Administration Intelligence AG

Unterstützte Signaturkarten und Kartenlesegeräte

Version MCard 1.24.0.0 vom 11.12.2015

Dokumentenversion 1.0

Inhalt

1 Einleitung 3
1.1 Aktuelle Hinweise 3
1.2 Hinweis zu Änderungen getesteter Produkte 4
2 Notwendige Schutzvorkehrungen für diese Anwendung 5
3 Unterstützte Betriebssysteme und JRE 7
4 Unterstützte Signaturkarten 8
5 Unterstützte Chipkartenlesegeräte 11
6 Unterstützte Kombinationen: 13
Impressum 28

1 Einleitung

Mit dieser Anwendung 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.

1.1 Aktuelle Hinweise

Unterstützung beA-Karte Basis

Die beA-Karte Basis, basierend auf dem Kartenbetriebssystem STARCOS 3.5, wird für die Schlüsselverwendung Authentisierung sowie Ver-/Entschlüsselung unterstützt. Die Nachladeoption eines qualifizierten Signaturzertifikates wird durch den Kartenhersteller voraussichtlich ab Q1/2016 angeboten und wurde bislang nicht getestet. Laut Herstelleraussage wird die Karte mit QES-Zertifikat dieselben Lesegeräte unterstützen.

Die Governikus GmbH & Co. KG wird im Auftrag der Bundesrechtsanwaltskammer die Signaturkarte mit QES-Funktionalität ebenfalls testen und aller Voraussicht nach, und soweit technisch möglich, in die MCard integrieren.

Deutsche Post Signtrust und DMDA GmbH Einstellung des Betriebs

Der Zertifizierungsdiensteanbieter Deutsche Post Signtrust und DMDA GmbH hat den Betrieb eingestellt. Die Signaturkarte dieses Anbieters wird nicht mehr unterstützt. Mehr Informationen auf der Webseite des Anbieters.

TC TrustCenter GmbH Einstellung des Betriebs

Der Zertifizierungsdiensteanbieter TC-Trustcenter hat den Betrieb im qualifizierten Bereich eingestellt. Die Signaturkarte dieses Anbieters wird nicht mehr unterstützt. Mehr Informationen auf der Webseite des Anbieters.

PKS-ECC-Signaturkarte Version 2.0 der TeleSec

Bei der Nutzung der Signaturkarte mit einer Kryptographie, basierend auf elliptischen Kurven (ECC), gibt es zurzeit folgende Einschränkungen:

- Für die Nutzung im kontaktlosen Modus für die Erzeugung einer QES ist nur die Verwendung des Kartenlesegeräts „cyberJack® RFID komfort“ rechtlich (nach Signaturgesetz) zulässig und technisch möglich.
- Das Signieren von XML-Daten mit dieser Signaturkarte ist nicht implementiert.
- Die Nutzung der Signaturkarte zum Entschlüsseln und Verschlüsseln ist technisch bedingt noch nicht möglich. Die notwendigen Parameter sind noch nicht ausreichend definiert, so dass die interoperable Verwendung (über diese Anwendung hinaus) noch nicht sichergestellt werden kann.

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. Die Governikus GmbH & Co. KG kann für derartige Funktionseinschränkungen, Fehler und dadurch verursachte Schadensverläufe nicht verantwortlich gemacht werden.

2 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 Anendung 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.

3 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 4c).

4 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 4c).

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 12345**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.

5 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 4c).

6 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 4c).

Unterstützte Terminalserver

Heutige Terminalserver-Software spielt über virtuelle USB-Schnittstellen dem Treiber eines Chipkartenlesegerätes vor, dass sich dieses am lokalen Rechner befindet, obwohl es sich tatsächlich an der Arbeitsstation des Nutzers befindet.

Dies funktioniert häufig sehr gut, bedeutet aber auch, dass für die Funktionsfähigkeit die Hersteller der Chipkartenlesegeräte (Treiber) und die Hersteller der Terminalserver-Software verantwortlich sind. Es liegt in der Regel nicht in der Verantwortung dieser Anwendung, wenn Kombinationen nicht funktionieren. Auch kann die Funktionsfähigkeit nicht durch Änderungen dieser Anwendung herbeigeführt werden.

