GOVERNIKUS

GOVERNIKUS
DATA BOREUM®

Systemanforderungen
Governikus DATA Boreum

Governikus DATA Boreum, Release 10.8.2

© 2023 Governikus GmbH & Co. KG

Inhaltsverzeichnis

1 Anforderungen Arbeitsplatzcomputer

Arbeitsplatzcomputer

Es gelten folgende Voraussetzungen:

- **Arbeitsplatzrechner**:
  - mindestens 4 GB RAM Arbeitsspeicher.
  - mindestens 1 GB Speicherplatz für die Anwendung
- **Rechte**: Auf Windows-Betriebssystemen sind für die Installation und den ersten Start von Governikus DATA Boreum Administrationsrechte erforderlich. Die weitere Benutzung danach erfordert keine Administrationsrechte.
- **Spracheinstellung im System**: Governikus DATA Boreum startet standardmäßig nur bei deutscher Systemspracheinstellung. Hat der Arbeitsplatzcomputer eine andere Systemsprache eingestellt, kann Governikus DATA Boreum über das Setzen des Parameters `-Duser.language=de` in der `ini`-Datei trotzdem gestartet werden.

1.1 Unterstützte Client-Betriebssysteme

Governikus DATA Boreum kann auf den folgenden Betriebssystemen eingesetzt werden.

- **Windows**: Windows 10 und 11
- **macOS**: macOS Ventura
- **Linux Distributionen**: Ubuntu 22.04

Bitte beachten, dass Sie für Windows, Linux und macOS jeweils eigene Installationsdateien zur Verfügung stehen.

1.2 Unterstützung von Terminalservern

Es wurden folgende Kombinationen aus Terminalservern, Serverbetriebssystemen und Clientbetriebssystemen getestet:

Citrix Virtual Apps and Desktops 7 (1811)

- **Client-Betriebssystem**: Windows 10 (SP2)
- **Server-Betriebssystem**: Windows Server 2016 (64 Bit)
- Terminalserver: Citrix Virtual Apps and Desktops 7 (1811)

Citrix XenApp 7.6

- **Client-Betriebssystem**: FUJITSU Thin Client FUTRO S720/S740 eLux RP V6.9.1100-3 mit PC/SC lite V1.8.25-4 (REINER SCT V3.99.5.10-1 und ohne CCID)
- **Server-Betriebssystem**: Windows Server 2016 64 Bit
- **Terminalserver**: Citrix XenApp 7.15

	Detaillierte Informationen zu den unterstützten Kombinationen aus Terminalserver, Chipkartenleser und Betriebssystem finden Sie in Kapitel 3.

1.3 Java Laufzeitumgebung

Bei der Installation von Governikus DATA Boreum (als .MSI) wird eine Java Laufzeitumgebung installiert (aktuell OpenJDK 11). Diese Installation beeinflusst andere, bereits auf Ihrem Computer installierte, Java-Versionen und Programme nicht. Wenn Sie DATA Boreum über das ZIP-Archiv nutzen, muss bereits ein JDK in Version 11 installiert und die `JAVA_HOME`-Systemvariable gesetzt sein.

1.4 Ausstattungsanforderung für das digitale Signieren

Für das digitale Signieren von Dateien benötigen Sie diese Ausstattung:

- Für die Erzeugung **qualifizierter** Signaturen
  - Eine Signaturkarte eines qualifizierten Vertrauensdiensteanbieters.
  - Ein Chipkartenleser (mit PIN-Pad)
- Für die Erstellung **fortgeschrittener** Signaturen:
  - Eine Schlüsselspeicherdatei (Keystore mit Dateiendung `p12`). Dies ist ein Dateiformat das dazu benutzt wird, private Schlüssel mit dem zugehörigen Zertifikat passwortgeschützt zu speichern (häufig auch SW-Zertifikat genannt).
- oder
  - Eine Signaturkarte eines Vertrauensdiensteanbieters, mit der man fortgeschrittene Signaturen erzeugen kann.
- Ein Chipkartenleser (PIN-Pad nicht erforderlich)

Eine Liste aller aktuell unterstützten Signaturkarten und Chipkartenleser ist im nachfolgenden Kapitel aufgeführt.

1.5 Voraussetzung für die Nutzung von Diensten

Governikus DATA Boreum greift für bestimmte Funktionen auf Server-Dienste zu:

- **Validierungsdienst (Certificate Validation Server - CVS)**: Der Validierungsdienst ist erforderlich für die Gültigkeitsprüfung qualifizierter digitaler Zertifikate im Rahmen der Signaturvalidierung. Für diese Prüfung müssen Sie einen CVS des Produkts DATA Varuna verwenden. Dieser Dienst wird von Ihrem Betreiber angeboten. Von der Governikus KG wird dieser Dienst für alle Kunden angeboten, die Governikus DATA Boreum über den Shop nutzen. Dies sind die Konfigurationsdaten für das CVS der Governikus KG:
  - **Server**: `http://cvs.governikus-asp.de/CertificateValidationServer/cvs`
  - **Zertifikat**: Zusätzlich müssen Sie das Zertifikat aus dem Keystore von DATA Varuna in den DATA Boreum Einstellungen hinterlegen. Dieser Keystore ist in der Konfiguration von DATA Varuna hinterlegt. Mit diesem Zertifikat wird die Signatur der Prüfantwort des CVS geprüft.

