4 Health QES C1 Bestätigung wurde erweitert auf Nach-folgeversion 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) 3)			
	D-TRUST Card 3.0 Multicard 1)			
	Neuer Personalausweis (nPA), wenn mit einem QES-Zertifikat der D-Trust personalisiert 4)	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

Zertifizierungs-diensteanbieter (akkreditiert mit Gütezeichen BNetzA)	Handelsname der Signaturkarte	Schlüsselver-wendung	Name der SSEE in der Bestätigungsur-kunde	Registrierungsnr. der Bestä-tigungsurkunde der SSEE
DATEV eG Zertifi-zierungsstelle (Z0004)	zertifizierte Signaturkarte für Berufs-träger der DATEV	Authentisierung Verschlüsselung QES	Sichere Signaturerstellungseinheit STARCOS 3.4 Health QES C1 Bestätigung wurde erweitert auf Nach-folgeversion 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
S-Trust, Deutscher Sparkassen Verlag GmbH (Z0035)	S-TRUST Card, SparkassenCard oder kontounabhängige GeldKarte	Authentisierung Verschlüsselung QES	Signaturerstellungseinheit ZKA Ban-king Signature Card, Version 6.6 der Giesecke & Devrient GmbH	TUVIT.93130.TU.05.2006 Nachtrag 1 vom 28.08.2006 Nachtrag 2 vom 18.10.2006 Nachtrag 3 vom 28.12.2010
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) kartenab-hängig die Erzeugung von bis zu 100 QES im Batchverfahren möglich.

3) Der ZDA gibt Signaturkarten nur im Rahmen von Projekten heraus.

4) Der mit einem qualifizierten Zertifikat personalisierte nPA kann technisch bedingt nicht für eine fortgeschrittene Signatur, für Ver- und Entschlüsse-lung sowie für zertifikatsbasierte Authentisierung verwendet werden, da das notwendige Schlüsselmaterial nicht vorhanden ist.

5) Kein Signieren von XML-Daten möglich.

6) Ver-/ und Entschlüsselung nur im CMS-Format möglich.

7) Gilt auch für Signaturkarte beA-Basis mit dem nachträglich aufgeladenen QES-Zertifikat

Tabelle 2b: Unterstützte Signaturkarten deutscher Zertifizierungsdiensteanbieter geeignet für eine QES

Zertifizierungs-diensteanbieter (angezeigt)	Handelsname der Signaturkarte	Schlüsselver-wendung	Name der SSEE in der Bestäti-gungsurkunde	Registrierungsnr. der Bestä-tigungsurkunde der SSEE
D-Trust GmbH	D-TRUST Card 3.0	Authentisierung Verschlüsse-lung QES	Sichere Signaturerstellungseinheit STARCOS 3.4 Health QES C1 Bestätigung wurde erweitert auf Nach-folgeversion 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) 3)			
	D-TRUST Card 3.0 Multicard 1)			
S-Trust, Deutscher Sparkassen Verlag GmbH	S-TRUST Card	Authentisierung Verschlüsse-lung QES	SEE ZKA Banking Signature Card, Version 6.6 der Giesecke & Devrient GmbH	TUVIT.93130.TU.05.2006 Nachtrag 1 vom 28.08.2006 Nachtrag 2 vom 18.10.2006 Nachtrag 3 vom 27.12.2010
		Authentisierung Verschlüsse-lung QES	SEE ZKA-Signaturkarte, Version 6.32 der Gemalto GmbH	TUVIT.93184.TU11.2010 Nachtrag 1 vom 19.05.2011 Nachtrag 2 vom 17.06.2013
		Authentisierung Verschlüsse-lung QES	Signaturerstellungseinheit ZKA Ban-king Signature Card, Version 7.1.2 der Giesecke & Devrient GmbH	TUVIT.93166.TU.06.2008 Nachtrag 1 vom 15.09.2009 Nachtrag 2 vom 28.12.2010
	S-TRUST Multisignaturkarte 1)	Authentisierung Verschlüsse-lung QES	Signaturerstellungseinheit ZKA-Signaturkarte, Version 6.32 M	TUVIT.93176.TU.05.2011
Deutsche Renten-versicherung Bund (DRV) 4)	Signaturkarte der Deutschen Renten-versicherung Bund (Einzelsignatur)	Verschlüsse-lung QES	Sichere Signaturerstellungseinheit CardOS V5.0 with Application for QES, V1.0	BSI.02136.TE.07.2013
	Multisignaturkarte der Deutschen Ren-tenversicherung Bund 1)	QES		

