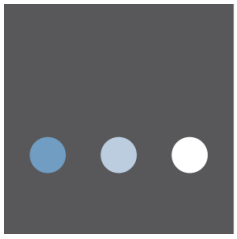

Governikus KG

Systemanforderungen

Governikus WebSigner

Governikus WebSigner, Release 2.7.3.0

Inhaltsverzeichnis

1 Anforderungen Arbeitsplatzcomputer

Arbeitsplatzcomputer

Es gelten folgende Voraussetzungen:

- **Prozessor**: AMD oder Intel
- **Speicher**: Minimal 50 MB Plattenspeicherplatz, minimal 512 MB RAM
- **Bildschirm**: Minimale Auflösung 1.024x768 Pixel
- **Rechte**: Für den erstmaligen Start des Governikus WebSigner bzw. jeweils einmalig nach der Installation einer neuen Java Laufzeitumgebung sind ggf. Administratorrechte erforderlich (siehe Abschnitt Java Laufzeitumgebung).

Unterstützte Betriebssysteme und Browser

Der Governikus WebSigner kann auf den folgenden Betriebssystemen eingesetzt werden.

Betriebssysteme	Unterstützte Browser
Windows XP Professional (**32Bit**)	Internet Explorer Version 8 Firefox aktuelle ESR-Version, siehe unten
Windows Vista (**32Bit**)	Internet Explorer Version 9 Firefox aktuelle ESR-Version, siehe unten
Windows 7 Professional (**32Bit** und **64Bit**)	Internet Explorer Version 10 und 11 Firefox aktuelle ESR-Version, siehe unten
Windows 8 Professional (**64Bit**)	Internet Explorer Version 10 und 11 Firefox aktuelle ESR-Version, siehe unten
Linux openSUSE 13.1 (**64Bit**)	Firefox aktuelle ESR-Version, siehe unten

Hinweis: Auf allen aufgeführten Betriebssystemen müssen aktuelle Service Packs installiert sein.

Hinweis: Bei Verwendung des Browsers Firefox muss JavaScript aktiviert sein, um zur aufrufenden Anwendung zurückkehren zu können.

Firefox ESR-Version

Die Governikus KG unterstützt Firefox nur in der Version "**E**xtended **S**upport **R**elease" (**ESR**). Informationen zur ESR-Version finden Sie hier: Mozilla Firefox Extended Support Release. Den Firefox Browser in der ESR-Version können Sie hier herunterladen: Firefox ESR. **Hinweis**: Auf dieser Seite müssen Sie zuerst solange herunterblättern, bis Sie zum Abschnitt "Fully Localized Versions" gelangen. Wählen Sie dann Ihre Sprache aus, z.B. German.

Sie können im Firefox-Browser über das Menü "Hilfe", unter der Option "Über Firefox" feststellen, welche Version Sie verwenden. Im Dialogfenster, unterhalb des "Nach Updates suchen" Buttons, muss die Zeile "Sie sind derzeit auf dem Update-Kanal **esr**" stehen. Wenn nicht, laden Sie bitte die **ESR** Version herunter und installieren Sie diese, ohne zuvor Ihre aktuelle Version zu deinstallieren. So werden alle Einstellungen beibehalten.

Hinweis: Firefox Browser in der ESR-Version werden vom Anbieter Mozilla ebenfalls regelmäßig aktualisiert und sind damit so sicher, wie die Versionen für den privaten Gebrauch.

Java Laufzeitumgebung

Die Verwendung des Governikus WebSigner erfordert eine Java Laufzeitumgebung (JRE) in der Version 7 des Herstellers ORACLE.

Achtung: Installieren Sie Java **immer** in der **32Bit** Version!

