Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Bundesamt für Informatik und Telekommunikation BIT

Version 2.5 21. April 2026

Anhang zum A006 Standard

Testbericht 2026 und Kartenliste

Projektname	Anhang zum A006 Standard
Departement	Eidgenössisches Finanzdepartement EFD
Amt	Bundesamt für Informatik und Telekommunikation BIT
Abteilung	PS-PSC-TRU
Status	Freigegeben
Ausgabedatum	21. April 2026

Beteiligter Personenkreis

Bearbeitende	Beatrice Metaj, Aline Ammann, Kamel Dridi
Genehmigende	SG-PKI Management Board
Benutzer	LRA-Officer
Zur Kenntnisnahme	Alle Product-Owner der Business-Unit TRU

NICHT KLASSIFIZIERT

Rimo Beatrice PVH6EU
Digital unterschrieben von Rimo Beatrice PVH6EU
Datum: 2026.04.23 11:54:20 +02'00'

Änderungsverzeichnis

Datum	Version	Autor	Änderung
29.04.2022	1.91	Kamel Dridi	**Initiale Version**
03.05.2022	1.92	Beatrice Metaj	**Anpassung der Versionen der PKI-Toolbox-Clients.** **MiddleWare** **PKI-ToolBox**
09.06.20222	1.93	Kamel Dridi	**Erste Testergebnisse**
22.06.20222	1.94	Kamel Dridi	**Definitive Version**
23.06.2022	1.95	Beatrice Metaj	**Inhaltskontrolle**
12.09.2022	1.96	Beatrice Metaj	**PKI Mgmt Board Empfehlungen und Kap. 4 eingefügt**
30.01.2023	1.99	Beatrice Metaj	**Das Dokument wird zur Publikation vorbereitet – auf die Freigabe wird noch gewartet – Status des Dokumentes ist «In Prüfung»!**
07.02.2023	2.00	Beatrice Metaj	**Freigabe durch Mgmt Board SG-PKI und Publikation**
23.11.2023	2.10	Aline Ammann	**Anpassung auf Vorgaben des CD-Bund**
24.11.2023	2.11	Aline Ammann	**Übersetzung und Anpassung Kapitel 2**
27.11.2023	2.12	Aline Ammann	**Übersetzung und Anpassung Kapitel 3**
28.11.2023	2.13	Aline Ammann	**Übersetzung und Anpassung Kapitel 3 – 5 (940er Karten offen)**
29.11.2023	2.14	Aline Ammann Kamel Dridi	**Ergänzung Kapitel 3 (940er Karten) und Kapitel 4.**
05.03.2024	2.2	Aline Ammann Beatrice Metaj	**Freigabe Version 2023/24 und Vorlage Mgmt. Board PKI zur Vernehmlassung**
02.04.2024	2.2	Beatrice Metaj	**Freigabe der Version 2.2 vom 05.03.2024 durch das Management Board**
06.01.2025	2.3	Kamel Dridi	**Anpassung neue Smartcard Gemalto MD 3930 NFC**
09.04.2025	2.3	Beatrice Metaj	**Freigabe Version 2.3 vom 06.1.2025 inkl. Gemalto MD 3930 NFC**

01.04.2026	2.4	Kamel Dridi	**Dekommissionierung Gemalto 830er Rev A und Rev B**
21.04.2026	2.5	Beatrice Rimo	**Dekommisionierte/obsolete Karten im Kap. 6 aufgelistet**

Inhaltsverzeichnis

1 Zweck des Dokuments

Dieses Dokument enthält die Ergebnisse von Tests, die mit verschiedenen Kartenzusammensetzungen, Middleware, Plattformumgebungen und der Verwendung von Zertifikaten in Standardanwendungen durchgeführt wurden.

Die Tests wurden ausschließlich auf der Grundlage der in Anhang zum A006 Standard definierten Fälle durchgeführt.