Zertifizierungs-diensteanbieter (angezeigt)	Handelsname der Signaturkarte	Schlüsselver-wendung	Name der SSEE in der Bestäti-gungsurkunde	Registrierungsnr. der Bestä-tigungsurkunde der SSEE
Bundesagentur für Arbeit 4)	Signaturkarte der Bundesagentur für Arbeit (BA)	Authentisierung Verschlüsse-lung 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) karten-abhängig die Erzeugung von bis zu 100 QES im Batchverfahren möglich.

3) die Signaturkarte wird nur im Rahmen von Projekten herausgegeben

4) Die Signaturkarte wird nur an Mitarbeiter der jeweiligen Behörde ausgegeben

Tabelle 2c: andere unterstützte Signaturkarten

Trustcenter	Handelsname der Signaturkarte	Schlüsselver-wendung	Name der SEE	Bemerkungen
A-Trust GmbH	A-TRUST premium	QES	Betriebssystem des Kartenchips: ACOS EMV-A04V1	Österreichische Signaturkarte geeig-net zur Erzeugung einer QES in Deutschland. Registrierungsnummer der Bestätigungsurkunde: T-Systems.02169.TE.10.2009 Nachtrag 1 vom 18.12.2008 Nachtrag 2 vom 19.05.2009 Nachtrag 3 vom 11.07.2012
Bundesnotarkam-mer, Zertifizie-rungsstelle (Z0003)	beA-Karte Basis	Authentisierung Verschlüsse-lung	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 T-Systems PKS-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	--	--
QuoVadis Trustlink Schweiz AG	QuoVadis Multisignaturkarte mit Funktionszertifikat ElDI-V/GeBüV	Fortgeschrittene Signatur	Siemens CardOS 4.4	BSI.02130.TE.07.2011

1) Die Signaturkarte wird nur an Mitarbeiter der jeweiligen Behörde ausgegeben.

2) Kein Signieren von XML-Daten möglich

Tabelle 3a: Unterstützte Chipkartenlesegeräte mit SigG-Bestätigung

Handelsname des Geräts	**Angaben aus der veröffentlichten Bestätigung bei der BNetzA**			**PIN-Pad**	**Standard**	**Schnittstelle**	
						PC	**Karte**
CardMan 3621	OMNIKEY GmbH	SAK Chipkartenterminal der Familie CardMan Trust CM3621, Firmware-Version 6.00	BSI.02057.TE.12.2005	ja	PC/SC	USB	kontakt
CardMan 3821	OMNIKEY GmbH	SAK Chipkartenterminal der Familie CardMan Trust CM3821, Firmware-Version 6.00	BSI.02057.TE.12.2005	ja	PC/SC	USB	kontakt
Cherry Smartboard G83-6744	Cherry GmbH	Chipkartenterminal der Familie SmartBoard xx44 Firmware-Version 1.04	BSI.02048.TE.12.2004	ja	PC/SC	USB	kontakt
Cherry SmartTerminal 2000 U	Cherry GmbH	Chipkartenterminal der Familie SmartTerminal ST-2xxx, Firmware Version 6.01	BSI.02124.TE.09.2010	ja	PC/SC	USB	kontakt
cyberJack e-com	Reiner SCT Kartenlesegeräte GmbH	cyberJack e-com, Version 3.0	TUVIT.93155.TE.09.2008	ja	PC/SC	USB	kontakt
cyberJack e-com plus	Reiner SCT Kartenlesegeräte GmbH	cyberJack e-com plus, Version 3.0	TUVIT.93156.TE.09.2008	ja	PC/SC	USB	kontakt
cyberJack pinpad Version 3	Reiner SCT Kartenlesegeräte GmbH	Chipkartenleser, cyberJack pinpad, Version 3.0	TUVIT.93107.TU.11.2004	ja	PC/SC	USB	kontakt
CyberJack RFID komfort	Reiner SCT Kartenlesegeräte GmbH	cyberJack® RFID komfort Version 2.0	TUVIT.93180.TU.12.2011	ja	PC/SC	USB	kontakt, kontaktlos
CyberJack RFID standard	Reiner SCT Kartenlesegeräte GmbH	cyberJack® RFID standard Version 1.2	TUVIT.93188.TU.07.2011	ja	PC/SC	USB	kontakt, kontaktlos
cyberJack secoder	Reiner SCT Kartenlesegeräte GmbH	Chipkartenleser cyberJack secoder Version 3.0	TUVIT.93154.TE.09.2008	ja	PC/SC	USB	kontakt
Fujitsu Siemens Chipkartenleser-	Fujitsu Siemens	Chipkartenleser-Tastatur KB SCR Pro, Sachnummer S26381-K329-V2xx HOS:01,	BSI.02082.TE.01.2007	ja	PC/SC	USB	kontakt