Ausstattungsanforderung für das digitale Signieren

Für das digitale Signieren von Dateien benötigen Sie diese Ausstattung:

- Für die Erzeugung **qualifizierter** Signaturen
  - Eine Signaturkarte eines angezeigten oder akkreditierten Zertifizierungsdienste-anbieters aus Deutschland.
  - Ein herstellererklärtes oder SigG-bestätigtes Chipkartenlesegerät (mit PIN-Pad)
- Für die Erstellung **fortgeschrittener** Signaturen:
  - Eine Zertifikatsdatei (`.p12`), ein Dateiformat, das dazu benutzt wird, private Schlüssel mit dem zugehörigen Zertifikat passwortgeschützt zu speichern (häufig auch SW-Zertifikat genannt).

Hinweis: Für eine vollständig Unterstützung aller Software-Zertifikate ist die Java-Erweiterung für starke Verschlüsselung (Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy) erforderlich.

Der Governikus WebSigner versucht die Erweiterung beim Start zu installieren, wenn die Erweiterung fehlt und die erforderlichen Administratorrechte vorhanden sind.

oder

  - Eine Signaturkarte eines Trustcenters, mit der man fortgeschrittene Signaturen erzeugen kann.
  - Ein Chipkartenlesegerät (PIN-Pad nicht erforderlich)

Eine Liste aller aktuell unterstützten Signaturkarten und Kartenleser ist im nachfolgenden Abschnitt aufgeführt.

2 Ab- und Ankündigungen für Folge-Releases

Ankündigung:

Keine

Abkündigung:

Seit dem 08. April 2014 stellt Microsoft für das Betriebssystems Windows XP SP3 keine Sicherheits-Patches mehr bereit. Dieser Umstand kann die für eine Signaturanwendungs-komponente geforderte hohe Sicherheit gegen potenzielle Bedrohungen beeinträchtigen. Für die Folgeversion wird die Unterstützung daher abgekündigt. Die Governikus KG empfiehlt, rechtzeitig auf eine aktuellere Windows-Version umzustellen.

3 Aktuelle Hinweise

Neue Signaturkarte der Bundesnotarkammer

Seit dem 1. April 2014 gibt die Bundesnotarkammer neue Stapel-Signaturkarten basierend auf dem Kartenbetriebssystem STARCOS 3.5 aus. Die neue Signaturkarte wird mit diesem Release unterstützt.

Neue Signaturkarte der DGN Deutsches Gesundheitsnetz Service

Die Einzel-Signaturkarte „sprintCard“ des Zertifizierungsdiensteanbieters DGN Deutsches Gesundheitsnetz Service GmbH wird mit diesem Release unterstützt.

Neue Signaturkarten der Deutsche Post Com GmbH Geschäftsfeld Signtrust

Seit Anfang 2014 plant der Zertifizierungsdiensteanbieter „Deutsche Post Com GmbH Geschäftsfeld Signtrust“ die Herausgabe von neuen Signaturkarten (SIGNTRUST CARD, SIGNTRUST MCARD 100, SIGNTRUST MCARD), die auf dem Kartenbetriebssystem STARCOS 3.5 basieren.
Die neuen SSEE wurden auf der Basis von Testkarten eingebunden. Die Funktionsfähigkeit der Wirkkarten kann daher nicht gewährleistet werden. Sollte eine Anpassung erforderlich sein, wird kurzfristig eine Aktualisierung der Anwendung erfolgen.

Neue Signaturkarte der DATEV eG

Die neue Signaturkarte des Zertifizierungsdiensteanbieters

- DATEV eG

wird mit einem der folgenden Releases unterstützt.

TC TrustCenter GmbH kündigt Einstellung des Betriebs an

Der Zertifizierungsdiensteanbieter TC-Trustcenter hat die Einstellung seiner Tätigkeit angekündigt. Mehr Informationen auf Website 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.

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.

4 Unterstützte Signaturkarten und Kartenleser

Im Folgenden sind die unterstützten Chipkartenlesegeräte, die unterstützten Signaturkarten sowie die unterstützten Kombinationen von Betriebssystem, Chipkartenlesegerät und Signaturkarten aufgeführt.