1.1 Aktualisierung des Dokuments

Dieses Dokument wird jährlich durch das BIT aktualisiert, basierend auf dem Entwicklungszyklus der TerraNova SG-PKI Software Suite, sowie den Marktbedingungen für Smartcards.

Der Kartenhersteller Gemalto liefert die Middleware, die mit den verkauften Karten kompatibel ist.

2 Testbeschreibung

2.1 Kartentypen

Um die Kompatibilität besser nachzuvollziehen, werden die Tests nach Kartentypen durchgeführt. Nachfolgende Karten werden beschrieben:

- Gemalto IDPrime MD930
- Gemalto IDPrime MD940
- Gemalto IDPrime 3930 (NFC)

Die nachfolgenden Issuing CAs und Policies sind für die Tests relevant:

- Enhanced CA 02 für Klasse B prestaged B
- Enhanced CA 02 für Klasse B prestaged B FUB
- Regulated CA 02 für Klasse A

2.2 Funktionalitäten

Die Funktionalität jeder Karte wird anhand der Verwaltung von Zertifikaten und der Verwendung von Zertifikaten bestimmt.

Die Tests werden auf den beiden Umgebungen Abnahme und Produktion ausgeführt.

2.2.1 Verwaltung von Zertifikaten

Nachfolgende Kriterien werden berücksichtigt, um die Verwaltung von Zertifikaten der Karte zu beurteilen:

- Injektion von Schlüssel
- Generierung des Zertifikats
- Importieren der Zertifikate auf die Karte
- Wiederherstellung von Schlüssel
- Entsperren des PIN-Codes
- Zertifikaterneuerung
- Zertifikatsrevokation
- Funktionalität NFC-Chip

2.2.2 Verwendung von Zertifikaten

2.2.2.1 Authentifizierung

- Windows-Anmeldung mit 2-Faktor-Authentifizierung.
- SAP mit Ultralogon und Secude
- SSO-Portal des ISC-EJPD

2.2.2.2 Signatur

- Senden und Empfangen von Nachrichten über Outlook mit S/MIME.
- Desktop Signer

2.2.2.3 Verschlüsselung und Entschlüsselung

- Senden und Empfangen von Nachrichten über Outlook
- ArmaSuisse SecureCenter

2.2.3 Software-Tools

2.2.3.1 Middleware

Software	Version
SafeNet Authentication Client R1	10.9.5624 POST_GA
SafeNet Authentication Client R2	10.9.6901.0 POST_GA

2.2.3.2 SG-PKI Toolbox

Tool	Version
BulkCardProduction	1.14.xxxxxx
Key Recovery	1.14.xxxxxx
CMC	1.14.xxxxxx
PIN Reset	1.14.xxxxxx
Revoke Wizard	1.14.xxxxxx
Token Unseal	1.14.xxxxxx
TN Admin	1.14.xxxxxx
Walk-In-Wizard	1.14.xxxxxx
Certificate Renewal	1.14.xxxxxx
Certificate Renewal 2	1.14.xxxxxx
SCMS Management	1.14.xxxxxx
SCMS Mailing	1.14.xxxxxx
1.14.xxxxxx	1.14.xxxxxx
SCMS Quality	1.14.xxxxxx
SCMS Production	1.14.xxxxxx
SMCS RIO	1.14.xxxxxx

2.2.3.3 Software der Bundesverwaltung

- Microsoft Windows
- Microsoft Outlook
- Desktop Signer
- SSO-Portal

2.2.4 Plattformen

- Standard-Workstation der Bundesverwaltung Windows 11 64-Bit
- APS 2020 Windows 11 64-Bit
- Key Injection Station
- Microsoft Edge

2.2.5 Readers / Reader Drives

- APS 2020 Windows 11 64-Bit
- Key Injection Station
- OMNIKEY HID 5422
- Microsoft usbccid-Smartcard-Leser (WUDF) RFID 10.0.26100.3323
- Kontakt

