A006 - Smartcard

Klassifizierung:	Nicht klassifiziert
Typ:	IKT-Standard
Ausgabedatum:	2024-12-01
Version:	4.0.0
Status:	Genehmigt
Ersetzt:	3.0.2
Verbindlichkeit:	Weisung
Genehmigt durch:	Bereich Digitale Transformation und IKT-Lenkung (DTI), am 2024-11-19
Geprüft durch:	- FUB Krypt - SG PKI, Identity & Trust / IDT - BBL
Beilagen:	- Beilage 1 zu A006: Spezifikation BIT - Beilage 2: zu A006: Spezifikation BBL

Inhaltsverzeichnis

Der Bereich Digitale Transformation und IKT-Lenkung (DTI) erlässt gestützt auf Artikel 17 Absatz 1 der Verordnung über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung (VDTI) [VDTI] nachfolgende Weisungen.

1 Anwendungsbereich

Dieses Dokument beschreibt die Vorgaben für die von der Bundesverwaltung eingesetzten Smartcards und Kryptochips und die für deren Einsatz nötigen Soft- und Hardwareelemente.

2 Geltungsbereich

Die Weisung gilt, wo für die Zusammenarbeit und zur Erfüllung von Behördenaufgaben zwingend Zertifikate der Swiss Government PKI auf einer Smartcard von der zuständigen Bundesbehörde vorausgesetzt werden.

3 Verbindlichkeit

Der Verbindlichkeitsgrad der einzelnen Vorgaben wird mittels der im Anhang B zusammengestellten, in Grossbuchstaben geschriebenen Schlüsselwörter gekennzeichnet.

4 Definitionen

Secure Desktop: Bildschirm, der nach dem gleichzeitigen Drücken der Tasten Ctrl+Alt+Del angezeigt wird.

Konfektionierung: Das Einbetten des Kryptochip in die Plastikkarte und die weiteren Bearbeitungsschritte für die Fertigstellung der physikalischen Smartcard (z. B. Bedrucken, Laminieren, Programmieren). Das Ergebnis der Konfektionierung wird als Smartcard bezeichnet.

Secure Key Injection (SKI): Diese Methode erlaubt es, geheime Schlüssel von einer Server-Anwendung über einen unsicheren Client PC sicher auf die Smartcard zu senden [SKI].

5 Beschaffung, Konfektionierung, Bestellung

1. Der Kryptochip MUSS durch das Bundesamt für Rüstung (armasuisse), beschafft werden.
2. Der Fertigungsprozess (Konfektionierung) der Smartcard MUSS durch das Bundesamt für Bauten und Logistik (BBL) erfolgen oder beauftragt werden.
3. Für den Beschaffungs-, Lieferungs-, und Konfektionierungsvorgang jedes Kryptochips und jeder Karte MUSS die Nachvollziehbarkeit gewährleistet sein.
4. Die Bestellung von Smartcards MUSS über das BBL erfolgen.
5. Der Kryptochip der von Kantonen, bundesnahen Betrieben und Dritten eigenständig beschafft wird MUSS die Spezifikationen «6.1 Kryptochip» erfüllen.
6. Die von Kantonen, bundesnahen Betrieben und Dritten eigenständig beschaffte, konfektionierte und bestellte Smartcard MUSS vor der Verwendung von der Swiss Government PKI prestaged werden.