Zur Nutzung freigeben wird daher nur eine Teilmenge der insgesamt durch diese Anwendung unterstützten Kombinationen von Betriebssystemen und Chipkartenlesegeräten.

Ob eine Kombination von Signaturkarte, Chipkartenleser, Terminalserversoftware, Serverbetriebssystem und Clientbetriebssystem unterstützt wird, ist der Tabelle „Unterstützte Einsatzumgebungen Terminalserver“ (Tabelle 5a bis 5b) zu entnehmen.

Tabelle 1: Unterstützte Betriebssysteme und JRE

Betriebssysteme	JRE Versionen und Updates	Abkündigung
Windows Vista SP2 – Basic, Home Premium, Business, Enterprise, Ultimate – jeweils 32 Bit und 64 Bit	8 Update 60 (32 Bit)	Spätestens zum 11.04.2017
Windows 7 SP1 – Home Basic, Home Premium, Professional, Ultimate, Enterprise – jeweils 32 Bit und 64 Bit	8 Update 60 (32 Bit)	
Windows 8 und 8.1: – Standard, Professional, Enterprise – 32 Bit	8 Update 60 (32 Bit)	
Windows 8 und 8.1: – Standard, Professional, Enterprise – 64 Bit	8 Update 60 (64 Bit)	
Windows 10: – Professional, Enterprise – 64 Bit	8 Update 60 (64 Bit)	
openSUSE 13.2 64 Bit	8 Update 60 (64 Bit)	
Ubuntu 14.04 LTS 64 Bit	8 Update 60 (64 Bit)	
Mac OS X 10.9 (Mavericks) 1)	8 Update 60	

1) Einschränkungen in der Funktionsunterstützung des Betriebssystems mit Governikus-Komponenten möglich

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

Zertifizierungs-diensteanbieter (akkreditiert mit Gütezeichen BNetzA)	Handelsname der Signaturkarte	QES Authentisierung Chiffrierung	Name der SSEE in der Bestätigungsurkunde	Registrierungsnr. der Bestätigungsurkunde der SSEE
Produktzentrum TeleSec der Deutschen Telekom AG (Z0001)	TeleSec PKS-Classic (Netkey 3.0)	✓	Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 1.1	TUVIT.93146.TE.12.2006 Nachtrag 1 vom 07.05.2010 Nachtrag 2 vom 20.03.2014
	TeleSec PKS-Classic Multisignatur (Netkey 3.0M) 1)			
	TeleSec PKS-ECC-Signaturkarte (SignatureCard 2.0) 5)	✓6)	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)			
Bundesnotarkammer, Zertifizierungsstelle (Z0003)	Bundesnotarkammer, Zertifizierungsstelle qualifizierte elektronische Signatur 2)	✓	Signaturerstellungseinheit STARCOS 3.2 QES Version 2	BSI.02114.TE.12.2008 Nachtrag 1 vom 08.03.2010
Bundesnotarkammer, Zertifizierungsstelle (Z0003)	beA-Karte Basis	Nur Authentisierung und Chiffrierung	Signaturerstellungseinheit STARCOS 3.5 ID ECC C1	SRC.00013.TE.10.2012
D-Trust GmbH (Z0017) 3)	D-TRUST Card 2.4	✓	Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P (oder SLE66CX642P), Software CardOS V4.3B Re_Cert with Applikation for Digitale Signature“	T-Systems.02182.TE.11. 2006 Nachtrag 1 vom 06.02.2007 Nachtrag 2 vom 06.05.2008
	D-TRUST Card 3.0	✓	Sichere Signaturerstellungseinheit STARCOS 3.4 Health QES C1 Die Nachfolgeversion STARCOS 3.4 Health QES C2 (siehe Nachtrag) wird auch unter dem Vertriebsnamen D-TRUST Card V3.0 geführt.	BSI.02120.TE.05.2009 Nachtrag vom 15.11.2010
	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)	Nur 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