Handelsname des	**Angaben aus der veröffentlichten Bestätigung bei der BNetzA**			**PIN**	**Stand-**	**Schnittstelle**	
Tastatur KB SCR Pro		Firmware Version 1.06					
Fujitsu Siemens Chipkartenleser-Tastatur Smartcase KB SCR eSIG	Fujitsu Siemens	SmartCase KB SCR eSIG (S26381-K529-Vxxx) Hardware Version HOS:01, Firmware-Version 1.20, Firmware-Version 1.21 gemäß Nachtrag vom 04.02.2011	BSI.02107.TE.03.2010 Nachtrag zur Bestätigung BSI.02107. TE.03.2010 vom 04.02.2011	ja	PC/SC	USB	kontakt
Kobil KAAN Advanced	Kobil Systems GmbH	Chipkartenterminal KAAN Advanced, Firmware-Version 1.02, Hardware Version K104R3, Firmware 1.19 gemäß Nachtrag zur Bestätigung	BSI.02050.TE.12.2006 Nachtrag zur Bestätigung vom 07.04. 2008: T-Systems. 02207.TU.04.2008	ja	PC/SC	USB	kontakt
SPR 332 usb (Chipdrive pinpad pro)	IDENTIVE GmbH (Nachfolger der SCM Microsystems GmbH)	Chipkartenleser SPR332, Firmware Version 6.01	BSI.02117.TE.02.2010	ja	PC/SC	USB	kontakt

Tabelle 3b: Unterstützte Chipkartenlesegeräte mit Herstellererklärung

Handelsname des Geräts	**Angaben aus der veröffentlichten Herstellererklärung bei der BNetzA**		**PIN-Pad**	**Standard**	**Schnittstelle**	
					PC	**Karte**
CARD STAR/ medic Version 2	CCV Deutschland GmbH	CARD STAR /medic2, Version M1.50G Herstellererklärung vom 01.09.2010, Version M1.53G gemäß 1. Nachtrag vom 15.04.2011	ja	CT-API	USB	kontakt
eHealth 8751 LAN	Omnikey	eHealth-BCS-Kartenterminal Omnikey eHealth 8751 LAN Version 2.06, FW 1.32 Herstellererklärung vom 29.07.2011	ja	CT-API	USB	kontakt
eHealth BCS 200	IDENTIVE GmbH (Nachfolger der SCM Microsystems GmbH)	eHealth Kartenterminal eHealth 200 BCS Version 02.00 Herstellererklärung vom 19.03.2010, 1. Nachtrag zur Herstellererklärung vom 20.01.2011	ja	PC/SC CT-API	USB	kontakt
GT900 BCS	german telematics	Chipkartenterminal eHealth GT900 BCS mit der Firmware-Version: 1.0.10 und der Hardwareversion: 2.0 / 2.0 SI / 2.0 SW, Herstellererklärung vom 07.07.2010	ja	CT-API	USB	kontakt
medCompact eHealth	Verifone (ehemals Hypercom)	medCompact eHealth BCS Version 02.00 Herstellererklärung vom 19.03.2010, Nachtrag 1 zur Herstellererklärung vom 20.01.2011	ja	CT-API	USB	kontakt
ORGA 6041 Version 2.07	Sagem Monetel GmbH	ORGA 6041 Version 2.07 Herstellererklärung vom 08.09.2010	ja	PC/SC CT-API	USB	kontakt

