Unterstützte Betriebssysteme – Chipkartenlesegeräte - Signaturkarten

DEHSt VPSMail 3.4.1

Karten-Leser-Ansteuerung (MCard) Version 2.13.0

Dokumentenversion: 3.4.1_3

Inhaltsverzeichnis

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 regelt.
- Qualifizierte elektronische Signaturerstellungseinheiten 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.

- Die Kartenerkennung der D-Trust Card 5.x wurde erweitert. Es werden auch die Karten mit dem Zusatz „2cc“ unterstützt, die ab 01/2025 vom Hersteller ausgegeben werden.
- Es wird die neue Signaturkarte des Herausgebers TeleSec basierend auf der QSCD TCOS Signature Card Version 3 unterstützt.
- Ab dieser Version der MCard wird bei Verwendung der D-Trust Card 5.1 die Card Access Number (CAN) im Windows-Profilordner gespeichert. Die CAN muss bei der ersten Verwendung der Karte und in korrekter Form eingegeben warden und ab der zweiten Verwendung nicht mehr, wenn derselbe Windows-Arbeitsplatzrechner verwendet wird. Unter Ubuntu und macOS steht diese Funktion derzeit nicht zur Verfügung.
-

Der in dieser Version eingesetzte Crypto-Provider lautet Bouncy Castle V1.80

Die Signaturkarten *D-Trust Card 5.1 M100* und *D-Trust Card 5.1 Multi* sowie die Siegelkarte *D-Trust Card 5.4 Multi* können für eine OSCI-Nachrichtensignatur derzeit nicht verwendet werden (bspw. mit dem VPS Mail Client).

1.2 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.

- Cyberjack secoder

	**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

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

2 Notwendige Schutzvorkehrungen für diese Anwendung

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 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 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 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 - Chipkartenleser - Signaturkarte

Bitte beachten Sie bei der Auswahl des Betriebssystems: Die Funktionsfähigkeit der unterstützten Chipkartenleser (siehe Tabellen 3a und 3b) 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“ (Tabelle 4a).

4 Unterstützte Signaturkarten

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 der Tabelle „Unterstützte Signaturkarten geeignet für eine qualifizierte Signatur (QES)“ (Tabelle 2a) 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.

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 der Tabelle „Unterstützte Signaturkarten geeignet für eine qualifizierte Signatur (QES)“ (Tabelle 2a).

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.

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 der Tabelle „Unterstützte Kombinationen Betriebssystem-Leser-Karten“ (Tabelle 4a).

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:

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**

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 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:

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.

5 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.

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 der Tabelle „Unterstützte Kombinationen Betriebssystem-Leser-Karten“ (Tabelle 4a).

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, 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 der Tabelle „Unterstützte Kombinationen Betriebssystem-Leser-Karten“ (Tabelle 4a).

Tabelle 1: Unterstützte Betriebssysteme und JRE

Betriebssysteme	Java-Version	Abkündigung
Microsoft Windows 10 64 Bit	Java 11 Update 25	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 25	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.

Tabelle 2a: 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 QES	Qualified Signature / Seal Creation Device TCOS 3.0 Signature Card, Version 2.0 Release 2/SLE78CLX1440P	SRC.00032.QSCD.12.2018 Nachtrag 3
	Signaturkarte Standard		Qualified Signature / Seal Creation Device TCOS Signature Card Version 3 Release 1/P71	SCR.00066.QSCD.12.2024
	Multisignaturkarte 3)			
D-Trust GmbH	D-TRUST Card 4.1a Standard	Authentisierung 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 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)			
DGN Service	sprintCard businessCard 4)	Authentisierung 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 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) karten-abhängig 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) karten-abhängig die Erzeugung von bis zu 254 QES im Batchverfahren möglich. Die Karten funktionieren nur kontaktbehaftet. Die Verschlüsselungsfunk-tionalität wird nur für die RSA-Schlüssel unterstützt.