Zertifizierungs-diensteanbieter (akkreditiert mit Gütezeichen BNetzA)	Handelsname der Signaturkarte	QES Authentisierung Chiffrierung	Name der SSEE in der Bestätigungsurkunde	Registrierungsnr. der Bestätigungsurkunde der SSEE
			Signaturerstellungseinheit „STARCOS 3.5 ID GCC C1R“	SRC.00014.TE.02.2012 Nachtrag 1 vom 06.02.2013
DATEV eG Zertifizierungsstelle (Z0004)	zertifizierte Signaturkarte für Berufsträger der DATEV	✓	Signaturerstellungseinheit STARCOS 3.2 QES Version 2	BSI.02114.TE.12.2008 Nachtrag 1 vom 08.03.2010
			Sichere Signaturerstellungseinheit STARCOS 3.4 Health QES C1 Die Nachfolgeversion STARCOS 3.4 Health	BSI.02120.TE.05.2009 Nachtrag vom 15.11.2010
S-Trust, Deutscher Sparkassen Verlag GmbH (Z0035)	S-TRUST Card, SparkassenCard oder kontounabhängige GeldKarte	✓	Signaturerstellungseinheit 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 28.12.2010
dgnservice (Z0033)	dgnservice Card	✓	Signaturerstellungseinheit STARCOS 3.2 QES Version 2	BSI.02114.TE.12.2008 Nachtrag 1 vom 08.03.2010
	businessCard 2)			
	dgnservice Card	Nur QES	Signaturerstellungseinheit STARCOS 3.5 ID ECC C1R	SRC.00021.TE.05.2013 Nachtrag 1 vom 14.11.2013
	businessCard 2)			

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 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 Entschlüsselung 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

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

Zertifizierungs-diensteanbieter (angezeigt)	Handelsname der Signaturkarte	QES Authentisie-rung Chiffrierung	Name der SSEE in der Bestätigungsur-kunde	Registrierungsnr. der Bestäti-gungsurkunde der SSEE
D-Trust GmbH	D-TRUST Card 3.0	✓	Sichere Signaturerstellungseinheit STARCOS 3.4 Health QES C1. Nachfolge-version STARCOS 3.4 Health QES C2 wird auch unter D-TRUST Card 3.0 geführt.	BSI.02120.TE.05.2009 Nachtrag vom 15.11.2010
	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	✓	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
		✓	SEE ZKA-Signaturkarte, Version 6.32 der Gemalto GmbH	TUVIT.93184.TU11.2010 Nachtrag 1 vom 19.05.2011
		✓	Signaturerstellungseinheit ZKA Banking 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)	✓	Signaturerstellungseinheit ZKA-Signaturkarte, Version 6.32 M	TUVIT.93176.TU.05.2011
Deutsche Renten-versicherung Bund (DRV) 4)	Signaturkarte der Deutschen Rentenversi-cherung Bund (Einzelsignatur)	Nur QES und Chiffrierung	Sichere Signaturerstellungseinheit CardOS V5.0 with Application for QES, V1.0	BSI.02136.TE.07.2013
	Multisignaturkarte der Deutschen Renten-versicherung Bund 1)	Nur QES		
Bundesagentur für Arbeit 4)	Signaturkarte der Bundesagentur für Ar-beit (BA)	✓	Sichere Signaturerstellungseinheit STARCOS 3.4 Health HBA C1	BSI.02135.TE.08.2011

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 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	Signatur Chiffrierung Authentisierung	Name der SEE	Bemerkungen
A-Trust GmbH	A-TRUST premium	Nur QES	Betriebssystem des Kartenchips: ACOS EMV-A05V1.	Österreichische Signaturkarte geeignet zur Erzeugung einer QES in Deutschland. Registrierungsnummer der Bestätigungsurkunde: T-Systems.02169.TE.10.2009
Deutschland-Online Infrastruktur (DOI) CA 1)	Signaturkarte der T-Systems Netkey 3.0	✓	Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 1.1	TUVIT.93146.TE.12.2006 Nachtrag 1 vom 07.05.2010
Europäisches Patentamt - European Patent Office (EPO)	Online Services Smart Card Epoline	Nur fortgeschrittene Signatur	--	--
Hessen-PKI 2)	Signaturkarte der T-Systems Netkey 3.0 und 3.01 mit Hessen-PKI-Zertifikat	Nur fortgeschrittene Signatur	SSEE TCOS 3.0 Signature Card, Version 1.1	Sichere SSEE. Registrierungsnr. der Bestätigungsurkunde der SSEE TUVIT.93146.TE.12.2006 Nachtrag 1 vom 07.05.2010
Landeshauptstadt Hannover (LHH) 3)	TeleSec PKS-Classic (Netkey 3.0) mit DOI-Zertifikat	✓	Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 1.1	TUVIT.93146.TE.12.2006 Nachtrag 1 vom 07.05.2010
	TeleSec -ECC-Signaturkarte (Signature-Card 2.0) mit DOI-Zertifikat		Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 2.0 Release 1/SLE78CLX1440P	SRC.00016.TE.11.2012
VR Bank	VR-BankCard VR-NetworldCard	✓	--	--
QuoVadis Trustlink Schweiz AG	QuoVadis Multisignaturkarte mit Funktionszertifikat ElDI-V/GeBüV	Nur fortgeschrittene Signatur	Siemens CardOS 4.4	BSI.02130.TE.07.2011

