Sagem Défense Sécurité
SAFRAN Group

CIBLE DE SECURITE

CARTE MORPHO CITIZ 32

(COMPOSANT ATMEL)

APPLICATION IAS-EGOV

Critères Communs version 2.2
EAL 4 Augmenté

(ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4)

Version Publique

Version 1.0
2006

Sagem Défense Sécurité
SAFRAN Group

SOMMAIRE

1. INTRODUCTION DE LA CIBLE DE SECURITE

1.1 IDENTIFICATION DE LA CIBLE DE SECURITE

Identification du document :

Titre	:	Cible de sécurité Carte Morpho-Citiz 32 – Composant Atmel : Application IAS-eGOV
Version de révision	:	1.1
Identifiant de la cible de sécurité	:	SK 00000 52269

Identification de la TOE :

Identifiant du composant	:	Composant Atmel : AT90SC12836RCT – (référence AT58819 Rev E)
Identifiant du composant masqué	:	MC32/AT58819E/1.0.1
Guide administrateur	:	SK 00000 51475 - 1.01 - MC32 - Guide administrateur
Guide utilisateur	:	SK 00000 51481 - 1.01 - MC32 - Guide utilisateur
Guide d'installation et de démarrage	:	SK 00000 51482 - 1.01 - MC32 - Procédure d'installation
Guide de livraison	:	SK 00000 25737 - 1.04 – Procédure de Livraison

Conformité aux CC :

Version	:	2.2
Niveau d'assurance	:	EAL4 augmenté des composants d'assurance ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4.
Niveau de résistance des fonctions	:	SOF – Elevé
Référence du certificat du composant	:	2005/20

1.2 VUE D'ENSEMBLE DE LA CIBLE DE SECURITE

Cette cible de sécurité spécifie les exigences fonctionnelles et d'assurance de sécurité, applicables à l'application d'administration électronique conforme IAS de la carte Morpho-Citiz 32 appelée ci-après application IAS-eGOV.

La TOE décrite dans le cadre de cette cible de sécurité se compose d'un logiciel embarqué sur un composant type carte à puce, référencé AT90SC12836RCT.

Le composant AT90SC12836RCT a fait l'objet d'une évaluation séparée. L'évaluation de la TOE est donc une composition de l'évaluation du logiciel embarqué sur le composant AT90SC12836RCT certifié en révision E sous la référence 2005/20.

Dans son environnement d'utilisation, l'application IAS-eGOV réalise les services d'administration électronique tels que définis dans les documents **[R10 – AREAK1]** et **[R11 – AREAK2]**.

L'application IAS-eGOV est un support au développement de l'administration électronique (e-administration) au travers des services disponibles répondant essentiellement aux nouveaux besoins de l'administration électronique (tels que définis par l'ADAE).

Dans le cadre des contextes de l'administration électronique, l'application IAS-eGOV offre des services de signature électronique répondant aux caractéristiques des dispositifs sécurisés de création de signature électronique (SSCD) permettant en particulier la mise en oeuvre de certificats dits « qualifiés ».

Cette cible de sécurité spécifie donc les exigences fonctionnelles de sécurité et les exigences d'assurance de sécurité applicables aux services de signature électronique dits « sécurisés » de l'application IAS-eGOV.

Dans son environnement d'utilisation, l'application IAS-eGOV réalise les services de signature électronique sécurisés conformes à la directive européenne **[R6 – Directive]** transcrite dans le profil de protection **[R4 – SSCD T3]**. Ces fonctions sont :

- La génération de bi-clé de signature électronique (SCD/SVD),
- La destruction de bi-clé de signature électronique (SCD/SVD),
- Le chargement de clé privée de signature électronique (SCD),
- La création de signature électronique.

Le niveau d'assurance du produit spécifié dans la présente cible de sécurité et de sa documentation est EAL 4 augmenté des composants d'assurance ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4.

Le niveau de résistance pour les exigences de sécurité fonctionnelles est « élevé » (SOF High).

1.3 CONFORMITE AUX CC

Cette cible de sécurité est conforme aux Critères Communs V2.2 **[R1 – CC]**.

Cette cible de sécurité est conforme au profil de protection **[R3 – SSCD T2]** et **[R4 – SSCD T3]**. Elle est également conforme au profil de protection **[R2 – 9911]**.

La cible de sécurité est pour sa part conforme à la partie 2 des Critères Communs V2.2 étendue par l'exigence FPT_EMSEC définie dans les profils de protection **[R3 – SSCD T2]** et **[R4 – SSCD T3]**.

La cible de sécurité est conforme à la partie 3 des CC.

1.4 ORGANISATION DU DOCUMENT

La présente cible de sécurité est organisée en 8 chapitres de la façon suivante :

Chapitre 1 : Présente introduction ;
Chapitre 2 : Description générale de la TOE qui fournit des informations générales sur la TOE qui permettent d'introduire les choix des exigences de sécurité ;
Chapitre 3 : Présentation de l'environnement de sécurité de la TOE dans lequel la TOE est exploitée. Il décrit en particulier les biens à protéger, les utilisateurs intervenant sur la TOE, les hypothèses ainsi que les menaces applicables et les politiques de sécurité organisationnelles ;
Chapitre 4 : Présentation des objectifs de sécurité satisfaits par la TOE dans son environnement d'utilisation.
Chapitre 5 : Présentation des exigences de sécurité satisfaites par la TOE et son environnement, en terme d'exigences fonctionnelles d'une part et d'exigences d'assurance sécurité d'autre part ;
Chapitre 6 : Présentation des définitions générales des fonctions de sécurité et des mesures d'assurance mises en œuvre par la TOE répondant aux exigences fonctionnelles et d'assurances ;
Chapitre 7 : Présentation des profils de protection existants auxquels la présente cible de sécurité se réfère ;

1.5 DOCUMENTS DE RÉFÉRENCE

[R1 – CC] : Common Criteria for Information Technology Security Evaluation- Version 2.2, January 2004.
[R2 – 9911] : Eurosmart Protection Profile, Smart Card Integrated Circuit With Embedded Software, PP/9911, v2.0, june 1999
[R3 – SSCD T2] : Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001.
[R4 – SSCD T3] : Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001.
[R5 – 9806] : Protection Profile, Smartcard Integrated Circuit PP/9806, v2, September 1998
[R6 – Directive] : DIRECTIVE 1999/93/EC DU PARLEMENT EUROPEEN ET DU CONSEIL du 13 décembre1999 sur un cadre communautaire pour les signatures électroniques.

[R7 – Algo] :	Algorithmes et paramètres des algorithmes, liste des algorithmes et des paramètres éligibles pour les signatures électroniques tels que définis dans la directive 1999/93/EC, article 9 sur le « Comité sur les signatures électroniques » de la Directive.
[R8 – AIP] :	SK 0000020920 – 1.23 – Spécifications fonctionnelles de l'application AIP SK 0000053628 - Addendum spécifications fonctionnelles de l'application AIP
[R9 – E-ADMIN] :	SK 0000020918 – 1.19 – Spécification de l'application E-ADMINISTRATION
[R10 – AREAK1] :	CWA 14890-1 : Application Interface for smart cards used as Secure Signature Creation Devices – Part 1: Basic requirements – Avril 2004 (AREA-K-1)
[R11 – AREAK2] :	CWA 14890-2 : Application Interface for smart cards used as Secure Signature Creation Devices – Part 2: Additional Services – Mai 2004 (AREA-K-2)
[R12 – 7816 – 4] :	ISO/IEC 7816 – 4: Identification cards Integrated circuits cards with contacts Part 4 – Inter-industry commands for interchange
[R13 – ERRATUM] :	Plate-forme commune pour l'e-ADMINISTRATION Spécification technique : Erratum à la version 1.01

1.6 TERMINOLOGIE

Administrateur : Un utilisateur qui effectue l'initialisation de la cible d'évaluation (TOE), la personnalisation de la TOE ou d'autres fonctions administratives pour la TOE.

Application de création de signature (SCA) : Application utilisée pour créer une signature électronique, exclusion faite du SSCD. c'est-à-dire, la SCA est un ensemble d'éléments d'application servant à :

(a) Effectuer la présentation des DTBS au signataire avant le processus de signature selon la décision du signataire,

(b) Envoyer une représentation des DTBS à la TOE si le signataire indique par une entrée ou une action non interprétable son intention de signer,

(c) Attacher la signature électronique qualifiée générée par la TOE aux données ou à fournir la signature électronique qualifiée comme des données distinctes.

Application de génération de certification (CGA) : Ensemble d'éléments d'application qui demande les données afférentes à la vérification de la signature à partir du SSCD pour la génération du certificat qualifié. La CGA demande la génération d'une paire SCD/SVD correspondante par le SSCD, si les SVD demandées n'ont pas encore été générées par le SSCD. La CGA vérifie l'authenticité des SVD au moyen (a) d'une preuve du SSCD de correspondance entre les SCD et les SVD et (b) d'une vérification de l'émetteur et de l'intégrité des SVD reçues.

Attribut de sécurité : Information associée à des sujets, des utilisateurs ou des objets, qui est utilisée pour l'application de la TSP.

Attributs de signature : Informations supplémentaires qui sont signées en même temps que le message de l'utilisateur.

Biens : Informations ou ressources à protéger par les contre-mesures d'une TOE

Certificat : Attestation électronique qui lie des SVD à une personne et confirme l'identité de cette personne. (défini dans la Directive [1], article 2.9)

Certificat qualifié : Certificat qui répond aux exigences visées à l'annexe I de la Directive [1] et qui est fourni par un CSP satisfaisant aux exigences visées à l'annexe II de la Directive [1]. (défini dans la Directive [1], article 2.10)

Cible d'évaluation (TOE) : Un produit ou un système TI et la documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation.

Cible de sécurité (ST) : Un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une TOE identifiée.

Directive : La directive 1999/93/EC du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques [1] est également nommée la 'Directive' dans le reste du PP.

Dispositif sécurisé de création de signature (SSCD) : Dispositif logiciel ou matériel configuré pour mettre en application SCD et qui satisfait aux exigences prévues à l'Annexe III de la Directive [1]. (défini dans la Directive [1], articles 2.5 et 2.6).

Données afférentes à l'authentification de référence (RAD)	:	Données stockées de manière permanente par la TOE pour la vérification de la tentative d'authentification en tant qu'utilisateur autorisé.
Données afférentes à la création de signature (SCD)	:	Données uniques, telles que des codes ou des clés cryptographiques privées, que le signataire utilise pour créer une signature électronique. (défini dans la Directive [1], article 2.4)
Données afférentes à la vérification de signature (SVD)	:	Données, telles que des codes ou des clés cryptographiques publiques, qui sont utilisés pour vérifier la signature électronique. (défini dans la Directive [1], article 2.7)
Données d'authentification	:	Informations utilisées pour vérifier l'identité annoncée d'un utilisateur.
Données d'authentification de vérification (VAD)	:	Données d'authentification, fournies en entrée par l'utilisateur ou données d'authentification, dérivées des caractéristiques biométriques de l'utilisateur.
Données devant être signées (DTBS)	:	Données électroniques devant être signées (comprenant à la fois le message de l'utilisateur et les attributs de la signature).
Données de la TSF (TSF data)	:	Données créées par et pour la TOE, qui pourraient affecter le fonctionnement de la TOE.
Données utilisateur (User data)	:	Données créées par et pour l'utilisateur, qui n'affectent pas le fonctionnement de la TSF.
Invalidation	:	Si un sujet ou un objet est invalidé, il n'est plus disponible dans le système. Il est logiquement détruit.
Objet	:	Entité sur lequel un sujet réalise des opérations. Lorsqu'un sujet est la cible d'une opération, il est vu comme un objet.
Objet de données signé (SDO)	:	Données électroniques auxquelles la signature électronique a été attachée ou associée logiquement comme une méthode d'authentification.
Prestataires de service de certification (CSP)	:	Toute entité ou une personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques. (défini dans la Directive [1], article 2.11)
Raffinement	:	L'addition de détails à un composant.
Représentation des données devant être signées (représentation des DTBS)	:	Données envoyées par la SCA à la TOE pour signature et étant : (a) Une valeur de hash des DTBS ou (b) Une valeur intermédiaire de hash d'une première partie des DTBS et une partie restante des DTBS ou (c) Les DTBS. La SCA indique à la TOE le cas de représentation des DTBS sauf indication implicite. La valeur de hash dans le cas (a) ou la valeur de hash intermédiaire du cas (b) est calculée par la SCA. La valeur de hash dans le cas (b) ou la valeur de hash intermédiaire du cas (c) est calculée par la TOE.
Rôle de l'utilisateur	:	Définit les droits qui sont associés à un utilisateur endossant un rôle. L'utilisateur est authentifié suivant son rôle.
Secret	:	Clés cryptographiques ou valeur de référence pour l'authentification d'un utilisateur basée sur la vérification de son code PIN (i.e. RAD)
Service de fourniture de SSCD	:	Service qui prépare et fournit un SSCD aux adhérents.
Signataire	:	Personne qui détient un SSCD et qui agit soit pour son propre compte, soit pour celui d'une entité ou personne physique ou morale qu'elle représente. (défini dans la Directive [1], article 2.3)
Signature électronique avancée	:	(définie dans la directive [1], article 2.2) Signature électronique qui satisfait aux exigences suivantes : (a) Etre uniquement liée au signataire ; (b) Permettre d'identifier le signataire ; (c) Etre créée par des moyens que le signataire puisse garder sous son contrôle exclusif ; (d) Etre liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.
Signature électronique qualifiée	:	Signature avancée basée sur un certificat qualifié, et créée par un dispositif sécurisé de création de signature conformément à la Directive [1], article 5, paragraphe 1.
SOF- Elevé (SOF-high)	:	Un niveau de la résistance d'une fonction de la TOE tel que l'analyse montre que la fonction concernée fournit une protection adéquate vis-à-vis d'une violation délibérément planifiée ou organisée de la sécurité de la TOE par

des attaquants possédant un potentiel d'attaque élevé.

Sujet	:	Entité active réalisant pour le compte d'un utilisateur ou comme partie de la TOE, des opérations sur les objets.
Système de création de signature (SCS)	:	Un système global qui crée une signature électronique. Le système de création de signature est composé de la SCA et du SSCD.
Utilisateur	:	Une entité (utilisateur humain ou entité TI externe) en dehors de la TOE qui interagit avec la TOE.
Autorité de domaine	:	Utilisateur ayant en charge l'administration d'un domaine dans l'architecture de fichier de la carte Morpho-Citiz 32.

1.7 GLOSSAIRE

AC	:	Autorité de Certification
ADAE	:	Agence pour le Développement de l'Administration Electronique
ADF	:	Application Directory File
ARR	:	Access Rules References
APDU	:	Application Protocol Data Unit
ATR	:	Answer To Reset
CC	:	Critères Communs
CGA	:	Certification Generation Application
CMD/RSP	:	Commande / Réponse
CSP	:	Certification Service Provider
CVC	:	Certificat Vérifiable par une Carte
DAC	:	Data Access Conditions
DES	:	Data Encryption Standard
DF	:	Directory File
DH	:	Diffie-Helmann
DTBS	:	Data To Be Signed
EAL	:	Evaluation Assurance Level
EF	:	Elementary File
EV	:	Electronic Value
FCI	:	File Control Information
IAS	:	Identification Authentification Signature
MF	:	Master File
OTP	:	One Time Programmable
PIN	:	Personal Identification Number
RAD	:	Reference Authentication Data
RSA	:	Rivest Shamir Adelman
SOF	:	Strength of function
SCA	:	Signature-Creation Application
SCD	:	Signature-Creation Data
SDO	:	Signed Data Object
SM	:	Secure Messaging
SSC	:	Secure Signature Creation
SSCD	:	Secure Signature-Creation Device
ST	:	Security Target
SVD	:	Signature-Verification Data
TI	:	Technologies de l'Information
TOE	:	Target Of Evaluation
TSF	:	TOE Security Functions
TSP	:	TOE Security Policy
VAD	:	Validation Authentication Data

2. DESCRIPTION DE LA TOE

2.1 TYPE DE PRODUIT

La carte Morpho-Citiz 32 est un produit de type « carte à puce » constitué des éléments matériels et logiciels suivants :

- Un logiciel embarqué conçu par Sagem Défense Sécurité.
- Un circuit intégré (CI) (matériel et logiciel dédié) conçu par la société Atmel. Ce micro-circuit appartient à la famille AT90SC sous la référence AT90SC12836RCT (référence AT58819 révision E) développé par la société Atmel, et certifié en révision E sous la référence 2005/20 et conformément au profil de protection [R5 – 9806]. Ce micro-circuit inclut une librairie logicielle cryptographique stockée en ROM : Toolbox 3.x en version 00.03.01.04. Le niveau d'assurance est EAL4 augmenté des exigences d'assurance ADV_IMP.2, ALC_DVS.2, AVA_VLA.4. Le niveau de résistance minimum pour les fonctions de sécurité est : SOF – High.

Le circuit intégré embarque un logiciel dont les caractéristiques sont mentionnées plus loin et comprenant notamment un système d'exploitation incluant des mécanismes de sécurité, ainsi que des applications réalisant les services de la carte Morpho-Citiz 32 et s'appuyant sur le système d'exploitation.

2.1.1 Architecture du logiciel embarqué

Le logiciel embarqué sur la carte Morpho-Citiz 32 se décompose en blocs logiciels qui réalisent les fonctionnalités suivantes :

- Fonctions de gestion des données (données « utilisateur » et secrets) ;
- Fonctions de gestion des traitements des authentifications « utilisateur » ;
- Fonctions de gestion des services de signature électronique sécurisée ;
- Fonction d'initialisation et de personnalisation de la carte Morpho-Citiz 32 ;

L'ensemble de ces blocs logiciels est instancié pour réaliser les applications suivantes :

- L'application d'initialisation et de personnalisation de la carte Morpho-Citiz 32 (notée ci-après AIP) conforme aux spécifications **[R8 – AIP]**. Cette application est invalidée en phase utilisateur ;
- L'application IAS-eGOV présente sur la carte Morpho-Citiz 32 en phase utilisateur (phase 7), conforme aux spécifications **[R9 – E-ADMIN]**. Elle réalise des services de type IAS répondant aux besoins de l'administration électronique. L'application IAS-eGOV peut être instanciée plusieurs fois ;

Le gestionnaire d'application dispatche les commandes vers l'application concernée et maintient une étanchéité dans l'usage des services (fonctions) de la carte entre les différentes applications qui les sollicitent.

L'architecture générale des applications de la carte Morpho-Citiz 32 est présentée dans le schéma de la Figure 1.

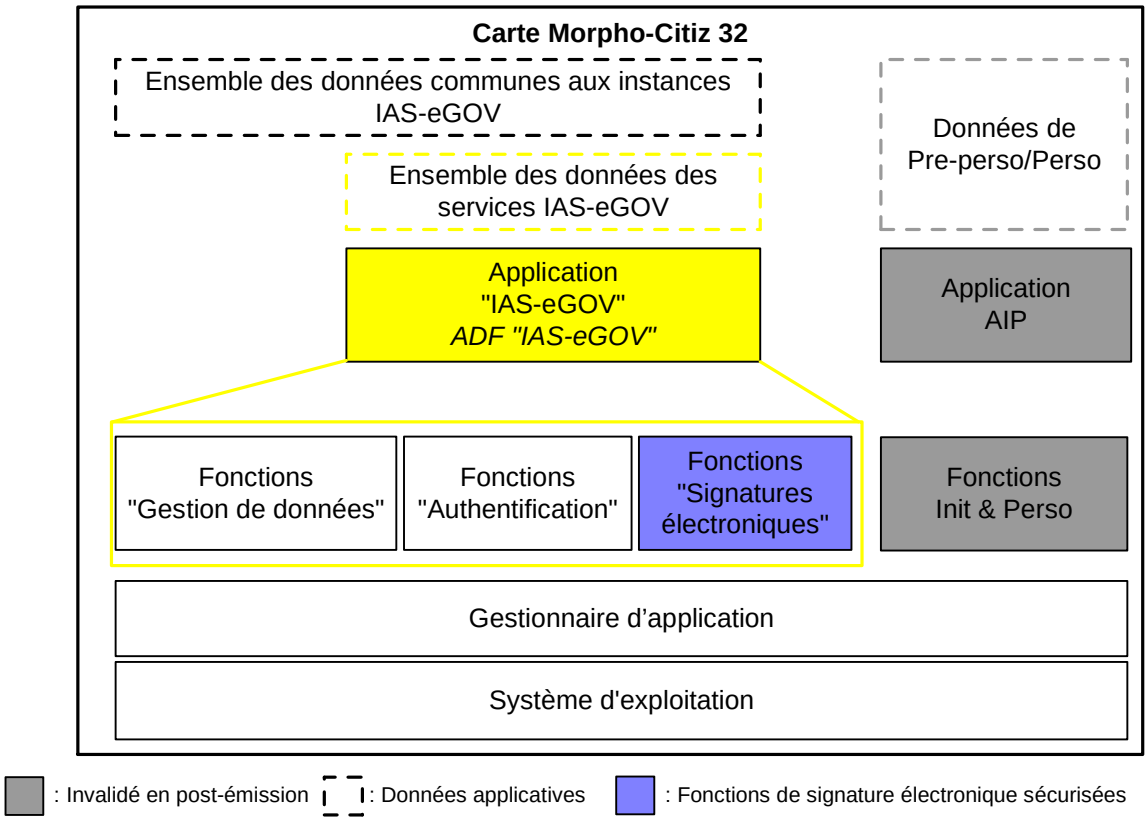

Figure 1 : Description de l'architecture de la carte Morpho-Citiz 32

2.1.2 Initialisation et personnalisation de la carte Morpho-Citiz 32

Compte tenu de l'architecture décrite précédemment, une application est définie comme étant une instance de blocs logiciels pour des données associées à cette application.

