Administration Intelligence AG

Unterstützte Signaturkarten und Kartenlesegeräte

Version MCard 3.4.1

© 2026 Administration Intelligence AG, Würzburg

Inhaltsverzeichnis

Änderungsverzeichnis 4

1 Einleitung 5
1.1 Aktuelle Hinweise 5
1.2 Abkündigungen 5
1.3 Hinweis zu Änderungen getesteter Produkte 5

2 Notwendige Schutzvorkehrungen für diese Anwendung 7

3 Unterstützte Betriebssysteme und JRE 9
Unterstützte Kombinationen: Betriebssystem - Chipkartenleser - Signaturkarte 9

4 Unterstützte Siegel- und Signaturkarten 10
Siegelkarten für eine qualifizierte elektronische Signatur (QES) 10
Signaturkarten für eine qualifizierte elektronische Signatur (QES) 10
Andere Signaturkarten 10
eToken 10
Unterstützte Kombinationen: Betriebssystem - Chipkartenleser - Signaturkarte 11
PIN-Management der unterstützten Signaturkarten 11
Beispiel PIN-Längen 11
Wichtiger Hinweis zu PIN-Längen 11
Beispiel Fehler bei PIN-Eingabe 11

5 Unterstützte Chipkartenleser 12
Für eine QES technisch unterstützte Chipkartenleser 12
Chipkartenleser ohne Pin-Pad 12
Unterstützte Kombinationen: Betriebssystem - Chipkartenleser - Signaturkarte 12
5.1 Installation von Chipkartenleser unter Linux 13
Einrichten von PC/SC auf dem System 13
Installieren von libccid 13
Stoppen des PC/SC-Daemons 13

6 Unterstützte Kombinationen: 14

Betriebssystem - Chipkartenleser - Signaturkarte 14
Unterstützte Terminalserver 14
Tabelle 1: Unterstützte Betriebssysteme und JRE 15
Tabelle 2a: Unterstützte Chipkarten geeignet für qualifizierte Siegel 16
Tabelle 2b: Unterstützte Signaturkarten geeignet für eine qualifizierte Signatur 17
Tabelle 2c: andere unterstützte Signaturkarten 19
Tabelle 3: Technisch unterstützte eToken (USB) 20
Tabelle 4a: Technisch unterstützte Chipkartenleser 21
Tabelle 4b: Unterstützte Chipkartenleser ohne PIN-Pad (Auswahl) 22
Tabelle 5a: Unterstützte Kombinationen Windows Betriebssysteme - Chipkartenleser - Signaturkarte 23
Tabelle 5b: Unterstützte Kombinationen Ubuntu 26.04 LTS (64 Bit) - Chipkartenleser - Signaturkarte 25

© 2026 Administration Intelligence AG, Würzburg

Tabelle 5c: Unterstützte Kombinationen macOS Golden Gate - Chipkartenleser - Signaturkarte 27
Tabelle 6a: Unterstützte Einsatzumgebungen Terminalserver 29
7 Impressum 31