3 Tests

3.1 Gemalto IDPrime MD930

3.1.1 Verwaltung von Zertifikaten und Karten (nur für Klasse B)

3.1.1.1 Schlüsselinjektion

#	Hilfsmittel	Datum	Details	Status
1	SafeNet Authentication Client	30.03.2026	Auslesen der Smartcards	OK
2	BulkCard Production	30.03.2026	Karten prestagen: Injektion von 9 Schlüsseln	OK

3.1.1.2 Generieren von Zertifikaten

#	Hilfsmittel	Datum	Details	Status
1	SafeNet Authentication Client	30.03.2026	Auslesen der erzeugten Zertifikate	OK
2	CMC	30.03.2026	Zertifikate werden generiert	OK
3	Walk-In-Wizard	30.03.2026	Zertifikate werden generiert	OK
4	SCMS Management	30.03.2026	Verwaltung der Zertifikate durch Import	OK

3.1.1.3 Wiederherstellung von Schlüsseln

#	Hilfsmittel	Datum	Details	Status
1	SafeNet Authentication Client	30.03.2026	Key Recovery, Importieren von alten Secure-E-Mail-Zertifikaten	OK
2	Key Recovery Wizard	30.03.2026	Key Recovery, Importieren von alten Secure-E-Mail-Zertifikaten	OK
3	TN Admin	30.03.2026	Auslesen von LRAO- und Adminzertifikaten	OK

3.1.1.4 Entsperren des PIN-Codes

#	Hilfsmittel	Datum	Details	Status
1	SafeNet Authentication Client	30.03.2026	Auslesen der Smartcards	OK
2	PIN-Reset	30.03.2026	Den PIN wechseln nach dem PINResetRequest	OK

3.1.1.5 Erneuerung

#	Hilfsmittel	Datum	Details	Status
1	SafeNet Authentication Client	30.03.2026	Auslesen der Smartcards	OK
2	Certificate Renewal 2 (mit CrossRenewal Funktionalität von Enhanced CA01 auf Enhanced CA02)	30.03.2026	Die neuen Zertifikate werden erzeugt und importiert Der Wechsel von der Enhanced CA01 auf die Enhanced CA02 erfolgt korrekt.	OK

3.1.1.6 Revokation

#	Hilfsmittel	Datum	Details	Status
1	SafeNet Authentication Client	30.03.2026	Auslesen der Smartcards	OK
2	CMC	30.03.2026	Revokation ausgewählter Zertifikate	OK
3	Revoke Wizard	30.03.2026	Revokation ausgewählter Smartcard	OK
4	TN Admin	30.03.2026	Revokation ausgewählter Smartcard	OK

3.1.2 Verwendung von Zertifikaten

3.1.2.1 Authentifizierung

#	Hilfsmittel	Version	Datum	Details	Status
1	Windows-Anmeldung mit 2-Faktor-Authentifizierung	Windows 11 Version 24H2 (26.100.8037)	30.03.2026	Anmeldung mit Smartcard und PIN	OK
2	SAP mit Ultralogon und EGate	egate.admin.ch	30.03.2026	Anmeldung mit Smartcard und PIN	OK
3	SSO-Portal des ISC-EJPD	ISC_EJPD SSO-Portal 4.12.1000	30.03.2026	Anmeldung mit Smartcard und PIN	OK

3.1.2.2 Signatur

#	Hilfsmittel	Version	Datum	Details	Status
1	Senden und Empfangen von Nachrichten über Outlook mit S/MIME	Outlook 2602 Build 19725.29179	30.03.2026	E-Mail signieren	OK
2	Desktop Signer	1.6.1.3	30.03.2026	PDF-Dokumente signieren	OK

3.1.2.3 Verschlüsselung und Entschlüsselung

#	Hilfsmittel	Version	Datum	Details	Status
1	Senden und Empfangen von Nachrichten über Outlook	Outlook 2602 Build 19725.29179	30.03.2026	Verschlüsselte Nachrichten senden und empfangen Signierte Nachrichten senden und empfangen Verschlüsselte und signierte Nachrichten senden und empfangen	OK
2	ArmaSuisse SecureCenter	SecureCenter Wiederverschlüsselung X.509 Umschlüsselung	30.03.2026	Dokumente wiederverschlüsseln	OK