DATA Boreum kann darüber hinaus folgende Dienste von DATA Deneb nutzen:

- **Zeitstempeldienst**: Anforderung von Zeitstempeln für digitale Signaturen
- **Signaturdienst**: Beauftragung von digitalen Signaturen für große Dateikontingente

Allgemeine Hinweise:

- Die o. g. Dienste müssen über die Serversoftware Governikus Suite zur Verfügung gestellt werden. Bitte fragen Sie Ihren Governikus-Betreiber nach den benötigten Konfigurationsdaten.
- Wenn Sie sich über einen Proxy-Server ins Internet verbinden, müssen Sie die Konfigurationsdaten dieses Proxy-Servers von Ihrem Systemadministrator erfragen und in Governikus DATA Boreum einstellen. Eine Anleitung dazu finden Sie im Handbuch.

1.6 Netzwerkeinstellungen

Bitte leiten Sie die folgenden Informationen ggf. an die Administratorin oder den Administrator weiter, wenn Sie bei der Installation oder bei der Verwendung der Anwendung Schwierigkeiten haben:

- Die gesamte Kommunikation findet über die Ports 80 und 443 statt.
- Von der Anwendung werden die Dienste HTTP, HTTPS, SOCKS und SOAP benötigt.
- Der MIME Type von `.jar` darf nicht verändert werden.
- Es dürfen keine `jar` Dateien gefiltert werden.
- Die HTTP Methode HEAD muss erlaubt sein (ist Standard).
- Bei Verwendung von Proxyservern mit Benutzer-Authentisierung werden folgende Authentisierungsverfahren unterstützt: Basic Authentifizierung, NTLM

Als Hosts sollte folgender Rechner erreichbar sein:

Server	DNS-Name	IP-Adresse
Download-Server	appl.governikus-asp.de	194.31.70.66
Validierungsserver (CVS)	https://cvs.governikus-asp.de/CertificateValidationServer/cvs	

2 Unverbindliche Erläuterung zum End of Lifecycle

Die Pflege der Software Governikus DATA Boreum erfolgt grundsätzlich wie folgt: Ergänzungen neuer Funktionalitäten sowie die Aufrechterhaltung der Funktionsfähigkeit und die Behebung von Fehlern erfolgen immer auf Basis des zuletzt veröffentlichten Release-Standes. Eine Anpassung vorausgegangener Releases erfolgt nicht.

Die Aufrechterhaltung der Funktionsfähigkeit sowie die Behebung von nutzungsverhindernden Fehlern erfolgt immer für die letzte Major-Version (x.0.0) oder Minor-Version (y.x.0). Die Lieferung von Hotfixes bzw. Umgehungen, Patches und Updates erfolgt dabei auf Basis des jeweils zuletzt veröffentlichten Patches (y.y.x) oder Minor-Version (y.y.x). Die Governikus KG stellt sicher, dass Patches abwärtskompatibel sind.

Für alle Editionen von Governikus DATA Boreum gilt ferner Folgendes:

Als Voraussetzung für die Pflege der Software gilt, dass Codeänderungen nur erfolgen können, solange rechtliche Rahmenbedingungen, Spezifikationen oder Normen keine massive Änderung erfordern, die mit vertretbarem Aufwand nur in neueren Systemen möglich sind und nur, solange die eingesetzte Software von Drittherstellern unterstützt wird, beziehungsweise solange Verfahren für Konformitätsnachweis, Evaluierung und Bestätigung gültig sind.

Diese Erläuterung ist für beide Seiten unverbindlich und wird nicht Bestandteil eines neuen oder bestehenden Vertrages. Vielmehr stellt sie klar, wie die Governikus KG den End of Lifecycle für die genannte Software plant. In dieser Detailierung ist diese Frage nicht in den Verträgen behandelt und verstößt somit auch nicht gegen diese. Es mag zukünftig Gründe geben, die heute nicht bekannt sind, aus denen die Governikus KG von diesen Regeln abweichen sollte oder muss.

3 Unterstützte Signaturkarten und Chipkartenleser

Im Folgenden sind die unterstützten Chipkartenleser, die unterstützten Signaturkarten sowie die unterstützten Kombinationen von Betriebssystem, Chipkartenleser und Signaturkarten aufgeführt. Diese Unterstützung wird durch eine Komponente der Governikus KG erbracht. Die hier verwendete Version ist:

MCard Release 2.11.0

Einleitung

Mit dieser Anwendung können Dokumente qualifiziert elektronisch signiert werden. Dafür werden eine geeignete Signaturkarte und ein technisch unterstützter Chipkartenleser benötigt. Es können fast alle

- Chipkartenleser verwendet werden, die in Deutschland für die Erzeugung einer qualifizierten elektronischen Signatur (QES) nach dem Signaturgesetz zugelassen waren. Seit dem 01.07.2016 gilt in Deutschland die eIDAS-Verordnung, die keine Zertifizierung mehr von geeigneten Chipkartenlesern regelt.
- Qualifizierte Signatur- und Siegelerstellungseinheiten (QSCD) verwendet werden, die durch qualifizierte Vertrauensdiensteanbieter aus Deutschland herausgegeben werden und mit denen man eine QES erzeugen kann.

3.1 Aktuelle Hinweise

Diese MCard-Version enthält im Vergleich zur Vorversion folgende Änderungen.