4.1 Unterstützte Chipkartenlesegeräte

Mit diesem Governikus WebSigner 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.

4.2 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 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.

4.3 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 c).

4.4 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 wie folgt:

- Bei Einzelsignaturkarten ist nach der PIN-Eingabe die Erzeugung einer QES möglich.
- Bei Stapelsignaturkarten sind nach der einmaligen PIN-Eingabe - kartenabhängig - bis zu 100 QES möglich (Batchverfahren).
- Bei Multisignaturkarten wird die Erzeugung von maximal 500 QES-Stapelsignaturen nach einer einmaligen PIN-Eingabe unterstützt (Batchverfahren). Die Erzeugung von Signaturen innerhalb eines festgelegten Zeitfensters ist nicht möglich.

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 c).

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.

4.5 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 c).

4.6 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 c).

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 5) zu entnehmen.

Tabelle 1: Unterstützte Betriebssysteme und JRE

Betriebssysteme	JRE Versionen und Updates	Abkündigung
Windows XP Professional SP3 2) – jeweils 32 Bit und 64 Bit	7 Update 51 (32 Bit)	Win XP wird mit der kommenden Version nicht mehr unterstützt.
Windows Vista SP2 – Basic, Home Premium, Business, Enterprise, Ultimate – jeweils 32 Bit und 64 Bit	7 Update 51 (32 Bit)	
Windows 7 SP1 – Home Basic, Home Premium, Professional, Ultimate, Enterprise – jeweils 32 Bit und 64 Bit	7 Update 51 (32 Bit)	
Windows 8 und 8.1: – Standard, Professional, Enterprise – 32 Bit	7 Update 51 (32 Bit)	
Windows 8 und 8.1: – Standard, Professional, Enterprise – 64 Bit	7 Update 51 (64 Bit)	
openSUSE 13.1 64 Bit	7 Update 51 (64 Bit)	

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

2) Der Hersteller stellt seit dem 08. April 2014 keine Sicherheitspatches mehr bereit. Ausgenommen davon sind geschlossene Nutzergruppen, die den kostenpflichtigen erweiterten Support erworben haben. Der Einsatz dieses Betriebssystems sollte nur dann erfolgen, wenn weiterhin die Versorgung mit Sicherheitspatches gewährleistet wird.

Tabelle 2a: Unterstützte Signaturkarten deutscher Zertifizierungsdiensteanbieter 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
	TeleSec PKS-Classic Multisignatur (Netkey 3.0M) 1)			
	TeleSec PKS-EEC-Signaturkarte (SignatureCard 2.0)	Nur QES und Authentisierung	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)			
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
			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

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 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
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
Deutsche Post Com GmbH Geschäftsfeld Signtrust (Z0002)	SIGNTRUST CARD	)	Signaturerstellungseinheit STARCOS 3.2 QES Version 2	BSI.02114.TE.12.2008 Nachtrag 1 vom 08.03.2010
	SIGNTRUST MCARD 100 2)			
	SIGNTRUST MCARD 1)			
	SIGNTRUST CARD	)	Signaturerstellungseinheit „STARCOS 3.5 ID GCC C1“	SRC.00008.TE.12.2010 Nachtrag 1 vom 06.02.2013
	SIGNTRUST MCARD 100 2)			
	SIGNTRUST MCARD 1)			
TC TrustCenter TrustCenter GmbH (Z0032)	TC QSign (limited) 5)	)	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
	TC QSign (unlimited) 1) 5)			
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 1. Nachtrag vom 08.03.2010
	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 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.

Zertifizierungs-diensteanbieter (akkreditiert mit Gütezeichen BNetzA)	Handelsname der Signaturkarte	QES Authentisierung Chiffrierung	Name der SSEE in der Bestätigungsurkunde	Registrierungsnr. der Bestätigungsurkunde der SSEE

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) Vertrieb der Signaturkarte wurde eingestellt.