Änderungsverzeichnis

Version	Datum	Bearbeiter	Beschreibung der Änderung
3.4.1	25.09.2026	TN	Änderungen am Kap. 1.1, 1.2, 4 sowie Tabellen 1 - 6b
2.12.5	27.11.2024	TN	Änderungen am Kap. 1.1 und Tabellen 2a bis 2c.
2.12.4	15.11.2024	TN	Änderungen am Kap. 1.1 und 1.2 sowie Tabellen 1, 4a bis 4c, 5a und 5b.
2.12.3	17.07.2024	JW, AWA	Bouncy Castle auf Version 1.78.1 erhöht
2.12.2	12.07.2024	TN	Änderungen am Kap. 1.1, Tabelle 2c und 3b, 4a bis 4c, Tabelle 3c entfernt
2.12.1	01.03.2024	TN	Änderungen an Kap. 1.1, Tabellen 4a bis 4c und 5b.
2.12.0	22.02.2024	TN	Änderungen an Kap. 1.1, 1.2, Tabellen 1, 2c, 4a bis 4c, 5a und 5b.
2.11.0	01.12.2023	TN	Änderungen an Kap. 1.1, 1.2, Tabellen 1, 2a bis 2c, 3a bis 3c, 4a bis 4c, 5a und 5b.
2.10.0	12.09.2023	TN	Änderungen an Kap. 1.1, 1.2, Tabellen 2b, 2c, 3a, 4a, 4b, 4c, 5a und 5b.
2.9.0	17.05.2023	OM	Bundesnotarkammer-Karte und der beA-Signatur-karte aus dem qualifizierten Bereich entfernt.
2.9.0	12.04.2023	OM	Zwischenversion nach Aufnahme der technischen Unterstützung der DGN 4.0 Karten.
2.8.1	22.11.2022	TN/OM	Versionierung geändert, Änderungen am Kap. 1.1 und Kap. 6
2.8.0	11.11.2022	TN	Änderungen an Tabelle 1, 2c, 4a, 4b, 4c, 5a und 5b
2.7.1	22.02.2022	TN	Änderungen an Tabelle 4a, 4b, 4c und 5a
2.7.0	24.01.2022	TN	Änderungen an Tabelle 1, 2c, 4a, 4b und 4c
2.6.0	28.10.2021	TN	Änderungen an Tabelle 1, 3a, 4a, 4b, 4c, 5a und 5b
2.5.7	01.06.2021	TN	Versionierung geändert, Änderungen am Kap. 1.1
2.5.5	01.04.2021	TN	Versionierung geändert, Änderungen am Kap. 1.1
2.5.4	15.03.2021	TN	Versionierung geändert, Änderungen am Kap. 1.1
2.5.1	05.02.2021	TN	Einführung eines Inhalts- und Änderungsverzeich-nisses, Änderungen am Kap. 1.1, Neues Kap. 5.1 hinzugefügt, Änderungen an Tabelle 1, 2b, 2c und 4c

© 2026 Administration Intelligence AG, Würzburg

1 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 von geeigneten Chipkartenlesern mehr regelt.

Qualified Signature Creation Devices (QSCD) verwendet werden, die durch qualifizierte Vertrauensdiensteanbieter aus Deutschland herausgegeben werden und mit denen man eine QES erzeugen kann.

1.1 Aktuelle Hinweise

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

- Es wurde ein Bug bei der Verwendung der D-Trust Card 6.1 / 6.4 behoben. Die Karte schreibt eine Mindest-Pinlänge von 6 nummerische Zeichen vor. Die MCard erwartete 8 Zeichen. Dieser Fehler wurde behoben.
- Diese Version der MCard unterstützt macOS 27 Golden Gate.

Der in dieser Version eingesetzte Crypto-Provider lautet Bouncy Castle V1.86.

Hinweis: Folgende Signatur- und Siegelkarten von D-Trust unterstützen nur den Signaturalgorithmus SHA384withECDSA.

- D-Trust Card 5.1 M100
- D-Trust Card 5.1 Multi
- D-Trust Card 5.4 Multi

Dieser Signaturalgorithmus wird mit der OSCI-Bibliothek in der Version 2.4.5 unterstützt.

1.2 Abkündigungen

- Keine

Hinweis: Seit der Version 2.12.0 der MCard wird die Funktion Verschlüsselung mit Signaturkarte nicht mehr unterstützt.

1.3 Hinweis zu Änderungen getesteter Produkte

© 2026 Administration Intelligence AG, Würzburg

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.

© 2026 Administration Intelligence AG, Würzburg

2 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

© 2026 Administration Intelligence AG, Würzburg

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.

© 2026 Administration Intelligence AG, Würzburg

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 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 4a und 4b) 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 5a bis 5c).

© 2026 Administration Intelligence AG, Würzburg

4 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 und erlaubt - unabhängig von der Kartenvariante - nach der PIN-Eingabe die Erzeugung von genau einer QES. Unterstützt werden auch Siegelkarten deutscher qualifizierter Vertrauensdiensteanbieter.

Qualifizierte Signaturkarten basieren auf sogenannte 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 2c) zu entnehmen.

eToken

Mit Einführung der eIDAS-VO ist auch der Einsatz von USB Token als QSCD in Deutschland

© 2026 Administration Intelligence AG, Würzburg

möglich. Diese Anwendung unterstützt auch die eToken deutscher qVDAs (Tabelle 3).