- Unterstützung neue D-Trust Card 5.1 (Ausprägung Standard, M100 und Multi)
- Unterstützung neue D-Trust Card 5.4 (Ausprägung Standard und Multi)

	**Hinweis**: Für die Nutzung der neuen Karten mit bestimmten Modellen des Lesegeräteherstellers Reiner SCT gibt es Einschränkungen. Weitere Informationen können den Tabellen 4a bis 4c sowie 5a und 5b entnommen werden. In Kürze werden durch den Hersteller neue Treiber bereitgestellt.

- Diese Version der MCard wurde in Java 11 kompiliert und ist unter Java 17 lauffähig.

Der in dieser Version eingesetzte Crypto-Provider lautet Bouncy Castle V1.76.

3.2 Abkündigungen

Die folgenden Chipkartenlesegeräte, Signaturkarten und Betriebssysteme werden mit diesem Release der MCard abgekündigt und können mit der nächsten Version der MCard nicht mehr verwendet werden.

- Ab der kommenden Version der MCard wird die Funktion Verschlüsselung mit Signaturkarte nicht mehr unterstützt.

3.3 Hinweis zu Änderungen getesteter Produkte

Alle in diesem Dokument gelisteten Karten und Chipkartenleser 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 Produktes führen. Die Governikus GmbH & Co. KG kann für derartige Funktionseinschränkungen, Fehler und dadurch verursachte Schadensverläufe nicht verantwortlich gemacht werden.

3.4 Notwendige Schutzvorkehrungen für diese Anwendung

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, 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 Sicherheits-Patches 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 Chipkartenleser 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 qualifizierten Vertrauensdiensteanbieter zum Umgang mit der persönlichen, geheimen Signatur-PIN sind ebenso zu beachten.

3.5 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 Sicherheits-Patches 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 Sicherheits-Patches 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 Sicherheits-Patches 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 - Chipkartenleser - Signaturkarte

Bitte beachten Sie bei der Auswahl des Betriebssystems: Die Funktionsfähigkeit der unterstützten Chipkartenleser (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 Chipkartenleser 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).

3.6 Unterstützte Siegel- und Signaturkarten

Siegelkarten für eine qualifizierte elektronische Signatur (QES)

Mit dieser Anwendung können Sie die von deutschen qualifizierten Vertrauensdiensteanbietern herausgegebenen Siegelkarten verwenden. Die Liste mit den unterstützten Siegelkarten ist der Tabelle „Unterstützte Siegelkarten geeignet für eine qualifizierte Signatur (QES)“ (Tabellen 2a) zu entnehmen. Die Siegelkarten erlauben nur die Erzeugung von qualifizierten Signaturen.

Signaturkarten für eine qualifizierte elektronische Signatur (QES)

Ebenfalls mit dieser Anwendung können Sie die meisten von qualifizierten Vertrauensdiensteanbietern herausgegebenen Signaturkarten aus Deutschland verwenden. Die Listen mit den unterstützten Signaturkarten für eine qualifizierte elektronische Signatur sind den Tabellen „Unterstützte Signaturkarten geeignet für eine qualifizierte Signatur (QES)“ (Tabellen 2b und 2c) 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 und durch diese Anwendung nicht eingeschränkt werden.

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 254 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.

Siegelkarten, die durch deutsche qualifizierte Vertrauensdiensteanbieter herausgegeben werden, können in den Ausprägungen Einzel- und Multisignatur verwenden werden.

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

Die unterstützten Signaturkarten müssen sich im Originalzustand befinden, d.h. so, wie sie durch den qVDA herausgegeben und zugestellt wurden. Es gibt eine Ausnahme: Wird von einem qVDA eine dezentrale Personalisierung einer Original-Signaturkarte angeboten, also das Nachladen von qualifizierten Zertifikaten, wird die Signaturkarte weiterhin unterstützt. 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 2d) zu entnehmen.

Unterstützte Kombinationen: Betriebssystem - Chipkartenleser - Signaturkarte

Die Funktionsfähigkeit der in den Tabellen aufgeführten Signaturkarten mit dieser Anwendung wurde für die in den Tabellen „Unterstützte Chipkartenleser“ aufgeführten Chipkartenleser 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 Chipkartenleser 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 Chipkartenleser. Abweichend davon kann es technisch bedingte Einschränkungen geben. Im Anwendungsfall ist stets die gemeinsame Schnittmenge der unterstützten PIN-Längen von Signaturkarte, Chipkartenleser und dieser Anwendung maßgeblich.

Beispiel PIN-Längen

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

Wichtiger Hinweis zu PIN-Längen

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 Chipkartenlesers. Oder fragen Sie den Herausgeber Ihrer Signaturkarte oder den Hersteller Ihres Chipkartenlesers, 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 Fehler bei PIN-Eingabe

Die richtige alte PIN ist 123456. Der Benutzer gibt aber versehentlich für die alte PIN 123456**66** ein, weil die Tastatur des Chipkartenlesers 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.

3.7 Unterstützte Chipkartenleser

Mit dieser Anwendung können fast alle Chipkartenleser mit Tastatur (PIN-Pad) und ausgewählte Chipkartenleser ohne PIN-Pad verwendet werden.