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

Zertifizierungs-diensteanbieter (angezeigt)	Handelsname der Signaturkarte	QES Authentisierung Chiffrierung	Name der SSEE in der Bestätigungsurkunde	Registrierungsnr. der Bestätigungsurkunde der SSEE
D-Trust GmbH	D-TRUST Card 2.4 qualified D-TRUST Multicard 1)	)	Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P (oder SLE66CX642P), Software CardOS V4.3B Re_Cert with Applikation 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 D-TRUST Card 3.0 Multicard 100 2) 3) D-TRUST Card 3.0 Multicard 1)	)	Sichere Signaturerstellungseinheit STARCOS 3.4 Health QES C1. Nachfolgeversion 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
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 Card Multi 1)	)	Signaturerstellungseinheit ZKA-Signaturkarte, Version 6.32 M	TUVIT.93176.TU.05.2011

Zertifizierungs-diensteanbieter (angezeigt)	Handelsname der Signaturkarte	QES Authentisierung Chiffrierung	Name der SSEE in der Bestätigungsurkunde	Registrierungsnr. der Bestätigungsurkunde der SSEE
Deutsche Rentenversicherung Bund (DRV) 4)	Signaturkarte der Deutschen Rentenversicherung Bund	)	Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P (oder SLE66CX642P), Software CardOS V4.3B Re_Cert with Application Digitale Signature“	T-Systems.02182.TE.11. 2006 Nachtrag 1 vom 06.02.2007 Nachtrag 2 vom 06.05.2008
	Multisignaturkarte der Deutschen Rentenversicherung Bund 1)			
	Signaturkarte der Deutschen Rentenversicherung Bund (Einzelsignatur)	Nur QES	Sichere Signaturerstellungseinheit CardOS V5.0 with Application for QES, V1.0	BSI.02136.TE.07.2013 (durch BSI erteilt aber noch nicht durch die BNetzA veröffentlicht)
	Multisignaturkarte der Deutschen Rentenversicherung Bund 1)			
Bundesagentur für Arbeit 4)	Signaturkarte der Bundesagentur für Arbeit (BA)	)	Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P (oder SLE66CX642P), Software CardOS V4.3B Re_Cert with Application Digitale Signature“	T-Systems.02182.TE.11.2006 Nachtrag 1 vom 06.02.2007 Nachtrag 2 vom 06.05.2008
			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	)	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
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
Europäisches Patentamt - European Patent Office (EPO)	Online Services Smart Card Epoline	Nur fortgeschrittene Signatur	--	--
VR Bank	VR-BankCard VR-NetworldCard	)	--	--
SwissSign AG	PostSuisseID	Nur fortgeschrittene Signatur	Siemens CardOS 4.3b	Schweizer Signaturkarte. Nur innerhalb der Schweiz für eine QES geeignet
QuoVadis Trustlink Schweiz AG	QuoVadis SuisseID	Nur fortgeschrittene Signatur	Siemens CardOS 4.3b	Schweizer Signaturkarte. Nur innerhalb der Schweiz für eine QES geeignet

Swisscom Schweiz AG	Qualified Certificate Diamant	Nur fortgeschrittene Signatur	Siemens CardOS 4.3b	Schweizer Signaturkarte. Nur innerhalb der Schweiz für eine QES geeignet

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.

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**	**Standa**	**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, 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
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
Kobil KAAN TrB@ank, EMV-TriCAP Reader und SecOVID Reader III	Kobil Systems GmbH	Signatur-Modul für die KOBIL Chipkartenterminals 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 (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	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	Standard	Schnittstelle	
				PC	Karte
CardMan 3121	Omnikey	nein	PC/SC	USB	kontakt
Omnikey Cardman 5321 RFID	Omnikey	nein	PC/SC	USB	kontakt, kontaktlos 1)
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

Hinweis: Die Geräte SCR 3310, SCR 3311 (Chipdrive desktop pro) und SCR 335 (Chipdrive micro pro) wurden mit der MCard-Version 1.21.0.0 abgekündigt.