6 Erforderliche Komponenten und Schnittstellen

6.1 Kryptochip

1. Der Kryptochip MUSS als asymmetrisches Verfahren ECC (mit 256, 384 und 512 Bit, z. B. Brainpool, Curve25519) unterstützen.
2. Der Kryptochip MUSS als asymmetrisches Verfahren RSA (mit 2048 und 4096 Bit) unterstützen.
3. Der Kryptochip SOLL als symmetrisches Verfahren AES mit 256 Bit unterstützen.
4. Der Kryptochip MUSS mindestens Speicher für 15 asymmetrische RSA-4096 Schlüsselpaare inklusiv Zertifikate aufweisen.
5. Der Kryptochip MUSS mindestens über eine FIPS 140-2 Level 2 Zertifizierung (oder eine vergleichbare Zertifizierung) verfügen.
6. Der Kryptochip MUSS mindestens über eine EAL5+ Zertifizierung verfügen.
7. Der Kryptochip MUSS eine hardware-beschleunigte Implementierung der kryptographischen Verfahren (AES; RSA und ECC) zur Verfügung stellen.
8. Der Kryptochip MUSS mindestens von folgenden Windows-Betriebssystemen unterstützt werden: Microsoft Windows 10 32/64-BIT und Windows Server ab 2012.
9. Der Kryptochip MUSS die Microsoft CryptoAPI (CSP, Minidriver oder CNG) und PKCS#11 Schnittstellen unterstützen. Jede Schnittstelle MUSS für die anderen transparent sein.
10. Der Kryptochip MUSS durch mindestens eine aktuelle Debian Distribution unterstützt werden.
11. Die Spezifikationen und der Source Code des Random Number Generators (RNG) auf dem Kryptochip MUSS einsehbar sein, allenfalls unter Non-Disclosure Agreement (NDA).
12. Die Spezifikationen und der Source Code der Schlüsselgenerierung auf dem Kryptochip (für symmetrische und asymmetrische Verfahren) MUSS einsehbar sein, allenfalls unter Non-Disclosure Agreement (NDA).
13. Die Beschreibung und detaillierte Spezifikationen der auf dem Kryptochip vorhandenen Applikationen/Software MUSS zur Verfügung gestellt werden.
14. Es MUSS sowohl eine PIN als auch ein PUK gesetzt werden können.
15. Bei der Initialisierung des Chips MUSS für PIN und PUK eine Policy definierbar sein. Diese Policy legt die Mindestlänge und die Komplexität dieser Werte fest.
16. Der Kryptochip MUSS die Funktionen PIN-Änderung und PIN Unlock zur Verfügung stellen. Diese müssen auf Windows aufgerufen werden können.

17. Der Kryptochip MUSS die Secure Key Injection (SKI) Funktion unterstützen.
18. Der Kryptochip SOLL eine kontaktlose Schnittstelle gemäss ISO 14443-A oder ISO 14443-B unterstützen.

6.2 Smartcard-Reader

1. Der Smartcard-Reader SOLL mindestens an einem USB-Port an den PC angeschlossen werden können.
2. Das kontaktlose Lesegerät (Bluetooth SC Reader, NFC) DARF eine kontaktlos-Schnittstelle gemäss ISO 14443 unterstützen.
3. Der Smartcard-Reader MUSS den PC/SC Standard [PC/SC v2.01] erfüllen.
4. Bei der Beschaffung der Büroautomationsgeräte MUSS die beschaffende Stelle die zu beschaffenden Geräte (z. B. Laptops, Tastaturen mit integrierten Smartcard-Readern) auf Kompatibilität mit den in der Bundesverwaltung eingesetzten Smartcards überprüfen. Das Testvorgehen MUSS durch die Swiss Government PKI genehmigt werden. Das Testergebnis MUSS der Swiss Government PKI gemeldet werden.

6.3 Smartcard (physikalische Sicht)

1. Die Smartcard MUSS die Grösse 85,60 mm × 53,98 mm und eine Stärke von 0.76 mm (gemäss ISO 7810 ID-1) aufweisen.
2. Das BBL MUSS in Abstimmung mit dem BIT und der DTI die Beilage 2 zu diesem Standard mit den Vorgaben für die Smartcard (physikalische Sicht) erstellen.
3. Das BBL KANN in der Beilage 5 zu diesem Standard auch die optionalen Komponenten und Schnittstellen (z.B. Transponderchip, RFID, Antennen für NFC) beschreiben.

6.4 Zugriff auf Smartcard

1. Unter Windows SOLL als Treiber der Minidriver nach der Smart Card Minidriver Specification v7 oder v7.07 [SCM] eingesetzt werden.
2. Unter Linux DARF der Kryptochip mit PKCS#11 [PKCS#11] angesprochen werden.

7 Allgemeine Bestimmungen

1. Der A006 – Smartcard MUSS im Intranet und Internet der BK publiziert werden.
2. Das BIT MUSS die Beilage 1 erarbeiten, aktuell halten und im Intranet und Internet der BK publizieren.
3. Das BBL MUSS die Beilage 2 im Intranet der DTI publizieren.
4. Der Antrag für die Aufnahme von nicht zugelassenen Smartcards in die Liste der zugelassenen Smartcards MUSS an den Führungsausschuss Standarddienste Bund (FSD) gemäss dessen Geschäftsreglements gerichtet werden.

8 Schlussbestimmungen

8.1 Aufhebung bisheriger Vorgaben

Der Standard A006 Version 3.0.2 wird aufgehoben.

8.2 Inkrafttreten

Der Standard tritt am Datum der Genehmigung in Kraft

Anhänge

A. Änderungen gegenüber Vorversion

Migration des Standards in neue Vorlage.

Ergänzung Ziffer 5, Punkt 5. und 6.