Für eine QES technisch unterstützte Chipkartenleser

Alle technisch unterstützten Chipkartenleser werden über ihre eigene USB-Schnittstelle an den PC angeschlossen. Die Verbindung vom PC zum Chipkartenleser wird über einen PC/SC-Treiber hergestellt, der zu installieren ist. Bitte informieren Sie sich beim Hersteller des Chipkartenlesers, wie der Treiber zu installieren ist. Im Kapitel 5.1 ist die Installation eines Chipkartenlesers unter Linux beschrieben.

Die Listen mit den für technisch unterstützten Chipkartenlesern sind den Tabellen „unterstützte Chipkartenleser“ (Tabellen 3a und 3b) zu entnehmen. Nach dem Signaturgesetz durften für eine QES nur die dort aufgeführten Chipkartenleser verwendet werden (mindestens HBCI-Klasse 2). Seit dem 01.07.2016 gilt in Deutschland die eIDAS-Verordnung, die keine Zertifizierung von geeigneten Chipkartenlesern regelt. Die Chipkartenleser (in Tabelle 3a und 3b) werden mit dieser Anwendung technisch unterstützt.

Es kann darüber hinaus keine Gewährleistung dafür übernommen werden, dass

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

Chipkartenleser ohne Pin-Pad

Diese Anwendung unterstützt auch Chipkartenleser, die keine sichere PIN-Eingabe erlauben (HBCI-Klasse 1). Es handelt sich ausschließlich um Geräte mit USB-Schnittstelle, die über einen PC/SC-Treiber angesprochen werden. Die Liste der unterstützten Chipkartenleser ohne PIN-Pad ist der Tabelle „Unterstützte Chipkartenleser ohne PIN-Pad“ (Tabelle 3c) zu entnehmen.

Neben diesen Geräten können auch viele weitere Chipkartenleser mit USB-Schnittstelle ohne PIN-Pad oder interne Chipkartenleser 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.

Unterstützte Kombinationen: Betriebssystem - Chipkartenleser - Signaturkarte

Die Funktionsfähigkeit der aufgeführten Chipkartenleser mit dieser Anwendung wurde für die in der Tabelle „unterstützte Betriebssysteme“ aufgeführten Betriebssysteme mit den bei den Herstellern der Chipkartenleser 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 Chipkartenleser 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).

3.8 Installation von Chipkartenleser unter Linux

Anders als bei Windows Client-Betriebssysteme, bei denen für die Installation eines Chipkartenlesers in der Regel der Windows Plug & Play Mechanismus oder ein Installationsprogramm des Herstellers verwendet wird, müssen unter Linux-Distributionen zuerst einige Vorbereitung für die Installation getroffen werden, die im Folgenden beschrieben sind.

Einrichten von PC/SC auf dem System

Das Linux-System muss für die standardisierte PC/SC-Schnittstelle vorbereitet werden, damit Chipkartenleser unterstützt werden. Geben Sie zum Installieren von `libpcsclite1` folgenden Befehl ein:

```
sudo apt-get install libpcsclite1
```

Geben Sie zum Installieren von `pcscd` folgenden Befehl ein:

```
sudo apt-get install pcscd
```

Installieren von libccid

Mit der Installation des PC/SC-Daemons wird üblicherweise auch `libccid` installiert. Ist dies nicht der Fall und `libccid` wird benötigt, kann diese auch manuell installiert mit diesem Befehl werden:

```
sudo apt-get install libccid
```

Prüfen Sie mit dem Debug-Modus des PC/SC-Daemons, ob PC/SC korrekt eingerichtet wurde und dass das gewünschte Chipkartenlesegerät erkannt wird. Um den PC/SC-Daemon für die Überprüfung im Debug-Modus zu starten, muss dieser evtl. zuerst gestoppt werden:

So erhalten Sie einen Überblick über die Services:

```
sudo service --status-all
```

Gibt es einen Eintrag `[+] pcscd`, dann läuft der Daemon bereits. So können Sie den Sie den Daemon stoppen:

```
sudo service pcscd stop
```

So starten Sie den Daemon im Debug-Modus:

```
sudo pcscd –adf
```

Jetzt wird auf der Konsole die Ausgabe des PC/SC-Daemons angezeigt. Schließen Sie diese Konsole nicht. Beim Einstecken des Chipkartenlesegerätes sollte dieses erkannt und erfolgreich initialisiert werden. Nach dem Einstecken der Signaturkarte sollte diese ebenfalls erkannt werden.

Stoppen des PC/SC-Daemons

Bei Bedarf kann der Daemon wieder mit `CTRL + C` im aktiven Konsolenfenster oder mit

```
sudo service pcscd stop
```

innerhalb eines zweiten Konsolenfensters gestoppt werden.

Um den Daemon wieder normal zu starten (für den allgemeinen Betrieb) geben Sie diesen Befehl ein:

```
sudo pcscd
```

3.9 Unterstützte Kombinationen: Betriebssystem - Chipkartenleser - Signaturkarte

In der Regel werden alle Kombinationen der in den Listen benannten Betriebssysteme, Chipkartenleser 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 Chipkartenleser 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 Chipkartenlesers für ein bestimmtes Betriebssystem bereitgestellt. Oder es liegt eine technische Inkompatibilität von Chipkartenleser und Signaturkarte vor.

Prüfen Sie daher bitte, ob Ihre Signaturkarte in Kombination mit Ihrem Chipartenleser 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 Chipkartenlesers 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 Chipkartenleser (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 Chipkartenleser.