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 5a bis 5c).

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 12345**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.

© 2026 Administration Intelligence AG, Würzburg

5 Unterstützte Chipkartenleser

Mit dieser Anwendung können fast alle Chipkartenleser mit Tastatur (PIN-Pad) und ausgewählte Chipkartenleser ohne PIN-Pad verwendet werden. Chipkartenleser müssen stets den jeweils aktuellen Treiber des jeweiligen Herstellers verwenden und müssen die aktuellen Firmware- Version nutzen. Beachten Sie hierzu die Hinweise der Hersteller.

Für eine QES technisch unterstützte Chipkartenleser

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 3b) 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).

© 2026 Administration Intelligence AG, Würzburg

5.1 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
```

© 2026 Administration Intelligence AG, Würzburg

6 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 oder Authentisierung mit einer elektronischen Signaturkarte/QSCD in Kombination mit einem bestimmten Chipkartenleser und einem bestimmten Betriebssystem nur eingeschränkt oder nicht funktioniert. Dieses kann unterschiedliche Gründe haben: 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.

© 2026 Administration Intelligence AG, Würzburg

Tabelle 1: Unterstützte Betriebssysteme und JRE

Betriebssysteme	Java-Version 1)	Abkündigung
Microsoft Windows 11 64 Bit	Java 17 Update 18	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/windowslifecycle-fact-sheet zu entnehmen. Nach Ablauf der Servicezeit wird ein Funktionsupdate von Windows 11 nicht mehr unterstützt.
Linux Ubuntu 26.04 LTS 64 Bit	Java 17 Update 18	Die LTS-Distribution wird für zwei Jahre ab Veröffentlichungszeitpunkt unterstützt. Mit Erscheinen der neuen LTS-Version erlischt die Unterstützung der Vorversion durch die MCard.
Apple macOS Golden Gate	Java 25 Update 4	Der Hersteller veröffentlicht einmal jährlich eine kostenlose Folgeversion. Mit Erscheinen der neuen Version erlischt die Unterstützung der Vorversion durch die MCard.

1) Die MCard ist lauffähig unter Java 17, 21 und 25. Mit der hier aufgeführten Version wurde die MCard zuletzt getestet.

© 2026 Administration Intelligence AG, Würzburg

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 BSI-DSZ-CC-1112-V2-2020 BSI-DSZ-CC-1112-V2-2021
	D-TRUST Card 5.4	QES	CardOS V6.0 ID R1.1 CardOS V6.0 ID R1.2	BSI-DSZ-CC-1162-V2-2023 BSI-DSZ-CC-1162-V3-2024
	D-TRUST Card 5.4 Multi 2) 3)			
	D-TRUST Card 6.4	QES	STARCOS 3.7 eIDAS C3	SRC.00070.QSCD.08.2024
	D-TRUST Card 6.4 Multi 2)			
Deutsche Telekom Security GmbH	Qualified.ID Multisiegelkarte 2)	QES	Qualified Signature / Seal Creation Device TCOS Signature Card Version 3 Release 1/P71	SCR.00066.QSCD.12.2024