Tabelle 3c: Unterstützte Chipkartenlesegeräte ohne PIN-Pad und für eine QES in Deutschland nicht geeignet

Handelsname des Geräts	**Hersteller**	**PIN-Pad**	**Stand-ard**	**Schnittstelle**	
				PC	**Karte**
CardMan 3121	Omnikey	nein	PC/SC	USB	kontakt
SCM SDI011 RFID	IDENTIVE GmbH (Nachfolger der SCM Microsystems GmbH)	nein	PC/SC	USB	kontakt, kontaktlos 1)
Cherry ST-1044U	ZF Electronics GmbH	nein	PC/SC	USB	kontakt
Cherry ST-1275	ZF Electronics GmbH	nein	PC/SC	USB	kontakt, kontaktlos 1)
CLOUD 4700 F Dual Interface USB Desktop Reader	IDENTIVE GmbH (Nachfolger der SCM Microsystems GmbH)	nein	PC/SC	USB	kontakt, kontaktlos 1)
CLOUD 2700 F Contact Smart Card Reader	IDENTIVE GmbH (Nachfolger der SCM Microsystems GmbH)	nein	PC/SC	USB	kontakt

1) nicht unterstützt

Tabelle 4a: Unterstützte Kombinationen Windows Betriebssysteme 7 SP1, 8, 8.1, 10 - Chipkartenlesegerät - Signaturkarte

Handelsnamen der Chipkartenleser mit SigG-Bestätigung / Herstellererklärung	Unterstützte Windows-Systeme: 7 - 8 - 10		Handelsnamen der Signaturkarten														
	Firmware	Treiber PC/SC	TeleSec PKS ECC	Bundesnotar-kammer	beA-Signatur	beA-Basis beA-Mitarbeiter	DATEV	D-TRUST Card 3.0	S-Trust Card	DGN SprintCard DGN BusinesCard	Personalausweis mit QES-Funktion	DRV Bund	BA-Signaturkarte	A-Trust Premium (QES)	DOI	EPO-Karte	VR Bank
Cherry® Smartboard G83-6744	01.04.00.00	1.2.24.27	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
Cherry® SmartTerminal 2000 U	6.01.00.00	4.53.0.0	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
cyberJack® e-com/ e-com plus	3.0.80/3.0.8	bc_7_2_5 (6.1.0.0)	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
cyberJack® pinpad Version 3/ secoder	3.0.12/3.0.19	bc_7_2_5 (6.1.0.0)	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
cyberJack® RFID standard kontakt	1.2.23	bc_7_2_5 (6.1.0.0)	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
cyberJack® RFID komfort kontakt	2.0.11	bc_7_2_5 (6.1.0.0)	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
cyberJack® RFID standard kontaktlos	1.2.23	bc_7_2_5 (6.1.0.0)	✓1)	-	-	-	-	-	-	-	✓2)	-	-	-	-	-	-
cyberJack® RFID komfort kontaktlos	2.0.11	bc_7_2_5 (6.1.0.0)	✓1)	-	-	-	-	-	-	-	✓2)	-	-	-	-	-	-
Fujitsu Siemens KB SCR eSIG	1.20	1.9.0.0	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
Fujitsu Siemens KB SCR Pro	1.06	1.2.24.0	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
Kobil KAAN Advanced	1.19	2013.1.24.1	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
Omnikey CardMan 3621, 3821	6.00	1.2.24.27	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
SPR 332 usb (Chipdrive pinpad pro)	6.01	4.53.0.0	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
ORGA 6041 Version 2.07	2.07	2.0.0.6	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
eHealth BCS 200	2.01	1.2.0.0	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
CARD STAR/ medic Version 2	M1.53G	WinUSB 2.76 und CTAPI 2.70, ct_api_usb.dll 4)	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
medCompact eHealth	02.00	CTAPI 03.00,cthyc32.dll 4)	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
GT900 BCS	1.0.10	ctgt900.dll 4) 6)	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
Omnikey 8751 eHealth LAN	1.3.2	ct8751com.dll 4) 6)	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
In Tabelle 3c aufgeführte Geräte ohne PIN-Pad (nicht für die QES zugelassen)			✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓