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	Java-Version	Abkündigung
Microsoft Windows 10 64 Bit	Java 11 Update 20	Der Hersteller stellt zweimal pro Jahr ein Funktionsupdate zur Verfügung. Der Service für die Editionen beträgt 18 bzw. 30 Monate ab Freigabedatum (je nach Ausprägung). Weitere Information sind unter https://support.microsoft.com/de-de/help/13853/windows-lifecycle-fact-sheet zu entnehmen. Nach Ablauf der Servicezeit wird ein Funktionsupdate von Windows 10 nicht mehr unterstützt.
Microsoft Windows 11 64 Bit	Java 11 Update 20	Der Hersteller stellt zweimal pro Jahr ein Funktionsupdate zur Verfügung. Der Service für die Editionen beträgt 24 bzw. 36 Monate ab Freigabedatum (je nach Ausprägung). Weitere Information sind unter https://support.microsoft.com/de-de/help/13853/windows-lifecycle-fact-sheet zu entnehmen. Nach Ablauf der Servicezeit wird ein Funktionsupdate von Windows 11 nicht mehr unterstützt.
Linux Ubuntu 22.04 LTS 64 Bit	Java 11 Update 21	Die LTS-Distribution wird für zwei Jahre ab Veröffentlichungszeitpunkt unterstützt. Mit Erscheinen der neuen LTS-Version unterstützt die MCard die Vorversion nicht mehr.
Apple macOS Sonoma	Java 11 Update 20 Temurin-11.0.20+8	Der Hersteller veröffentlicht einmal jährlich eine kostenlose Folgeversion. Mit Erscheinen der neuen Version wird die Vorversion durch die MCard nicht mehr unterstützt..

Tabelle 2a: Unterstützte Chipkarten geeignet für qualifizierte Siegel

Qualifizierter Vertrauensdienste-anbieter	Handelsname der Chipkarte	Schlüssel-verwendung	Name der QSCD 1) in der Zertifizierungsurkunde	Zertifizierungsurkunde
D-Trust GmbH	D-TRUST Card 4.4a	QES	CardOS DI V5.4 QES Version 1.0	BSI-DSZ-CC-1112-2020
	D-TRUST Card 4.4a Multicard 2)			
	D-TRUST Card 5.4		CardOS V6.0 ID R1.1	BSI-DSZ-CC-1162-V2-2023 Nachtrag noch nicht veröffentlicht.
	D-TRUST Card 5.4 Multicard 2)			

1) Qualified Signature Creation Device (QSCD)

2) Multisiegelkarte. 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.

Tabelle 2b: Unterstützte Signaturkarten geeignet für eine qualifizierte Signatur

Qualifizierter Vertrauensdienste-anbieter	Handelsname der Chipkarte	Schlüssel-verwendung	Name der QSCD 1) in der Zertifizierungsurkunde	Zertifizierungsurkunde
Deutsche Telekom Security GmbH	Signaturkarte Light	Authentisierung Verschlüsselung QES	Qualified Signature / Seal Creation Device TCOS 3.0 Signature Card, Version 2.0 Release 2/SLE78CLX1440P	SRC.00032.QSCD.12.2018
	Signaturkarte Standard			
	Multisignaturkarte 3)			
D-Trust GmbH	D-TRUST Card 4.1a Standard	Authentisierung Verschlüsselung QES	CardOS DI V5.4 QES Version 1.0	BSI-DSZ-CC-1112-2020
	D-TRUST Card 4.1a Multi 100 2)			
	D-TRUST Card 4.1a Multi 3)			
	D-TRUST Card 4.1a UPC			
	D-TRUST Card 5.1 Standard		CardOS V6.0 ID R1.1	BSI-DSZ-CC-1162-V2-2023
	D-TRUST Card 5.1 Multi 100 2)			
	D-TRUST Card 5.1 Multi 3)			

Qualifizierter Vertrauensdienste-anbieter	Handelsname der Chipkarte	Schlüssel-verwendung	Name der QSCD 1) in der Zertifizierungsurkunde	Zertifizierungsurkunde
DGN Service	sprintCard businessCard 4)	Authentisierung Verschlüsselung QES	Qualified Signature Creation Device STARCOS 3.7 HBA G2.1 (R2)	SRC.000047.QSCD.06.2022
D-TRUST GmbH Medisign Deutsche Telekom AG	Elektronischer Heilberufsausweis (eHBA)	Authentisierung Verschlüsselung QES	Qualified Signature Creation Device STARCOS 3.7 HBA G2.1 (R2)	SRC.000047.QSCD.06.2022

1) Qualified Signature Creation Device (QSCD)

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) 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.

4) 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 254 QES im Batchverfahren möglich. Die Karten funktionieren nur kontaktbehaftet. Die Verschlüsselungsfunktionalität wird nur für die RSA-Schlüssel unterstützt.