Tabelle 4a: Unterstützte Kombinationen Windows Betriebssysteme XP, Vista, 7- Chipkartenlesegerät - Signaturkarte

Handelsnamen der Chipkartenlesegeräte mit SigG-Bestätigung/Herstellererklärung	Windows XP, Vista, Windows 7			Handelsnamen der Signaturkarten																		
	Firmware	Treiber PC/SC	TeleSec PKS Classic	TeleSec PKS ECC (neu)	BNotK Starcos 3.2	BnotK Starcos 3.5 (neu)	DATEV Starcos 3.2	D-Trust Card 2.4	D-Trust Card 3.0 (neu)	Signtrust Card Starcos 3.2	Signtrust Card Starcos 3.5 (neu)	TC QSign	S-Trust Card	dgnSprintCard dgnBusinessCard	nPA QES	DRV Bund Card OS 3.4b und 5.0	BA Card OS 4.3 b und Starcos 3.4	A-Trust premium (QES)	Netkey 3.0 (DOI, Hessen-PKI)	EPO-Karte	VR Bank
Cherry® Smartboard G83-6744	01.04.00.00	1.2.20.0	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
Cherry® SmartTerminal 2000 U	6.01.00.00	4.53.0.0	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
cyberJack® e-com/ e-com plus	3.0.69/3.0.4	bc_6_10_8 (6.0.7.3)	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
cyberJack® pinpad Version 3/ secoder	3.0.12/3.0.14	bc_6_10_8 (6.0.7.3)	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
cyberJack® RFID standard kontakt	1.2.16	bc_6_10_8 (6.0.7.3)	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
cyberJack® RFID komfort kontakt	2.0.7	bc_6_10_8 (6.0.7.3)	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 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	1.12.0.0	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
Fujitsu Siemens KB SCR Pro	1.06	1.2.20.0	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
Kobil KAAN Advanced	1.19	2013.1.24.1	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
Kobil SecOVID 3, EMV-TriCap/ Trib@nk	82.23/79.23	2013.1.24.1	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
Omnikey CardMan 3621, 3821	6.00	1.2.20.0	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
ORGA 6041 Version 2.07	2.07	2.0.0.6	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
eHealth BCS 200	2.01	1.2.0.0	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
CARD STAR/ medic Version 2	M1.53G	WinUSB 2.51 und CTAPI 2.70, ct_api_com.dll 4)	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
medCompact eHealth	02.00	CTAPI 0300, cthyc32.dll 4)	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
GT900 BCS	1.0.10	ctgt900.dll von Support-CD 1.3 4)	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
Omnikey 8751 e-Health LAN	1.3.2	ct8751com.dll von Support-CD 4)	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
In Tabelle 2c aufgeführte Geräte ohne PIN-Pad (nicht für die QES zugelassen)			✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓

1) nur QES, fortgeschrittene Signatur und Authentisierung, keine Ver- und Entschlüsselung mit der TeleSec PKS-ECC Signaturkarte möglich

2) nur QES

3) nur Signatur

4) nur CT-API, dll nur 32 Bit Java

Tabelle 4b: Unterstützte Kombinationen Windows 8 - Chipkartenlesegerät - Signaturkarte