1) Ver-/ und Entschlüsselung nur im CMS-Format möglich

2) nur QES

3) nur Signatur
4) nur CT-API, dll nur 32 Bit Java
5) nur Authentisierung und Verschlüsselung
6) Keine Treiber für Windows 8, 8.1 und 10 verfügbar

Tabelle 4b: Unterstützte Kombinationen OpenSUSE 13.2 (64 Bit), Ubuntu 14.04 LTS (64 Bit) - Chipkartenlesegerät – Signaturkarte

Handelsnamen der Chipkartenleser mit SigG-Bestätigung / Herstellererklärung	OpenSUSE 13.2 (64 Bit) Ubuntu 14.04 LTS (64 Bit)		Handelsnamen der Signaturkarten														
	Firmware	PCSC-lite Version 1.8.14 6)	TeleSec PKS ECC	Bundesnotar-kammer	beA-Signatur	beA- Basis beA-Mitarbeiter	DATEV	D-TRUST Card 3.0	S-Trust Card	DGN SprintCard DGN BusinessCard	Personalausweis mit QES-Funktion	DRV Bund	BA-Signaturkarte	A-Trust Premium (QES)	DOI	EPO-Karte	VR Bank
Cherry® Smartboard G83-6744	01.04.00.00	ifdokccid-lnx-4.0.5	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
Cherry® SmartTerminal 2000 U	6.01.00.00	scmccid 5.0.31	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
cyberJack® e-com/ e-com plus	3.0.80/3.0.8	ifd-cyberJack 3.99.5 SP9	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
cyberJack® pinpad Version 3/ secoder	3.0.12/3.0.19	ifd-cyberJack 3.99.5 SP9	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
cyberJack® RFID standard kontakt	1.2.23	ifd-cyberJack 3.99.5 SP9	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
cyberJack® RFID komfort kontakt	2.0.11	ifd-cyberJack 3.99.5 SP9	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
cyberJack® RFID standard kontaktlos	1.2.23	ifd-cyberJack 3.99.5 SP9	✓1)	-	-	-	-	-	-	-	✓2)	-	-	-	-	-	-
cyberJack® RFID komfort kontaktlos	2.0.11	ifd-cyberJack 3.99.5 SP9	✓1)	-	-	-	-	-	-	-	✓2)	-	-	-	-	-	-
Fujitsu Siemens KB SCR eSIG	1.20	CCID 1.4.20-4.2 6)	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
Fujitsu Siemens KB SCR Pro	1.06	ifdokccid-lnx-4.0.5	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
Kobil KAAN Advanced	1.19	CCID 1.4.20 6)	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
Omnikey CardMan 3621, 3821	6.00	ifdokccid-lnx-4.0.5	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
SPR 332 usb (Chipdrive pinpad pro)	6.01	scmccid 5.0.31	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
ORGA 6041 Version 2.07	2.07	V 1.7	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
eHealth BCS 200	2.01	V1.05	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
CARD STAR/ medic Version 2	M1.53G	WinUSB 2.76 und CTAPI 2.70, ct_api_usb.dll 4)	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
medCompact eHealth	02.00	CTAPI 03.00,cthyc32.dll 4)	✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓
GT900 BCS	1.0.10	Keine Treiber verfügbar	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Omnikey 8751 eHealth LAN	1.3.2	Keine Treiber verfügbar	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
In Tabelle 3c aufgeführte Geräte ohne PIN-Pad (nicht für die QES zugelassen)			✓1)	✓	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓1)	✓3)	✓

1) Ver-/ und Entschlüsselung nur im CMS-Format möglich

2) nur QES

3) nur Signatur
4) nur CT-API, dll nur 32 Bit Java
5) nur Authentisierung und Verschlüsselung

6) Bei generischen CCID-Treibern muss der Name des Lesers mit * angeführt werden