1) Die Signaturkarte wird nur an Mitarbeiter von Behörden im Kontext DVDV ausgegeben.

2) Die Signaturkarte wird nur an Mitarbeiter hessischer Behörden ausgegeben. Diese Signaturkarte kann zusätzlich auch mit einem qualifizierten Signaturzertifikat (mit Anbieterakkreditierung) des Public Key Service des Produktzentrum TeleSec der Deutschen Telekom AG personalisiert werden. Die QES wird dann unterstützt.

3) Die Signaturkarte wird nur an Mitarbeiter von Behörden der Landeshauptstadt Hannover ausgegeben.

Tabelle 3a: Unterstützte Chipkartenlesegeräte mit SigG-Bestätigung

Handelsname des Geräts	Angaben aus der veröffentlichten Bestätigung bei der BNetzA			PIN-Pad	Stand-ard	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 Karten-lesegeräte GmbH	cyberJack e-com, Version 3.0	TUVIT.93155.TE.09.2008	ja	PC/SC	USB	kontakt
cyberJack e-com plus	Reiner SCT Karten-lesegeräte GmbH	cyberJack e-com plus, Version 3.0	TUVIT.93156.TE.09.2008	ja	PC/SC	USB	kontakt
cyberJack pinpad Version 3	Reiner SCT Karten-lesegeräte GmbH	Chipkartenleser, cyberJack pinpad, Version 3.0	TUVIT.93107.TU.11.2004	ja	PC/SC	USB	kontakt
CyberJack RFID kom-fort	Reiner SCT Karten-lesegeräte GmbH	cyberJack® RFID komfort Version 2.0	TUVIT.93180.TU.12.2011	ja	PC/SC	USB	kontakt, kontaktlos
CyberJack RFID standard	Reiner SCT Karten-lesegeräte GmbH	cyberJack® RFID standard Version 1.2	TUVIT.93188.TU.07.2011	ja	PC/SC	USB	kontakt, kontaktlos
cyberJack secoder	Reiner SCT Karten-lesegeräte GmbH	Chipkartenleser cyberJack secoder Version 3.0	TUVIT.93154.TE.09.2008	ja	PC/SC	USB	kontakt
Fujitsu Siemens Chipkartenleser-Tastatur KB SCR Pro	Fujitsu Siemens	Chipkartenleser-Tastatur KB SCR Pro, Sach-nummer S26381-K329-V2xx HOS:01, Firmware Version 1.06	BSI.02082.TE.01.2007	ja	PC/SC	USB	kontakt
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, Firmwareversion 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

Handelsname des Geräts	Angaben aus der veröffentlichten Bestätigung bei der BNetzA			PIN-Pad	Stand-ard	Schnittstelle	
Kobil KAAN Ad-vanced	Kobil Systems GmbH	Chipkartenterminal KAAN Advanced, Firmware Version 1.02, Hardware Version K104R3, Firmware 1.19 gemäß Nachtrag zur Bestäti-gung	BSI.02050.TE.12.2006 Nachtrag zur Bestätigung vom 07.04. 2008: T-Systems. 02207.TU.04.2008	ja	PC/SC	USB	kontakt
Kobil KAAN TrB@ank, EMV-TriCAP Reader und SecOVID Reader III	Kobil Systems GmbH	Signatur-Modul für die KOBIL Chipkartentermi-nals KAAN TriB@nk (FW 79.23), EMV-TriCAP (FW 82.23)und SecOVID Reader III (FW 82.23)	T-Systems 02246.TE. 10.2010	ja	PC/SC	USB	kontakt
SPR 332 usb (Chip-drive 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	Stand-ard	Schnittstelle	
					PC	Karte
CARD STAR/ medic Version 2	celectronic 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 Firmwareversion: 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 Vista, 7 SP1, 8, 8.1, 10 - Chipkartenlesegerät - Signaturkarte