De façon générale, l'instance d'une application est réalisée en créant :

- Un fichier ADF associé à l'application et portant une arborescence de répertoires et de fichiers de données de l'application. Ces données sont traitées par le logiciel réalisant les fonctionnalités de l'application ;
- Un fichier ADF de type CIA de l'application et portant sur une structure de répertoires et de fichiers regroupant les informations indiquant l'état en cours des éléments cryptographique de l'application (Identifiants des clés disponibles, état de ces clés, …). L'ADF de type CIA est optionnel ;

L'initialisation et la personnalisation (application AIP) permettent de réaliser avant la phase utilisateur, les traitements suivants :

- Création des instances de l'application IAS-eGOV,
- Personnalisation de ces instances.

L'application AIP de la carte Morpho-Citiz 32 est invalidée après la phase de personnalisation et avant la phase utilisateur.

Une fois créées et personnalisées les instances de l'application IAS-eGOV peuvent alors être sélectionnées via une commande « SELECT ». Ainsi l'utilisateur de la carte Morpho-Citiz 32 ne peut réaliser l'un des services d'une instance de l'application IAS-eGOV que si elle est sélectionnée.

2.1.3 Services de l'application IAS-eGOV

L'application IAS-eGOV réalise un ensemble de services via les commandes conformes à **[R9 – E-ADMIN]** disponibles uniquement en phase utilisateur. L'accès à ces services dépend du rôle de l'utilisateur, de l'état de la carte Morpho-Citiz 32 et de l'état de l'application réalisant le service.

Service de gestion de données de l'utilisateur :

Ce service est réalisé par l'application IAS-eGOV sur les données gérées par l'application. Il réalise l'ensemble des opérations de gestion des données et des secrets accessibles à un utilisateur autorisé, en faisant appel aux fonctions décrites dans le chapitre 2.1.4.

Les données des instances de l'application IAS-eGOV sont cloisonnées, c'est-à-dire que l'une des instances ne peut accéder aux données de l'autre (exception faite des données explicitement partagées).

Service d'authentification des utilisateurs :

Ce service est réalisé par l'application IAS-eGOV sur les données gérées par l'application.

L'application IAS-eGOV réalise le service d'authentification en faisant appel aux fonctions d'authentification décrites dans le chapitre 2.1.4.

Service de signature électronique sécurisé :

Ce service est réalisé par l'application IAS-eGOV sur les données gérées par l'application.

Pour réaliser le service de signature électronique sécurisé l'application IAS-eGOV fait appel aux fonctions de signature électronique sécurisé décrites dans le chapitre 2.1.4.

2.1.4 Blocs fonctionnels

Les chapitres suivants décrivent les fonctions de la carte Morpho-Citiz 32 réalisant les traitements de gestion de données, de signature électronique et d'authentification pour le compte des instances de l'application IAS-eGOV.

2.1.4.1 Gestion des données

Les données stockées dans la carte Morpho-Citiz 32 sont organisées en arborescence de répertoires et de fichiers, conforme à la norme **[R12 – 7816 – 4]**.

Les objets supportés par la carte Morpho-Citiz 32 :

La carte Morpho-Citiz 32 supporte les objets suivants :

- **Les répertoires et les fichiers** réalisant la structure de données ;
- **Les objets TLV** contenus dans les répertoires (au même titre que les fichiers) mais accessibles par nommage ;
- **Les secrets** dans lesquels sont stockés les clés cryptographiques et les codes PIN.

Cycle de vie des objets :

Les cycles de vie des objets « fichier » et « secret »sont définis par les états présentés ci-après.

Etats communs aux fichiers et aux secrets :

- **Création** : Cet état est temporaire dans le sens où, si l'objet créé n'est pas passé dans un des états opérationnels avant le reset de la carte, cet objet est détruit (le passage de l'état « en création » à l'un des états « Opérationnel » est irréversible) ;
- **Opérationnel – Activé** : l'objet existe, il est opérationnel et est activé ;
- **Opérationnel – Désactivé** : L'objet existe, il est opérationnel mais n'est pas activé ;

- **Opérationnel – Terminé** : L'objet existe mais il est accessible uniquement en lecture (Le passage à l'état terminé est irréversible) ;

Etats spécifiques aux secrets :

- **Non opérationnel – Bloqué** : Etat spécifique aux secrets qui correspond à un secret dont l'utilisation par les fonctions cryptographiques, a été bloquée suite à une alarme sur les compteurs de ratification et/ou d'usage (Cet état est réversible via une commande spécifique) ;
- **Non opérationnel – Vide** : Etat spécifique aux secrets qui correspond à un secret ne contenant aucune valeur de clé cryptographique ou de code PIN. Dans cet état, le secret n'est pas opérationnel dans le sens où il ne peut être utilisé pour réaliser des opérations cryptographiques ou d'authentification. Cet état est réversible via une commande de chargement de valeurs de clé ou de code PIN ;

Accès aux objets :

Tout objet (répertoire, fichier, secret, TLV) auquel sont rattachées des conditions d'accès ne peut être accédé que si ces conditions d'accès sont vérifiées.

La vérification des conditions d'accès est réalisée en comparant les conditions d'accès définies dans le **DAC** de l'objet avec l'état en cours de l'**état de sécurité carte**.

Les conditions d'accès à un objet sont associés à des secrets d'authentification (code PIN, clé d'authentification) ou à l'établissement d'un canal de confiance (SMC, SMI). De cette façon, lorsqu'un utilisateur est authentifié ou un canal de confiance est établi, cette information est mémorisée dans l'état de sécurité carte. L'état de sécurité carte est mis à jour, lorsque l'authentification de l'utilisateur n'est plus valide ou lorsque le canal de sécurité est interrompu.**Fonctions de gestion de données :**

Les fonctions de gestion de données réalisent les services de gestion de la structure de données des instances de l'application IAS-eGOV.

- **Création de répertoire** : Permet la création de répertoires (Fichier de type DF).
- **Création de fichier** : Permet la création de fichiers de type EF.
- **Suppression de répertoire** : Permet la suppression d'un répertoire (fichier de type DF).
- **Suppression de fichier** : Permet la suppression d'un fichier de type EF.
- **Gestion du cycle de vie d'un fichier/répertoire :** Permet à l'utilisateur autorisé de modifier l'état d'un fichier/répertoire dans son cycle de vie, à l'exception du MF.
- **Mise à jour / Ecriture de données d'un fichier** : Permet l'écriture de données dans un fichier sélectionné.
- **Lecture de données d'un fichier** : Permet la lecture de données dans un fichier sélectionné.
- **Création d'un TLV** : Permet la création d'un TLV.
- **Mise à jour / Ecriture d'une donnés dans un TLV** : Permet l'écriture de données (incluant l'effacement) dans un objet TLV sélectionné.
- **Lecture d'une donnée dans un TLV :** Permet la lecture de données dans un objet TLV sélectionné.
- **Gestion du cycle de vie d'un secret :** Permet à l'utilisateur autorisé de modifier l'état d'un secret dans son cycle de vie.
- **Déblocage d'un secret :** Permet à de débloquer un code PIN ou une clé cryptographique qui se trouve dans l'état « Bloqué ».
- **Création d'un secret**: Permet la création d'un secret.
- **Mise à jour / Ecriture d'un secret** : Permet la mise à jour d'un code PIN ou d'une clé cryptographique.

- **Lecture des informations d'un secret** : Permet la lecture d'informations associées à un secret ou de clés publiques.
- **Génération d'un bi-clé** : Permet la génération d'un bi-clé d'authentification, de signature ou de confidentialité asymétrique.

2.1.4.2 Authentification des utilisateurs

Nature de l'authentification :

Les fonctions d'authentification réalisent les services d'authentification des utilisateurs des instances de l'application IAS-eGOV. L'authentification des utilisateurs est basée sur le rôle assuré par un utilisateur lors de son accès aux services d'une application. Les opérations d'authentification des utilisateurs se font sur la base de différents types de secret, associés aux rôles supportés, à savoir :

- Un code d'authentification dit « code PIN » pour l'authentification du porteur pour les accès aux données et à la création de signature électronique qualifiée ;
- Un code d'authentification dit « code PUK » pour l'authentification de l'utilisateur pour l'opération de déblocage du code PIN auquel le code PUK est associé ;
- Une clé symétrique pour l'authentification de l'utilisateur (sans mise en œuvre de SM) permettant l'accès à la gestion de données ;
- Une clé symétrique (stockée en carte) pour une authentification mutuelle permettant la mise à jour de données de la carte via l'établissement d'un canal de confiance ;
- Un certificat de type CVC + réponse à un défi fourni à la carte et authentifiant l'utilisateur via la vérification du certificat à partir d'une clé racine en carte pour l'accès à la gestion des données ;
- Un certificat de type CVC ou X509 permettant l'authentification de la carte ;

Fonctions d'authentification :

Ces fonctions réalisent l'authentification des utilisateurs des instances de l'application IAS-eGOV. Ces fonctions contribuent à résoudre les conditions d'accès aux objets de la carte Morpho-Citiz 32.

- **Vérification de code PIN/PUK** : Permet l'authentification du porteur ou du code PUK associé ;
- **Authentification mutuelle symétrique** : Permet l'authentification mutuelle carte/utilisateur suivant un schéma symétrique, et basée sur l'utilisation de clés TDES de taille 112 bits ;
- **Authentification externe symétrique** : Permet l'authentification d'un utilisateur sur la base de clés TDES de taille 112 bits ;
- **Authentification mutuelle asymétrique-DH :** Permet l'authentification mutuelle carte/utilisateur reposant sur un protocole Diffie-Helmann (DH) et basée sur des certificats CVC (clé RSA jusqu'à 2048 bits) ;
- **Authentification externe asymétrique** : Permet l'authentification d'un utilisateur basée sur certificats CVC utilisateur (Clé RSA jusqu'à 2048 bits) ;
- **Authentification interne asymétrique** : Permet l'authentification de la carte basée sur un certificat « carte » CVC ou X509[1] (Clé RSA jusqu'à 2048 bits) ;

2.1.4.3 Signature électronique

Ces fonctions réalisent pour le compte de l'utilisateur de l'application IAS-eGOV, la création de signatures électroniques ainsi que la gestion des données mise en œuvre dans le cadre de cette signature électronique.

Fonctions de gestion des SCD/SVD :

- Génération de SCD/SVD,

[1] Les certificats X 509 sont utilisées uniquement dans le cadre d'une authentification carte pour des sessions SSL et ne sont donc pas interprétés par la carte Morpho-Citiz 32.

- Destruction de SCD/SVD,
- Chargement, stockage et utilisation de SCD.

Fonctions de signature :

- Création de signature électronique,

« signature qualifiée » / « signature non-qualifiée » :

La carte Morpho-Citiz 32 réalise le service de signature électronique suivant deux modes de fonctionnement :

- Le mode « signature qualifiée » pour laquelle la conformité aux profils de protections **[R3 – SSCD T2]** et **[R4 – SSCD T3]** est exigée ;
- Le mode « signature non-qualifiée » pour laquelle les exigences concernant l'utilisation de certificats qualifiés tel que défini au § 3.4 dans les politiques organisationnelles, ne sont pas applicables. La conformité aux profils de protections **[R3 – SSCD T2]** et **[R4 – SSCD T3]** n'est alors pas exigée ;

La mode est défini par le cadre d'utilisation de la carte Morpho-Citiz 32 et en particulier lors de sa personnalisation, i.e. chargement de certificats qualifiés ou non.

2.1.4.4 Confidentialité – Intégrité

Fonctions de canal de confiance « Secure Messaging » :

L'établissement d'un canal de confiance nécessite l'authentification mutuelle entre la carte et le produit TI communiquant avec la carte. Cette authentification mutuelle peut se faire via une authentification symétrique (mutuelle) ou asymétrique. Les fonctions de canal de confiance réalisent les traitements associés à l'établissement et à la gestion d'un canal de confiance. Ce canal de confiance supporte les services suivants :

- **Intégrité (SMI)** : Intégrité sur les commandes et les réponses échangées entre la carte Morpho-Citiz 32 et un produit TI. L'établissement d'une session assurant le SMI fait l'objet d'une authentification mutuelle préalable ;
- **Confidentialité (SMC)** : Confidentialité sur les commandes et les réponses échangées entre la carte Morpho-Citiz 32 et un produit TI. L'établissement d'une session SMC fait l'objet d'une authentification mutuelle préalable ;

Sur la base de ces deux services, il existe deux modes de sécurisation sur les CMD/RSP échangées lors d'une session de canal de confiance :

- Sécurisation en intégrité : SMI ;
- Sécurisation en intégrité et en confidentialité : SMI et SMC ;

Fonctions de confidentialité :

La carte Morpho-Citiz 32 met en œuvre des fonctions de chiffrement permettant de garantir la confidentialité des secrets et des données sensibles. Ces fonctions sont :

- **Déchiffrement asymétrique de secret** : Permet de déchiffrer un secret chiffré, à l'aide d'une clé RSA de déchiffrement de secrets ;
- **Chiffrement symétrique de données** : Permet de chiffrer des données dans le cadre d'un SM, à l'aide d'une clé TDES de chiffrement de données ;

Fonction d'intégrité :

La carte Morpho-Citiz 32 met en œuvre une fonction de calcul d'intégrité permettant de garantir l'intégrité des secrets et des données sensibles. Cette fonction utilise un MAC pour calculer/vérifier l'intégrité de la donnée (MAC Retail).

2.2 CYCLE DE VIE DU PRODUIT

Le cycle de vie correspond au cycle de vie d'un produit « carte à puce ». Il se décompose en 7 phases :

Phase 1 ***Développement du logiciel embarqué de la carte à puce***
Sagem Défense Sécurité est responsable du développement du logiciel intégré à la carte à puce et de la spécification des exigences d'initialisation du circuit intégré.

Phase 2 ***Développement du circuit intégré (CI)***
Atmel conçoit le CI, développe le logiciel dédié du CI et transmet les informations, le logiciel et les outils au logiciel embarqué du développeur (Sagem DS), par des procédures sécurisées de vérification et de livraison. A partir du circuit intégré, du logiciel dédié et du logiciel embarqué, il construit la base de données du circuit intégré de la carte à puce, indispensable à la réalisation du masque du circuit intégré.

Phase 3 ***Fabrication et test du circuit intégré***
Atmel est responsable de la production du circuit intégré, qui se déroule en trois étapes principales : fabrication, test et initialisation du circuit intégré.

Phase 4 ***Encapsulation et test du circuit intégré***
Le **constructeur de conditionnement du circuit intégré** est responsable du conditionnement (encapsulation) et du test du circuit intégré.

Phase 5 ***Finition du produit Carte à puce***
Le **constructeur de la carte à puce** est responsable de la finition et du test de la carte à puce.

Phase 6 ***Personnalisation de la carte à puce***
Le **personnalisateur** est responsable de la personnalisation de la carte à puce et des derniers tests.

Phase 7 ***Exploitation de la carte à puce***
L'**émetteur de carte à puce** est responsable de la livraison du produit à l'**utilisateur final**, ainsi que de la fin du cycle de vie.

Le rôle du logiciel embarqué conçu en phase 1 est de contrôler et de protéger la TOE pendant les phases 4 à 7 (exploitation du produit).

Les exigences de sécurité globales de la TOE stipulent qu'il est obligatoire pendant la phase de développement d'anticiper les menaces des phases suivantes. C'est pourquoi cette cible de sécurité adresse les fonctions mises en oeuvre dans les phases 4 à 7 mais qui restent développées pendant la phase 1.

La Figure 2 décrit le cycle de vie du produit carte à puce.

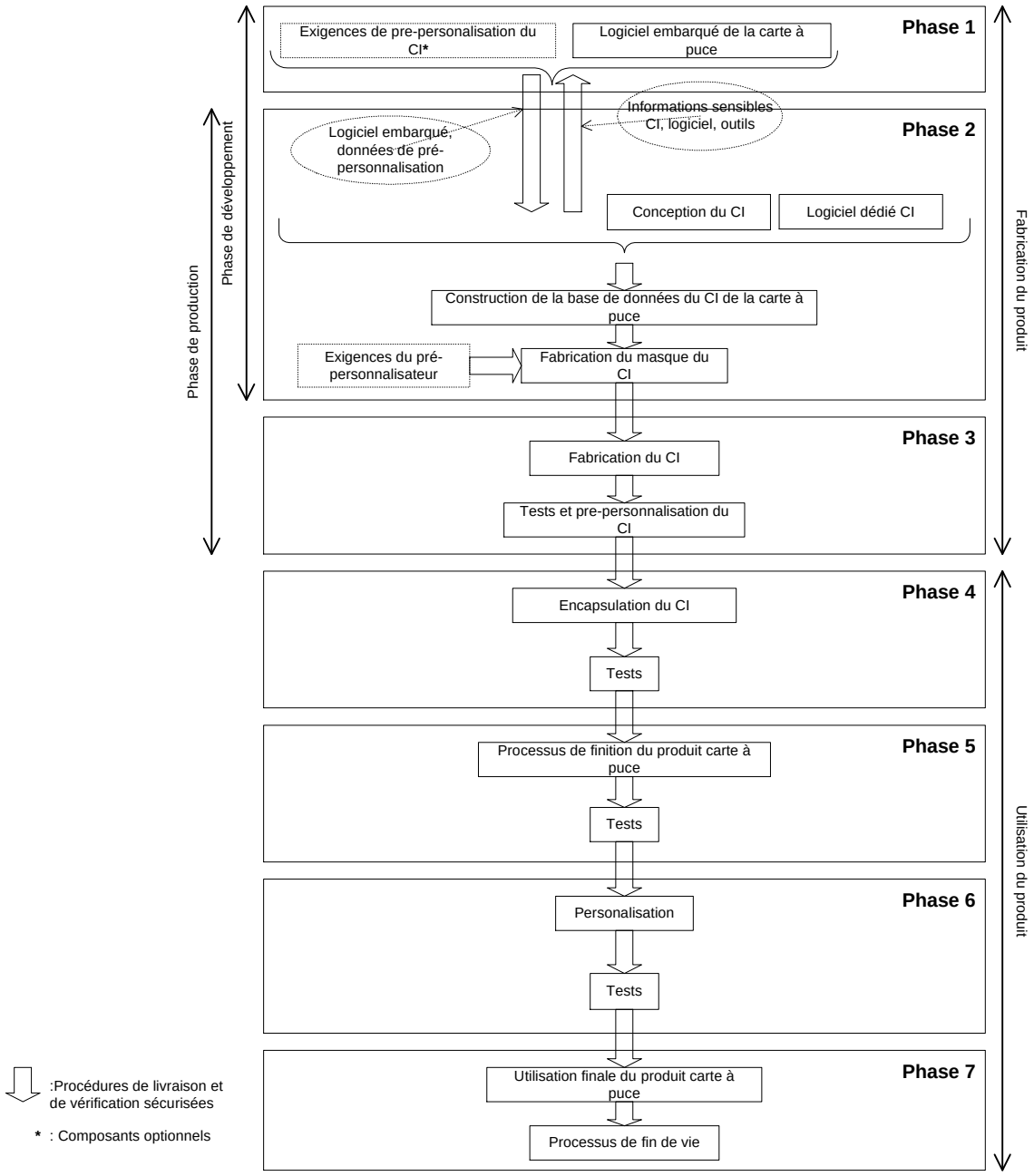

Figure 2 : Cycle de vie du produit carte à puce

L'ensemble logiciel et matériel est conçu durant les phases 1 à 3. L'application IAS-eGOV est quant à elle, conçue en phase 1.

Ces différentes phases peuvent être mises en œuvre dans des lieux différents. Des procédures doivent être mises en place pour le processus de livraison de la TOE, et doivent être appliquées à l'intérieur de chaque phase comme entre chaque phase. Cela inclut toute forme de livraison effectuée de la phase 1 à la phase 6, y compris :

- Livraison intermédiaire de la TOE ou de la TOE en cours de fabrication à l'intérieur d'une même phase ;
- Livraison de la TOE ou de la TOE en cours de fabrication d'une phase à la phase suivante.

Le développement de l'application comprend les phases de spécification, conception, codage, tests et qualification.