Tabelle 2c: andere unterstützte Signaturkarten

Vertrauensdienste-anbieter	Handelsname der Chipkarte	Schlüssel-verwendung	Name der SSCD 1)	Bemerkungen
Bundesnotarkammer, Zertifizierungsstelle	beA-Karte Mitarbeiter	Authentisierung Verschlüsselung	Java Card Open Platform (JCOP)	--
Bundesnotarkammer, Zertifizierungsstelle	Justiz-Paket R-Karte zur Authentisierung Fernsignatur	Authentisierung Verschlüsselung	Java Card Open Platform (JCOP)	--
Europäisches Patentamt – European Patent Office (EPO)	Online Services Smart Card Epoline	Fortgeschrittene Signatur	--	--

Tabelle 3a: Technisch unterstützte Chipkartenleser

Handelsname des Geräts	Hersteller	Angaben zur technischen Unterstützung	Zertifizierungsurkunde	PIN-Pad	Standard	Schnittstelle	
						PC	Karte
Cherry Smartboard 1.0	Cherry GmbH	Chipkartenleser der Sicherheitsklasse 2	-	ja	PC/SC	USB	kontakt
Cherry SmartTerminal 2100	Cherry GmbH	Chipkartenleser der Sicherheitsklasse 2	-	ja	PC/SC	USB	kontakt
Cherry KC 1000 SC-Z	Cherry GmbH	FW-Version 2.2.0	BSI-DSZ-CC-0970-V2-2018	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 komfort FON	Reiner SCT Kartenlesegeräte GmbH	Barrierefreier Chipkartenleser der Sicherheitsklasse 3	-	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
CyberJack one	Reiner SCT Kartenlesegeräte GmbH	Chipkartenleser der Sicherheitsklasse 3	-	ja	PC/SC	USB	kontakt
SPR 332 usb (Chipdrive pinpad pro)	IDENTIVE GmbH	Chipkartenleser SPR332, Firmware Version 6.01	BSI.02117.TE.02.2010	ja	PC/SC	USB	kontakt
ORGA 930 Care	Worldline Healthcare GmbH	Für den Offline-Betrieb geeignet	Keine Gematik-Zulassung	ja	PC/SC	USB	kontakt

Tabelle 3b: Technisch unterstützte Chipkartenleser mit CT-API-Schnittstelle

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

Tabelle 3c: Unterstützte Chipkartenleser ohne PIN-Pad (Auswahl)

Handelsname des Geräts	Hersteller	PIN-Pad	Standard	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

Handelsname des Geräts	Hersteller	PIN-Pad	Standard	Schnittstelle	
				PC	Karte
Cherry ST-1275	ZF Electronics GmbH	nein	PC/SC	USB	kontakt, kontaktlos 1)
CLOUD 4700 F Dual Interface USB Desktop Reader	IDENTIVE GmbH	nein	PC/SC	USB	kontakt, kontaktlos 1)
CLOUD 2700 F Contact Smart Card Reader	IDENTIVE GmbH	nein	PC/SC	USB	kontakt

1) nicht unterstützt

Tabelle 4a: Unterstützte Kombinationen Windows Betriebssysteme - Chipkartenleser - Signaturkarte

Handelsnamen der technisch unterstützten Chipkartenleser mit Pin-Pad	Microsoft Windows 5)		Handelsnamen der Signaturkarten							
	Firmware	Treiber PC/SC	beA-Mitarbeiter 3)	Bundesnotarkammer R-Karte für Fernsignatur 3)	DGN sprintCard DGN businessCard	D-Trust Card 4.1a, 4.1a UPC, 4.4a	D-Trust Card 5.1, 5.4	EPO-Karte 2)	eHBA G2.1	TeleSec Qualified ID
Cherry® Secure Smartboard 1.0	N/A	5.0.4	✓	✓	✓	✓4)	✓4) 6)	✓	✓	✓1)
Cherry® ST-2100	7.10	4.57.0.1	✓	✓	✓	✓4)	✓4) 6)	✓	✓	✓1)
Cherry® KC 1000 SC-Z	2.0.0	1.0.5.152	✓	✓	✓	✓4)	✓4)	✓	✓	✓1)
cyberJack® one	1.2.11	Driver Package 1.2.0	✓	✓	✓	✓4)	✓4) 6)	✓	✓	✓1)
cyberJack® secoder	3.0.28	Driver Package 1.2.0	✓	✓	✓	✓4)	✓4) 6)	✓	✓	✓1)
cyberJack® RFID standard kontakt	1.2.60	Driver Package 1.2.0	✓	✓	✓	✓4)	✗ 7)	✓	✓	✓1)
cyberJack® RFID komfort kontakt	2.0.46	Driver Package 1.2.0	✓	✓	✓	✓4)	✗ 7)	✓	✓	✓1)
cyberJack® RFID komfort FON kontakt	2.0.37	Driver Package 1.2.0	✓	✓	✓	✓4)	✗ 7)	✓	✓	✓1)
cyberJack® RFID standard kontaktlos	1.2.60	Driver Package 1.2.0	✓	✓	-	-	✗ 7)	-	-	✓1)
cyberJack® RFID komfort kontaktlos	2.0.46	Driver Package 1.2.0	✓	✓	-	-	✗ 7)	-	-	✓1)
cyberJack® RFID komfort FON kontaktlos	2.0.37	Driver Package 1.2.0	✓	✓	-	-	✗ 7)	-	-	✓1)
SPR 332 V2	7.06	4.57.0.1	✓	✓	✓	✓4)	✓4) 6)	✓	✓	✓1)
ORGA 930 Care	5.3.0	3.0.0.0	-	-	-	-	-	-	-	-
In Tabelle 3c aufgeführte Geräte ohne PIN-Pad			✓	✓	✓	✓4)	✓4)	✓	✓	✓1)