Handelsnamen der Chipkartenlesegeräte mit SigG-Bestätigung / Herstellererklärung	Windows Versionen: Vista - 7 SP1 - 8 - 8.1 - 10		Handelsnamen der Signaturkarten														
	Firmware	Treiber PC/SC	TeleSec PKS Classic	TeleSec PKS ECC	Bundesnotar-kammer	beA-Karte Basis	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)	Netkey 3.0 (DOI, Hessen-PKI)	EPO-Karte	VR Bank
Cherry® Smartboard G83-6744	01.04.00.00	1.2.24.27	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
Cherry® SmartTerminal 2000 U	6.01.00.00	4.53.0.0	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® e-com/ e-com plus	3.0.69/3.0.4	bc_6_10_8 (6.0.7.3)	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® pinpad Version 3/ secoder	3.0.12/3.0.14	bc_6_10_8 (6.0.7.3)	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® RFID standard kontakt	1.2.16	bc_6_10_8 (6.0.7.3)	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® RFID komfort kontakt	2.0.7	bc_6_10_8 (6.0.7.3)	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® RFID standard kontaktlos	1.2.16	bc_6_10_8 (6.0.7.3)	-	✓1)	-	-	-	-	-	-	-	-	-	-	-	-	-
cyberJack® RFID komfort kontaktlos	2.0.7	bc_6_10_8 (6.0.7.3)	-	✓1)	-	-	-	-	-	-	✓2)	-	-	-	-	-	-
Fujitsu Siemens KB SCR eSIG	1.20	1.9.0.0	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
Fujitsu Siemens KB SCR Pro	1.06	1.2.24.0	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
Kobil KAAN Advanced	1.19	2013.1.24.1	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
Kobil SecOVID 3, EMV-TriCap/-b@nk	82.23/79.23	2013.1.24.1	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
Omnikey CardMan 3621, 3821	6.00	1.2.24.27	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
SPR 332 usb (Chipdrive pinpad pro)	6.01	4.53.0.0	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
ORGA 6041 Version 2.07	2.07	2.0.0.6	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
eHealth BCS 200	2.01	1.2.0.0	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
CARD STAR/ medic Version 2	M1.53G	WinUSB 2.76 und CTAPI 2.70, ct_api_usb.dll 4)	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
medCompact eHealth	02.00	CTAPI 03.00,cthyc32.dll 4)	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
GT900 BCS	1.0.10	ctgt900.dll 4) 6)	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
Omnikey 8751 eHealth LAN	1.3.2	ct8751com.dll 4) 6)	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
In Tabelle 3c aufgeführte Geräte ohne PIN-Pad (nicht für die QES zugelassen)			✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓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), Ubunto 12.04 LTS (64 Bit) - Chipkartenlesegerät - Signaturkarte