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) unendlich viele QES im Batchverfahren möglich. Die Erzeugung von Siegel innerhalb eines festgelegten Zeitfensters ist nicht möglich.

3) Diese Karte kann in OSCI-Clients eingesetzt werden, die die OSCI-Bibliothek ab der Version 2.4.5 verwenden.

© 2026 Administration Intelligence AG, Würzburg

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	Qualified.ID Light	Authentisierung QES	Qualified Signature / Seal Creation Device TCOS 3.0 Signature Card, Version 2.0 Release 2/SLE78CLX1440P	SRC.00032.QSCD.12.2018 Nachtrag 3
	Qualified.ID Standard		Qualified Signature / Seal Creation Device TCOS Signature Card Version 3 Release 1/P71	SCR.00066.QSCD.12.2024
	Qualified.ID Multi 3)			
D-Trust GmbH	D-TRUST Card 4.1a Std.	Authentisierung QES	CardOS DI V5.4 QES Version 1.0	BSI-DSZ-CC-1112-2020 BSI-DSZ-CC-1112-V2-2020 BSI-DSZ-CC-1112-V2-2021
	D-TRUST Card 4.1a UPC			
	D-TRUST Card 5.1 Std.	Authentisierung QES	CardOS V6.0 ID R1.1 CardOS V6.0 ID R1.2	BSI-DSZ-CC-1162-V2-2023 BSI-DSZ-CC-1162-V3-2024
	D-TRUST Card 5.1 Multi 100 2) 5)			
	D-TRUST Card 5.1 Multi 3) 5)			
	D-TRUST Card 6.1 Std.	Authentisierung QES	STARCOS 3.7 eIDAS C3	SRC.00070.QSCD.08.2024
	D-TRUST Card 6.1 Multi 100			
	D-TRUST Card 6.1 Multi			
DGN Service	sprintCard businessCard 4)	Authentisierung QES	Qualified Signature Creation Device STARCOS 3.7 HBA G2.1 (R2)	SRC.000047.QSCD.06.2022

© 2026 Administration Intelligence AG, Würzburg

Qualifizierter Vertrauensdienste-anbieter	Handelsname der Chipkarte	Schlüssel-verwendung	Name der QSCD 1) in der Zertifizierungsurkunde	Zertifizierungsurkunde
Deutsche Telekom AG D-TRUST GmbH Medisign SHC+CARE	Elektronischer Heilberufsausweis (eHBA)	Authentisierung QES	Qualified Signature Creation Device STARCOS 3.7 HBA G2.1 (R2)	SRC.000047.QSCD.06.2022
SIGN 8	SIGN 8 Signaturkarte	QES	IAS Classic V4.4.2 with MOC server v1.1 on MultiApp V4.0.1 IAS Classic v5.2 on MultiApp V5.0	ANSSI-CC-2018/24 ANSSI-CC-2021/54

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) unendlich viele QES im Batchverfahren möglich. Die Erzeugung von Siegel 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.

5) Diese Karte kann in OSCI-Clients eingesetzt werden, die die OSCI-Bibliothek ab der Version 2.4.5 verwenden.

© 2026 Administration Intelligence AG, Würzburg

Tabelle 2c: andere unterstützte Signaturkarten

Vertrauensdienste- anbieter	Handelsname der Chipkarte	Schlüssel-verwendung	Name der SSCD 1)	Bemerkungen
Bundesnotarkammer, Zertifizierungsstelle	beA-Karte Mitarbeiter	Authentisierung	Java Card Open Platform (JCOP)	--
Bundesnotarkammer, Zertifizierungsstelle	Justiz-Paket R-Karte zur Authentisierung Fernsignatur	Authentisierung	Java Card Open Platform (JCOP)	--