Inhaltliche Überarbeitung von Ziffer 2, Ziffer 6.1 und Ziffer 6.2 und Ziffer 7, Punkt 2. Und 3.

B. Bedeutung der Schlüsselwörter zur Bestimmung des Verbindlichkeitsgrades

Der Verbindlichkeitsgrad der einzelnen Vorgaben wird im Dokument mittels folgender in Grossbuchstaben geschriebenen Schlüsselwörter gekennzeichnet:

MUSS	Vorgabe, die einzuhalten ist (gewährte Ausnahmen ausgenommen)
DARF NICHT	Option, die nicht gewählt werden darf
DARF	Die Option ist explizit erlaubt. Die Nutzer entscheiden, ob sie die Option nutzen möchten. – Betrifft die Vorgabe eine IKT-Lösung, muss der Anbieter der Lösung die Option anbieten.
SOLL	Option, die im Normalfall zu wählen ist. Es kann jedoch ohne Ausnahmegewährung der DTI davon abgewichen werden, insbesondere wenn die Wirtschaftlichkeit oder Sicherheit andernfalls nicht mehr gewährleistet werden können. Die Abweichung von der Vorgabe ist jedoch schriftlich zu begründen.
KANN	Akzeptierte Option. – Betrifft die Vorgabe eine Lösung, entscheidet der Anbieter der Lösung darüber, ob er die Option unterstützen will.

C. Abkürzungen

Kürzel	***Bedeutung***
armasuisse	Bundesamt für Rüstung im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport
BBL	Bundesamt für Bauten und Logistik im Eidgenössischen Finanzdepartement
VDTI	Verordnung über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung vom 25. November 2020
BIT	Bundesamt für Informatik und Telekommunikation
CNG	Cryptography Next Generation: wurde mit der Windows Version 7 eingeführt und erlaubt den Einsatz der durch das NIST in der Suite B definierten Algorithmen.

Kürzel	***Bedeutung***
CNG/CSP	Der Crypto Next Generation Key Storage Provider (KSP) und der Microsoft Smart Card Base Cryptographic Service Provider können mit Hilfe des vom Kartenhersteller gelieferten Minidrivers [SCM] auf die Smartcard zugreifen.
DH	Diffie Hellmann, Schlüsselaustauschprotokoll
FSD	Führungsausschuss Standarddienste Bund
DTI	Bereich Digitale Transformation und IKT-Lenkung (DTI)
ISO	International Standards Organisation
NDA	Non-Disclosure Agreement
NFC	Near Field Communication
PC/SC	Personal Computer – Smartcard Interface
PIN	Persönliche Identifikationsnummer
PKCS#11	Public Key Cryptographic Standard Number 11, von RSA LABORATORIES geschaffener Standard, siehe [PKCS#11]. Die aktuelle Version ist 2.20.
PUK	Personal Unblocking Key
RNG	Random Number Generator
RSA	Kryptosystem, das nach seinen Erfindern Rivest, Shamir und Adleman benannt ist.
SKI	Secure Key Injection
SR	Systematische Sammlung des Bundesrechts
TAV	Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur, Anhang zu SR 943.032.1

D. Referenzen

[VDTI] Verordnung über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung vom 25. November 2022 (Stand am 01. Januar 2022); SR 172.010.58 https://www.fedlex.admin.ch/eli/cc/2020/988/de

[EMBAV] Verordnung über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAV); SR 172.019.1 – https://www.fedlex.admin.ch/eli/cc/2023/754/de

[PC/SC v2.01] PC/SC Workgroup Specifications Overview

PC/SC Workgroup – We set the standard for integrating smart cards and smart card readers into the mainstream computing environment. (pcscworkgroup.com)

[PKCS#11] Cryptographic Token Interface Standard

https://www.cryptsoft.com/pkcs11doc/STANDARD/pkcs-11v2-20.pdf

[SCM] Smart Card Minidriver Versions

https://msdn.microsoft.com/en-us/library/windows/hardware/dn631754https://learn.microsoft.com/en-us/windows-hardware/drivers/smartcard/smart-card-minidriver-versions

[SKI] Secure Key Injection

https://msdn.microsoft.com/en-us/library/windows/hardware/dn468772(v=vs.85).aspxhttps://learn.microsoft.com/en-us/windows-hardware/drivers/smartcard/secure-key-injection

[TAV] Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur

http://www.bakom.admin.ch/themen/internet/00467/index.html?lang=dehttps://www.bakom.admin.ch/bakom/de/home/das-bakom/organisation/rechtliche-grundlagen/vollzugspraxis/technische-und-administrative-vorschriften/sr-943-032-1.html