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

2) Nur fortgeschrittene Signatur

3) Nur Authentisierung

4) D-TRUST Card 4.4 und 5.4 (Siegelkarte) nur QES

5) Die unterstützten Windows-Betriebssysteme sind der Tabelle 1 zu entnehmen

6) Pin-Eingabe nur Klasse 1 möglich

7) Aktualisierter Treiber mit Unterstützung dieser Geräteklasse ist noch nicht verfügbar

Tabelle 4b: Unterstützte Kombinationen Ubuntu 22.04 LTS (64 Bit) - Chipkartenleser - Signaturkarte

Handelsnamen der technisch unterstützten Chipkartenleser mit Pin-Pad	Ubuntu 22.04 LTS		Handelsnamen der Signaturkarten							
	Firmware	PCSC-lite Version 1.9.5-3	beA-Mitarbeiter 3)	Bundesnotarkammer R-Karte für Fernsignatur 3)	DGN sprintCard DGN businessCard	D-Trust Card 4.1, 4.1 UPC, 4.4	D-Trust Card 5.1, 5.4	EPO-Karte 2)	eHBA G2.1	TeleSec Qualified ID
Cherry® Secure Smartboard 1.0	N/A	CCID 1.5.0-2 5)	✓6)	✓6)	✓6)	✓4) 6)	✓4) 6)	✓6)	✓6)	✓1) 6)
Cherry® ST-2100	7.10	CCID 1.5.0-2 5)	✓	✓	✓6)	✓4) 6)	✓4) 6)	✓6)	✓6)	✓1) 6)
Cherry® KC 1000 SC-Z	2.0.0	CCID 1.5.0-2 5)	✓6)	✓6)	✓6)	✓4) 6)	✓4) 6)	✓6)	✖	✓1) 6)
cyberJack® one	1.2.11	3.99.5final.sp15 amd64	✓	✓	✓	✓4)	✓4) 6)	✓	✓	✓1)
cyberJack® secoder	3.0.28	3.99.5final.sp15 amd64	✓	✓	✓	✓4)	✓4) 6)	✓	✓	✓1)
cyberJack® RFID standard kontakt	1.2.60	3.99.5final.sp15 amd64	✓	✓	✓	✓4)	✖ 7)	✓	✓	✓1)
cyberJack® RFID komfort kontakt	2.0.46	3.99.5final.sp15 amd64	✓	✓	✓	✓4)	✖ 7)	✓	✓	✓1)
cyberJack® RFID komfort FON kontakt	2.0.37	3.99.5final.sp15 amd64	✓	✓	✓	✓4)	✖ 7)	✓	✓	✓1)
cyberJack® RFID standard kontaktlos	1.2.60	3.99.5final.sp15 amd64	✓	✓	✓	-	✖ 7)	-	-	✓1)
cyberJack® RFID komfort kontaktlos	2.0.46	3.99.5final.sp15 amd64	✓	✓	✓	-	✖ 7)	-	-	✓1)
cyberJack® RFID komfort FON kontakt	2.0.28	3.99.5final.sp15 amd64	✓	✓	✓	-	✖ 7)	-	-	✓1)
SPR 332 V2	7.06	CCID 1.4.31-1	✓	✓	✓	✓4)	✓4) 6)	✓	✓	✓1)
ORGA 930 Care	5.3.0	Kein Treiber verfügbar	-	-	-	-	-	-	-	-
In Tabelle 3c aufgeführte Geräte ohne PIN-Pad			✓	✓	✓	✓4)	✓4)	✓	✓	✓1)

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

2) Nur fortgeschrittene Signatur

3) Nur Authentisierung

4) D-TRUST Card 4.4 und 5.4 (Siegelkarte) nur QES

5) Es muss der Name im generischen CCID-Treiber mit * angeführt werden

6) Pin-Eingabe nur Klasse 1 möglich

7) Aktualisierter Treiber steht noch nicht zum Download bereit

Tabelle 4c: Unterstützte Kombinationen macOS Sonoma - Chipkartenleser - Signaturkarte

Handelsnamen der technisch unterstützten Chipkartenleser mit Pin-Pad	macOS Ventura		Handelsnamen der Signaturkarten							
	Firmware	PCSC-lite Version 11	beA-Mitarbeiter 3)	Bundesnotarkammer R-Karte für Fernsignatur 3)	DGN sprintCard DGN businesCard	D-Trust Card 4.1, 4.1 UPC, 4.4	D-Trust Card 5.1, 5.4	EPO-Karte 2)	eHBA G2.1	TeleSec Qualified ID
Cherry® Secure Smartboard 1.0	N/A	Kein Treiber verfügbar	-	-	-	-	-	-	-	-
Cherry® ST-2100	7.10	scmccid 5.0.41	✓5)	✓5)	✓5)	✓5)	✓5)	✓5)	✓5)	✓1) 5)
Cherry® KC 1000 SC-Z	2.0.0	scmccid 5.0.41	✓5)	✓5)	✓5)	✓4) 5)	✓4) 5)	✓5)	✓5)	✓1) 5)
cyberJack® one	1.2.11	pcsc-cyberJack 3.99.5 sp15	✓	✓	✓	✓4)	✓4) 5)	✓	✓	✓1)
cyberJack® secoder	3.0.28	pcsc-cyberJack 3.99.5 sp15	✓	✓	✓	✓4)	✓4) 5)	✓	✓	✓1)
cyberJack® RFID standard kontakt	1.2.60	pcsc-cyberJack 3.99.5 sp15	✓	✓	✓	✓4)	✖ 6)	✓	✓	✓1)
cyberJack® RFID komfort kontakt	2.0.46	pcsc-cyberJack 3.99.5 sp15	✓	✓	✓	✓4)	✖ 6)	✓	✓	✓1)
cyberJack® RFID komfort FON kontakt	2.0.37	pcsc-cyberJack 3.99.5 sp15	✓	✓	✓	✓4)	✖ 6)	✓	✓	✓1)
cyberJack® RFID standard kontaktlos	1.2.60	pcsc-cyberJack 3.99.5 sp15	✓	✓	✓	-	✖ 6)	-	-	✓1)
cyberJack® RFID komfort kontaktlos	2.0.46	pcsc-cyberJack 3.99.5 sp15	✓	✓	✓	-	✖ 6)	-	-	✓1)
cyberJack® RFID komfort FON kontakt	2.0.28	pcsc-cyberJack 3.99.5 sp15	✓	✓	✓	-	✖ 6)	-	-	✓1)
SPR 332 V2	7.06	scmccid 5.0.41	✓5)	✓5)	✓5)	✓4) 5)	✓4) 5)	✓5)	✓5)	✓1) 5)
ORGA 930 Care	5.3.0	-	-	-	-	-	-	-	-	-
In Tabelle 3c aufgeführte Geräte ohne PIN-Pad			Nicht getestet							

