Annexe 1 du Standard A006

Rapport 2022 des tests et liste des cartes

Nom du projet: **Annexe 1 du Standard A006**

Numéro du projet:

Version: **2.0**

Etat	En élaboration	En vérification	Approuvé
	☐	☐	×

Beteiligter Personenkreis	
Auteur:	Metaj Beatrice PS-PSC-TRU, Kamel Dridi BS-BSC-Testi1
Approbation:	SG-PKI Mgmt Board
Utilisateurs:	LRAO
Pour information:	Alle PS-POs

Suivi des modifications			
Date	**Version**	**Auteur**	**Modification**
29.04.2022	1.91	Kamel Dridi	Initialversion
03.05.2022	1.92	Beatrice Metaj	Adaptation des versions des clients PKI-Toolbox - MiddleWare - PKI-ToolBox
09.06.20222	1.93	Kamel Dridi	Premiers résultats des tests
22.06.20222	1.94	Kamel Dridi	Version definitive
23.06.2022	1.95	Beatrice Metaj	Contrôle du contenu
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

Contenu

1 But de l’annexe 1 du Standard A006

Ce document contient les résultats des tests réalisés avec les différentes compositions de cartes, middleware, environnements de plateforme et usage des certificats dans les applications standard.

Les tests sont effectués sur la seule base des cas définis dans l’annexe 1 du stantards A006.

1.1 Mise à jour de l’annexe 1 du Standard A006

L’annexe 1 du Standard A006 fait l’objet d’une mise à jour annuelle, sur la base du cycle de développement de la suite logicielle SG-PKI TerraNova, ainsi que les conditions du marché des cartes à puces.

Les producteurs de cartes Gemalto délivrent les Middlewares compatibles avec les cartes vendues.

La mise à jour du présent document est assurée par l’OFIT

2 Description des tests

2.1 Type de cartes

Afin de mieux comprendre les comptabilités, les tests sont réalisés par type de carte. Ces cartes sont :

- Gemalto IDPrime MD930
- Gemalto IDPrime MD830 Rev. A
- Gemalto IDPrime MD830 Rev. B
- Gemalto IDPrime MD840

Pour les issuing CAs et Policies

- CA2 Enhanced pour classe B prestaged B BUND
- CA2 Enhanced pour classe B prestaged B FUB
- CA02 regulated pour classe A

2.2 Fonctionnalités

Pour chaque cartes, les fonctionnalités sont testées en deux groupes : gestion des certificats et utilisation des certificats.

Les tests sont executés dans les deux environnements Acceptance et Production.

2.2.1 Gestion des certificats et des cartes

- Injection des clefs
- Génération ce certificats
- Importation des certificats sur la carte
- Récupération de clefs
- Déblocage du code PIN
- Renouvellement
- Révocation

2.2.2 Utilisation des certificats

2.2.2.1 Authentification

- Ouverture de session Windows avec authentification à 2 facteurs
- SAP avec Ultralogon et Secude
- Portail SSO du CSI-DFJP

2.2.2.2 Signature

- Envoi et réception de messages par Outlook avec S/MIME
- Open eGov LocalSigner
- Desktop Signer

2.2.2.3 Chiffrement/déchiffrement

- Envoi et réception de messages par Outlook
- ArmaSuisse SecureCenter

2.2.3 Outils logiciels

2.2.3.1 Middleware

Safenet Authentication Client	10.8.1803.0 R2

2.2.3.2 SG-PKI ToolBox

BulkCardProduction	1.10.xxxxx
Key Recovery	1.10.xxxxx
LRA (CMC)	1.10.xxxxx
PIN-Reset	1.10.xxxxx
Register Smartcard Wizard	1.10.xxxxx
Revoke Wizard	1.10.xxxxx
Token Unseal	1.10.xxxxx
TN Admin	1.10.xxxxx
Walk-In-Wizard	1.10.xxxxx
SCMS Management	1.10.xxxxx
SCMS Mailing	1.10.xxxxx
SCMS Documents	1.10.xxxxx
SCMS Quality	1.10.xxxxx
SCMS Production	1.10.xxxxx
SCMS RIO	1.10.xxxxx
Certificate Renewal	1.10.xxxxx

2.2.3.3 Logiciels de l'administration fédérale

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

2.2.4 Plateformes

- Station de travail standard de l'administration fédérale Windows 10 64bits
- APS 2020 Windows 10 64 bits
- Key Injection Station
- Microsoft Edge