Handelsnamen der Chipkartenlesegeräte mit SigG-Bestätigung/Herstellererklärung	Windows 8		Handelsnamen der Signaturkarten																		
	Firmware	Treiber PC/SC	TeleSec PKS Classic	TeleSec PKS ECC (neu)	BNotK Starcos 3.2	BnotK Starcos 3.5 (neu)	DATEV Starcos 3.2	D-Trust Card 2.4	D-Trust Card 3.0 (neu)	Signtrust Card Starcos 3.2	Signtrust Card Starcos 3.5 (neu)	TC QSign	S-Trust Card	dgnSprintCard dgnBusinessCard	nPA QES	DRV Bund Card OS 3.4b und 5.0	BA Card OS 4.3 b und Starcos 3.4	A-Trust premium (QES)	Netkey 3.0 (DOI, Hessen-PKI)	EPO-Karte	VR Bank
Cherry® Smartboard G83-6744	01.04.00.00	1.2.15.0	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
Cherry® SmartTerminal 2000 U	6.01.00.00	4.53.0.0	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
cyberJack® e-com/ e-com plus	3.0.69/3.0.4	bc_6_10_8 (6.0.7.3)	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
cyberJack® pinpad Version 3/ secoder	3.0.12/3.0.14	bc_6_10_8 (6.0.7.3)	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
cyberJack® RFID standard kontakt	1.2.16	bc_6_10_8 (6.0.7.3)	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
cyberJack® RFID komfort kontakt	2.0.7	bc_6_10_8 (6.0.7.3)	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 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)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
Fujitsu Siemens KB SCR Pro	1.06	1.2.15.0	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
Kobil KAAN Advanced	1.19	2011.12.19.4	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
Kobil SecOVID 3, EMV-TriCap/ Trib@nk	82.23/79.23	2011.12.19.4	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
Omnikey CardMan 3621, 3821	6.00	1.2.15.0	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
ORGA 6041 Version 2.07	2.07	2.0.0.6	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
eHealth BCS 200	2.01	1.2.0.0	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
CARD STAR/ medic Version 2	M1.53G	Keine Treiber verfügbar	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

medCompact eHealth	02.00	CTAPI 0300, cthyc32.dll 4)	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
GT900 BCS	1.0.10	Keine Treiber verfügbar	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Omnikey 8751 e-Health LAN	1.3.2	Keine Treiber verfügbar	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
In Tabelle 2c aufgeführte Geräte ohne PIN-Pad (nicht für die QES zugelassen)			✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓

1) nur QES, fortgeschrittene Signatur und Authentisierung, keine Ver- und Entschlüsselung mit der TeleSec PKS-ECC Signaturkarte möglich

2) nur QES

3) nur Signatur

4) nur CT-API, dll nur 32 Bit Java

Tabelle 4c: Unterstützte Kombinationen OpenSUSE 13.1 (64 Bit) - Chipkartenlesegerät - Signaturkarte