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

2) Nur fortgeschrittene Signatur

3) Nur Authentisierung

4) D-TRUST Card 4.4 und 5.4 (Siegelkarte) nur QES

5) Pin-Eingabe nur Klasse 1 möglich

6) Aktualisierter Treiber steht noch nicht zum Download bereit

Tabelle 5a: Unterstützte Einsatzumgebungen Terminalserver

Clientbetriebssystem:	Windows 10 1)					
Serverbetriebssystem:	Windows Server 2016 64 Bit					
Terminalserver:	Citrix Virtual Apps and Desktops 7 (1811)					
Handelsnamen der technisch unterstützten Chipkartenleser mit Pin-Pad	**Chipkartenleser**		**Handelsnamen der Signaturkarten**			
	Firmware	**Treiber PC/SC**	**BNotK R-Karte für Fernsignatur 3)** **beA-Mitarbeiter 3)**	**D-Trust Card 4.1, 4.1 UPC, 4.4**	**D-Trust Card 5.1, 5.4**	**DGN sprintCard** **DGN businessCard**
Cherry® ST-2100	7.10	4.57.0.1	✓	✓ 2)	✓ 2)	✓
Cherry® KC 1000 SC-Z	2.0.0	1.0.5.152	✓	✓ 2)	✓2)	✓
cyberJack® secoder	3.0.28	Driver Package 1.2.0	✓	✓ 2)	✓ 2) 4)	✓
cyberJack® RFID standard kontakt	1.2.60	Driver Package 1.2.0	✓	✓ 2)	✖ 5)	✓
cyberJack® RFID komfort kontakt	2.0.46	Driver Package 1.2.0	✓	✓ 2)	✖ 5)	✓
SPR 332 V2	7.06	4.57.0.1	✓	✓ 2)	✓ 2)	✓

1) Der Hersteller stellt zweimal pro Jahr ein Funktionsupdate von Windows 10 zur Verfügung. Der Service für die Editionen beträgt 18 bzw. 30 Monate ab Freigabedatum (je nach Ausprägung).
Weitere Information sind unter https://support.microsoft.com/de-de/help/13853/windows-lifecycle-fact-sheet zu entnehmen. Nach Ablauf der Servicezeit wird ein Funktionsupdate von Windows 10 nicht mehr unterstützt.

2) D-TRUST Card 4.4 und 5.4 nur QES

3) Nur Authentisierung

4) Pin-Eingabe nur Klasse 1 möglich

5) Aktualisierter Treiber mit Unterstützung dieser Geräteklasse ist noch nicht verfügbar

Tabelle 5b: Unterstützte Einsatzumgebungen Terminalserver

Clientbetriebssystem:	FUJITSU Thin Client FUTRO S720/S740 eLux RP V6.9.1100-3 mit PC/SC lite V1.8.25-4 (REINER SCT V3.99.5.10-1 und ohne CCID)			
Serverbetriebssystem:	Windows Server 2016 64 Bit			
Terminalserver:	Citrix XenApp 7.15			
Handelsnamen der technisch unterstützten Chipkartenleser mit Pin-Pad	**Chipkartenleser**		**Handelsnamen der Signaturkarten**	
	Firmware	**Treiber PC/SC 1)**	**D-TRUST 4.1, 4.1 UPC, 4.4**	**D-TRUST 5.1, 5.4**
cyberJack® e-com plus	3.0.80	pcsc-cyberJack 3.99.5 sp15	✓ 2)	✓ 2) 3)
cyberJack® standard kontakt	1.2.60	pcsc-cyberJack 3.99.5 sp15	✓ 2)	✗ 2) 4)
cyberJack® komfort kontakt	2.0.46	pcsc-cyberJack 3.99.5 sp15	✓ 2)	✗ 2) 4)

1) Bei generischen CCID-Treibern muss der Name des Lesers mit * angeführt werden
2) D-TRUST Card 4.4 (Siegelkarte) nur QES
3) Pin-Eingabe nur Klasse 1 möglich
4) Aktualisierter Treiber mit Unterstützung dieser Geräteklasse ist noch nicht verfügbar