2.2.5 Readers / Reader Drives

- OMNIKEY HID 3121 (attention voir aussi chap. 4 !)
- APS 2020 Windows 10 64 bits
- Key Injection Station
- Smardcard Reader Driver R01.12.6.5 x32/x32 für PNIKEY 3121/3621/3821

3 Tests

3.1 Gemalto IDPrime MD830 Rev. B

3.1.1 Gestion des certificats et des cartes

3.1.1.1 Injection des clefs

#	Outil	Date, Heure	Détails	1
1	Safenet Authentication Client	01-06-2002	Lire les smartcards	OK
2	BulkCardProduction	03-06-2022	Faire le perstaging des smartcards: Injection des 9 clées	OK

3.1.1.2 Génération de certificats

#	Outil	Date, Heure	Détails	1
1	Safenet Authentication Client	02-06-2022	Lire des des certificats crées	OK
2	LRA (CMC)	02-06-2022	Création des Certificats	OK
3	Walk-In-Wizard	02-06-2022	Création des Certificats	OK
4	SCMS Management	LRA (CMC)	Mangement des Certificats par import	OK

3.1.1.3 Récupération de clefs

#	Outil	Date, Heure	Détails.	1
1	Safenet Authentication Client	25-05-2022	KeyRecovery, Import des anciens secure-email-certificats	OK
2	Key Recovery	30-05-2022	KeyRecovery, Import des anciens secure-email-certificats	OK
3	TN Admin	30-05-2022	Lire le s certificats des LRAOS et Admins	OK

3.1.1.4 Déblocage du code PIN

#	Outil	Date, Heure	Détails.	1
1	Safenet Authentication Client	20-05-2022	Lire les smartcards	OK
2	PIN-Reset	20-05-2022	Changer le PIN aprés PINResetRequest	OK

3.1.1.5 Renouvellement

#	Outil	Date, Heure	Détails	1
1	Safenet Authentication Client	14-05-2022	Lire les Smartcards	OK
2	Certificate Renewal	25-06-2022	Lire les nouveaus certificats	OK

1=Station de travail standard de l'administration fédérale Windows 7 32bits; 2=Station de travail standard de l'administration fédérale Windows 7 64bits; 3=APS 2020 Windows 10 64 bits; 4=VDI Thin Client (Windows 7 32 bits); 5=VDI avec le client Citrix Receiver (par le Web); 6=Station LRA, 7=Key Injection Station

3.1.1.6 Révocation

#	Outil	Date, Heure	Détails	1
1	Safenet Authentication Client	20-05-2022	Lire les Smartcards	OK
2	LRA (CMC)	20-05-2022	Choisir le certificate et revocation	OK
3	Revoke Wizard	30-05-2022	Revocation-Wizard :Choisir la smartcard et revocation	OK
4	TN Admin	30-05-2022	TNAdmin:Choisir la smartcard et revocation	OK

3.1.2 Utilisation des certificats

3.1.2.1 Authentification

#	Outil	Version	Date, Heure	Détails
1	Ouverture de session Windows avec authentification à 2 facteurs	Windows 10 Version 19042.1706	07-06-2022	Avec la smardcard s' authenticier avec la carte et le PIN
2	SAP avec Ultralogon et eGate	eGate.admin.ch	30-05-2022	Avec la smardcard s' authenticier avec la carte et le PIN
3	Portail SSO du CSI-DFJP	ESC_EJPD SSO-Portal 3.3.0.1000	07-06-2022	Avec la smardcard s' authenticier avec la carte et le PIN

3.1.2.2 Signature

#	Outil	Version	Date, Heure	Détails
1	Envoi et réception de messages par Outlook avec S/MIME	Outlook 2016	30-05-2022	Signé et crypté
2	Open eGov LocalSigner	4.2.13	30-06-2022	Signer des documents PDF
3	Desktop Signer	V.1.1.6.5	08-06-2022	Signer des documents PDF

3.1.2.3 Chiffrement/déchiffrement

#	Outil	Version	Date, Heure	Détails
1	Envoi et réception de messages par Outlook	Outlook 2016	07-06-2022	Envoyer et recevoir des messages chiffrés Envoyer et recevoir des messages cryptés Envoyer et recevoir des messages chiffrés et cryptés
2	ArmaSuisse SecureCenter	Réchiffrément Secure center X.509	07-06-2022	Ré-chiffrer des documents