Deutsche Rentenver-sicherung Bund	DRV Mitarbeiterausweis 6.0	Fortgeschrittene Signatur	CardOS V6.0 ID R1.1	BSI-DSZ-CC-1162-V2-2023

© 2026 Administration Intelligence AG, Würzburg

Tabelle 3: Technisch unterstützte eToken (USB)

Qualifizierter Vertrauensdienste- anbieter	Handelsname der Chipkarte /	Schlüssel-verwendung	Hardware	Standard	Zertifizierungsurkunde
SIGN 8	SIGN 8 USB Token	QES	SafeNet eToken 5110	PC/SC	ANSSI-CC-2018/24 ANSSI-CC-2021/54

© 2026 Administration Intelligence AG, Würzburg

Tabelle 4a: Technisch unterstützte Chipkartenleser

Handelsname des Geräts	Hersteller	Angaben zur technischen Unterstützung	PIN-Pad	Standard	Schnittstelle	
					PC	Karte
Cherry Secure Board 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	ja	PC/SC	USB	kontakt
CyberJack RFID komfort	Reiner SCT Kartenlesegeräte GmbH	cyberJack® RFID komfort Version 2.0	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	ja	PC/SC	USB	kontakt, kontaktlos
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	ja	PC/SC	USB	kontakt
ORGA 930 Care	Worldline Healthcare GmbH	Für den Offline-Betrieb geeignet	ja	PC/SC	USB	kontakt

© 2026 Administration Intelligence AG, Würzburg

Tabelle 4b: 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
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

© 2026 Administration Intelligence AG, Würzburg

Tabelle 5a: Unterstützte Kombinationen Windows Betriebssysteme - Chipkartenleser - Signaturkarte

Handelsnamen der technisch unterstützten Chipkartenleser mit PinPad	Microsoft Windows 5)		Handelsnamen der Signatur- und Siegelkarten									
	Firmware	Treiber PC/SC	beA-Mitarbeiter 3) Bundesnotarkammer	Justiz-Paket R-Karte für Fernsignatur 3)	DGN sprintCard DGN businessCard	D-Trust Card 4.1a, 4.1a UPC, 4.4a 4)	D-Trust Card 5.1, 5.4 4)	D-Trust Card 6.1, 6.4 4)	DRV-Bund 1)	eHBA G2.1	SIGN 8 Signaturkarte	TeleSec Qualified ID 7)
Cherry® Secure Board 1.0	1.1.0.0	5.0.4	✓	✓	✓	✓	✓6)	✓	-	✓	✓6)	✓6)
Cherry® ST-2100	7.10	4.57.0.1	✓	✓	✓	✓	✓6)	✓	-	✓	✓6)	✓
Cherry® KC 1000 SC-Z	2.0.0	1.0.5.152	✓	✓	✓	✓	✓6)	✓	-	✓	✓6)	✓
cyberJack® one	1.2.11	Driver Package 1.6.2	✓	✓	✓	✓	✓6)	✓	-	✓	×	✓
cyberJack® RFID standard kontakt	1.2.73	Driver Package 1.6.2	✓	✓	✓	✓	✓	✓	✓	✓	✓6)	✓
cyberJack® RFID komfort kontakt	2.0.49	Driver Package 1.6.2	✓	✓	✓	✓	✓	✓	✓	✓	✓6)	✓
cyberJack® RFID komfort FON kontakt	2.0.49	Driver Package 1.6.2	✓	✓	✓	✓	✓	✓	-	✓	✓6)	✓
cyberJack® RFID standard kontaktlos	1.2.73	Driver Package 1.6.2	✓	✓	-	-	✓	-	✓6)	-	-	-
cyberJack® RFID komfort kontaktlos	2.0.49	Driver Package 1.6.2	✓	✓	-	-	✓	-	✓6)	-	-	-
cyberJack® RFID komfort FON kontaktlos	2.0.49	Driver Package 1.6.2	✓	✓	-	-	✓	-	✓6)	-	-	-

© 2026 Administration Intelligence AG, Würzburg

Handelsnamen der technisch unterstützten Chipkartenleser mit PinPad	Microsoft Windows 5)		Handelsnamen der Signatur- und Siegelkarten									