La livraison comprend la livraison du code au fondeur ainsi que la livraison des paramètres d'initialisation et personnalisation.

2.3 PRESENTATION DE LA TOE

La cible d'évaluation (TOE) est décrite dans ce chapitre est l'application IAS-eGOV. Cette TOE, dénommée ci-après « application IAS-eGOV ».

2.3.1 Limites de la TOE

La TOE est l'application IAS-eGOV de la carte Morpho-Citiz 32. Elle se compose des éléments suivants :

- Le système d'exploitation ;
- Le gestionnaire d'application ;
- Les fonctions du logiciel embarqué de la carte Morpho-Citiz 32 mises en œuvre dans les services de l'application IAS-eGOV ;

La TOE est présentée dans le schéma de la Figure 4.

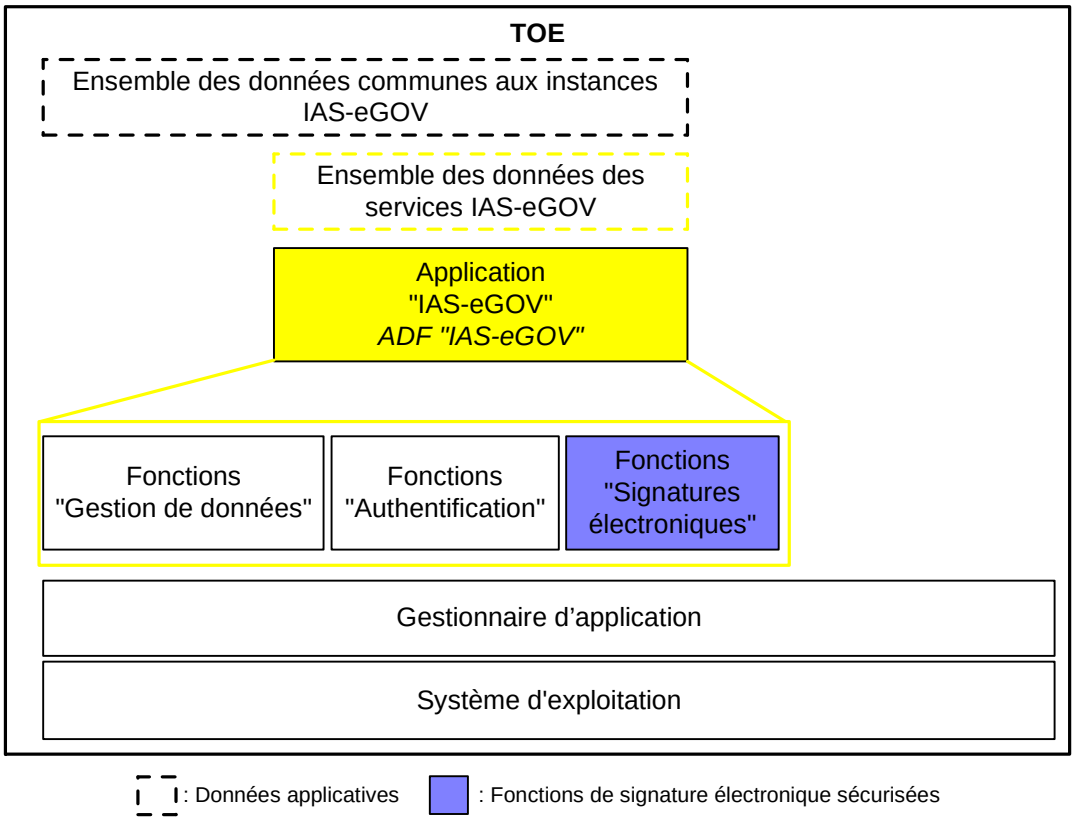

Figure 4 : Services de l'application IAS-eGOV

2.3.2 Description de la TOE

L'application IAS-eGOV assure les services décrits dans le chapitre 2.1.3 sur les données gérées par l'application.

Les données liées à l'application IAS-eGOV sont :

- L'ensemble des données liées (en particulier les données à signer et les certificats à stocker dans la carte) à l'application IAS-eGOV ;
- L'ensemble regroupant les clés cryptographiques associées aux services de l'application IAS-eGOV ainsi que le (ou les) code PIN utilisé pour authentifier le porteur ;

L'application IAS-eGOV réalise également les traitements de signatures électroniques sécurisées à savoir :

(1) La génération de SCD et de la SVD correspondante ou chargement de SCD,

(2) La création de signatures qualifiées :

a. après avoir permis aux données devant être signées (DTBS) de s'afficher correctement par l'environnement adapté,

b. en utilisant des fonctions de contrôle qui sont, selon **[R7 – Algo]**, déclarées comme adaptées aux signatures électroniques qualifiées,

c. après authentification adaptée du signataire par la TOE,

d. en utilisant une fonction de signature cryptographique adaptée qui utilise des paramètres cryptographiques adaptés déclarés comme adaptés selon **[R7 – Algo]**.

La TOE garantit le secret des SCD. Pour éviter une utilisation non autorisée des SCD, la TOE permet une authentification de l'utilisateur et un contrôle d'accès. La TOE met en œuvre des mesures TI pour prendre en charge un chemin de confiance vers un appareil sécurisé d'interface humaine.

La TOE conserve le RAD pour vérifier la VAD fournie par le signataire.

La TOE est initialisée pour une utilisation par le signataire en, au choix :

(1) Important un SCD,

(2) générant une paire SCD/SVD,

Seul le signataire légitime peut utiliser les SCD durant le processus de création de signature et durant la validité des paires SCD/SVD.

La TOE stocke les SCD et peut exporter les SVD. Les SVD correspondant aux SCD du signataire sont incluses dans le certificat du signataire par les prestataires de service de certification (CSP). La TOE détruit les SCD n'étant plus utilisées pour la génération de signatures.

En phase utilisateur, la TOE autorise la création de nouvelles paires SCD/SVD. Les SCD précédentes doivent être détruites avant la création de nouvelles paires SCD/SVD.

L'utilisateur du service de création de signature électronique de la TOE, présente les données devant être signées (DTBS) au signataire, et prépare la représentation des DTBS que le signataire souhaite signer pour effectuer la fonction cryptographique de la signature. La TOE retourne une signature électronique qualifiée.

Gestion des SCD/SVD dans le cycle de vie de la TOE :

La Figure 5 décrit le cycle de vie de la TOE dans sa fonction de SSCD.

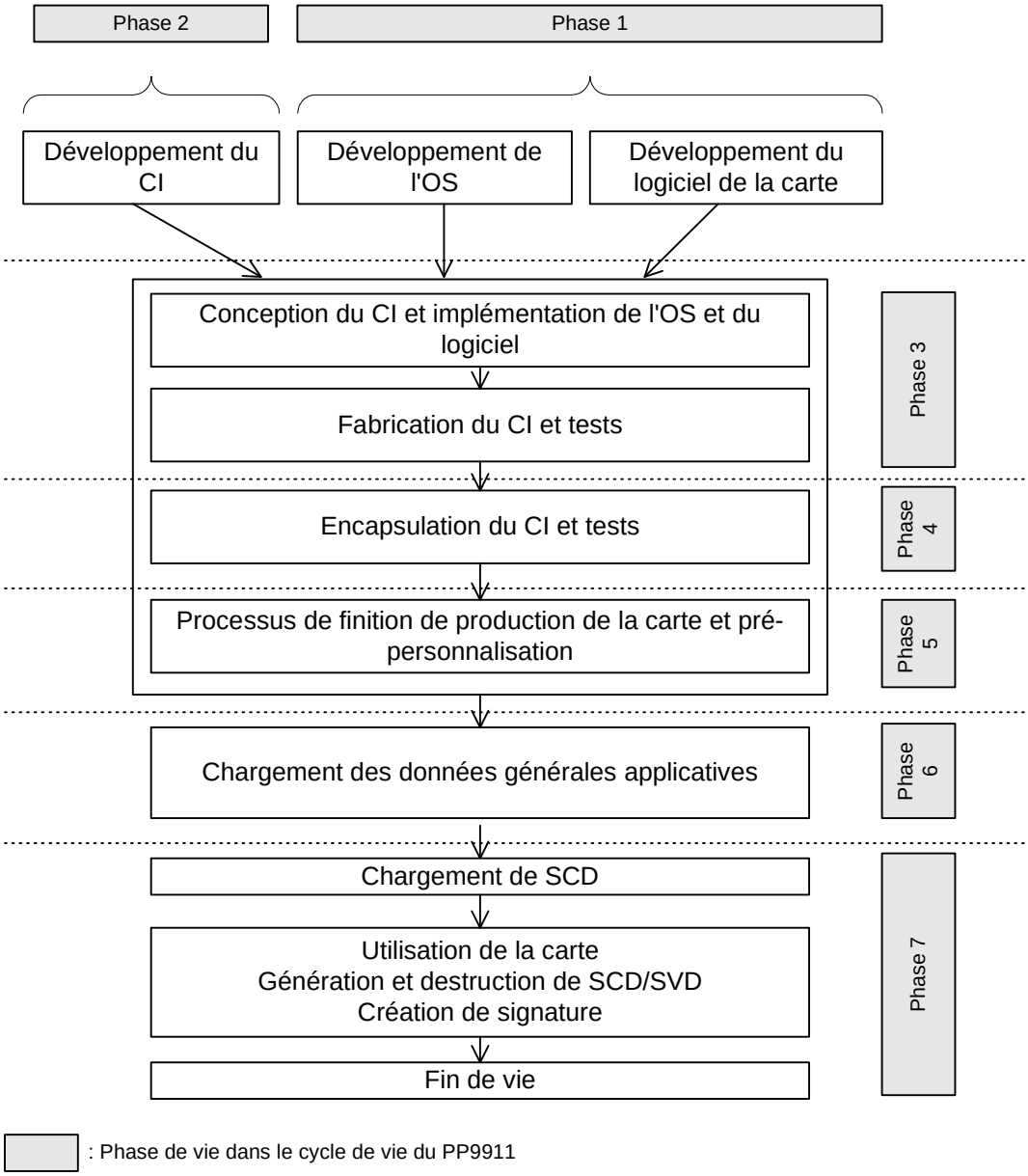

Figure 5 : Cycle de vie du SSCD

2.4 ENVIRONNEMENT DE LA TOE

2.4.1 Description de son environnement :

Considérant la TOE, quatre types d'environnement sont définis :

- L'environnement de développement et de fabrication (phase 1 à 4),
- L'environnement de pré-personnalisation (phase 5) et de personnalisation (phase 6) de la carte,
- Environnement utilisateur (phase 7) durant lequel la TOE est opérationnelle,

– Environnement de fin de vie de la TOE (phase 7) durant lequel la TOE est rendue non-opérationnelle.

2.4.2 Utilisation de la TOE dans son environnement

Dans l'environnement de l'utilisateur final, la TOE est utilisée pour créer des signatures qualifiées.

2.4.3 Phases logiques de la TOE

Au cours de sa fabrication et de son exploitation, la TOE traverse plusieurs phases de vie logiques. Ces phases sont classées selon une séquence logique contrôlée. Le passage d'une phase à la phase suivante doit s'effectuer sous contrôle de la TOE.

Configuration du CI	Phases logiciel embarqué	Phases	Autorité de contrôle (Rôle)
Test	-	3	-
Utilisateur	Initialisation	4 et 5	Pré-personnalisateur (administrateur)
Utilisateur	Personnalisation	6	Personnalisateur (administrateur)
Utilisateur	Utilisateur final	7	Autorité de domaine et émetteur (administrateur)
Utilisateur	Fin de vie	7	Émetteur (administrateur)

Tableau 1 : Phases logiques de la TOE

La configuration de l'environnement de la TOE est déterminée par la configuration du circuit intégré (test ou utilisateur du circuit intégré), et par le cycle de vie de l'environnement de la TOE (pré-personnalisation, personnalisation, utilisateur final, fin de vie) fournis par le logiciel embarqué.

Une fois la configuration déterminée, la TOE ne peut pas revenir à une configuration précédente. Les différentes étapes sont précisées dans Tableau 1, et seul l'administrateur autorisé peut mettre en œuvre le passage d'une phase à la suivante.

Pour l'application IAS-eGOV, le passage de l'état « Non-Active » à l'état « Active » est réalisé à l'issu de l'initialisation et de la personnalisation de la carte Morpho-Citiz 32 qui permet en particulier la création des deux ADF (ADF et ADF.CIA). Le chargement des données de personnalisation est fait lors de la personnalisation. Les opérations d'initialisation et de personnalisation sont réalisées sous le contrôle du pré-personnalisateur et du personnalisateur qui agissent sur la TOE en tant qu'administrateur et via les commandes de l'application d'initialisation et de personnalisation (AIP).

En phase utilisateur, l'utilisateur peut utiliser les services de l'application IAS-eGOV. Au cours de la phase de fin de vie, la TOE est invalidée, ce qui signifie que toutes les commandes sont rejetées.

Quelle que soit la phase de vie, le changement de phase de vie est irréversible.

2.5 UTILISATEURS ET ROLES

Les utilisateurs de la TOE sont les entités, personnels ou matériels, ayant une interaction avec la TOE via ses interfaces externes. Le tableau ci-dessous présente les différents utilisateurs de la TOE et précise les rôles qui leur sont associés.

2.5.1 Utilisateurs « génériques »

Encarteur : Utilisateur qui intervient en phase d'encartage et assure l'administration de la TOE. Il renseigne en particulier un numéro d'encarteur et un numéro de série. (Phase 4 et 5)

Personnalisateur	:	Utilisateur qui intervient en phase de personnalisateur et assure l'administration de la TOE. Il invalide lui-même ses accès aux services d'administration en fin de phase de personnalisation par désactivation de la clé de fabrication.	(Phase 6)
Emetteur	:	Utilisateur qui intervient en phase utilisateur. Il peut créer/supprimer des domaines pour une application. Il réalise également la création et la mise à jour de secrets pour les domaines et les applications auxquels il accède. Il peut également désactiver/activer une application.	(Phase 7)
Autorités de domaine	:	Utilisateur qui gère un ou plusieurs domaines. Il peut créer/supprimer des domaines pour un domaine père. Il réalise également la création et la mise à jour de secrets pour les domaines auxquels il accède. Il peut également désactiver/activer un domaine si ce dernier n'est pas une application.	(Phase 7)
Porteur	:	Porteur de la carte Morpho-Citiz 32 bénéficiant des services des instances de l'application IAS-eGOV	(Phase 7)

2.5.2 Signature électronique sécurisée : Utilisateurs

Afin de garantir la conformité aux profils de protection **[R3 – SSCD T2]** et **[R4 – SSCD T3]**, les utilisateurs suivants sont définis pour les services de signature électronique sécurisés :

S.USER	:	Utilisateur final de la TOE qui peut être identifié comme S.Admin ou S.Signatory	(Phase 7)
S.Admin	:	Utilisateur qui est en charge d'effectuer l'initialisation de la TOE, la personnalisation de la TOE ou d'autres fonctions administratives pour la TOE.	(Phase 7)
S.Signatory	:	Utilisateur qui détient la TOE et l'utilise pour son propre compte ou pour le compte d'une personne ou d'une entité morale ou physique qu'il représente.	(Phase 7)

Agent de menace défini pour les services de signature électronique sécurisés :

S.OFFCARD : Attaquant. Humain ou processus agissant pour son compte étant situé hors de la TOE. L'objectif principal de l'attaquant S.OFFCARD est d'accéder aux informations sensibles applicatives. L'attaquant a **un niveau potentiel d'attaque élevé** et **ne connaît aucun secret**.

3. ENVIRONNEMENT DE SECURITE DE LA TOE

3.1 LES BIENS A PROTEGER

La liste des biens à protéger par la TOE est constituée d'un ensemble de fonctions et de données pouvant être classées comme suit :

- Les fonctions de sécurité de l'application IAS-eGOV ;
- Les données utilisateurs ;
- Les données de la TSF ;

Auxquelles s'ajoute le logiciel embarqué incluant les documents de spécification, le code source et les documents de conception associés.

3.1.1 Les fonctions de l'application IAS-eGOV

Les fonctions sont supportées par le code exécutable stocké en mémoire ROM.

Identifiant	Fonctions
FCT.1	Authentification externe asymétrique
FCT.2	Authentification interne asymétrique
FCT.3	Authentification externe symétrique
FCT.4	Authentification interne symétrique
FCT.5	Authentification mutuelle symétrique
FCT.6	Chiffrement/déchiffrement de données
FCT.7	Authentification mutuelle asymétrique
FCT.8	Calcul de sceau sur des données externes
FCT.9	Création d'une signature électronique
FCT.10	Génération d'un bi-clé d'authentification
FCT.11	Génération d'un bi-clé de signature (SCD/SVD)
FCT.12	Ajout d'une clé cryptographique
FCT.13	Etablissement de clé de session
FCT.14	Déchiffrement asymétrique d'un secret
FCT.15	Activation d'une clé cryptographique
FCT.16	Déblocage d'une clé cryptographique
FCT.17	Activation d'un code porteur
FCT.18	Déblocage du code porteur
FCT.19	Vérification du code porteur
FCT.20	Mise à jour de code porteur
FCT.21	Création de fichiers ou de répertoires
FCT.22	Suppression de fichier/répertoire
FCT.23	Ecriture/lecture dans un fichier ou un objet TLV à accès contrôlé

Tableau 2 : Liste des fonctions sensibles

3.1.2 Les données utilisateurs

Les données utilisateur sont des informations stockées dans l'enceinte de la TOE. Les utilisateurs peuvent intervenir sur ces données dans le cadre de la politique de sécurité (TSP). La TSF pour sa part ne donne

aucune signification particulière à ces données qui sont protégées en intégrité ou en intégrité et accès en lecture/écriture restreint à l'utilisateur autorisé. Elles sont regroupées dans le tableau suivant :

Identifiant	Données	Protection
D.USE.1	Donnée en accès libre en lecture et protégée en écriture	Intégrité et écriture restreinte à l'utilisateur autorisé
D.USE.2	Données protégées en accès lecture et en écriture	Intégrité et lecture restreinte à l'utilisateur autorisé
D.USE.3	Données de signature électronique	Intégrité

Tableau 3 : Liste des données « utilisateur » sensibles

3.1.3 Les données de la TSF

Les données TSF sont des informations utilisées par la TSF pour réaliser la politique de sécurité (TSP). Les données de la TSF, peuvent être modifiées par les utilisateurs la TSP l'autorise. Ces données doivent être protégées en intégrité ou en intégrité et en confidentialité. Elles sont regroupées dans le tableau suivant :

Identifiant	Données	Protection
D.TSF.1	Clés TDES pour le déchiffrement de secrets et le chiffrement/déchiffrement de données externes	Intégrité et confidentialité
D.TSF.2	Clés privées RSA et les paramètres DH pour les authentifications internes et externes asymétriques	Intégrité et confidentialité
D.TSF.3	Clés privées RSA pour le déchiffrement de secrets	Intégrité et confidentialité
D.TSF.4	Certificats et clés publique associée	Intégrité
D.TSF.5	Clés de session TDES utilisés pour la confidentialité (K_{ENC}) et l'intégrité (K_{MAC}) dans les sessions SM	Intégrité et confidentialité
D.TSF.6	Clés TDES d'intégrité pour l'exportation et l'importation de données	Intégrité et confidentialité
D.TSF.7	Codes confidentiels du porteur (PIN de référence)	Intégrité et confidentialité
D.TSF.8	Codes de déblocage des codes PIN de référence (code PUK)	Intégrité et confidentialité
D.TSF.9	Attributs de sécurité de la TOE	Intégrité

Tableau 4 : Liste des données sensibles de la TSF

3.1.4 Signature électronique sécurisée : Définition des biens SSCD

Les biens de la TOE pour les services de signature électronique sécurisés sont ceux définis dans les profils de protection **[R3 – SSCD T2]** et **[R4 – SSCD T3]**, à savoir :

SCD : Clé privée utilisée pour effectuer une opération de signature électronique (la confidentialité des SCD doit être préservée).
SVD : Clé publique liée aux SCD et utilisée pour effectuer une vérification de la signature électronique (l'intégrité des SVD lors de l'exportation doit être préservée).
DTBS[2] : Ensemble de données ou leur représentation devant être signées (leur intégrité doit être préservée).
VAD : Code PIN saisi par le porteur pour effectuer une opération de signature (la confidentialité et l'authenticité des VAD telles que nécessaires pour la méthode d'authentification sont exigées)
RAD : Code PIN de référence utilisé pour identifier et authentifier le porteur (l'intégrité et la confidentialité des RAD doivent être préservées)
SSC : Fonction de création de signature sécurisée de la carte Morpho-Citiz 32 utilisant les SCD : (la qualité de la fonction doit être préservée de telle sorte qu'elle puisse participer à la validité légale des signatures électroniques).
SIG : Signature électronique : (La non-falsification des signatures électroniques doit être garantie).

[2] Ainsi que la représentation des DTBS.