3.2 Gemalto IDPrime MD830 Rev. A

3.2.1 Gestion des certificats et des cartes (seulement pour Classe B)

3.2.1.1 Injection des clefs

#	Outil	Date, Heure	Détails	1
1	Safenet Authentication Client	01-06-2002	Lire les Smartcards	OK
2	BulkCardProduction	03-06-2022	Faire lepPerstagei des smartcards: Injection de 9 clées	OK

3.2.1.2 Génération de certificats

#	Outil	Date, Heure	Détails	1
1	Safenet Authentication Client	02-06-2022	Lire des des certificats crées	OK
2	LRA (CMC)	02-06-2022	Création des Certificats	OK
3	Walk-In-Wizard	02-06-2022	Création des Certificats	OK
4	SCMS Management	02-06-2022	Mangement des Certificats par import	OK

3.2.1.3 Récupération de clefs

#	Outil	Date, Heure	Détails.	1
1	Safenet Authentication Client	25-05-2022	KeyRecovery, Import des anciens secure-email-certificats	OK
2	Key Recovery	30-05-2022	KeyRecovery, Import des anciens secure-email-certificats	OK
3	TN Admin	30-05-2022	Lire les certificats des LRAOS et Admins	OK

3.2.1.4 Déblocage du code PIN

#	Outil	Date, Heure	Détails.	1
1	Safenet Authentication Client	20-05-2022	Lire des smartcard	OK
2	PIN-Reset	20-05-2022	Changer le PIN aprés PINReserRequest	OK

3.2.1.5 Renouvellement

#	Outil	Date, Heure	Détails	1
1	Safenet Authentication Client	14-05-2022	Lire des smartcards	OK
2	Certificate Renewal	25-06-2022	Lire les nouveaux certificats	OK

3.2.1.6 Révocation

#	Outil	Date, Heure	Détails	1
1	Safenet Authentication Client	20-05-2022	Lire des smartcard	OK
2	LRA (CMC)	20-05-2022	Choisir le certificate et revocation	OK
3	Revoke Wizard	30-05-2022	Revocation-Wizard :Choisir la smartcard et revocation	OK
4	TN Admin	30-05-2022	TNAdmin:Choisir la smartcard et revocation	OK

3.2.2 Utilisation des certificats

3.2.2.1 Authentification

#	Outil	Version	Date, Heure	Détails	1
1	Ouverture de session Windows avec authentification à 2 facteurs	Windows 10 Version 19042.1706	07-06-2022	Avec la smardcard s' authentifier avec la carte et le PIN	OK
2	SAP avec Ultralogon et eGate	eGate.admin.ch	30-05-2022	Avec la smardcard s' authentifier avec la carte et le PIN	OK
3	Portail SSO du CSI-DFJP	ESC_EJPD SSO-Portal 3.3.0.1000	07-06-2022	Avec la smardcard s' authentifier avec la carte et le PIN	OK

3.2.2.2 Signature

#	Outil	Version	Date, Heure	Détails.	1
1	Envoi et réception de messages par Outlook avec S/MIME	Outlook 2016	30-05-2022	Signé et crypté	OK
2	Open eGov LocalSigner	4.2.13	30-06-2022	Signer des documents PDF	OK
3	Desktop Signer	V.1.1.6.5	08-06-2022	Signer des documents PDF	OK

3.2.2.3 Chiffrement/déchiffrement

#	Outil	Version	Date, Heure	Détails	1
1	Envoi et réception de messages par Outlook	Outlook 2016	07-06-2022	Envoyer et recevoir des messages chiffrés Envoyer et recevoir des messages cryptés Envoyer et recevoir des messages chiffrés et cryptés	OK
2	ArmaSuisse SecureCenter	Réchiffrage Secure center X.509 Umschlüsselung	07-06-2022	Réchiffrer des Documents	OK

3.3 Gemalto IDPrime MD930

3.3.1 Gestion des certificats et des cartes (seulement pour classe B)

3.3.1.1 Injection des clefs

#	Outil	Date, Heure	Détails	1
1	Safenet Authentication Client	01-06-2002	Lire des smartcards	OK
2	BulkCardProduction	03-06-2022	Faire le perstageing des smartcards: Injection de 9 clées	OK

3.3.1.2 Génération de certificats

#	Outil	Date, Heure	Détails	1
1	Safenet Authentication Client	02-06-2022	Lire des des certificats crées	OK
2	LRA (CMC)	02-06-2022	Création des Certificats	OK
3	Walk-In-Wizard	02-06-2022	Création des Certificats	OK
4	SCMS Management	02-06-202	Mangement des Certificats par import	OK