Handelsnamen der Chipkartenlesegeräte mit SigG-Bestätigung/Herstellererklärung	OpenSUSE 13.1 (64 Bit)		Handelsnamen der Signaturkarten																		
	Firmware	Treiber für Daemon-PCSC-lite Version 1.8.8	TeleSec PKS Classic	TeleSec PKS ECC (neu)	BNotK Starcos 3.2	BnotK Starcos 3.5 (neu)	DATEV Starcos 3.2	D-Trust Card 2.4	D-Trust Card 3.0 (neu)	Signtrust Card Starcos 3.2	Signtrust Card Starcos 3.5 (neu)	TC QSign	S-Trust Card	dgnSprintCard dgnBusinessCard	nPA QES	DRV Bund Card OS 3.4b und 5.0	BA Card OS 4.3 b und Starcos 3.4	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)	┘	)	┘	)	)	┘	)	)	)	)	-	)	)	) 2)	┘	) 3)	)
Cherry® SmartTerminal 2000 U	6.01.00.00	scmccid 5.0.27	)	) 1)	)	)	)	)	)	)	)	)	)	)	-	)	)	) 2)	) 3)	) 3)	)
cyberJack® e-com/ e-com plus	3.0.69/3.0.4	ifd-cyberJack 3.99.5 SP5	)	) 1)	)	)	)	)	)	)	)	)	)	)	-	)	)	) 2)	) 3)	) 3)	)
cyberJack® pinpad Version 3/ secoder	3.0.12/3.0.14	ifd-cyberJack 3.99.5 SP5	)	) 1)	)	)	)	)	)	)	)	)	)	)	-	)	)	) 2)	) 3)	) 3)	)
cyberJack® RFID standard kontakt	1.2.16	ifd-cyberJack 3.99.5 SP5	)	) 1)	)	)	)	)	)	)	)	)	)	)	-	)	)	) 2)	) 3)	) 3)	)
cyberJack® RFID komfort kontakt	2.0.7	ifd-cyberJack 3.99.5 SP5	)	) 1)	)	)	)	)	)	)	)	)	)	)	-	)	)	) 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	Kein Treiber verfügbar	)	) 1)	)	)	)	)	)	)	)	)	)	)	-	)	)	) 2)	) 3)	) 3)	)
Fujitsu Siemens KB SCR Pro	1.06	ifdokccid-lnx-4.0.5	┘	) 1)	┘	)	┘	)	)	┘	)	)	)	)	-	)	)	) 2)	┘	) 3)	)
Kobil KAAN Advanced	1.19	CCID 1.4.12 5)	)	) 1)	)	)	)	)	)	)	)	)	)	)	-	)	)	) 2)	) 3)	) 3)	)
Kobil SecOVID 3, EMV-TriCap/ Trib@nk	82.23/79.23	CCID 1.4.12 5)	)	) 1)	)	)	)	)	)	)	)	)	)	)	-	)	)	) 2)	) 3)	) 3)	)
Omnikey CardMan 3621, 3821	6.00	ifdokccid-lnx-4.0.5	┘	) 1)	┘	)	┘	)	)	┘	)	)	)	)	-	)	)	) 2)	┘	) 3)	)

Handelsnamen der Chipkartenlesegeräte mit SigG-Bestätigung/Herstellererklärung	OpenSUSE 13.1 (64 Bit)		Handelsnamen der Signaturkarten																		
	Firmware	Treiber für Daemon-PCSC-lite Version 1.8.8 5)	TeleSec PKS Classic	TeleSec PKS ECC (neu)	BNotK Starcos 3.2	BnotK Starcos 3.5 (neu)	DATEV Starcos 3.2	D-Trust Card 2.4	D-Trust Card 3.0 (neu)	Signtrust Card Starcos 3.2	Signtrust Card Starcos 3.5 (neu)	TC QSign	S-Trust Card	dgnSprintCard dgnBusinessCard	nPA QES	DRV Bund Card OS 3.4b und 5.0	BA Card OS 4.3 b und Starcos 3.4	A-Trust premium (QES)	Netkey 3.0 (DOI, Hessen-PKI)	EPO-Karte	VR Bank
ORGA 6041 Version 2.07	2.07	V 1.7	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
eHealth BCS 200	2.01	V 1.04	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
CARD STAR/ medic Version 2	M1.53G	libctapi-celectronic.so. 0.0.0 von CD 2.3 4)	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
medCompact eHealth	02.00	libcthyc-01.04.so 4)	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
GT900 BCS	1.0.10	Kein Treiber verfügbar	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Omnikey 8751 e-Health LAN	1.3.2	Kein Treiber verfügbar	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
In Tabelle 2c aufgeführte Geräte ohne PIN-Pad (nicht für die QES zugelassen)			Nicht getestet																		

1) nur QES, fortgeschrittene Signatur und Authentisierung, keine Ver- und Entschlüsselung mit der TeleSec PKS-ECC Signaturkarte möglich

2) nur QES

3) nur Signatur

4) nur ct-api, Java 32 Bit

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

Tabelle 5: Unterstützte Einsatzumgebungen Terminalserver

Clientbetriebssystem:		Windows XP Prof. SP3 32 Bit 5)
Serverbetriebssystem:		Windows 2003 Server R2 SP2 64 Bit
Terminalserver:		Citrix Metaframe Presentation Server 4.5 Windows Terminal Server 2003