3.2 LES HYPOTHESES

Le Tableau 5 présente les hypothèses retenues pour la présente TOE et leurs correspondances avec les profils de protections **[R2 – 9911]**, **[R2 – 9911]** et **[R4 – SSCD T3]**.

Hypothèses pour la TOE	PP 9911	PP SSCD type 2	PP SSCD type3
A.CGA		A.CGA	A.CGA
A.SCA		A.SCA	A.SCA
A.SCD_Generate		A.SCD_Generate	
A.DEV_ORG	A.DEV_ORG		
A.DLV_PROTECT	A.DLV_PROTECT		
A.DLV_AUDIT	A.DLV_AUDIT		
A.DLV_RESP	A.DLV_RESP		
A.USE_TEST	A.USE_TEST		
A.USE_PROD	A.USE_PROD		
A.USE_DIAG	A.USE_DIAG		

Tableau 5 : Correspondances ST/PP – hypothèses pour la TOE

3.2.1 Hypothèses définies dans [R2 – 9911]

3.2.1.1 Hypothèses en phase 1

A.DEV_ORG
Des procédures traitant de mesures techniques, physiques, organisationnelles et liées au personnel quant à la confidentialité et à l'intégrité du logiciel embarqué de la carte à puce (ex. : code source et tous les documents associés) et des informations propriétaires du concepteur du microcircuit (outils, logiciels, documentation…) doivent exister et être appliquées lors du développement des logiciels.

3.2.1.2 Hypothèses sur les processus de livraison (phases 4 à 7)

Des procédures doivent garantir le contrôle du processus de livraison et de stockage de la cible d'évaluation et la conformité à ses objectifs tels que décrits dans les hypothèses suivantes :

A.DLV_PROTECT
Lors de sa livraison et de son stockage, des procédures doivent assurer une protection matérielle de la TOE ainsi que la protection des informations relatives à la TOE.

A.DLV_AUDIT
Des procédures doivent assurer que des actions correctives sont exécutées en cas de dysfonctionnement du processus de livraison et de stockage.

A.DLV_RESP
Des procédures doivent assurer que les personnes traitant de la procédure de livraison possèdent les compétences requises.

3.2.1.3 Hypothèses sur les phases 4 à 6

A.USE_TEST
On suppose que les tests de fonctionnalité appropriés de la cible d'évaluation sont mis en œuvre aux phases 4, 5 et 6.

A.USE_PROD
On suppose que des procédures de sécurité sont mises en œuvre lors de toutes les opérations de fabrication et de test aux phases 4, 5 et 6 afin de préserver la confidentialité et l'intégrité de la cible d'évaluation et de ses données de fabrication et de test (afin d'éviter toute possibilité de copie, de modification, de rétention, de vol ou d'utilisation non autorisée).

3.2.1.4 Hypothèses sur la phase 7

A.USE_DIAG
On suppose que des protocoles et des procédures de communications sécurisées sont utilisés entre la carte à puce et le terminal.

3.2.2 Hypothèses définies dans [R3 – SSCD T2] et [R4 – SSCD T3]

Hypothèse du profil de protection **[R3 – SSCD T2]** :

A.SCD_Generate *Génération fiable de SCD/SVD*
Si une autre partie que le signataire génère la paire SCD/SVD pour un signataire, alors :
(a) cette partie utilisera un SSCD pour la génération de SCD/SVD,
(b) la confidentialité du SCD sera garantie jusqu'à ce que le SCD soit sous le seul contrôle du signataire et
(c) le SCD ne sera pas utilisé pour de la création de signature jusqu'à ce que le SCD soit sous le seul contrôle du signataire.
(d) La génération de SCD/SVD est invoquée seulement par des utilisateurs autorisés
(e) Le SSCD Type 1 assure l'authenticité du SVD qu'il a créé et exporté

Hypothèses communes aux profils de protection **[R3 – SSCD T2]** et **[R4 – SSCD T3]** :

A.CGA *Application fiable de génération de certification*
La CGA protège l'authenticité du nom du signataire et les SVD dans le certificat qualifié par une signature avancée du CSP.

A.SCA *Application fiable de création de signature*
Le signataire utilise uniquement une SCA fiable. La SCA génère et envoie la représentation des DTBS des données que le signataire souhaite signer dans une forme appropriée pour la signature par la TOE.

3.3 LES MENACES

Le Tableau 6 présente les menaces retenues pour la présente TOE et leurs correspondances avec les profils de protections **[R2 – 9911]**, **[R3 – SSCD T2]** et **[R4 – SSCD T3]**.

Menaces pour la TOE	PP 9911	PP SSCD type 2	PP SSCD 3
T.Hack_Phys		T.Hack_Phys	T.Hack_Phys
T.SCD_Divulg		T.SCD_Divulg	T.SCD_Divulg
T.SCD_Derive		T.SCD_Derive	T.SCD_Derive
T.Sig_Forgery		T.Sig_Forgery	T.Sig_Forgery
T.Sig_Repud		T.Sig_Repud	T.Sig_Repud
T.SVD_Forgery		T.SVD_Forgery	T.SVD_Forgery
T.DTBS_Forgery		T.DTBS_Forgery	T.DTBS_Forgery
T.SigF_Misuse		T.SigF_Misuse	T.SigF_Misuse
T.CLON	T.CLON		
T.DIS_INFO	T.DIS_INFO		
T.DIS_DEL	T.DIS_DEL		
T.DIS_ES1	T.DIS_ES1		
T.DIS_TEST_ES	T.DIS_TEST_ES		
T.T_DEL	T.T_DEL		
T.T_TOOLS	T.T_TOOLS		
T.T_SAMPLE2	T.T_SAMPLE2		
T.T_MOD_DEL	T.T_MOD_DEL		
T.MOD	T.MOD		
T.DIS_DEL1	T.DIS_DEL1		
T.DIS_DEL2	T.DIS_DEL2		
T.MOD_DEL1	T.MOD_DEL1		
T.MOD_DEL2	T.MOD_DEL2		
T.DIS_ES2	T.DIS_ES2		
T.T_ES	T.T_ES		
T.T_CMD	T.T_CMD		
T.MOD_LOAD	T.MOD_LOAD		
T.MOD_EXE	T.MOD_EXE		
T.MOD_SHARE	T.MOD_SHARE		

T.MOD_SOFT	T.MOD_SOFT		

Tableau 6 : Correspondances ST/PP – menaces pour la TOE

3.3.1 Menaces définies dans [R2 – 9911]

Les menaces sont réparties entre :

- Les menaces contre lesquelles une protection spécifique doit être intégrée à la cible d'évaluation (classe I),
- Les menaces contre lesquelles une protection spécifique doit être intégrée à l'environnement (classe II).

3.3.1.1 Clonage partiel ou total de la TOE non autorisé

T.CLON
Le clonage fonctionnel de la cible d'évaluation (total ou partiel) paraît s'appliquer à toutes les phases du cycle de vie de la cible d'évaluation, de la phase 1 à la phase 7, mais seules les phases 1 et 4 à 7 sont considérées ici, dans la mesure où le clonage fonctionnel aux phases 2 et 3 se trouve uniquement dans le champ d'application du profil de protection des microcircuits des cartes à puces. En général, cette menace est dérivée de menaces spécifiques combinant la divulgation non autorisée, la modification ou le vol de biens à différentes phases.

3.3.1.2 Menaces sur la phase 1

Pendant la phase 1, trois types de menaces doivent être considérés :

a) : Les menaces sur le logiciel embarqué des cartes à puces et son environnement de développement, telles que la divulgation non autorisée, la modification ou le vol du logiciel embarqué de la carte à puce et/ou des données d'initialisation en phase 1.
b) : Les menaces sur les biens transmis par le concepteur du microcircuit au développeur du logiciel de la carte à puce pendant la phase de développement du logiciel embarqué de la carte à puce.
c) : Les menaces sur le logiciel embarqué de la carte à puce et sur les données d'initialisation transmises au cours du processus de livraison par le développeur du logiciel de la carte à puce au concepteur du microcircuit.

Divulgation non autorisée des biens

Ce type de menace couvre la divulgation non autorisée de biens par des attaquants qui peuvent avoir diverses compétences techniques, ressources et motivations. De tels attaquants doivent également avoir une connaissance technique du produit.

T.DIS_INFO *(type b)*
Divulgation non autorisée de biens fournis par le concepteur du microcircuit au développeur du logiciel embarqué de la carte à puce, telle que divulgation d'informations sensibles sur la spécification du microcircuit, sur la conception et la technologie, les logiciels et outils, le cas échéant.

T.DIS_DEL *(type c)*
Divulgation non autorisée du logiciel embarqué de la carte à puce et de toute donnée d'application supplémentaire (telle que les exigences d'initialisation des microcircuits) pendant la phase de livraison au concepteur du microcircuit.

T.DIS_ES1 *(type a)*
Divulgation non autorisée du logiciel embarqué (spécifications techniques ou détaillées, code d'implémentation) et/ou données applicatives (telles que codes secrets, paramètres de contrôle du système de protection, spécifications et implémentation des mécanismes de sécurité).

T.DIS_TEST_ES *(type a et c)*

Divulgation non autorisée des programmes de test du logiciel embarqué de la carte à puce ou de toute autre information liée.

Vol ou utilisation non autorisée des biens

Les attaquants potentiels peuvent avoir accès à la cible d'évaluation et effectuer des opérations sans y être autorisés. Par exemple, un tel attaquant peut personnaliser, modifier ou influencer le produit de manière à accéder au système d'application de la carte à puce.

T.T_DEL *(type c)*
Vol du logiciel embarqué de la carte à puce et de toute donnée d'application supplémentaire (telle que les exigences de pré-personnalisation) pendant la phase de livraison au concepteur du microcircuit.

T.T_TOOLS *(type a et b)*
Vol ou utilisation non autorisée des outils de développement du logiciel embarqué de la carte à puce (tels que PC, logiciel de développement, bases de données)

T.T_SAMPLE2 *(type a)*
Vol ou utilisation non autorisée d'échantillons de la cible d'évaluation (ex. : microcircuit dessoudé avec logiciel embarqué)

Modification non autorisée des biens

La cible d'évaluation peut être sujette à différents types d'attaques logiques ou physiques susceptibles de compromettre la sécurité. Du fait de l'usage prévu pour la cible d'évaluation (son environnement peut être hostile), la sécurité de la cible d'évaluation peut être contournée ou compromise, réduisant ainsi les mécanismes de sécurité de la cible d'évaluation et désactivant leur capacité à gérer la sécurité de la cible d'évaluation. Ce type de menace inclut la mise en œuvre de chevaux de Troie hostiles.

T.T_MOD_DEL *(type c)*
Modification non autorisée du logiciel embarqué de la carte à puce et de toute donnée applicative supplémentaire (telle que les exigences d'initialisation des microcircuits) pendant la phase de livraison au concepteur du microcircuit.

T.MOD *(type a)*
Modification non autorisée du logiciel embarqué et/ou des données applicatives ou de toute information liée (spécifications techniques).

3.3.1.3 Menaces sur les livraisons pour la phase 1 et les phases 4 à 6

Menaces sur les données transmises au cours du processus de livraison du développeur de la carte à puce au fabricant de boîtiers de microcircuits, au fabricant du processus de finition ou au personnalisateur.

Ces menaces sont décrites ci-dessous :

T.DIS_DEL1
Divulgation non autorisée de données applicatives pendant la livraison au fabricant des boîtiers de microcircuits, au fabricant du processus de finition ou au personnalisateur.

T.DIS_DEL2
Divulgation non autorisée de données applicatives livrées au fabricant des boîtiers de microcircuits, au fabricant du processus de finition ou au personnalisateur.

T.MOD_DEL1
Modification non autorisée de données applicatives pendant la livraison au fabricant des boîtiers de microcircuits, au fabricant du processus de finition ou au personnalisateur.

T.MOD_DEL2
Modification non autorisée de données applicatives livrées au fabricant des boîtiers de microcircuits, au fabricant du processus de finition ou au personnalisateur.

3.3.1.4 Menaces sur les phases 4 à 7

Les menaces envisagées au cours de ces phases peuvent être réparties selon trois types :

- Divulgation non autorisée de biens,
- Vol ou utilisation non autorisée de biens,
- Modification non autorisée de biens.

Divulgation non autorisée des biens

Ce type de menace couvre la divulgation non autorisée de biens par des attaquants qui peuvent avoir diverses compétences techniques, ressources et motivations. De tels attaquants peuvent également avoir une connaissance technique du produit.

T.DIS_ES2
Divulgation non autorisée du logiciel embarqué et de données applicatives (telles que systèmes de protection des données, partitionnement de la mémoire, programmes et clés de cryptographie).

Vol ou utilisation non autorisée des biens

Les attaquants potentiels peuvent avoir accès à la cible d'évaluation et effectuer des opérations sans y être autorisés. Par exemple, ces attaquants peuvent personnaliser le produit de manière non autorisée ou tenter d'accéder frauduleusement au système de la carte à puce.

T.T_ES
Vol ou utilisation non autorisée de la cible d'évaluation (ex. : microcircuit dessoudé avec logiciel embarqué).

T.T_CMD
Utilisation non autorisée d'instructions, de commandes ou de séquence de commandes envoyées à la cible d'évaluation

Modification non autorisée des biens

La cible d'évaluation peut être sujette à différents types d'attaques logiques ou physiques susceptibles de compromettre la sécurité. Du fait de l'usage prévu pour la cible d'évaluation (son environnement peut être hostile), les éléments de sécurité de la cible d'évaluation peuvent être contournés ou compromis, réduisant ainsi les mécanismes de sécurité de la cible d'évaluation et désactivant leur capacité à gérer la sécurité de la cible d'évaluation. Ce type de menace inclut la mise en œuvre de chevaux de Troie hostiles, de portes dérobées, le téléchargement de virus ou de programmes non autorisés.

T.MOD_LOAD
Chargement non autorisé de programmes.

T.MOD_EXE
Exécution non autorisée de programmes.

T.MOD_SHARE
Modification non autorisée du comportement du programme par interaction de différents programmes.

T.MOD_SOFT
Modification non autorisée du logiciel embarqué de la carte à puce et des données applicatives.

3.3.1.5 Classification des menaces

Le tableau ci-dessous indique les relations entre les phases du cycle de vie de la carte à puce, les menaces et les types de menaces :

Menaces	Phase 1	Phase 4	Phase 5	Phase 6	Phase 7
T.CLON	Classe II	Classe I	Classe I	Classe I	Classe I
T.DIS_INFO	Classe II				
T.DIS_DEL	Classe II				
T.DIS_DEL1	Classe II				
T.DIS_DEL2		Classe II	Classe II	Classe II	
T.DIS_ES1	Classe II				
T.DIS_TEST_ES	Classe II				
T.DIS_ES2		Classe I	Classe I	Classe I	Classe I
T.T_DEL	Classe II				
T.T_TOOLS	Classe II				
T.T_SAMPLE2	Classe II				
T.T_ES		Classe I	Classe I	Classe I	Classe I
T.T_CMD		Classe I	Classe I	Classe I	Classe I
T.T_MOD_DEL	Classe II				
T.MOD_DEL1	Classe II				
T. MOD_DEL2		Classe II	Classe II	Classe II	
T.MOD	Classe II				
T.MOD_SOFT		Classe I	Classe I	Classe I	Classe I
T.MOD_LOAD		Classe I	Classe I	Classe I	Classe I
T.MOD_EXE		Classe I	Classe I	Classe I	Classe I
T.MOD_SHARE		Classe I	Classe I	Classe I	Classe I

Tableau 7 : Classification des menaces

Classe I : Menaces amenant des protections mise en œuvre par la TOE.
Classe II : Menaces amenant des protections mises en œuvre par l'environnement de la TOE.

3.3.2 Menaces définies dans [R3 – SSCD T2] et [R4 – SSCD T3]

Les menaces suivantes sont celles définies dans le profil de protection **[R3 – SSCD T2]** et **[R4 – SSCD T3]**. L'agent de menace est un humain ou un processus agissant pour son compte et situé hors de la TOE. L'objectif principal de l'attaquant est d'accéder aux informations sensibles liées aux services de signature électronique sécurisés. L'attaquant a une attaque potentielle de niveau élevé et ne connaît aucun secret.

T.Hack_Phys *Attaques physiques par les interfaces de la TOE*
Un attaquant interagit avec les interfaces de la TOE pour exploiter les vulnérabilités, ce qui a pour résultat des compromissions de sécurité arbitraires. Cette menace concerne tous les biens.

T.SCD_Divulg *Stockage, copie et diffusion des données de création de signature*
Un attaquant peut stocker, copier les SCD en dehors de la TOE. Un attaquant peut diffuser les SCD au cours de leur génération, de leur stockage et de leur utilisation pour la création de signature dans la TOE.

T.SCD_Derive *Trouver les données de création de signature*
Un attaquant trouve les SCD dans des données publiques connues, telles que les SVD correspondant aux SCD ou les signatures créées au moyen des SCD ou d'autres données communiquées en dehors de la TOE, ce qui sont une menace pour la confidentialité des SCD.

T.Sig_Forgery *Contrefaçon de la signature électronique*
Un attaquant falsifie l'objet des données signées et peut-être également sa signature électronique créée par la TOE et la violation de l'intégrité de l'objet des données signées n'est pas détectable par le signataire ou par des tiers. La signature générée par la TOE est soumise à des attaques délibérées d'experts possédant un fort potentiel d'attaque à l'aide de connaissances avancées en terme de principes et concepts de sécurité employés par la TOE.

T.Sig_Repud *Répudiation des signatures*

Si un attaquant peut menacer avec succès l'un des biens, la non-répudiation de la signature électronique est alors compromise. Le signataire est ainsi capable de nier avoir signé des données à l'aide des SCD dans la TOE sous son contrôle même si la signature est vérifiée avec succès par rapport aux SVD contenues dans son certificat non révoqué.

T.SVD_Forgery *Contrefaçon des données de vérification de signature*
Un attaquant falsifie les SVD présentées par la TOE à la CGA. Il en résulte une perte de l'intégrité des SVD dans le certificat du signataire.

T.DTBS_Forgery *Contrefaçon de la représentation des DTBS*
Un attaquant modifie la représentation des DTBS envoyées par la SCA. Ainsi, la représentation des DTBS utilisée par la TOE pour la signature ne correspond pas aux DTBS que le signataire a l'intention de signer.

T.SigF_Misuse *Mauvaise utilisation de la fonction de création de signature de la TOE*
Un attaquant utilise mal la fonction de création de signature de la TOE pour créer un SDO pour les données que le signataire n'a pas décidé de signer. La TOE est soumis à des attaques délibérées d'experts possédant un fort potentiel d'attaque à l'aide de connaissances avancées en terme de principes et de concepts de sécurité employés par la TOE.

3.4 LES POLITIQUES DE SECURITE ORGANISATIONNELLES

Les politiques de sécurité organisationnelles de la TOE sont celles définies dans les profils de protection **[R3 – SSCD T2]** et **[R4 – SSCD T3]**. Elles sont applicables lorsque la TOE est utilisée dans le cadre du service de création de signature électronique qualifiée. Dans le cas contraire, elles ne sont pas applicables.

P.CSP_Qcert *Certificat qualifié*
Le CSP utilise une CGA de confiance pour générer le certificat qualifié pour les SVD générées par le SSCD. Les certificats qualifiés contiennent au moins les éléments définis à l'Annexe I de la Directive, c'est-à-dire entre autres le nom du signataire et les SVD correspondant aux SCD mises en application dans la TOE sous le seul contrôle du signataire. Le CSP garantit que l'utilisation de la TOE pour la signature est prouvée par l'intermédiaire du certificat ou d'autres informations disponibles publiquement.

P.Qsign *Signatures électroniques qualifiées*
Le signataire utilise un système de création de signature pour signer les données à l'aide de signatures électroniques qualifiées. Les DTBS sont présentées au signataire par la SCA. La signature électronique qualifiée est basée sur un certificat qualifié (conformément à l'Annexe 1 de la Directive) et est créée par un SSCD.

P.Sigy_SSCD *TOE en tant que dispositif sécurisé de création de signature*
La TOE met en application les SCD utilisées pour la création de la signature sous le seul contrôle du signataire. Les SCD utilisées pour la génération de la signature ne peuvent apparaître qu'une fois en pratique.

4. OBJECTIFS DE SECURITE

Cette section identifie et définit les objectifs de sécurité de la TOE et de son environnement. Les objectifs de sécurité reflètent l'intention constatée et contrecarrent les menaces identifiées, tout en se conformant aux politiques de sécurité organisationnelles et hypothèses identifiées.

Les objectifs de sécurité de la TOE et de son environnement sont ceux définis dans le profil de protection **[R2 – 9911]**, **[R3 – SSCD T2]** et **[R4 – SSCD T3]**.

4.1 OBJECTIFS DE SECURITE POUR LA TOE

Le Tableau 8 présente les objectifs de sécurité retenues pour la présente TOE et leurs correspondances avec les profils de protections **[R2 – 9911]**, **[R3 – SSCD T2]** et **[R4 – SSCD T3]**.