5) Die Karte kann nicht im OSCI-Kontext eingesetzt werden, weil die OSCI-Spezifikation den Algorithmus SHA384withECDSA aktuell nicht unter-stützt.

Tabelle 3a: Technisch unterstützte Chipkartenleser

Handelsname des Geräts	Hersteller	Angaben zur technischen Unter-stützung	Zertifizierungsurkunde	PIN-Pad	Standard	Schnittstelle	
						PC	Karte
Cherry Secure Board 1.0	Cherry GmbH	Chipkartenleser der Sicherheits-klasse 2	-	ja	PC/SC	USB	kontakt
Cherry SmartTerminal 2100	Cherry GmbH	Chipkartenleser der Sicherheits-klasse 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 Kar-tenlesegeräte GmbH	cyberJack® RFID komfort Version 2.0	TUVIT.93180.TU.12.2011	ja	PC/SC	USB	kontakt, kontaktlos
CyberJack RFID komfort FON	Reiner SCT Kar-tenlesegeräte GmbH	Barrierefreier Chipkartenleser der Sicherheitsklasse 3	-	ja	PC/SC	USB	kontakt, kontaktlos
CyberJack RFID stand-ard	Reiner SCT Kar-tenlesegeräte GmbH	cyberJack® RFID standard Version 1.2	TUVIT.93188.TU.07.2011	ja	PC/SC	USB	kontakt, kontaktlos
CyberJack one	Reiner SCT Kar-tenlesegeräte GmbH	Chipkartenleser der Sicherheits-klasse 3	-	ja	PC/SC	USB	kontakt

Handelsname des	Hersteller	Angaben zur technischen Unter-	Zertifizierungsurkunde	PIN-	Standard	Schnittstelle	
SPR 332 usb (Chip-drive 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: 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

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

Handelsnamen der technisch unterstützten Chipkartenleser mit Pin-Pad	Microsoft Windows 5)		Handelsnamen der Signatur- und Siegelkarten								
	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 4)	D-Trust Card 5.1, 5.4 4)	DRV-Bund 1)	EPO-Karte 2)	eHBA G2.1	TeleSec Qualified ID 7)
Cherry® Secure Board 1.0	1.1.0.0	5.0.4	✓	✓	✓	✓	✓6)	-	✓	✓	✓
Cherry® ST-2100	7.10	4.57.0.1	✓	✓	✓	✓	✓6)	-	✓	✓	✓
Cherry® KC 1000 SC-Z	2.0.0	1.0.5.152	✓	✓	✓	✓	✓6)	-	✓	✓	✓
cyberJack® one	1.2.11	Driver Package 1.5.0	✓	✓	✓	✓	✓6)	-	✓	✓	✓
cyberJack® RFID standard kontakt	1.2.71	Driver Package 1.5.0	✓	✓	✓	✓	✓	✓	✓	✓	✓
cyberJack® RFID komfort kontakt	2.0.47	Driver Package 1.5.0	✓	✓	✓	✓	✓	✓	✓	✓	✓
cyberJack® RFID komfort FON kontakt	2.0.47	Driver Package 1.5.0	✓	✓	✓	✓	✓	✓	✓	✓	✓
cyberJack® RFID standard kontaktlos	1.2.71	Driver Package 1.5.0	✓	✓	-	-	✓	✓6)	-	-	✓
cyberJack® RFID komfort kontaktlos	2.0.47	Driver Package 1.5.0	✓	✓	-	-	✓	✓6)	-	-	✓
cyberJack® RFID komfort FON kontaktlos	2.0.47	Driver Package 1.5.0	✓	✓	-	-	✓	✓6)	-	-	✓
SPR 332 V2	7.06	4.57.0.1	✓	✓	✓	✓	✓6)	-	✓	✓	✓
ORGA 930 Care	5.3.0	3.0.0.0	-	-	-	-	-	-	-	✓	-
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 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) Unterstützt wird nur die kontaktbehaftete Schnittstelle