	Firmware	Treiber PC/SC	beA-Mitarbeiter 3) Bundesnotarkammer	Justiz-Paket R-Karte für Fernsignatur 3)	DGN sprintCard DGN businessCard	D-Trust Card 4.1a, 4.1a UPC, 4.4a 4)	D-Trust Card 5.1, 5.4 4)	D-Trust Card 6.1, 6.4 4)	DRV-Bund 1)	eHBA G2.1	SIGN 8 Signaturkarte	TeleSec Qualified ID 7)
SPR 332 V2	7.06	4.57.0.1	✓	✓	✓	✓	✓6)	✓	-	✓	✓6)	✓
ORGA 930 Care	5.3.0	3.0.0.0	-	-	-	-	-	-	-	✓	✓6)	-
In Tabelle 3b aufgeführte Geräte ohne PIN-Pad 6)			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

1) Ausgabe dieser Signaturkarte erfolgt nur an Behördenmitarbeitenden DRV-Bund
2) Nur fortgeschrittene Signatur
3) Nur Authentisierung
4) D-Trust Card 4.4, 5.4 und 6.4 (Siegelkarte) nur QES
5) Die unterstützten Windows-Betriebssysteme sind der Tabelle 1 zu entnehmen
6) Pin-Eingabe nur Klasse 1 möglich
7) Unterstützt wird nur die kontaktbehaftete Schnittstelle

© 2026 Administration Intelligence AG, Würzburg

Tabelle 5b: Unterstützte Kombinationen Ubuntu 26.04 LTS (64 Bit) - Chipkartenleser - Signaturkarte

Handelsnamen der technisch unterstützten Chipkartenleser mit PinPad	Ubuntu 26.04 LTS		Handelsnamen der Signatur- und Siegelkarten									
	Firmware	PCSC-lite Version 2.4.1 5)	beA-Mitarbeiter 3) Bundesnotarkammer	Justiz-Paket R-Karte für Fernsignatur 3)	DGN businessCard DGN sprintCard	D-Trust Card 4.1, 4.1 UPC, 4.4 4)	D-Trust Card 5.1, 5.4 4)	D-Trust Card 6.1, 6.4 4)	DRV-Bund 1)	eHBA G2.1	SIGN 8 Signaturkarte	TeleSec Qualified ID 7)
Cherry® Secure Board 1.0	1.1.0.0	CCID 1.6.1	✓6)	✓6)	✓6)	×	✓6)	✓	-	✓6)	✓6)	×
Cherry® ST-2100	7.10	libccid.so 1.7.1	✓	✓	✓	✓	✓6)	✓	-	✓	✓6)	✓
Cherry® KC 1000 SC-Z	2.0.0	CCID 1.6.1	✓6)	✓6)	✓6)	✓6)	✓6)	✓	-	×	×	✓
cyberJack® one	1.2.11	3.99.5final.sp18	✓	✓	✓	✓	✓6)	✓	-	✓	✓6)	✓
cyberJack® RFID standard kontakt	1.2.74	3.99.5final.sp18	✓	✓	✓	✓	✓	✓	✓	✓	✓6)	✓
cyberJack® RFID komfort kontakt	2.0.50	3.99.5final.sp18	✓	✓	✓	✓	✓	✓	✓	✓	✓6)	✓
cyberJack® RFID komfort FON kontakt	2.0.50	3.99.5final.sp18	✓	✓	✓	✓	✓	✓	-	✓	✓6)	✓
cyberJack® RFID standard kontaktlos	1.2.74	3.99.5final.sp18	-	-	-	-	✓	-	✓6)	-	-	-
cyberJack® RFID komfort kontaktlos	2.0.50	3.99.5final.sp18	-	-	-	-	✓	-	✓6)	-	-	-

© 2026 Administration Intelligence AG, Würzburg

Handelsnamen der technisch unterstützten Chipkartenleser mit PinPad	Ubuntu 26.04 LTS		Handelsnamen der Signatur- und Siegelkarten									
	Firmware	PCSC-lite Version 2.4.1 5)	beA-Mitarbeiter 3) Bundesnotarkammer	Justiz-Paket R-Karte für Fernsignatur 3)	DGN businessCard DGN sprintCard	D-Trust Card 4.1, 4.1 UPC, 4.4 4)	D-Trust Card 5.1, 5.4 4)	D-Trust Card 6.1, 6.4 4)	DRV-Bund 1)	eHBA G2.1	SIGN 8 Signaturkarte	TeleSec Qualified ID 7)
cyberJack® RFID komfort FON kontaktlos	2.0.47	3.99.5final.sp18	-	-	-	-	✓	-	✓6)	-	-	-
SPR 332 V2	7.06	libccid.so 1.7.1	✓	✓	✓	✓	✓6)	✓	-	✓	✓6)	✓
ORGA 930 Care	5.3.0	Kein Treiber verfügbar	-	-	-	-	-	-	-	-	✓6)	-