Objectifs de sécurité pour la TOE	PP 9911	PP SSCD type 2	PP SSCD type3
OT.EMSEC_Design		OT.EMSEC_Design	OT.EMSEC_Design
OT.Lifecycle_Security		OT.Lifecycle_Security	OT.Lifecycle_Security
OT.SCD_Secrecy		OT.SCD_Secrecy	OT.SCD_Secrecy
OT.SCD_SVD_Corresp		OT.SCD_SVD_Corresp	OT.SCD_SVD_Corresp
OT.SVD_Auth_TOE		OT.SVD_Auth_TOE	OT.SVD_Auth_TOE
OT.Tamper_ID		OT.Tamper_ID	OT.Tamper_ID
OT.Tamper_Resistance		OT.Tamper_Resistance	OT.Tamper_Resistance
OT.SCD_Transfer		OT.SCD_Transfer	
OT.Init			OT.Init
OT.SCD_Unique			OT.SCD_Unique
OT.DTBS_Integrity_TOE		OT.DTBS_Integrity_TOE	OT.DTBS_Integrity_TOE
OT.Sigy_SigF		OT.Sigy_SigF	OT.Sigy_SigF
OT.Sig_Secure		OT.Sig_Secure	OT.Sig_Secure
O.TAMPER_ES	O.TAMPER_ES		
O.CLON	O.CLON		
O.OPERATE	O.OPERATE		
O.FLAW	O.FLAW		
O.DIS_MECHANISM2	O.DIS_MECHANISM2		
O.DIS_MEMORY	O.DIS_MEMORY		
O.MOD_MEMORY	O.MOD_MEMORY		

Tableau 8 : Correspondances ST/PP – objectifs de sécurité pour la TOE

4.1.1 Objectifs de sécurité définis dans [R2 – 9911]

La TOE doit employer les technologies les plus avancées afin d'assurer les objectifs de sécurité informatique suivants et, pour ce faire, lorsque des fonctionnalités de sécurité physiques des microcircuits sont utilisées, les spécifications de ces fonctionnalités de sécurité physiques des microcircuits doivent être respectées. Lorsque les fonctionnalités de sécurité physiques des microcircuits ne sont pas utilisées, les objectifs de sécurité doivent être atteints par d'autres moyens.

O.TAMPER_ES
La cible d'évaluation doit empêcher les attaques sur ses éléments de sécurité critiques. Des mécanismes de sécurité doivent en particulier empêcher la modification non autorisée de paramètres fonctionnels, d'attributs de sécurité et de codes secrets tels que les marqueurs de séquence du cycle de vie et les clés de cryptographie. Le logiciel embarqué doit être conçu pour éviter les interprétations des signaux électriques issus des parties matérielles de la cible d'évaluation.

O.CLON

La fonctionnalité de la cible d'évaluation doit être protégée du clonage.

O.OPERATE
La cible d'évaluation doit assurer la continuité du fonctionnement correct de ses fonctions de sécurité.

O.FLAW
La cible d'évaluation ne doit pas contenir de défauts de conception, de mise en œuvre ou de fonctionnement.

O.DIS_MECHANISM2
La cible d'évaluation doit assurer que les mécanismes de sécurité du logiciel embarqué sont protégés contre la divulgation non autorisée.

O.DIS_MEMORY
La cible d'évaluation doit assurer que les informations sensibles stockées en mémoire sont protégées contre la divulgation non autorisée.

O.MOD_MEMORY
La cible d'évaluation doit assurer que les informations sensibles stockées en mémoire sont protégées contre toute corruption ou modification non autorisées.

4.1.2 Objectifs de sécurité définis dans [R3 – SSCD T2] et [R4 – SSCD T3]

Objectif du profil de protection **[R3 – SSCD T2]** :

OT.SCD_Transfer *Transfert sécurisé de SCD entre SSCD*
La TOE doit assurer la confidentialité du SCD transféré entre des SSCDs.

Objectifs du profil de protection **[R4 – SSCD T3]** :

OT.Init *Génération des SCD/SVD*
La TOE fournit des fonctions de sécurité pour garantir que la génération des SCD et des SVD est invoquée par des utilisateurs autorisés uniquement.

OT.SCD_Unique *Caractère unique des données de création de signature*
La TOE doit garantir la qualité cryptographique de la paire SCD/SVD pour la signature électronique qualifiée. Les SCD utilisées pour la génération de la signature ne peuvent en pratique apparaître qu'une seule fois et ne peuvent pas être reconstruites à partir des SVD. Dans ce contexte, « en pratique qu'une seule fois » signifie que la probabilité de SCD identiques est quantité insignifiante.

Objectifs communs aux profils de protection **[R3 – SSCD T2]** et **[R4 – SSCD T3]** :

OT.EMSEC_Design *Fournir une sécurité physique aux émanations*
Concevoir et construire la TOE pour pouvoir contrôler la production d'émanations intelligibles dans des limites spécifiées.

OT.Lifecycle_Security *Sécurité du cycle de vie*
La TOE doit détecter les défauts au cours de l'initialisation, de la personnalisation et de l'utilisation opérationnelle. La TOE doit fournir des techniques de destruction sûres pour les SCD en cas de nouvelle génération.

OT.SCD_Secrecy *Confidentialité des données de création de signature*
La confidentialité des SCD (utilisées pour la génération de signature) est suffisamment protégée contre les attaques à fort potentiel.

OT.SCD_SVD_Corresp *Correspondance entre les SVD et les SCD*
La TOE doit garantir la correspondance entre les SVD et les SCD. La TOE doit vérifier sur demande la correspondance entre les SCD stockées dans la TOE et les SVD si elles ont été envoyées à la TOE.

OT.SVD_Auth_TOE *La TOE garantit l'authenticité des SVD*

La TOE fournit des moyens permettant à la CGA de vérifier l'authenticité des SVD qui ont été exportées par cette TOE.

OT.Tamper_ID *Détection de l'intrusion*
La TOE fournit des fonctions système qui détectent l'intrusion physique d'un composant du système et utilise ces fonctions pour limiter les brèches de sécurité.

OT.Tamper_Resistance *Résistance à l'intrusion*
La TOE évite ou résiste à l'intrusion physique avec des dispositifs et des composants « système » spécifiés.

OT.Init *Génération des SCD/SVD*
La TOE fournit des fonctions de sécurité pour garantir que la génération des SCD et des SVD est invoquée par des utilisateurs autorisés uniquement.

OT.SCD_Unique *Caractère unique des données de création de signature*
La TOE doit garantir la qualité cryptographique de la paire SCD/SVD pour la signature électronique qualifiée. Les SCD utilisées pour la génération de la signature ne peuvent en pratique apparaître qu'une seule fois et ne peuvent pas être reconstruites à partir des SVD. Dans ce contexte, « en pratique qu'une seule fois » signifie que la probabilité de SCD identiques est quantité insignifiante.

OT.DTBS_Integrity_TOE *Vérification de l'intégrité de la représentation des DTBS*
La TOE doit vérifier que la représentation des DTBS reçues de la SCA n'a pas été modifiée au cours du transfert entre la SCA et la TOE. La TOE elle-même doit garantir que la représentation des DTBS n'est pas modifiée par la TOE également. Il faut noter que cela n'entre pas en conflit avec le processus de création de signature où les DTBS elles-mêmes peuvent être « hachées » par la TOE.

OT.Sigy_SigF *Fonction de génération de signature pour le signataire légitime uniquement*
La TOE fournit une fonction de génération de signature pour le signataire légitime uniquement et protège les SCD contre une utilisation par autrui. La TOE doit résister aux attaques à fort potentiel.

OT.Sig_Secure *Sécurité cryptographique de la signature électronique*
La TOE génère au moyen de techniques de chiffrement robustes, des signatures électroniques qui ne peuvent pas être falsifiées sans connaître les SCD. Les SCD ne peuvent pas être reconstruites à l'aide des signatures électroniques. Les signatures électroniques doivent pouvoir résister à ces attaques même si ces dernières sont réalisées avec un fort potentiel d'attaque.

4.2 OBJECTIFS DE SECURITE POUR L'ENVIRONNEMENT DE LA TOE

Le Tableau 9 présente les objectifs de sécurité retenues pour l'environnement de la présente TOE et leurs correspondances avec les profils de protections **[R2 – 9911]**, **[R3 – SSCD T2]** et **[R4 – SSCD T3]**.

Objectifs de sécurité pour l'env. de la TOE	PP 9911	PP SSCD type 2	PP SSCD type3
OE.SCD_SVD_Corresp		OE.SCD_SVD_Corresp	
OE.SCD_Transfer		OE.SCD_Transfer	
OE.SCD_Unique		OE.SCD_Unique	
OE.CGA_Qcert			OE.CGA_Qcert
OE.SVD_Auth_CGA			OE.SVD_Auth_CGA
OE.HI_VAD			OE.HI_VAD
OE.SCA_Data_Intend			OE.SCA_Data_Intend
O.DEV_TOOLS	O.DEV_TOOLS		
O.DEV_DIS_ES	O.DEV_DIS_ES		
O.SOFT_DLV	O.SOFT_DLV		
O.INIT_ACS	O.INIT_ACS		
O.SAMPLE_ACS	O.SAMPLE_ACS		
O.DLV_PROTECT	O.DLV_PROTECT		
O.DLV_AUDIT	O.DLV_AUDIT		
O.DLV_RESP	O.DLV_RESP		
O.DLV_DATA	O.DLV_DATA		
O.TEST_OPERATE	O.TEST_OPERATE		
O.USE_DIAG	O.USE_DIAG		

Tableau 9 : Correspondances ST/PP – objectifs de sécurité pour l'environnement de la TOE

4.2.1 Objectifs de sécurité pour l'environnement de la TOE

Ces objectifs sont définis dans **[R2 – 9911]**.

4.2.1.1 Objectifs pour la phase 1

O.DEV_TOOLS
Le logiciel embarqué de la carte à puce, doit être conçu de manière sécurisée, par l'usage exclusif d'outils de développement de logiciels (compilateurs assembleurs, éditeurs de liens, simulateurs…) et d'outils de test d'intégration logiciel-matériel (émulateurs) assurant l'intégrité des programmes et des données.

O.DEV_DIS_ES
Le développeur du logiciel embarqué doit utiliser des procédures établies afin de contrôler le stockage et l'usage des outils de développement classifiés ainsi que de la documentation classifiée, afin de garantir l'intégrité et la confidentialité des biens de la cible d'évaluation.
Il doit être garanti que les outils ne sont fournis et accessibles qu'au personnel autorisé de chaque partie.
Il doit être garanti que les informations confidentielles relatives aux biens définis, ne sont fournies au personnel autorisé de chaque partie que sur la base de la nécessité de les connaître.

O.SOFT_DLV
Le logiciel embarqué de la carte à puce doit être, livré par le développeur du logiciel embarqué de la carte à puce (Phase 1) au concepteur du microcircuit via une procédure de livraison et de vérification sécurisée capable d'assurer l'intégrité du logiciel et sa confidentialité, le cas échéant.

O.INIT_ACS
Les données d'initialisation ne doivent être accessibles qu'à un personnel autorisé (procédures physiques, organisationnelles, techniques et relatives au personnel).

O.SAMPLE_ACS
Les échantillons utilisés pour effectuer des tests ne doivent être accessibles qu'à un personnel autorisé.

4.2.1.2 Objectifs pour les processus de livraison (phases 4 à 7)

O.DLV_PROTECT
Des procédures doivent assurer la protection du matériel/informations de la cible d'évaluation lors de la livraison. Elles comprennent les objectifs suivants :
- Non-divulgation des informations relatives à la sécurité ;
- Identification des éléments à livrer ;
- Respect des règles de confidentialité (niveau de confidentialité, - bordereau d'envoi, accusé de réception) ;
- Protection physique contre les dommages externes ;
- Procédures sécurisées de stockage et de manipulation (y compris des cibles d'évaluation refusées) ;
- Traçabilité des cibles d'évaluation en cours de livraison, incluant les paramètres suivants :
    - Les détails sur l'origine et l'expédition ;
    - La réception, accusé de réception ;

Les emplacements des équipements et des informations.

O.DLV_AUDIT
Les procédures doivent assurer que des actions correctives sont entreprises en cas de dysfonctionnement du processus de livraison (y compris, le cas échéant, toute non-conformité aux accords de confidentialité) et mettent en évidence tout non-respect de ce processus.

O.DLV_RESP
Les procédures doivent assurer que le personnel (du service expédition, du transporteur, du service réception) intervenant lors de la procédure de livraison possède les compétences, la formation et les connaissances requises par les exigences de cette procédure et soit capable d'agir en adéquation totale avec les attentes citées ci-dessus.

4.2.1.3 Objectifs pour les processus de livraison de la phase 1 à 4, 5 et 6

O.DLV_DATA

Les données « applicatives » doivent être livrées par le développeur du logiciel embarqué (phase 1) soit au fabricant des boîtiers de microcircuits, au fabricant du processus définition ou au personnalisateur via une procédure de livraison et de vérification sécurisée capable d'assurer l'intégrité et la confidentialité des données applicatives.

4.2.1.4 Objectifs pour les phases 4 à 6

O.TEST_OPERATE
Des tests de fonctionnalité appropriés de la cible d'évaluation doivent être mis en œuvre aux phases 4 à 6.
Au cours de toutes les opérations de fabrication et de test, des procédures de sécurité doivent être mises en œuvre sur les phases 4, 5 et 6 afin d'assurer la confidentialité et l'intégrité de la cible d'évaluation et de ses données de fabrication et de test.

4.2.1.5 Objectifs pour la phase 7

O.USE_DIAG
Des protocoles et procédures de communications sécurisées doivent être utilisés entre la carte à puce et le terminal.

4.2.2 Objectifs de sécurité pour l'environnement TI de la TOE

Ces objectifs sont définis dans les profils de protection **[R3 – SSCD T2]** et **[R4 – SSCD T3]**.

Objectifs de sécurité pour l'environnement TI de la TOE dans **[R3 – SSCD T2]** :

OE.SCD_SVD_Corresp *Correspondance entre SVD et SCD*
Le SSCD Type 1 doit assurer la correspondance entre le SVD et le SCD. Le SSCD Type 1 doit vérifier la correspondance entre le SCD envoyée à la TOE et le SVD envoyée au CGA ou à la TOE.

OE.SCD_Transfer *Transfert sécurisé de SCD entre SSCD*
Le SSCD Type 1 doit assurer la confidentialité de la SCD transférée à la TOE. Le SSCD Type 1 doit prévenir l'exportation d'une SCD qui a déjà été utilisée pour la génération de signature par un SSCD type 2. La SCD doit être détruite dans le SSCD Type 1 à chaque fois qu'elle est exportée dans la TOE.

OE.SCD_Unique *Unicité des données de création de signature*
Le SSCD Type 1 doit assurer la qualité cryptographique de la paire SCD/SVD pour la signature électronique qualifiée. La SCD utilisée pour la génération de signature ne peuvent en pratique apparaître qu'une seule fois et ne peuvent pas être reconstruites à partir des SVD. Dans ce contexte, « en pratique qu'une seule fois » signifie que la probabilité de SCD identiques est quantité insignifiante.

Objectifs de sécurité pour l'environnement TI de la TOE communs à **[R3 – SSCD T2]** et **[R4 – SSCD T3]** :

OE.CGA_Qcert *Génération de certificats qualifiés*
La CGA génère des certificats qualifiés qui comprennent entre autres
(a) le nom du signataire contrôlant la TOE ;
(b) la SVD correspondant à la SCD mise en œuvre dans la TOE sous le seul contrôle du signataire ;
(c) la signature avancée du CSP.

OE.SVD_Auth_CGA *La CGA vérifie l'authenticité de la SVD*
La CGA vérifie que le SSCD est l'émetteur de la SVD reçue et que de la SVD reçue est intègre. La CGA vérifie la correspondance entre la SCD dans SSCD du signataire et la SVD du certificat qualifié.

OE.HI_VAD *Protection des VAD*
Si un dispositif externe fournit une interface humaine pour l'authentification de l'utilisateur, ce dispositif garantira la confidentialité et l'intégrité de la VAD, nécessaires à la méthode d'authentification utilisée.

OE.SCA_Data_Intend *Données devant être signées*

La SCA :

(a) génère la représentation des DTBS des données qui ont été présentées en tant que DTBS et que le signataire a l'intention de signer sous une forme adaptée à la signature par la TOE ;

(b) envoie la représentation des DTBS à la TOE et permet la vérification de l'intégrité de la représentation des DTBS par la TOE ;

(c) attache la signature produite par la TOE aux données ou la fournit séparément.

5. EXIGENCES DE SECURITE TI

Ce chapitre présente les exigences de sécurité pour la TOE.

Les exigences fonctionnelles pour la TOE, définies dans ces chapitres sont celles définies dans les profils de protections **[R2 – 9911] [R3 – SSCD T2]** et **[R4 – SSCD T3]**. Le Tableau 10 présente la répartition des exigences pour ces deux profils de protection.

SFR pour la TOE	PP 9911	PP SSCD type 2	PP SSCD type3
Audit de sécurité			
FAU_SAA.1	FAU_SAA.1		
Support cryptographique			
FCS_CKM.1			FCS_CKM.1
FCS_CKM.3	FCS_CKM.3		
FCS_CKM.4	FCS_CKM.4	FCS_CKM.4	FCS_CKM.4
FCS_COP.1	FCS_COP.1	FCS_COP.1	FCS_COP.1
Protection des données utilisateur			
FDP_ACC.1		FDP_ACC.1	FDP_ACC.1
FDP_ACC.2	FDP_ACC.2		
FDP_ACF.1	FDP_ACF.1	FDP_ACF.1	FDP_ACF.1
FDP_DAU.1	FDP_DAU.1		
FDP_ETC.1	FDP_ETC.1	FDP_ETC.1	FDP_ETC.1
FDP_ITC.1	FDP_ITC.1	FDP_ITC.1	FDP_ITC.1
FDP_RIP.1	FDP_RIP.1	FDP_RIP.1	FDP_RIP.1
FDP_SDI.2	FDP_SDI.2	FDP_SDI.2	FDP_SDI.2
FDP_UCT.1		FDP_UCT.1	
FDP_UIT.1		FDP_UIT.1	FDP_UIT.1
Identification et authentification			
FIA_AFL.1	FIA_AFL.1	FIA_AFL.1	FIA_AFL.1
FIA_ATD.1	FIA_ATD.1	FIA_ATD.1	FIA_ATD.1
FIA_UAU.1	FIA_UAU.1	FIA_UAU.1	FIA_UAU.1
FIA_UAU.3	FIA_UAU.3		
FIA_UAU.4	FIA_UAU.4		
FIA_UID.1	FIA_UID.1	FIA_UID.1	FIA_UID.1
FIA_USB.1	FIA_USB.1		
Administration de la sécurité			
FMT_MOF.1	FMT_MOF.1	FMT_MOF.1	FMT_MOF.1
FMT_MSA.1	FMT_MSA.1	FMT_MSA.1	FMT_MSA.1
FMT_MSA.2	FMT_MSA.2	FMT_MSA.2	FMT_MSA.2
FMT_MSA.3	FMT_MSA.3	FMT_MSA.3	FMT_MSA.3
FMT_MTD.1	FMT_MTD.1	FMT_MTD.1	FMT_MTD.1
FMT_SMF.1			
FMT_SMR.1	FMT_SMR.1	FMT_SMR.1	FMT_SMR.1
Protection de la vie privée			
FPR_UNO.1	FPR_UNO.1		
Protection de la TSF			
FPT_AMT.1		FPT_AMT.1	FPT_AMT.1
FPT_EMSEC.1		FPT_EMSEC.1	FPT_EMSEC.1
FPT_FLS.1	FPT_FLS.1	FPT_FLS.1	FPT_FLS.1
FPT_PHP.1		FPT_PHP.1	FPT_PHP.1
FPT_PHP.3	FPT_PHP.3	FPT_PHP.3	FPT_PHP.3
FPT_SEP.1	FPT_SEP.1		
FPT_TDC.1	FPT_TDC.1		
FPT_TST.1	FPT_TST.1	FPT_TST.1	FPT_TST.1
Chemins et canaux de confiance			
FTP_ITC.1		FTP_ITC.1	FTP_ITC.1
FTP_TRP.1		FTP_TRP.1	FTP_TRP.1

Tableau 10 : Correspondances ST/PP – exigences de sécurité pour la TOE

5.1 SUJETS, OBJETS ET ATTRIBUTS DE SECURITE DE LA TOE

5.1.1 Liste des sujets de la TOE

Liste sujets	Description
SUB_GEST	Processus qui réceptionne toutes les commandes venant du terminal et les dispatche vers un autre processus (SUB_APPLI, SUB_AIP).
SUB_AIP	Processus activé par défaut par SUB_GEST durant les phases d'initialisation et de personnalisation. SUB_AIP est un objet pour SUB_GEST.
SUB_APPLI	Processus réalisant les services associés de l'application IAS-eGOV et qui est activé par SUB_GEST durant la phase « user » lorsque la commande est une commande SELECT. SUB_APPLI est un objet pour SUB_GEST.
SUB_CRYPTO	Processus activé par SUB_APPLI pour réaliser des opérations cryptographiques ou les opérations utilisant le code porteur. SUB_CRYPTO est un objet pour SUB_APPLI et pour SUB_AIP.
SUB_GF	Processus activé par SUB_APPLI pour gérer les objets OB_FILE. SUB_GF est un objet pour SUB_APPLI et pour SUB_AIP.
SUB_GS	Processus activé par SUB_APPLI pour gérer les objets OB_SECRET. SUB_GS est un objet pour SUB_APPLI et pour SUB_AIP.
SUB_GT	Processus activé par SUB_APPLI pour gérer les objets OB_TLV. SUB_GT est un objet pour SUB_APPLI et pour SUB_AIP.