3.2 Gemalto IDPrime MD3930

3.2.1 Verwaltung von Zertifikaten und Karten (nur für Klasse B)

3.2.1.1 Schlüsselinjektion

#	Hilfsmittel	Datum	Details	Status
1	SafeNet Authentication Client	30.03.2026	Auslesen der Smartcards	OK
2	BulkCard Production	30.03.2026	Karten prestagen: Injektion von 9 Schlüsseln	OK

3.2.1.2 Generieren von Zertifikaten

#	Hilfsmittel	Datum	Details	Status
1	SafeNet Authentication Client	30.03.2026	Auslesen der erzeugten Zertifikate	OK
2	CMC	30.03.2026	Zertifikate werden generiert	OK
3	Walk-In-Wizard	30.03.2026	Zertifikate werden generiert	OK
4	SCMS Management	30.03.2026	Verwaltung der Zertifikate durch Import	OK

3.2.1.3 Wiederherstellung von Schlüsseln

#	Hilfsmittel	Datum	Details	Status
1	SafeNet Authentication Client	30.03.2026	Key Recovery, Importieren von alten Secure-E-Mail-Zertifikaten	OK
2	Key Recovery Wizard	30.03.2026	Key Recovery, Importieren von alten Secure-E-Mail-Zertifikaten	OK
3	TN Admin	30.03.2026	Auslesen von LRAO- und Adminzertifikaten	OK

3.2.1.4 Entsperren des PIN-Codes

#	Hilfsmittel	Datum	Details	Status
1	SafeNet Authentication Client	30.03.2026	Auslesen der Smartcards	OK
2	PIN-Reset	30.03.2026	Den PIN wechseln nach dem PINResetRequest	OK

3.2.1.5 Erneuerung

#	Hilfsmittel	Datum	Details	Status
1	SafeNet Authentication Client	30.03.2026	Auslesen der Smartcards	OK
2	Certificate Renewal 2 (mit CrossRenewal Funktionalität von Enhanced CA01 auf Enhanced CA02)	30.03.2026	Die neuen Zertifikate werden erzeugt und importiert Der Wechsel von der Enhanced CA01 auf die Enhanced CA02 erfolgt korrekt.	OK

3.2.1.6 Revokation

#	Hilfsmittel	Datum	Details	Status
1	SafeNet Authentication Client	30.03.2026	Auslesen der Smartcards	OK
2	CMC	30.03.2026	Revokation ausgewählter Zertifikate	OK
3	Revoke Wizard	30.03.2026	Revokation ausgewählter Smartcard	OK
4	TN Admin	30.03.2026	Revokation ausgewählter Smartcard	OK

3.2.2 Verwendung von Zertifikaten

3.2.2.1 Authentifizierung

#	Hilfsmittel	Version	Datum	Details	Status
1	Windows-Anmeldung mit 2-Faktor-Authentifizierung	Windows 11 Version 24H2 (26.100.8037)	30.03.2026	Anmeldung mit Smartcard und PIN	OK
2	SAP mit Ultralogon und EGate	egate.admin.ch	30.03.2026	Anmeldung mit Smartcard und PIN	OK
3	SSO-Portal des ISC-EJPD	ISC_EJPD SSO-Portal 4.1.2.1000	30.03.2026	Anmeldung mit Smartcard und PIN	OK

3.2.2.2 Signatur

#	Hilfsmittel	Version	Datum	Details	Status
1	Senden und Empfangen von Nachrichten über Outlook mit S/MIME	Outlook 2016	30.03.2026	E-Mail signieren	OK
2	Desktop Signer	1.1.6.5	30.03.2026	PDF-Dokumente signieren	OK