3.3.1.3 Récupération de clefs

#	Outil	Date, Heure	Détails.	1
1	Safenet Authentication Client	25-05-2022	KeyRecovery, Import des anciens certificats secure-email-	OK
2	Key Recovery	30-05-2022	KeyRecovery, Import des anciens certificats secure-email-	OK
3	TN Admin	30-05-2022	Lire les certificats des LRAOs et Admins	OK

3.3.1.4 Déblocage du code PIN

#	Outil	Date, Heure	Détails.	1
1	Safenet Authentication Client	20-05-2022	Lire des smartcards	OK
2	PIN-Reset	20-05-2022	Changer le PIN aprés PINResetRequest	OK

3.3.1.5 Renouvellement

#	Outil	Date, Heure	Détails	1
1	Safenet Authentication Client	14-05-2022	Lire des martcards	OK
2	Certificate Renewal	25-06-2022	Lire les nouveaus certificats	OK

1=Station de travail standard de l'administration fédérale Windows 7 32bits; 2=Station de travail standard de l'administration fédérale Windows 7 64bits; 3=APS 2020 Windows 10 64 bits; 4=VDI Thin Client (Windows 7 32 bits); 5=VDI avec le client Citrix Receiver (par le Web); 6=Station LRA, 7=Key Injection Station

3.3.1.6 Révocation

#	Outil	Date, Heure	Détails	1
1	Safenet Authentication Client	20-05-2022	Lire des martcards	OK
2	LRA (CMC)	20-05-2022	Choisir le certificate et revocation	OK
3	Revoke Wizard	30-05-2022	Revocation-Wizard :Choisir la smartcard et revocation	OK
4	TN Admin	30-05-2022	TNAdmin:Choisir la smartcard et revocation	OK

3.3.2 Utilisation des certificats

3.3.2.1 Authentification

#	Outil	Version	Date, Heure	Détails
1	Ouverture de session Windows avec authentification à 2 facteurs	Windows 10 Version 19042.1706	07-06-2022	Avec la smardcard s' authenticier avec la carte et le PIN
2	SAP avec Ultralogon et eGate	eGate.admin.ch	30-05-2022	Avec la smardcard s' authenticier avec la carte et le PIN
3	Portail SSO du CSI-DFJP	ESC_EJPD SSO-Portal 3.3.0.1000	07-06-2022	Avec la smardcard s' authenticier avec la carte et le PIN

3.3.2.2 Signature

#	Outil	Version	Date, Heure	Détails
1	Envoi et réception de messages par Outlook avec S/MIME	Outlook 2016	30-05-2022	Signé et crypté
2	Open eGov LocalSigner	4.2.13	30-06-2022	Signer des documents PDF
3	Desktop Signer	V.1.1.6.5	08-06-2022	Signer des documents PDF

3.3.2.3 Chiffrement/déchiffrement

#	Outil	Version	Date, Heure	Détails
1	Envoi et réception de messages par Outlook	Outlook 2016	07-06-2022	Envoyer et recevoir des messages chiffrés Envoyer et recevoir des messages cryptés Envoyer et recevoir des messages chiffrés et cryptés
2	ArmaSuisse SecureCenter	Réchiffrage Secure center X.509	07-06-2022	Réchiffrer des dokuments

3.4 Gemalto IDPrime MD840 Rev. B

3.4.1 Gestion des certificats et des cartes (seulement pour Classe A – qualified signature certificates)

#	Outil	Version	Date, Heure	Détails	1
1	CMC	1.10	22-05-2022	Lire et initialisation de la smartcard	OK
2	SafeNetClient	10.8.R2	22-05-2022	Import du certificat sur la smartcard par le menu export	OK
3	Open eGov LocalSigner	4.2.13	22-05-2022	Signer des documents PDF	OK
4	DesktopSigner	V.1.1.6.5	22-05-2022	Signer des documents PDF	OK

4 En phase d'évaluation

#	HW	Status	Description	Plan de délivrement
1	OmniKey 5422	En phase d'évaluation Non délivrée	Le lecteur externe OmniKey 3121 n'est plus supporté par SAC 10.8. Le lecteur supporté par la middleware de Safenet est le Omnikey 5422. Ce lecteur est en phase d'évaluation et pas encore délivré par la SG-PKI	Q1/2023