In Tabelle 3b aufgeführte Geräte ohne PIN-Pad 6)			✓	✓	✓	✓	✓	✓	-	✓	✓	✓

1) Ausgabe dieser Signaturkarte erfolgt nur an Behördenmitarbeitenden DRV-Bund
2) Nur fortgeschrittene Signatur
3) Nur Authentisierung
4) D-Trust Card 4.4, 5.4 und 6.4 (Siegelkarte) nur QES
5) Bei generischen CCID-Treibern muss der Name mit * angeführt werden
6) Pin-Eingabe nur Klasse 1 möglich
7) Unterstützt wird nur die kontaktbehaftete Schnittstelle

© 2026 Administration Intelligence AG, Würzburg

Tabelle 5c: Unterstützte Kombinationen macOS Golden Gate - Chipkartenleser - Signaturkarte

Handelsnamen der technisch unterstützten Chipkartenleser mit PinPad	macOS Golden Gate		Handelsnamen der Signatur- und Siegelkarten									
	Firmware	PCSC-lite 2.4.0	beA-Mitarbeiter 3) Bundesnotarkammer	Justiz-Paket R-Karte für Fernsignatur 3)	DGN businesCard DGN sprintCard	D-Trust Card 4.1, 4.1 UPC, 4.4 4)	D-Trust Card 5.1, 5.4 4)	D-Trust Card 6.1, 6.4 4)	DRV-Bund 1)	eHBA G2.1	SIGN 8 Signaturkarte	TeleSec Qualified ID 7)
Cherry® Secure Board 1.0	1.1.0.0	LibCCID 1.5.1	✓	✓	✓	×	✓5)	✓	-	✓	✓6)	×
Cherry® ST-2100	7.10	LibCCID 1.5.1	✓6)	✓6)	✓	×	✓5)	✓	-	✓6)	✓6)	×
Cherry® KC 1000 SC-Z	2.0.0	LibCCID 1.5.1	✓	×	✓	✓	✓5)	✓	-	✓	✓6)	✓
cyberJack® one	1.2.11	pcsc-cyberJack 3.99.5 sp16	✓	✓	✓	✓	✓5)	✓	-	✓	×	✓
cyberJack® RFID standard kontakt	1.2.74	pcsc-cyberJack 3.99.5 sp16	✓	✓	✓	✓	✓	✓	✓	✓	✓6)	✓
cyberJack® RFID komfort kontakt	2.0.50	pcsc-cyberJack 3.99.5 sp16	✓	✓	✓	✓	✓	✓	✓	✓	✓6)	✓
cyberJack® RFID komfort FON kontakt	2.0.50	pcsc-cyberJack 3.99.5 sp16	✓	✓	✓	✓	✓	✓	✓	✓	✓6)	✓
cyberJack® RFID standard kontaktlos	1.2.74	pcsc-cyberJack 3.99.5 sp16	-	-	-	-	✓	-	✓5)	-	-	-
cyberJack® RFID komfort kontaktlos	2.0.50	pcsc-cyberJack 3.99.5 sp16	-	-	-	-	✓	-	✓5)	-	-	-

© 2026 Administration Intelligence AG, Würzburg

Handelsnamen der technisch unterstützten Chipkartenleser mit PinPad	macOS Golden Gate		Handelsnamen der Signatur- und Siegelkarten									
	Firmware	PCSC-lite 2.4.0	beA-Mitarbeiter 3) Bundesnotarkammer	Justiz-Paket R-Karte für Fernsignatur 3)	DGN businesCard DGN sprintCard	D-Trust Card 4.1, 4.1 UPC, 4.4 4)	D-Trust Card 5.1, 5.4 4)	D-Trust Card 6.1, 6.4 4)	DRV-Bund 1)	eHBA G2.1	SIGN 8 Signaturkarte	TeleSec Qualified ID 7)
cyberJack® RFID komfort FON kontaktlos	2.0.47	pcsc-cyberJack 3.99.5 sp16	-	-	-	-	✓	-	✓5)	-	-	-
SPR 332 V2	7.06	SCMCCID 5.0.41	✓	✓	✓	✓	✓5)	✓5)	-	✓6)	✓6)	✓6)
ORGA 930 Care	5.3.0	-	-	-	-	-	-	-	-	-	-	-
In Tabelle 3b aufgeführte Geräte ohne PIN-Pad 5)			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

1) Ausgabe dieser Signaturkarte erfolgt nur an Behördenmitarbeitenden DRV-Bund
2) Nur fortgeschrittene Signatur
3) Nur Authentisierung
4) D-Trust Card 4.4, 5.4 und 6.4 (Siegelkarte) nur QES
5) Pin-Eingabe nur Klasse 1 möglich
6) Pin-Eingabe nur Klasse 1 möglich, Pin-Eingabe über Tastatur muss im Client aktiv eingeschaltet werden