Handelsnamen der Chipkartenlesegeräte mit SigG-Bestätigung / Herstellererklärung	OpenSUSE 13.2 (64 Bit) Ubunto 12.04 LTS (64 Bit)		Handelsnamen der Signaturkarten														
	Firmware	PCSC-lite Version 1.8.11 6)	TeleSec PKS Classic	TeleSec PKS ECC	Bundesnotar-kammer	beA-Karte Basis	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)	Netkey 3.0 (DOI, Hessen-PKI)	EPO-Karte	VR Bank
Cherry® Smartboard G83-6744	01.04.00.00	ifdokccid-lnx-4.0.5	✘	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✘	✓3)	✓
Cherry® SmartTerminal 2000 U	6.01.00.00	scmccid 5.0.31	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® e-com/ e-com plus	3.0.69/3.0.4	ifd-cyberJack 3.99.5 SP5	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® pinpad Version 3/ secoder	3.0.12/3.0.14	ifd-cyberJack 3.99.5 SP5	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® RFID standard kontakt	1.2.16	ifd-cyberJack 3.99.5 SP5	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® RFID komfort kontakt	2.0.7	ifd-cyberJack 3.99.5 SP5	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® RFID standard kontaktlos	1.2.16	ifd-cyberJack 3.99.5 SP5	-	✓1)	-	-	-	-	-	-	-	-	-	-	-	-	-
cyberJack® RFID komfort kontaktlos	2.0.7	ifd-cyberJack 3.99.5 SP5	-	✓1)	-	-	-	-	-	-	✓2)	-	-	-	-	-	-
Fujitsu Siemens KB SCR eSIG	1.20	Keine Treiber verfügbar	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Fujitsu Siemens KB SCR Pro	1.06	ifdokccid-lnx-4.0.5	✘	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✘	✓3)	✓
Kobil KAAN Advanced	1.19	CCID 1.4.18 6)	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
Kobil SecOVID 3, EMV-TriCap/-b@nk	82.23/79.23	CCID 1.4.18 6)	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
Omnikey CardMan 3621, 3821	6.00	ifdokccid-lnx-4.0.5	✘	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✘	✓3)	✓
SPR 332 usb (Chipdrive pinpad pro)	6.01	scmccid 5.0.31	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
ORGA 6041 Version 2.07	2.07	V 1.7	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
eHealth BCS 200	2.01	V1.05	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
CARD STAR/ medic Version 2	M1.53G	WinUSB 2.76 und CTAPI 2.70, ct_api_usb.dll 4)	✘	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✘	✓3)	✓
medCompact eHealth	02.00	CTAPI 03.00,cthyc32.dll 4)	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓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)	✓3)	✓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

Tabelle 4c: Unterstützte Kombinationen Mac OS X 10.9 (Mavericks) - Chipkartenlesegerät - Signaturkarte

Handelsnamen der Chipkartenlesegeräte mit SigG-Bestätigung / Herstellererklärung	Mac OS X 10.9		Handelsnamen der Signaturkarten															
	Firmware	PCSC-lite Version 1.4.0 4)	TeleSec PKS Classic	TeleSec PKS ECC	Bundesnotar-kammer	beA-Karte Basis	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)	Netkey 3.0 (DOI, Hessen-PKI)	EPO-Karte	VR Bank
Cherry® Smartboard G83-6744	01.04.00.00	ifdokccid-mac 4.2.1	✘	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✘	✓3)	✓
Cherry® SmartTerminal 2000 U	6.01.00.00	scmccid 5.0.35	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® e-com/ e-com plus	3.0.69/3.0.4	ifd-cyberJack 3.99.5 SP7	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® pinpad Version 3/ secoder	3.0.12/3.0.14	ifd-cyberJack 3.99.5 SP7	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® RFID standard kontakt	1.2.16	ifd-cyberJack 3.99.5 SP7	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® RFID komfort kontakt	2.0.7	ifd-cyberJack 3.99.5 SP7	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® RFID standard kontaktlos	1.2.16	ifd-cyberJack 3.99.5 SP7	-	✓1)	-	-	-	-	-	-	-	-	-	-	-	-	-
cyberJack® RFID komfort kontaktlos	2.0.7	ifd-cyberJack 3.99.5 SP7	-	✓1)	-	-	-	-	-	-	✓2)	-	-	-	-	-	-
Fujitsu Siemens KB SCR eSIG	1.20	Keine Treiber verfügbar	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Fujitsu Siemens KB SCR Pro	1.06	ifdokccid-mac 4.2.1	✘	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✘	✓3)	✓
Kobil KAAN Advanced	1.19	CCID 1.4.18	✘	✘	✘	✘	✘	✘	✘	✘	-	✘	✘	✘	✘	✘	✘
Kobil SecOVID 3, EMV-TriCap/-b@nk	82.23/79.23	CCID 1.4.18	✘	✘	✘	✘	✘	✘	✘	✘	-	✘	✘	✘	✘	✘	✘
Omnikey CardMan 3621, 3821	6.00	ifdokccid-lnx-4.2.1	✘	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✘	✓3)	✓
SPR 332 usb (Chipdrive pinpad pro)	6.01	scmccid 5.0.35	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
In Tabelle 3c aufgeführte Geräte ohne PIN-Pad (nicht für die QES zugelassen)			Nicht getestet														