5.1.2 Liste des objets de la TOE

Liste objets	Description
OB_FILE	Objet désignant de façon générique les objets suivants : OB_DFILE, OB_EFILE, OB_TLV, OB_SECRET. De façon générale un OB_FILE est un objet sur lequel sont appliqués des contrôles d'accès en lecture/écriture et création/suppression et de changement d'état hormis l'objet OB_TLV.
OB_DFILE	Répertoire de type ADF ou DF, stocké en E²PROM qui contient des OB_FILE.
OB_EFILE	Fichier élémentaire EF stocké en E²PROM et contenant des données utilisateurs ou propriétaires.
OB_TLV	Données de type TLV = Tag Longueur Valeur. Ils regroupent les données de types paramètres carte. Quand ils sont accessibles, ils sont accessibles en mise à jour et en lecture.
OB_SECRET	Objet contenant une clé cryptographique ou un code PIN ainsi que les informations de sécurité qui leur sont associées. Il est stocké dans des fichiers OB_FILE (SECRET_INFO & SECRET_DATA).
OB_TEMP	Objet désignant les données temporaires qui sont stockées en mémoire RAM et qui sont utilisées dans des opérations sécurisées.
OB_I/O	Buffers utilisés pour les communications externes.

5.1.3 Liste des attributs de sécurité de la TOE

Liste Attributs	Description
Checksum buffer I/O	Checksum pour la gestion de l'intégrité des buffers I/O avant et après les traitements réalisés par SUB_CRYPTO : - Corrompu/Non-corrompu.
Checksum répertoire/fichier	Checksum pour la gestion de l'intégrité des données du répertoire ou du fichier : - Corrompu/Non-corrompu.
Checksum secret	Checksum pour la gestion de l'intégrité d'une clé ou d'un code PIN : - Corrompu/Non-corrompu.
Checksum TLV	Checksum pour la gestion de l'intégrité du paramètre stocké dans l'objet TLV : - Corrompu/Non-corrompu.
DAC : Contrôle d'accès aux fichiers et aux répertoires	Cet attribut définit les conditions d'accès aux objets auxquels il se rattache. Sa structure se présente comme suit : *DAC = [(Opération1, (liste des conditions pour l'opération1)), ((Opération2, (liste des conditions pour l'opération2)), …]* Les opérations sont l'écriture ou la lecture de données dans le fichier concerné. Les conditions pour une opération sont : - ALWAYS : Opération toujours autorisée ; - NEVER : Opération jamais autorisée ; - USERx : Opération autorisée si USERx authentifié ; - SMI : Opération autorisée si la sécurisation de la commande est SMI ; - SMC : Opération autorisée si la sécurisation de la commande est SMI +SMC. A chaque objet (répertoire, fichier, secret ou TLV) est associé un attribut qui indique les conditions d'accès. Le DAC est comparé aux attributs de sécurité en cours dans l'état de sécurité carte.
Entête de commande	Les champs « CLA, INS, P1, P2 » de la commande sont utilisés pour analyser la commande.
Etat de sécurité carte	Cet attribut contient les états de sécurité en cours pour la carte Morpho-Citiz 32. Il se compose des attributs suivants : - Le ou les utilisateurs authentifiés sur les différents domaines : Lorsqu'un utilisateur est authentifié avec succès, son authentification sur un domaine est renseignée dans l'état de sécurité carte ; - La portée des authentifications : La validité des statuts d'authentification des utilisateurs est fonction du domaine sur lequel sont associés les secrets d'authentification ; - Canal de confiance (SM) en cours : Indique si un SMI/SMC est établi ; Les statuts d'authentification d'un domaine sont initialisés à « aucun utilisateur authentifié » lorsque les opérations sortent du domaine. Les canaux de confiances en cours sont initialisés à « aucun SM » et « aucune nature en cours » à chaque nouvelle

	opération (i.e. à chaque nouvelle commande).
Etat secret	Attribut définissant l'état en cours d'un OB_SECRET : - Créé/Activé/Désactivé/Terminé/bloqué ;
Etat fichier	Attribut définissant l'état en cours d'un OB_FILE (exception faite des OB_TLV) : - Créé/Activé/Désactivé/Terminé ;
Compteur d'utilisation	Attribut associé à un secret et limitant le nombre maximum d'utilisation du secret.
Groupe de Ratification	Attribut associé à un secret et comptant les échecs d'authentification successifs sur ce secret : PTC : Compteur de ratification PTL : Nombre maximum de présentation
Phase de vie carte	Cet attribut définit la phase de vie dans laquelle se trouve la carte : INIT/PERSO/USER/BLOQUE/FIN DE VIE
Statut de l'application	Cet attribut définit l'état en cours de l'application : Il décrit les différents états de l'application : - Active/Non-Active ; - Sélectionnée/Repos ; - Bloquée/Non-bloquée ;
Table des services	Cet attribut définit les droits d'accès des sujets aux services que réalisent les sujets qu'ils sollicitent. Par exemple, SUB_APPLI appelle SUB_CRYPTO pour réaliser les services de traitements cryptographiques.
Type d'algorithme	Cet attribut est utilisé pour contrôler l'association « clé/algorithme », i.e. : AUTH_INT, AUTH_EXT, ENC/DEC, MAC, GEN_SIGN, VERIF_SIGN, SEC_ DEC.
Type de clé	Cet attribut définit l'usage de la clé : - AUTH_INT : Authentification interne ; - AUTH_EXT : Authentification externe ; - ENC/DEC : Chiffrement / déchiffrement de données ; - MAC : Calcul de MAC ; - GEN_SIGN : Génération de signature électronique ; - VERIF_SIGN :Vérification de signature électronique ; - SEC_ DEC : Déchiffrement de secrets ;
Type de l'objet	Cet attribut est utilisé pour définir le type d'un objet : MF/ADF/DF/EF/SECRET/TLV.

5.1.4 Attributs de sécurité définis dans [R3 – SSCD T2] et [R4 – SSCD T3]

Les attributs de sécurité de l'utilisateur, les composants de la TOE et les états associés sont :

Utilisateur, sujet ou objet auquel l'attribut est associé	Attribut	Etat
Groupe d'attributs généraux		
Utilisateur	Rôle	Administrateur/Signataire
Groupe d'attributs d'initialisation		
Utilisateur	Gestion des SCD/SVD	Autorisé/Non-autorisé
SCD	Importation sécurisée de SCD autorisée	Non/Oui
Groupe d'attributs de création de signature		
SCD	SCD opérationnelles	Non/Oui
DTBS	Envoyées par une CSA autorisée	Non/Oui

5.2 DEFINITION DES EXIGENCES FONCTIONNELLES DE SECURITE POUR LA TOE

5.2.1 Audit de sécurité (FAU)

FAU_SAA.1 Analyse de violation potentielle

FAU_SAA.1.1 La TSF doit pouvoir appliquer un ensemble de règles en surveillant les événements audités et indiquer, en fonction de ces règles, une violation potentielle de la TSP.

FAU_SAA.1.2 La TSF doit appliquer les règles suivantes pour la surveillance des événements audités :

1. Accumulation ou combinaison des **[affectation : événements auditables suivants]** connus pour indiquer une violation potentielle de la sécurité ;

Affectation : Evènements auditables

- Modification du mode opératoire par l'environnement (capteur) ;
- Tentative de violation du contrôle d'accès ;
- Echec d'autotest mémoire (ROM, E²PROM, RAM) ;
- Echec d'intégrité sur un répertoire/fichier, sur l'entête d'un fichier, sur un objet TLV, un buffer I/O, sur une clé ou sur un code PIN ;
- Erreur d'intégrité du générateur d'aléa et du crypto processeur.

2. Autres règles : **[sans objet]**.

5.2.2 Support cryptographique (FCS)

FCS_CKM.1 Génération de clés cryptographiques

FCS_CKM.1.1 La TSF doit générer des clés cryptographiques conformément à l'algorithme de génération de clé cryptographique **[affectation: Liste des algorithmes de génération de clés]** et aux tailles spécifiées de clés cryptographiques **[affectation: Tailles de clés associées]** respectant la **[Liste des normes]**.

Affectation **Voir Tableau 11**

Liste des algorithmes de génération de clés	Tailles de clé	Liste des normes
Génération de clé RSA	1024 à 2048 bits	**[R10 – AREAK1]**, **[R11 – AREAK2]**

Tableau 11 : Génération de clés cryptographiques

FCS_CKM.3 Accès aux clés cryptographiques

FCS_CKM.3.1 La TSF doit réaliser **[affectation : un accès aux clés cryptographiques]** conformément à **[affectation : une méthode d'accès aux clés cryptographiques]** spécifiée qui satisfait aux normes suivantes : **[sans objet]**

Affectation **Type de l'accès**

Accès aux SCD/SVD en écriture/lecture pour effectuer les opérations de génération/destruction de SCD/SVD et de chargement de SCD/SVD dans les blocs de traitements cryptographiques pour la génération de signatures électroniques.

Méthode d'accès aux clés cryptographiques

Accès en lecture / écriture du code exécuté en mémoire ROM vers une clé stockée dans l'E²PROM par l'intermédiaire de la RAM protégée en intégrité et confidentialité.

FCS_CKM.4 Destruction de clés cryptographiques

FCS_CKM.4.1 La TSF doit détruire les clés cryptographiques conformément à **[affectation : une méthode de destruction de clés cryptographiques]** spécifiée qui satisfait aux normes suivantes : **[sans objet]**

Affectation **Méthode de destruction :**

Effacement de la mémoire EEPROM contenant la clé.

Raffinement SSCD Les SCD sont détruites sur demande du Signataire ou de l'Administrateur. La destruction de la SCD existante est obligatoire avant la re-génération par la TOE de la paire SCD/SVD ou le re-chargement de la SCD dans la TOE.

FCS_COP.1 Opération cryptographique

FCS_COP.1.1 La TSF doit exécuter **[affectation : liste des opérations cryptographiques]** conformément à un algorithme cryptographique **[affectation : algorithme cryptographique]** et avec des tailles de clés cryptographiques **[affectation : tailles des clés cryptographiques]** spécifiés qui satisfont à ce qui suit : **[affectation : liste des normes]**.

Affectation **Voir Tableau 12**

Liste des opérations cryptographiques	Algorithmes	Tailles de clé	Liste des normes
Calcul de cryptogrammes d'authentification	MAC RETAIL	112 bits	ISO 9797-1 – Algo n°3
Calcul de MAC	MAC RETAIL	112 bits	ISO 9797-1 – Algo n°3
Chiffrement/déchiffrement	TDES	112 bits	ISO 10116 / X9.52-1998
Calcul de cryptogrammes d'authentification carte	RSA	De 1024 à 2048 bits	ISO9796-2 couplé avec CVC
Calcul de cryptogrammes d'authentification SSL	RSA	De 1024 à 2048 bits	Signature PKCS#1 V2.1 – padding v 1.5
Déchiffrement asymétrique	RSA	De 1024 à 2048 bits	Chiffrement PKCS#1 V2.1 – padding v 1.5
Vérification de la correspondance SCD/SVD	Calcul de clé RSA	De 1024 à 2048 bits	Signature PKCS#1 V2.1 – padding v 1.5
Création de signature électronique	RSA	De 1024 à 2048 bits	Signature PKCS#1 V2.1 – padding v 1.5
Calcul de HASH	DTBS-Hash	N/A	SHA-1 et SHA-2 **[R10 – AREAK1]**, **[R11 – AREAK2]**, **[R13 – ERRATUM]**
Echange de clé DH	DH	De 1024 à 2048 bits	**[R10 – AREAK1]**, **[R11 – AREAK2]**

Tableau 12 : Opérations cryptographiques

5.2.3 Protection de données utilisateur (FDP)

FDP_ACC.1 Contrôle d'accès partiel

Itération SSCD

FDP_ACC.1.1 /SFP Initialisation Les TSF doivent appliquer la **[SFP d'initialisation]** lors de **[la génération de paire SCD/SVD]** par l'Utilisateur.

Itération SSCD

FDP_ACC.1.1 /SFP Personnalisation Les TSF doivent appliquer la **[SFP de personnalisation]** lors de **[la création des RAD]** par l'Administrateur.

Itération SSCD

FDP_ACC.1.1 /SFP Transfert de SVD Les TSF doivent appliquer la **[SFP Transfert des SVD]** lors de **[l'importation ou l'exportation des SVD]** par l'Utilisateur.

	Itération SSCD
FDP_ACC.1.1 /SFP de création de signature	Les TSF doivent appliquer la **[SFP de création de signature]** lors de : 1. **[l'envoi de représentation des DTBS par la SCA]**, 2. **[la signature de la représentation des DTBS par le Signataire]**.
	Itération SSCD
FDP_ACC.1.1 /SFP Importation de SCD	La TSF doit appliquer la **[SFP Importation de SCD]** lors de **[l'importation de SCD par l'utilisateur]**.

FDP_ACC.2 Contrôle d'accès complet

	Itération
FDP_ACC.2.1 /APPLI	La TSF doit appliquer la **[affectation : SFP de contrôle d'accès aux services « IAS-eGOV »]** aux **[affectation : liste des sujets et objets]** et à toutes les opérations sur les sujets et objets couverts par la SFP.
Affectation	**Liste des sujets :** - SUB_GEST, SUB_APPLI, SUB_AIP ; **Liste des objets :** - SUB_APPLI, SUB_AIP ; **Contrôle d'accès aux services « IAS-eGOV » :** - SUB_AIP n'est pas sélectionnable ; - Seul SUB_GEST active SUB_APPLI si la commande « SELECT » porte sur l'application IAS-eGOV ; - SUB_GEST interdit l'appel à un service d'un sujet par un autre sujet si cet appel n'est pas valide ; - SUB_APPLI traite une commande si le format de la commande est valide ;
FDP_ACC.2.2 /APPLI	La TSF doit garantir que toutes les opérations entre chaque sujet du TSC et chaque objet du TSC, sont couvertes par une SFP de contrôle d'accès.
	Itération
FDP_ACC.2.1 /FILE	La TSF doit appliquer la **[affectation : SFP de contrôle d'accès aux fichiers]** aux **[affectation : liste des sujets et objets]** et à toutes les opérations sur les sujets et objets couverts par la SFP.
Affectation	**Liste des sujets :** - SUB_APPLI, SUB_GF ; **Liste des objets :** - SUB_GF, OB_DFILE, OB_EFILE ; **Contrôle d'accès aux fichiers :** - SUB_APPLI accède aux objets OB_DFILE et OB_EFILE uniquement si une application est sélectionnée et si ces objets sont accessibles par l'application sélectionnée ; - SUB_APPLI accède aux objets OB_DFILE et OB_EFILE uniquement par l'intermédiaire de SUB_GF ; - SUB_GF crée pour le compte de SUB_APPLI un OB_DFILE ou un OB_EFILE dans l'OB_DFILE courant uniquement si l'état de l'OB_DFILE courant est cohérent avec l'opération et si les conditions d'accès de cet OB_DFILE pour la création sont vérifiées ; - SUB_GF ne crée jamais en phase utilisateur et pour le compte de SUB_APPLI un OB_DFILE ou un OB_EFILE dans un OB_DFILE si cet OB_DFILE n'est pas sous l'ADF courant et n'est pas sous le DF courant ;

- SUB_GF ne crée jamais en phase utilisateur et pour le compte de SUB_APPLI un OB_DFILE de type ADF ;
- SUB_GF supprime pour le compte de SUB_APPLI un OB_DFILE ou un OB_EFILE courant uniquement si l'état du fichier est cohérent avec l'opération et si les conditions d'accès pour la suppression de cet objet sont vérifiées ;
- SUB_GF ne supprime jamais en phase utilisateur et pour le compte de SUB_APPLI un OB_DFILE si cet OB_DFILE contient un OB_DFILE ou un OB_EFILE ou si l'OB_DFILE à supprimer est le MF ou un ADF ;
- SUB_GF accède pour les opérations de lecture/écriture pour le compte de SUB_APPLI aux données stockées dans un OB_EFILE uniquement si l'objet OB_EFILE est intègre, si son état est cohérent avec l'opération et si les conditions d'accès en écriture/lecture sur cet OB_EFILE sont vérifiées ;
- SUB_GF accède pour les opérations d'activation, désactivation ou terminaison d'un objet OB_DFILE ou OB_EFILE si l'état de l'objet accédé est cohérent avec l'opération et si les conditions d'accès en activation, désactivation ou terminaison sur cet objet sont vérifiées ;

FDP_ACC.2.2 /FILE La TSF doit garantir que toutes les opérations entre chaque sujet du TSC et chaque objet du TSC, sont couvertes par une SFP de contrôle d'accès.

Itération

FDP_ACC.2.1 /TLV La TSF doit appliquer la **[affectation : SFP de contrôle d'accès aux paramètres TLV]** aux **[affectation : liste des sujets et objets]** et à toutes les opérations sur les sujets et objets couverts par la SFP.

Affectation

Liste des sujets :

- SUB_APPLI, SUB_GT ;

Liste des objets :

- SUB_GT, OB_DFILE, OB_TLV ;

Contrôle d'accès aux paramètres TLV :

- SUB_APPLI accèdent aux objets OB_TLV uniquement par l'intermédiaire de SUB_GT ;
- SUB_GT crée pour le compte de SUB_APPLI un OB_TLV dans l'OB_DFILE courant uniquement si l'état de l'OB_DFILE courant est cohérent avec l'opération et si les conditions d'accès de cet OB_DFILE pour la création sont vérifiées ;
- SUB_GT accède en lecture / écriture aux paramètres stockés dans un OB_TLV, pour le compte de SUB_APPLI, uniquement si les conditions d'accès pour l'opération de lecture/écriture sur cet OB_TLV sont vérifiées ;

FDP_ACC.2.2 /TLV La TSF doit garantir que toutes les opérations entre chaque sujet du TSC et chaque objet du TSC, sont couvertes par une SFP de contrôle d'accès.

Itération

FDP_ACC.2.1 /SEC La TSF doit appliquer la **[affectation : SFP de contrôle d'accès aux secrets]** aux **[affectation : liste des sujets et objets]** et à toutes les opérations sur les sujets et objets couverts par la SFP.

Affectation

Liste des sujets :

- SUB_APPLI, SUB_CRYPTO, SUB_GS ;

Liste des objets :

- SUB_GS, OB_FILE, OB_SECRET, SUB_CRYPTO ;

Contrôle d'accès aux secrets :

- Seul SUB_CRYPTO et SUB_APPLI accèdent aux objets OB_SECRET et uniquement par l'intermédiaire de SUB_GS ;

- SUB_GS n'accède jamais en lecture aux valeurs de clés symétriques ou de clés privées de bi-clés asymétrique ou d'un code PIN, contenus dans OB_SECRET pour le compte de SUB_APPLI ;
- SUB_GS crée pour le compte de SUB_APPLI un OB_SECRET dans le répertoire OB_DFILE courant si les conditions d'accès et l'état de cet OB_DFILE pour la création sont vérifiées ;
- SUB_GS accède en écriture aux OB_SECRET pour le compte de SUB_APPLI ou SUB_CRYPTO si l'OB_SECRET est dans l'état Créé ou Activé et si les conditions d'accès et l'état de l'objet OB_SECRET pour une opération d'écriture sont vérifiées ;
- SUB_GS accède pour le compte de SUB_APPLI, pour les opérations d'activation, désactivation ou terminaison d'un objet OB_SECRET si l'état du secret est cohérent avec l'opération et si les conditions d'accès pour l'opération sur cet objet sont vérifiées ;
- SUB_GS accède pour le compte de SUB_APPLI, pour l'opération de déblocage d'un objet OB_SECRET si l'état du secret est cohérent avec l'opération et si les conditions d'accès pour l'opération sur le ou les compteurs de ce secret, sont vérifiées ;
- SUB_GS transfert dans les blocs de traitements cryptographiques les OB_SECRET pour le compte de SUB_CRYPTO si les conditions d'accès pour l'utilisation du secret sont vérifiées et si OB_SECRET est intègre et n'est pas bloqué ;
- SUB_CRYPTO réalise pour le compte de SUB_APPLI une opération cryptographique avec les OB_SECRET transférés dans les blocs de traitements cryptographiques ;
- SUB_APPLI accède à SUB_CRYPTO pour des opérations cryptographique avec des OB_SECRET si la clé et l'algorithme utilisés sont cohérents pour opération cryptographique ;

FDP_ACC.2.2 /SEC La TSF doit garantir que toutes les opérations entre chaque sujet du TSC et chaque objet du TSC, sont couvertes par une SFP de contrôle d'accès.