3.2.2.3 Verschlüsselung und Entschlüsselung

#	Hilfsmittel	Version	Datum	Details	Status
1	Senden und Empfangen von Nachrichten über Outlook	Outlook 2602 Build 19725.29179	30.03.2026	Verschlüsselte Nachrichten senden und empfangen Signierte Nachrichten senden und empfangen Verschlüsselte und signierte Nachrichten senden und empfangen	OK
2	ArmaSuisse SecureCenter	SecureCenter Wiederverschlüsselung X.509 Umschlüsselung	30.03.2026	Dokumente wiederverschlüsseln	OK

3.2.3 Verwaltung von Zertifikaten und Karten (nur für Klasse B)

3.2.3.1 Schlüsselinjektion

#	Hilfsmittel	Datum	Details	Status
1	SafeNet Authentication Client	30.03.2026	Auslesen der Smartcards	OK
2	BulkCard Production	30.03.2026	Karten prestagen: Injektion von 9 Schlüsseln	OK

3.2.3.2 Generieren von Zertifikaten

#	Hilfsmittel	Datum	Details	Status
1	SafeNet Authentication Client	30.03.2026	Auslesen der erzeugten Zertifikate	OK
2	CMC	30.03.2026	Zertifikate werden generiert	OK
3	Walk-In-Wizard	30.03.2026	Zertifikate werden generiert	OK
4	SCMS Management	30.03.2026	Verwaltung der Zertifikate durch Import	OK

3.2.3.3 Wiederherstellung von Schlüsseln

#	Hilfsmittel	Datum	Details	Status
1	SafeNet Authentication Client	30.03.2026	Key Recovery, Importieren von alten Secure-E-Mail-Zertifikaten	OK
2	Key Recovery Wizard	30.03.2026	Key Recovery, Importieren von alten Secure-E-Mail-Zertifikaten	OK
3	TN Admin	30.03.2026	Auslesen von LRAO- und Adminzertifikaten	OK

3.2.3.4 Entsperren des PIN-Codes

#	Hilfsmittel	Datum	Details	Status
1	SafeNet Authentication Client	30.03.2026	Auslesen der Smartcards	OK
2	PIN-Reset	30.03.2026	Den PIN wechseln nach dem PINResetRequest	OK

3.2.3.5 Erneuerung

#	Hilfsmittel	Datum	Details	Status
1	SafeNet Authentication Client	30.03.2026	Auslesen der Smartcards	OK
2	Certificate Renewal 2 (mit CrossRenewal Funktionalität von Enhanced CA01 auf Enhanced CA02)	30.03.2026	Die neuen Zertifikate werden erzeugt und importiert Der Wechsel von der Enhanced CA01 auf die Enhanced CA02 erfolgt korrekt.	OK

3.2.3.6 Revokation

#	Hilfsmittel	Datum	Details	Status

1	SafeNet Authentication Client	30.03.2026	Auslesen der Smartcards	OK
2	CMC	30.03.2026	Revokation ausgewählter Zertifikate	OK
3	Revoke Wizard	30.03.2026	Revokation ausgewählter Smartcard	OK
4	TN Admin	30.03.2026	Revokation ausgewählter Smartcard	OK

3.2.4 Verwendung von Zertifikaten

3.2.4.1 Authentifizierung

#	Hilfsmittel	Version	Datum	Details	Status
1	Windows-Anmeldung mit 2-Faktor-Authentifizierung	Windows 11 Version 24H2 Build (26100.8037)	30.03.2026	Anmeldung mit Smartcard und PIN	OK
2	SAP mit Ultralogon und EGate	egate.admin.ch	30.03.2026	Anmeldung mit Smartcard und PIN	OK
3	SSO-Portal des ISC-EJPD	ISC_EJPD SSO-Portal 4.1.2.1000	30.03.2026	Anmeldung mit Smartcard und PIN	OK