1) Ver-/ und Entschlüsselung nur im CMS-Format möglich
2) nur QES
3) nur Signatur
4) Bei generischen CCID-Treibern muss der Name des Lesers mit * angeführt werden
5) nur Authentisierung und Verschlüsselung

Tabelle 5a: Unterstützte Einsatzumgebungen Terminalserver

Clientbetriebssystem:	Windows 7 SP1 32 Bit																
Serverbetriebssystem:	Windows Server 2012 R2 64 Bit																
Terminalserver:	Citrix XenApp 7.5																
Handelsnamen der Chipkartenlesegeräte mit SigG-Bestätigung / Herstellererklärung	**Chipkartenlesegerät**		**Handelsnamen der Signaturkarten**														
	Firmware	**Treiber PC/SC 4)**	**TeleSec PKS Classic**	**TeleSec PKS ECC**	**Bundesnotar-kammer**	**beA-Karte Basis**	**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)**	**Netkey 3.0 (DOI, Hessen-PKI)**	**EPO-Karte**	**VR Bank**
Cherry® SmartTerminal 2000 U	6.01.00.00	4.53.0.0	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® e-com	3.0.69	bc_6_10_8 (6.0.7.3)	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® RFID komfort kontakt	2.0.7	bc_6_10_8 (6.0.7.3)	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® RFID komfort kontaktlos	2.0.7	bc_6_10_8 (6.0.7.3)	-	✓1)	-	-	-	-	-	-	✓2)	-	-	-	-	-	✓
Omnikey 3621/3821	6.00	1.2.24.27	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓

1) Ver-/ und Entschlüsselung nur im CMS-Format möglich
2) nur QES
3) nur Signatur
4) Bei generischen CCID-Treibern muss der Name des Lesers mit * angeführt werden
5) nur Authentisierung und Verschlüsselung

Tabelle 5b: Unterstützte Einsatzumgebungen Terminalserver

Clientbetriebssystem:	Thin Client elux RL V3.7.1-1 mit PC/SC lite V2.1.6.4-5 und CCID V1.4.0-1															
Serverbetriebssystem:	Windows 2003 Server R2 SP2 64 Bit															
Terminalserver:	Windows Terminal Server 2003															
Handelsnamen der Chipkartenlesegeräte mit SigG-Bestätigung / Herstellererklärung	**Chipkartenlesegerät**		**Handelsnamen der Signaturkarten**													
	Firmware	**Treiber PC/SC 4)**	**TeleSec PKS Classic**	**TeleSec PKS ECC**	**Bundesnotar-kammer**	**beA-Karte Basis**	**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)**	**Netkey 3.0 (DOI, Hessen-PKI)**	**EPO-Karte**	**VR Bank**
Kobil KAAN Advanced	1.19	CCID V1.4.0-1	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® e-com plus	3.0.7	CCID V1.4.0-1	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓
cyberJack® RFID komfort kontakt	2.0.7	CCID V1.4.0-1	✓	✓1)	✓	✓5)	✓	✓	✓	✓	-	✓	✓	✓2)	✓3)	✓3)	✓

1) Ver-/ und Entschlüsselung nur im CMS-Format möglich
2) nur QES
3) nur Signatur
4) Bei generischen CCID-Treibern muss der Name des Lesers mit * angeführt werden
5) nur Authentisierung und Verschlüsselung

Impressum

Die Administration Intelligence AG ist bei der Redaktion dieses Dokuments mit der größtmöglichen Sorgfalt vorgegangen. Inhaltliche Lücken, Fehler und fehlerhafte Interpretationen können dennoch nicht ausgeschlossen werden. Die Administration Intelligence AG haftet nicht für technische Fehler in diesem Dokument. Die Beschreibungen in diesem Dokument stellen keine zugesicherte Eigenschaft im Rechtssinne dar.

Administration Intelligence AG
Steinbachtal 2B
97082 Würzburg
Telefon: 0931-88061-70
Fax: 0931-88061-40
www.ai-ag.de
E-Mail: info@ai-ag.de

Vorstand: Dr. Christian Schneider (Vors.), Alexander N. Müller
Aufsichtsratsvorsitzender: Prof. Dr. Rainer Thome
Registernummer: HRB 7176