Itération SSCD

FDP_ACC.2.1 La TSF doit appliquer la **[affectation : SFP de contrôle d'accès aux secrets de « signature électronique sécurisée »]** aux **[affectation : liste des sujets et objets]** et à toutes les opérations sur les sujets et objets couverts par la SFP.

Affectation

Liste des sujets :

- Signataire ;
- Administrateur ;

Liste des objets :

- SCD ;
- SVD ;
- DTBS ;

Contrôle d'accès aux secrets de « signature électronique sécurisée » :

- Les objets SCD/SVD sont accessibles en écriture pour génération d'une paire SCD/SVD uniquement si l'utilisateur est le signataire ou le l'administrateur et si l'utilisateur a les droits de gestion des objets SCD/SVD ;
- Les objets SCD/SVD sont accessibles en écriture pour une destruction d'une paire SCD/SVD uniquement si l'utilisateur est le signataire ou l'administrateur ;
- Les objets SCD ne sont jamais accessibles en lecture pour une exportation ;
- Les objets SVD sont accessibles en lecture pour une exportation d'une SVD uniquement si l'utilisateur est l'administrateur ou le signataire ;
- Les objets SCD sont accessibles en utilisation pour une création de signature sur des objets DTBS uniquement si l'utilisateur est le signataire utilisant une SCD « opérationnelle » pour signer des DTBS ;

- Les objets DTBS sont accessibles en écriture pour chargement d'une « représentation de DTBS » uniquement si la CSA est autorisée ;
- Les objets DTBS ne sont pas accessibles en lecture pour la création de signature avec une SCD opérationnelle si l'objet DTBS n'a pas était envoyé par une CSA autorisée ;

FDP_ACC.2.2 La TSF doit garantir que toutes les opérations entre chaque sujet du TSC et chaque objet du TSC, sont couvertes par une SFP de contrôle d'accès.

FDP_ACF.1 Contrôle d'accès basé sur les attributs de sécurité

Itération

FDP_ACF.1.1 /APPLI La TSF doit appliquer la **[affectation : SFP de contrôle d'accès aux services « IAS-eGOV »]** aux objets en se basant sur **[affectation : la liste des attributs de sécurité]**.

FDP_ACF.1.2 /APPLI La TSF doit appliquer les règles suivantes pour déterminer si une opération entre des sujets contrôlés et des objets contrôlés est autorisée.

Affectation **Règles :**

1. SUB_GEST active SUB_APPLI sur réception d'une commande « SELECT » si :
   - L'**entête de commande** est en cohérente avec le statut de la **phase de vie carte** ;
   - L'**entête de commande** est valide et correspond à une commande « SELECT » de l'application IAS-eGOV ;
   - Le **checksum du répertoire/fichier** de SUB_APPLI est correct ;
2. SUB_GEST interdit l'appel à un service si :
   - Le sujet appelé et le sujet appelant ne sont pas cohérents avec la **table des services** ;
3. SUB_APPLI traite la commande reçue si :
   - L'**entête de commande** est cohérente avec le statut de la **phase de vie carte** et l'**état fichier** de l'ADF sélectionné ;
   - L'**entête de commande** est cohérente avec le **statut de l'application** de SUB_APPLI ;

Liste des attributs de sécurité :

- Entête de commande ;
- Table des services ;
- Phase de vie carte ;
- Statut de l'application ;
- Checksum fichier/répertoire ;
- Etat fichier ;

FDP_ACF.1.3 /APPLI La TSF doit autoriser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : **[affectation : sans objet]**.

FDP_ACF.1.4 /APPLI La TSF doit refuser explicitement l'accès de sujets à des objets en fonction de **[affectation : Règles spécifiques]**.

Affectation **Règles spécifiques :**

1. SUB_GEST n'active pas SUB_AIP si :
   - **Phase de vie carte** est : USER, BLOQUE ou FIN DE VIE ;

Itération

FDP_ACF.1.1 /FILE La TSF doit appliquer la **[affectation : SFP de contrôle d'accès aux fichiers]** aux objets en se basant sur **[affectation : la liste des attributs de sécurité]**.

FDP_ACF.1.2 /FILE La TSF doit appliquer les règles suivantes pour déterminer si une opération entre des sujets contrôlés et des objets contrôlés est autorisée.

Affectation **Règles :**

1. SUB_APPLI active SUB_GF pour réaliser les opérations de création / suppression / lecture / écriture / activation / désactivation / terminaison sur un OB_DFILE /

OB_EFILE si **l'entête de commande** et le **type de l'objet** sont cohérents ;

2. SUB_GF réalise l'opération de création d'un fichier OB_DFILE / OB_EFILE dans un OB_DFILE courant si :
   - Le **type de l'objet** du fichier créé est DF ou EF ;
   - L'**état fichier** du fichier courant est cohérent avec l'opération ;
   - Le **DAC** est cohérent avec l'**état de sécurité carte** ;
3. SUB_GF réalise les opérations de suppression d'un fichier OB_DFILE / OB_EFILE courant si :
   - Le **type de l'objet** du fichier supprimé différent de MF ;
   - L'**état fichier** du fichier courant à supprimer est cohérent avec l'opération ;
   - Le **DAC** est cohérent avec l'**état de sécurité carte** ;
   - Pour un OB_DFILE, il ne contient aucun objet ou des objets de type SECRET ou TLV (ces derniers sont alors détruits) ;
4. SUB_GF réalise les opérations de lecture / écriture dans un fichier OB_DFILE / OB_EFILE courant si :
   - Le **checksum répertoire/fichier** du fichier accédé est correct ;
   - L'**état fichier** du fichier accédé est cohérent avec l'opération ;
   - Le **DAC** est cohérent avec l'**état de sécurité carte** ;
5. SUB_GF réalise les opérations d'activation / désactivation et terminaison d'un OB_DFILE / OB_EFILE courant si :
   - Le **type de l'objet** du fichier supprimé différent de MF ;
   - L'**état fichier** du fichier accédé est cohérent avec l'opération ;
   - Le **DAC** est cohérent avec l'**état de sécurité carte** ;

Liste des attributs de sécurité :

- Entête de commande ;
- Type de l'objet ;
- Checksum répertoire/fichier ;
- DAC ;
- Etat de sécurité carte ;
- Etat fichier ;

FDP_ACF.1.3 /FILE La TSF doit autoriser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : **[affectation : sans objet]**.

FDP_ACF.1.4 /FILE La TSF doit refuser explicitement l'accès de sujets à des objets en fonction de **[affectation : Règles spécifiques]**.

Affectation **Règles spécifiques :**

1. SUB_GF n'accède jamais en création / écriture / lecture / activation / désactivation / terminaison si le **type de l'objet** de l'OB_FILE accédé est SECRET ou TLV ;
2. SUB_GF n'accède jamais en phase utilisateur en création d'un OB_DFILE / OB_EFILE dans un OB_DFILE courant si :
   - La **phase de vie carte** est : BLOQUE et FIN DE VIE ;
   - L'**état de sécurité carte** n'indique pas qu'un SMI est valide ;
   - Le fichier créé est de **type** MF ou ADF ;
   - L'**état fichier** de l'OB_DFILE courant est Désactivé ou Terminé ;
3. SUB_GF n'accède jamais en suppression d'un OB_DFILE / OB_EFILE dans un OB_DFILE courant si :
   - La **phase de vie carte** est : BLOQUE et FIN DE VIE ;
   - L'objet supprimé est de **type** MF, ADF ;
4. SUB_GF n'accède jamais en activation d'un OB_DFILE / OB_EFILE courant si :
   - L'**état fichier** du fichier courant est Terminé ;
5. SUB_GF n'accède jamais en désactivation d'un OB_DFILE/OB_EFILE courant si :
   - L'**état fichier** du fichier courant est Terminé ;
   - Le fichier courant est de **type** MF ;
6. SUB_GF n'accède jamais en terminaison d'un OB_DFILE / OB_EFILE si :
   - Le fichier est **type** de MF ;
   - Le fichier n'est pas le fichier courant ;

Itération

FDP_ACF.1.1 /TLV La TSF doit appliquer la **[affectation : SFP de contrôle d'accès aux paramètres TLV]** aux objets en se basant sur **[affectation : la liste des attributs de sécurité]**.

FDP_ACF.1.2 /TLV La TSF doit appliquer les règles suivantes pour déterminer si une opération entre des sujets contrôlés et des objets contrôlés est autorisée.

Affectation **Règles :**

1. SUB_APPLI active SUB_GT pour réaliser les opérations de création / lecture / écriture dans un OB_TLV si **l'entête de commande** et le **type de l'objet** sont cohérents ;
2. SUB_GT réalise la création d'un OB_TLV dans un OB_DFILE courant si :
   - L'**état fichier** du OB_DFILE courant est cohérent l'opération ;
   - Le **DAC** est cohérent avec l'**état de sécurité carte** ;
3. SUB_GT réalise les opérations de lecture / écriture dans un OB_TLV si :
   - Le **checksum TLV** de OB_TLV est correct ;
   - Le **DAC** est cohérent avec l'**état de sécurité carte** ;

Liste des attributs de sécurité :

- Entête de commande ;
- Type de l'objet ;
- Checksum TLV ;
- DAC ;
- Etat de sécurité carte ;
- Etat fichier ;

FDP_ACF.1.3 /TLV La TSF doit autoriser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : **[affectation : sans objet]**.

FDP_ACF.1.4 /TLV La TSF doit refuser explicitement l'accès de sujets à des objets en fonction de **[affectation :Règles spécifiques]**.

Affectation **Règles spécifiques :**

1. SUB_GT n'accède jamais en suppression à un OB_TLV ;

Itération

FDP_ACF.1.1 /SEC La TSF doit appliquer la **[affectation : SFP de contrôle d'accès aux secrets]** aux objets en se basant sur **[affectation : la liste des attributs de sécurité]**.

FDP_ACF.1.2 /SEC La TSF doit appliquer les règles suivantes pour déterminer si une opération entre des sujets contrôlés et des objets contrôlés est autorisée.

Affectation **Règles :**

1. SUB_APPLI active SUB_GS pour accéder aux OB_SECRET si **l'entête de commande** et le **type de l'objet** sont cohérents ;
2. SUB_GS réalise l'opération de création d'un OB_SECRET dans un OB_DFILE courant si :
   - L'**état fichier** de l'OB_DFILE courant est cohérent pour l'opération ;
   - Le **DAC** est cohérent avec l'**état de sécurité carte** ;
3. SUB_GS accède à OB_SECRET en écriture / lecture / déblocage / activation / désactivation / terminaison si :
   - L'**état secret** de l'OB_SECRET est cohérent avec l'opération ;
   - Le **groupe de ratification** ou le **compteur d'utilisation** ou le **compteur d'erreur** de l'OB_SECRET n'indiquent pas un « blocage » du secret pour les opérations de lecture / écriture / activation / désactivation / terminaison ;
   - Le **DAC** du secret est en concordance avec l'**état de sécurité carte** pour l'opération ;
4. SUB_GS réalise les opérations d'activation / désactivation et terminaison d'un OB_SECRET si :

- L'**état du secret** est cohérent avec l'opération ;
- Le **DAC** du secret est cohérent avec l'**état de sécurité carte** ;

5. SUB_GS accède au transfert d'un OB_SECRET dans les blocs de traitements cryptographiques pour le compte de SUB_CRYPTO si :
   - Le **type de clé** et le **type d'algorithme** sont cohérents ;
   - Le **groupe de ratification** ou le **compteur d'utilisation** ou le **compteur d'erreur** n'indiquent pas un « blocage » du secret ;
   - Le **checksum répertoire/fichier** contenant OB_SECRET est correct ;
   - L'**Etat secret** du secret OB_SECRET est à « activé » ;
   - Le **DAC** du secret OB_SECRET est en concordance avec l'**état de sécurité carte** ;

Liste des attributs de sécurité :

- Type de clé ;
- Type d'algorithme ;
- Groupe de ratification ;
- Checksum répertoire/fichier ;
- DAC ;
- Etat de sécurité carte ;
- Etat secret ;
- Etat fichier ;

FDP_ACF.1.3 /SEC La TSF doit autoriser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : **[affectation : sans objet]**.

FDP_ACF.1.4 /SEC La TSF doit refuser explicitement l'accès de sujets à des objets en fonction de **[affectation : Règles spécifiques]**.

Affectation **Règles spécifiques :**

1. SUB_GS n'accède jamais en lecture pour le compte de SUB_APPLI, aux valeurs de clés symétriques ou de clés privées de bi-clés asymétrique ou d'un code PIN, contenus dans OB_SECRET ;
2. SUB_GS n'accède jamais en écriture à un OB_SECRET pour le compte de SUB_APPLI, si l'**état de sécurité carte** n'indique pas qu'un SMI et un SMC sont valides ;
3. SUB_GS ne supprime jamais un OB_SECRET ;

Itération SSCD

FDP_ACF.1.1 /SFP Initialisation La TSF doit appliquer la **[affectation : SFP d'initialisation]** aux objets en se basant sur **[affectation : Le groupe d'attributs généraux]** et **[affectation : Le groupe d'attributs d'initialisation]**.

FDP_ACF.1.2 /SFP Initialisation La TSF doit appliquer les règles suivantes pour déterminer si une opération entre des sujets contrôlés et des objets contrôlés est autorisée.

Affectation **Règles :**

1. L'utilisateur dont l'attribut de sécurité **rôle** est défini à Administrateur ou à Signataire et dont l'attribut de sécurité **gestion des SCD/SVD** est défini à Autorisé peut générer une paire SCD/SVD.

FDP_ACF.1.3 /SFP Initialisation La TSF doit autoriser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : **[affectation : sans objet]**.

FDP_ACF.1.4 /SFP Initialisation La TSF doit refuser explicitement l'accès de sujets à des objets en fonction de **[affectation : Règles spécifiques]**.

Affectation **Règles spécifiques :**

1. L'utilisateur dont l'attribut de sécurité **rôle** est défini à Administrateur ou à Signataire et dont l'attribut de sécurité **gestion des SCD/SVD** est défini à Non-autorisé ne peut pas générer une paire SCD/SVD.

Itération SSCD

FDP_ACF.1.1 /SFP Personnalisation La TSF doit appliquer la **[affectation : SFP de personnalisation]** aux objets en se basant sur **[affectation : Le groupe d'attributs généraux]**.

FDP_ACF.1.2 /SFP Personnalisation La TSF doit appliquer les règles suivantes pour déterminer si une opération entre des sujets contrôlés et des objets contrôlés est autorisée.

Affectation **Règles :**

1. L'utilisateur dont l'attribut de sécurité **rôle** est défini à Administrateur est autorisé à créer un RAD.

FDP_ACF.1.3 /SFP Personnalisation La TSF doit autoriser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : **[affectation : sans objet]**.

FDP_ACF.1.4 /SFP Personnalisation La TSF doit refuser explicitement l'accès de sujets à des objets en fonction de **[affectation : sans objet]**.

Itération SSCD

FDP_ACF.1.1 /SFP Transfert de SVD La TSF doit appliquer la **[affectation : SFP Transfert des SVD]** aux objets en se basant sur **[affectation : Le groupe d'attributs généraux]**.

FDP_ACF.1.2 /SFP Transfert de SVD La TSF doit appliquer les règles suivantes pour déterminer si une opération entre des sujets contrôlés et des objets contrôlés est autorisée.

Affectation **Règles :**

1. L'utilisateur dont l'attribut de sécurité **rôle** est défini à Administrateur ou à Signataire est autorisé à exporter des SVD.

FDP_ACF.1.3 /SFP Transfert de SVD La TSF doit autoriser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : **[affectation : sans objet]**.

FDP_ACF.1.4 /SFP Transfert de SVD La TSF doit refuser explicitement l'accès de sujets à des objets en fonction de **[affectation : sans objet]**.

Itération SSCD

FDP_ACF.1.1 /SFP de création de signature La TSF doit appliquer la **[affectation : SFP de création de signature]** aux objets en se basant sur **[affectation : Le groupe d'attributs généraux]** et **[affectation : Le groupe d'attributs de création de signature]**.

FDP_ACF.1.2 /SFP de création de signature La TSF doit appliquer les règles suivantes pour déterminer si une opération entre des sujets contrôlés et des objets contrôlés est autorisée.

Affectation **Règles :**

1. L'utilisateur dont l'attribut de sécurité **rôle** est défini à Signataire est autorisé à créer des signatures électroniques pour les DTBS envoyées par une SCA autorisée, avec des SCD par le Signataire dont l'attribut de sécurité **SCD opérationnelles** est défini à Oui.

FDP_ACF.1.3 /SFP de création de signature La TSF doit autoriser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : **[affectation : sans objet]**.

FDP_ACF.1.4 /SFP de création de signature La TSF doit refuser explicitement l'accès de sujets à des objets en fonction de **[affectation : Règles spécifiques]**.

Affectation **Règles spécifiques :**

(a) L'utilisateur dont l'attribut de sécurité **rôle** est défini à Signataire n'est pas autorisé à créer des signatures électroniques pour les DTBS qui ne sont pas envoyées par une SCA autorisée, avec des SCD du Signataire dont l'attribut de sécurité **SCD opérationnelles** est défini à Oui.

(b) L'utilisateur dont l'attribut de sécurité **rôle** est défini à Signataire n'est pas autorisé à créer des signatures électroniques pour les DTBS envoyées par une SCA autorisée, avec des SCD du Signataire dont l'attribut de sécurité SCD opérationnelles est défini à Non.

Itération SSCD

FDP_ACF.1.1 /SFP Importation de SCD La TSF doit appliquer la **[affectation : SFP Importation de SCD]** aux objets en se basant sur **[affectation : Le groupe d'attributs généraux]** et **[affectation : Le groupe d'attributs d'initialisation]**.

FDP_ACF.1.2 /SFP Importation de SCD La TSF doit appliquer les règles suivantes pour déterminer si une opération entre des sujets contrôlés et des objets contrôlés est autorisée.

Affectation **Règles :**

1. L'utilisateur dont l'attribut de sécurité **rôle** est défini à Administrateur ou Signataire et avec l'attribut de sécurité **Gestion des SCD/SVD** positionné à Autorisé est autorisé à importer des SCD si l'attribut de sécurité **Importation sécurisée de SCD autorisée** est positionné à Oui.

FDP_ACF.1.3 /SFP Importation de SCD La TSF doit autoriser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : **[affectation : sans objet]**.

FDP_ACF.1.4 /SFP Importation de SCD La TSF doit refuser explicitement l'accès de sujets à des objets en fonction de **[affectation : Règles spécifiques]**.

Affectation **Règles spécifiques :**

(a) L'utilisateur dont l'attribut de sécurité **rôle** est défini à Administrateur ou Signataire et avec l'attribut de sécurité **Gestion des SCD/SVD** positionné à Non autorisé n'est pas autorisé à importer des SCD si l'attribut de sécurité **Importation sécurisée de SCD autorisée** est positionné à Oui.

(b) L'utilisateur dont l'attribut de sécurité **rôle** est défini à Administrateur ou Signataire et avec l'attribut de sécurité **Gestion des SCD/SVD** positionné à Autorisé n'est pas autorisé à importer des SCD si l'attribut de sécurité **Importation sécurisée de SCD autorisée** est positionné à Non.

FDP_DAU.1 Authentification des données élémentaires

Itération

FDP_DAU.1.1 La TSF doit offrir une capacité de générer une preuve pouvant être utilisée comme garantie de la validité des **[affectation : Liste des objets ou types d'informations suivants]**

Affectation **Liste des objets et des informations :**

- OB_SECRET (clés et codes PIN) ;
- OB_FILE (contenu de fichier) ;
- OB_TLV (des données propriétaires application) ;

FDP_DAU.1.2 La TSF doit offrir à **[affectation : liste des sujets]** l'aptitude de vérifier la preuve de la validité des informations indiquées.

Affectation **Liste des sujets :**

- SUB_APPLI ;
- SUB_GS ;
- SUB_GT ;
- SUB_GF ;

Itération SSCD

FDP_DAU.1.1 La TSF doit offrir une capacité de générer une preuve pouvant être utilisée comme garantie de la validité des **[affectation : Liste des objets ou types d'informations suivants]**

Affectation **Liste des objets et des informations :**

- SCD
- SVD ;
- RAD ;
- DTBS ;

FDP_DAU.1.2 La TSF doit offrir à **[affectation : liste des sujets]** l'aptitude de vérifier la preuve de la validité des informations indiquées.