3.2.4.2 Signatur

#	Hilfsmittel	Version	Datum	Details	Status
1	Senden und Empfangen von Nachrichten über Outlook mit S/MIME	Outlook 2602 Build 19725.29179	30.03.2026	E-Mail signieren	OK
2	Desktop Signer	1.6.1.3	30.03.2026	PDF-Dokumente signieren	OK

3.2.4.3 Verschlüsselung und Entschlüsselung

#	Hilfsmittel	Version	Datum	Details	Status
1	Senden und Empfangen von Nachrichten über Outlook	Outlook 2602 Build 19725.29179	30.03.2026	Verschlüsselte Nachrichten senden und empfangen Signierte Nachrichten senden und empfangen Verschlüsselte und signierte Nachrichten senden und empfangen	OK
2	ArmaSuisse SecureCenter	SecureCenter Wiederverschlüsselung X.509 Umschlüsselung	30.03.2026	Dokumente wiederverschlüsseln	OK

999

3.3 Gemalto IDPrime MD940

3.3.1 Verwaltung von Zertifikaten und Karten (Nur für Klasse A – qualifizierte Signaturzerti-fikate)

Hinweis: Bitte Bemerkungen zur Gemalto IDPrime MD940 im Kapitel 6 beachten!

#	Hilfsmittel	Version	Datum	Details	Status
1	CMC	1.13.2,16841	30.03.2026	Auslesen und Initialisierung der Smartcard	OK
2	SafeNet Authentication Client	10.9.6901.0	30.03.2026	Importieren des Zertifikats auf die Smartcard durch das Export-Menu	OK
3	SafeNet Authentication Client	10.9 6901.0	30.03.2026	Importieren des Zertifikats auf die Smartcard durch das Export-Menu	OK
4	DesktopSigner	1.6.1.3	30.03.2026	PDF-Dokumente signieren	OK

4 Reader Kompatibilität

Reader	Kompatibilität					Freigabe (Ja/Nein)
	MD830 Rev. A	**MD830 Rev. B**	**MD930**	**MD940**	**3930 (NFC)**	
OMNIKEY 5422	OK	OK	OK	OK	OK	Ja
Keyboard	NOK	NOK	NOK	NOK	NOK	Nein
NFC-Reader HP/DELL/Lenovo Standard BAB Clients 2024	NA	NA	NA	NA	OK	Nein

4.1 Begründung

Der Reader OMNIKEY 3121 wird seit der SAC-Version 10.8 nicht länger unterstützt und wird daher vom BIT nicht mehr supported. Ebenfalls sollten die Keyboard-Reader nicht verwendet werden, da aufgrund unterschiedlich verbauter Chips die Kompatibilität nicht garantiert ist.

Die Gemalto ID Prime 3930 Karten mit NFC- Funktionalität sind im Rahmen eines Projektes getestet worden und neu für den allgemeinen Einsatz mit Klasse B Zertifikaten freigegeben.

5 In der Evaluationsphase

Hardware	Status	Beschreibung	Geplante Evaluation
Gemalto IDPrime 3930	EVALUIERT,	**NFC-Smartcard** mit dem Kryptochip der gemalto IDPrime MD 930	02.03.2024 Evaluierung erfolgt und Karte **freigegeben ab 01.04.2025 und im A006 (Anhang) getestet**

6 Dekommissionierte Kartentypen

Hardware	Status	(ab) Datum	Bemerkung
Gemalto IDPrime MD830	Dekommissioniert	30.03.2026	Einsatz der Karte nicht mehr zulässig.
Gemalto IDPrime MD830 Rev B	Dekommissioniert	30.03.2026	Einsatz der Karte für Neuausstellung nur noch bis Ende 2026 erlaubt.
Gemalto ID Prime MD940	obsolet	01.01.2026	**Ab 01.01.2026 werden KEINE Klasse A Zertifikate mehr auf Smartcards ausgestellt. Die 940er Karte ist demnach obsolet, sobald die bestehenden Klasse A Zertifikaten abgelaufen sind.**