Handelsnamen der Chipkartenlesegeräte mit SigG-Bestätigung/Herstellererklärung	**Chipkartenlesegerät**		**Handelsnamen der Signaturkarten**																		
	Firmware	**Treiber PC/SC**	**TeleSec PKS Classic**	**TeleSec PKS ECC (neu)**	**BNotK Starcos 3.2**	**BnotK Starcos 3.5 (neu)**	**DATEV Starcos 3.2**	**D-Trust Card 2.4**	**D-Trust Card 3.0 (neu)**	**Signtrust Card Starcos 3.2**	**Signtrust Card Starcos 3.5 (neu)**	**TC QSign**	**S-Trust Card**	**dgnSprintCard dgnBusinessCard**	**nPA QES**	**DRV Bund Card OS 3.4b und 5.0**	**BA Card OS 4.3 b und Starcos 3.4**	**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)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
cyberJack® e-com	3.0.69	6.10.8	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
Kobil KAAN Advanced	1.19	2013.1.24.1	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
Omnikey 3821	6.00	1.2.20.0	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓

Clientbetriebssystem:		Windows XP Prof. SP3 32 Bit 5)
Serverbetriebssystem:		Windows 2008 Server Enterprise 32 Bit
Terminalserver:		Windows Terminal Server 2008

Handelsnamen der Chipkartenlesegeräte mit SigG-Bestätigung/Herstellererklärung	**Chipkartenlesegerät**		**Handelsnamen der Signaturkarten**																		
	Firmware	**Treiber PC/SC**	**TeleSec PKS Classic**	**TeleSec PKS ECC (neu)**	**BNotK Starcos 3.2**	**BnotK Starcos 3.5 (neu)**	**DATEV Starcos 3.2**	**D-Trust Card 2.4**	**D-Trust Card 3.0 (neu)**	**Signtrust Card Starcos 3.2**	**Signtrust Card Starcos 3.5 (neu)**	**TC QSign**	**S-Trust Card**	**dgnSprintCard dgnBusinessCard**	**nPA QES**	**DRV Bund Card OS 3.4b und 5.0**	**BA Card OS 4.3 b und Starcos 3.4**	**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)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
cyberJack® e-com	3.0.69	6.10.8	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
Kobil KAAN Advanced	1.19	2013.1.24.1	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
Omnikey 3821	6.00	1.2.20.0	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓

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 (neu)**	**BNotK Starcos 3.2**	**BnotK Starcos 3.5 (neu)**	**DATEV Starcos 3.2**	**D-Trust Card 2.4**	**D-Trust Card 3.0 (neu)**	**Signtrust Card Starcos 3.2**	**Signtrust Card Starcos 3.5 (neu)**	**TC QSign**	**S-Trust Card**	**dgnSprintCard dgnBusinessCard**	**nPA QES**	**DRV Bund Card OS 3.4b und 5.0**	**BA Card OS 4.3 b und Starcos 3.4**	**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)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
cyberJack® e-com plus	3.0.7	CCID V1.4.0-1	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓
cyberJack® RFID komfort kontakt	2.0.7	CCID V1.4.0-1	✓	✓ 1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓ 2)	✓ 3)	✓ 3)	✓

1) nur QES, fortgeschrittene Signatur und Authentisierung, keine Ver- und Entschlüsselung mit der TeleSec PKS-ECC Signaturkarte möglich

2) nur QES

3) nur Signatur

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

5) Der Hersteller stellt seit dem 08. April 2014 keine Sicherheitspatches mehr bereit. Ausgenommen davon sind geschlossene Nutzergruppen, die den kostenpflichtigen erweiterten Support erworben haben. Der Einsatz dieses Betriebssystems sollte nur dann erfolgen, wenn weiterhin die Versorgung mit Sicherheitspatches gewährleistet wird.