7) Unterstützt wird nur die kontaktbehaftete Schnittstelle
8) Unterstützt wird nur TCOS 3.0 Signature Card, Version 2.0 Release 2

© 2026 Administration Intelligence AG, Würzburg

Tabelle 6a: Unterstützte Einsatzumgebungen Terminalserver

Clientbetriebssystem:	Windows 11 1)							
Serverbetriebssystem: **Terminalserver:**	Windows Server 2022 64 Bit Citrix Virtual Apps and Desktops 7 (2402 LTSR)							
Handelsnamen der technisch unterstützten Chipkartenleser mit Pin-Pad	**Chipkartenleser**		**Handelsnamen der Signatur- und Siegelkarten**					
	Firmware	**Treiber PC/SC**	**Justiz-Paket R-Karte für Fernsignatur / Signaturkarte beA-Mitarbeiter** 3)	**D-Trust Card 4.1, 4.1 UPC, 4.4** 2)	**D-Trust Card 5.x und 6.x** 2)	**DGN sprintCard / businessCard**	**SIGN 8 Signaturkarte**	**TeleSec Qualified ID** 7)
Cherry® ST-2100	7.10	4.57.0.1	✓	✓	✓ 4)	✓	✓	✓
Cherry® KC 1000 SC-Z	2.0.0	1.0.5.152	✓	✓	✓ 4)	✓	✓	✓
cyberJack® RFID standard kontakt	1.2.74	Driver Package 1.5.0	✓	✓	✓	✓	✓	✓
cyberJack® RFID komfort kontakt	2.0.50	Driver Package 1.5.0	✓	✓	✓	✓	✓	✓
SPR 332 V2	7.06	4.57.0.1	✓	✓	✓4)	✓	✓	✓
In Tabelle 3b aufgeführte Geräte ohne PIN-Pad 5)			✓	✓	✓ 4)	✓	✓	✓

1) Der Hersteller stellt zweimal pro Jahr ein Funktionsupdate von Windows 11 zur Verfügung. Der Service für die Editionen beträgt 24 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 11 nicht mehr unterstützt.

2) D-Trust Card 4.4, 5.4 und 6.4 (Siegelkarte) nur QES

3) Nur Authentisierung

4) Pin-Eingabe bei D-Trust Card 5.x nur Klasse 1 möglich, Pin-Eingabe über Tastatur muss im Client aktiv eingeschaltet werden 5) Pin-Eingabe nur Klasse 1 möglich

© 2026 Administration Intelligence AG, Würzburg

Tabelle 6b: Unterstützte Einsatzumgebungen Terminalserver

Clientbetriebssystem: **Serverbetriebssystem:**	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) Windows Server 2016 64 Bit			
Terminalserver:	Citrix XenApp 7.15			
Handelsnamen der technisch unterstützten Chipkartenleser mit Pin-Pad	**Chipkartenleser**		**Handelsnamen der Signatur- und Siegelkarten**	
	Firmware	**Treiber PC/SC 1)**	**D-TRUST 4.1, 4.1 UPC, 4.4 2)**	**D-TRUST 5.1, 5.4 2)**
cyberJack® standard kontakt	1.2.74	pcsc-cyberJack 3.99.5 sp18	✓	✓
cyberJack® komfort kontakt	2.0.50	pcsc-cyberJack 3.99.5 sp18	✓	✓

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

© 2026 Administration Intelligence AG, Würzburg

7 Impressum

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

Administration Intelligence AG
Steinbachtal 2B
97082 Würzburg
Telefon: 0931-73046-200
Fax: 0931-73046-99-200
www.ai-ag.de
E-Mail: info@ai-ag.de

Vorstand: Dr. Christian Schneider (Vors.), Christian Baltes, Frank Linneberg
Aufsichtsratsvorsitzender: Prof. Dr. Rainer Thome
Registernummer: HRB 717

© 2026 Administration Intelligence AG, Würzburg