Affectation **Liste des sujets :**

- Signataire ;
- Administrateur ;

FDP_ETC.1 Exportation de données de l'utilisateur sans attributs de sécurité

Itération

FDP_ETC.1.1 La TSF doit appliquer les **[affectation : liste des SFP de contrôle d'accès]** lors de l'exportation de données de l'utilisateur, contrôlées par la ou les SFP, vers l'extérieur du TSC.

Affectation **Liste des SFP de contrôle d'accès :**

- SFP de contrôle d'accès aux services « IAS-eGOV » ;
- SFP de contrôle d'accès aux fichiers ;
- SFP de contrôle d'accès aux paramètres TLV ;
- SFP de contrôle d'accès aux secrets ;

FDP_ETC.1.2 La TSF doit exporter les données de l'utilisateur sans les attributs de sécurité associés aux données de l'utilisateur.

Itération SSCD

FDP_ETC.1.1 /Transfer de SVD La TSF doit appliquer les **[affectation : SFP Transfert des SVD]** lors de l'exportation de données de l'utilisateur, contrôlées par la ou les SFP, vers l'extérieur du TSC.

FDP_ETC.1.2 /Transfer de SVD La TSF doit exporter les données de l'utilisateur sans les attributs de sécurité associés aux données de l'utilisateur.

FDP_ITC.1 Importation de données de l'utilisateur sans attributs de sécurité

Itération

FDP_ITC.1.1 La TSF doit appliquer la **[affectation : liste des SFP de contrôle d'accès]** lors de l'importation de données de l'utilisateur contrôlées par la SFP en provenance de l'extérieur du TSC.

Affectation **Liste des SFP de contrôle d'accès :**

- SFP de contrôle d'accès aux services « IAS-eGOV » ;
- SFP de contrôle d'accès aux fichiers ;
- SFP de contrôle d'accès aux paramètres TLV ;
- SFP de contrôle d'accès aux secrets ;

FDP_ITC.1.2 La TSF doit ignorer tout attribut de sécurité associé aux données de l'utilisateur lorsqu'elles sont importées depuis l'extérieur du TSC.

FDP_ITC.1.3 La TSF doit appliquer les règles suivantes lors de l'importation de données de l'utilisateur contrôlées par la SFP en provenance de l'extérieur du TSC **[règles complémentaires de contrôle d'importation : sans objet].**

Itération SSCD

FDP_ITC.1.1 /SCD La TSF doit appliquer la **[affectation : SFP Importation de SCD]** lors de l'importation de données de l'utilisateur contrôlées par la SFP en provenance de l'extérieur du TSC.

FDP_ITC.1.2 /SCD La TSF doit ignorer tout attribut de sécurité associé aux données de l'utilisateur lorsqu'elles sont importées depuis l'extérieur du TSC.

FDP_ITC.1.3 /SCD La TSF doit appliquer les règles suivantes lors de l'importation de données de l'utilisateur contrôlées par la SFP en provenance de l'extérieur du TSC : **[La SCD doit être envoyée par un SSCD autorisé].**

Itération SSCD

FDP_ITC.1.1 /DTBS La TSF doit appliquer la **[affectation : SFP de création de signature]** lors de l'importation de données de l'utilisateur contrôlées par la SFP en provenance de l'extérieur du TSC.

FDP_ITC.1.2 /DTBS La TSF doit ignorer tout attribut de sécurité associé aux données de l'utilisateur lorsqu'elles sont importées depuis l'extérieur du TSC.

FDP_ITC.1.3 /DTBS La TSF doit appliquer les règles suivantes lors de l'importation de données de l'utilisateur contrôlées par la SFP en provenance de l'extérieur du TSC : **[La représentation des DTBS doit être envoyée par une CSA autorisée].**

FDP_RIP.1 Protection partielle des informations résiduelles

Itération

FDP_RIP.1.1 La TSF doit garantir que toute information contenue précédemment dans une ressource est rendue inaccessible lors de la **[sélection : désallocation de la ressource]** pour les objets suivants **[affectation :Liste des objets]**

Affectation **Liste des objets :**

- OB_SECRET ;
- OB_FILE ;
- OB_TLV ;
- OB_I/O ;
- OB_TEMP ;

Itération SSCD

FDP_RIP.1.1 La TSF doit garantir que toute information contenue précédemment dans une ressource est rendue inaccessible lors de la **[sélection : désallocation de la ressource]** pour les objets suivants **[affectation :Liste des objets]**

Affectation **Liste des objets :**

- SCD ;
- VAD ;
- RAD ;

FDP_SDI.2 Contrôle de l'intégrité des données stockées et action à entreprendre

Itération

FDP_SDI.2.1 La TSF doit contrôler les données de l'utilisateur stockées au sein du TSC à la recherche **[affectation : d'erreurs d'intégrité sur checksum]** sur tous les objets, en en se basant sur les attributs suivants **[affectation : Liste des attributs]**

Affectation **Liste des attributs**

- Checksum des répertoires et des fichiers ;
- Checksum secret ;
- Checksum TLV ;
- Checksum des buffers I/O avant et après une opération de SUB_CRYPTO ;

FDP_SDI.2.2 En cas de détection d'une erreur d'intégrité, la TSF doit **[affectation : refuser l'utilisation des données corrompues]**.

Itération SSCD

FDP_SDI.2.1 /Données persistantes La TSF doit contrôler les données de l'utilisateur stockées au sein du TSC à la recherche **[affectation : d'erreurs d'intégrité]** sur tous les objets, en en se basant sur les attributs suivants **[affectation : données stockées de manière permanente avec vérification d'intégrité]**

Raffinement **Données persistantes[3] :**

- SCD ;
- RAD ;
- SVD (si stocké de manière permanente dans la TOE) ;

FDP_SDI.2.2 /Données persistantes En cas de détection d'une erreur d'intégrité, la TSF doit :

1. **[refuser l'utilisation des données corrompues**
2. **informer le Signataire de l'erreur d'intégrité]**

Itération

FDP_SDI.2.1 /DTBS La TSF doit contrôler les données de l'utilisateur stockées au sein du TSC à la recherche **[affectation : d'erreurs d'intégrité]** sur tous les objets, en en se basant sur les attributs suivants **[affectation : données stockées avec vérification d'intégrité]**

Raffinement **Données temporaires[4] :**

- La représentation des DTBS ;

FDP_SDI.2.2 /DTBS En cas de détection d'une erreur d'intégrité, la TSF doit :

1. **[refuser l'utilisation des données corrompues**
2. **informer le Signataire de l'erreur d'intégrité]**

FDP_UCT.1 Confidentialité élémentaire des données échangées

FDP_UCT.1.1 /Réception La TSF doit appliquer la **[SFP Importation de SCD]** pour pouvoir **[recevoir]** les objets de manière à les protéger de toute divulgation non autorisée.

[3] Les données stockées de manière permanente par la TOE ont pour attribut de données utilisateur « données stockées de manière permanente avec vérification d'intégrité »

[4] La représentation des DTBS, temporairement stockée par la TOE a pour attribut de données utilisateur « données stockées avec vérification d'intégrité »

FDP_UIT.1 Intégrité de l'échange de données

	Itération SSCD
FDP_UIT.1.1 /Transfert de SVD	La TSF doit appliquer la **[SFP Transfert des SVD]** pour pouvoir **[transmettre]** les données de l'utilisateur de façon à éviter les erreurs **[de modification]** et **[d'insertion]**.
FDP_UIT.1.2 /Transfert de SVD	La TSF doit pouvoir déterminer lors de la réception des données de l'utilisateur si une **[modification]** ou une **[insertion]** a eu lieu.
	Itération SSCD
FDP_UIT.1.1 /TOE DTBS	La TSF doit appliquer la **[SFP de création de signature]** pour pouvoir **[recevoir]** les données de l'utilisateur de façon à éviter les erreurs **[de modification]**, **[de suppression]** et **[d'insertion]**.
FDP_UIT.1.2 /TOE DTBS	La TSF doit pouvoir déterminer lors de la réception des données de l'utilisateur si une **[modification]**, une **[suppression]** ou une **[insertion]** a eu lieu.

5.2.4 Identification et authentification (FIA)

FIA_AFL.1 Gestion d'un échec de l'authentification

	Itération
FIA_AFL.1.1	La TSF doit détecter le fait que **[affectation : les nombres suivants de]** tentatives d'authentification infructueuses ont eu lieu en relation avec **[affectation : l'authentification des utilisateurs des services de l'application IAS-eGOV en phase utilisateur]**.
Affectation	**Nombres de tentatives :** - 3 tentatives successives d'authentification du porteur ; - 5 tentatives successives d'authentification de l'émetteur ;
FIA_AFL.1.2	Quand le nombre spécifié de tentatives d'authentification infructueuses a été atteint ou dépassé, la TSF doit **[affectation : Liste des actions]**.
Affectation	**Liste des actions :** - Blocage du code PIN ; - Blocage du code PUK ;
	Itération SSCD
FIA_AFL.1.1	La TSF doit détecter le fait que **[affectation : le nombre suivant de]** tentatives d'authentification infructueuses ont eu lieu suite à **[des échecs de tentatives d'authentification consécutives]**.
Affectation	**Nombre de tentatives :** - 5 tentatives successives d'authentification du signataire ;
FIA_AFL.1.2	Quand le nombre spécifié de tentatives d'authentification infructueuses a été atteint ou dépassé, la TSF doit **[affectation : bloquer le RAD]**.
Raffinement	Quand le RAD est bloqué, toute nouvelle tentative d'authentification échoue.

FIA_ATD.1 Définition des attributs de l'utilisateur

	Itération
FIA_ATD.1	La TSF doit maintenir la liste suivante d'attributs de sécurité appartenant à des utilisateurs individuels : **[affectation : Liste des attributs de sécurité]**
Affectation	**Liste des attributs de sécurité :** - Etat fichier ; - Etat secret ; - Etat de sécurité carte ;
	Itération SSCD
FIA_ATD.1	La TSF doit maintenir la liste suivante d'attributs de sécurité appartenant à des utilisateurs

individuels : **[affectation : RAD]**

FIA_UAU.1 Programmation de l'authentification

Itération

FIA_UAU.1.1 La TSF doit autoriser que **[affectation : Toutes les actions transitant par la TSF, excepté celles identifiées ci-dessous,]** soient effectuées pour le compte de l'utilisateur avant qu'il ne soit authentifié.

Affectation **Liste des actions non autorisées avant authentification de l'utilisateur :**

- La création ou la suppression d'un répertoire ou d'un fichier ;
- Gestion du cycle de vie d'un fichier ;
- La génération ou l'ajout d'un secret ;
- Gestion du cycle de vie d'un secret ;
- L'écriture ou la lecture de données confidentielles de l'utilisateur ;

FIA_UAU.1.2 La TSF doit exiger que chaque utilisateur soit authentifié avec succès avant d'autoriser toute autre action transitant par la TSF pour le compte de cet utilisateur.

Itération SSCD

FIA_UAU.1.1 La TSF doit autoriser que **[affectation : Liste des actions]** soient effectuées pour le compte de l'utilisateur avant qu'il ne soit authentifié.

Affectation **Liste des actions :**

1. L'identification de l'utilisateur par des moyens de la TSF requis par FIA_UID.1 ;
2. La création d'un canal de confiance entre la TOE et un SSCD de Type 1 par des moyens de la TSF requis par FTP_ITC/Importation de SCD ;
3. La création d'un chemin de confiance entre l'utilisateur local et la TOE par des moyens de la TSF requis par FTP_TRP.1/TOE ;
4. La création d'un canal de confiance entre la SCA et la TOE par des moyens de la TSF requis par FTP_ITC.1/Importation des DTBS ;

FIA_UAU.1.2 La TSF doit exiger que chaque utilisateur soit authentifié avec succès avant d'autoriser toute autre action transitant par la TSF pour le compte de cet utilisateur.

Note L'« utilisateur local » mentionné dans le composant FIA_UAU.1.1 est l'utilisateur utilisant le canal de confiance fourni entre la SCA dans l'environnement de la TOE et la TOE comme mentionné par FTP_TRP.1/SCA et FTP_TRP.1/TOE.

FIA_UAU.3 Authentification infalsifiable

FIA_UAU.3.1 La TSF doit **[sélection : empêcher]** l'utilisation de données d'authentification qui ont été contrefaites par un utilisateur quelconque de la TSF.

FIA_UAU.3.2 La TSF doit **[sélection : empêcher]** l'utilisation de données d'authentification qui ont été copiées par tout autre utilisateur de la TSF.

FIA_UAU.4 Mécanismes d'authentification à usage unique

Itération

FIA_UAU.4.1 La TSF doit empêcher la réutilisation des données d'authentification liées à **[affectation : la liste des authentifications]**.

Affectation **Liste des authentifications :**

- Authentification de l'émetteur ;
- Authentification des autorités de domaine ;

Itération SSCD

FIA_UAU.4.1 La TSF doit empêcher la réutilisation des données d'authentification liées à **[affectation : la liste des authentifications]**.

Affectation **Liste des authentifications :**

- Authentification du Signataire ;
- Authentification de l'Administrateur ;

FIA_UID.1 Programmation de l'identification

Itération

FIA_UID.1.1 La TSF doit autoriser que **[affectation : Toutes les actions transitant par la TSF,]** soient effectuées pour le compte de l'utilisateur avant qu'il ne soit identifié.

FIA_UID.1.2 La TSF doit exiger que chaque utilisateur soit identifié avec succès avant d'autoriser toute autre action transitant par la TSF pour le compte de cet utilisateur.

Itération SSCD

FIA_UID.1.1 La TSF doit autoriser que **[affectation : Liste des actions]** soient effectuées pour le compte de l'utilisateur avant qu'il ne soit identifié.

Affectation **Liste des actions :**

1. La création d'un canal de confiance entre la TOE et un SSCD Type 1 par des moyens de la TSF requis par FTP_ITC.1/Importation de SCD ;
2. La création d'un chemin de confiance entre l'utilisateur local et la TOE par des moyens de la TSF requis par FTP_TRP.1/TOE ;
3. La création d'un canal de confiance entre la SCA et la TOE par des moyens de la TSF requis par FTP_ITC.1/Importation des DTBS ;

FIA_UID.1.2 La TSF doit exiger que chaque utilisateur soit identifié avec succès avant d'autoriser toute autre action transitant par la TSF pour le compte de cet utilisateur.

FIA_USB.1 Lien utilisateur-sujet

FIA_USB.1.1 La TSF doit relier les attributs de sécurité de l'utilisateur appropriés avec les sujets agissant pour le compte de cet utilisateur.

5.2.5 Gestion de la sécurité (FMT)

Les actions suivantes sont prises en compte pour le management des fonctions dans FMT.

SFR	Action de gestion	SFR	Action de gestion	SFR	Action de gestion
FAU_SAA.1	NA	FIA_AFL.1	a)	FMT_MTD.1	a)
FSC_CKM.3	a)	FIA_ATD.1	a)	*FMT_SMF.1*	*NM*
FCS_CKM.4	a)	FIA_UAU.1	a)	FMT_SMR.1	NA
FCS_COP.1	NM	FIA_UAU.3	NM	FPR_UNO.1	NA
FDP_ACC.2	NM	FIA_UAU.4	NM	FPT_FLS.1	NM
FDP_ACF.1	a)	FIA_UID.1	NA	FPT_PHP.3	NA
FDP_DAU.1	a)	FIA_USB.1	a)	FPT_SEP.1	NM
FDP_ETC.1	NM	FMT_MOF.1	a)	FPT_TDC.1	NM
FDP_ITC.1	a)	FMT_MSA.1	a)	FPT_TST.1	NA
FDP_RIP.1	NA	FMT_MSA.2	NM		
FDP_SDI.2	NA	FMT_MSA.3	a)		

NA : Non Applicable
NM : No Management (pas d'action de gestion identifiée dans les critères)
a) : Actions de gestion a) des CC retenues

FMT_MOF.1 Administration du comportement des fonctions de sécurité

Itération

FMT_MOF.1.1 La TSF doit restreindre l'aptitude de **[sélection : déterminer le comportement, désactiver, activer, modifier le comportement]** des fonctions **[affectation : liste des fonctions] aux [affectation : rôles autorisés identifiés]**.

Affectation **Voir Tableau 13 :**

Itération SSCD

FMT_MOF.1.1 La TSF doit restreindre l'aptitude de **[sélection : activer]** des fonctions **[affectation : la fonction de création de signature]** aux **[affectation : Signataire]**.

Comportements	Fonctions	Rôles
Activer / désactiver	Les opérations d'initialisation	Pré-personnalisateur
Activer / désactiver	Les opérations de personnalisation	Personnalisateur
Activer	La création d'un secret	Autorités de domaines ou Emetteur
Activer	La création ou la suppression de répertoires ou de fichiers	Autorités de domaines ou Emetteur
Activer	La gestion du cycle de vie des fichiers ou des répertoires	Autorités de domaines ou Emetteur
Activer	La gestion du cycle de vie d'un secret	Autorités de domaines ou Emetteur
Désactivé	Le blocage d'une clé cryptographique	Autorités de domaines ou Emetteur
Désactivé	Le blocage d'un code PIN	Emetteur
Activer	Le changement d'un code PIN	Emetteur ou porteur
Activé / Désactivé	Le blocage d'une clé cryptographique hors clés SCD/SVD	Autorités de domaines ou Emetteur
Activé / Désactivé	Le blocage d'une clé cryptographique de type SCD/SVD	Emetteur et signataire
Activer	Le changement (chargement) d'une clé cryptographique hors clés SCD/SVD	Autorités de domaines ou Emetteur
Activer	Le changement (génération ou chargement) d'une clé cryptographique de type SCD/SVD	Emetteur et signataire
Activer / Désactiver	Le blocage de l'application	Emetteur

Tableau 13 : Comportements/fonctions/rôles

FMT_MSA.1 Administration des attributs de sécurité

Itération

FMT_MSA.1.1 La TSF doit mettre en œuvre la **[affectation : liste des SFP de contrôle d'accès]** pour restreindre aux **[affectation : administrateurs suivants]** la possibilité **[affectation : d'exécuter les opérations suivantes sur]** les attributs de sécurité suivants :

Affectation **Liste des SFP de contrôle d'accès :**

- SFP de contrôle d'accès aux services « IAS-eGOV » ;
- SFP de contrôle d'accès aux fichiers ;
- SFP de contrôle d'accès aux paramètres TLV ;
- SFP de contrôle d'accès aux secrets ;

La TSF doit restreindre à :

- L'émetteur ou l'autorité de domaine, la possibilité de ré-initialiser le compteur PTC de l'attribut **groupe de ratification** et l'attribut **compteur d'utilisation** ;
- L'émetteur ou l'autorité de domaine, la possibilité de modifier l'attribut **Etat secret** à « Activé » ;
- L'émetteur la possibilité de modifier l'attribut **statut de l'application** ;
- L'émetteur ou l'autorité de domaine, la possibilité de charger les attributs **type de fichier**, **d'état fichier** et **DAC** lors de la création d'un répertoire ou d'un fichier dans un répertoire appartenant à son domaine ;
- L'autorité de domaine ou à l'émetteur la possibilité de charger les attributs **type de clé**, **DAC** et **Etat secret** lors de l'ajout d'un secret.

Itération SSCD

FMT_MSA.1.1 Administrateur La TSF doit mettre en œuvre la **[affectation : SFP d'initialisation et la SFP Importation de SCD]** pour restreindre à l'**[administrateur]** la possibilité de **[modifier]** les attributs de sécurité **[Gestion des SCD/SVD et Importation sécurisée de SCD autorisée]**

FMT_MSA.1.1 Signataire La TSF doit mettre en œuvre la **[affectation : SFP de création de signature]** pour restreindre au **[signataire]** la possibilité de **[modifier]** les attributs de sécurité **[SCD opérationnelles]**

FMT_MSA.2 Attributs de sécurité sûrs

FMT_MSA.2.1 La TSF doit garantir que seules des valeurs sûres sont acceptées pour les attributs de sécurité.

FMT_MSA.3 Initialisation statique d'attribut

Itération

FMT_MSA.3.1 La TSF doit mettre en œuvre **[affectation : la liste des SFP de contrôle d'accès]** afin de fournir des valeurs par défaut **[restrictives]** pour les attributs de sécurité qui sont utilisés pour appliquer la SFP.

Affectation **Liste des SFP de contrôle d'accès :**

- SFP de contrôle d'accès aux services « IAS-eGOV » ;
- SFP de contrôle d'accès aux fichiers ;
- SFP de contrôle d'accès aux paramètres TLV ;
- SFP de contrôle d'accès aux secrets ;

Raffinement **Création de répertoires ou de fichiers (SFP de contrôle d'accès aux fichiers)**

- Les attributs « **type de fichier**, **DAC** » doivent être fournis par l'administrateur de domaine ou par l'émetteur lors de la création de répertoires ou de fichiers ;
- Les attributs « **type de clé**, **DAC**, **Etat secret** » doivent être fournis par l'administrateur de domaine ou par l'émetteur lors de l'ajout d'une clé ;
- L'attribut « **état de sécurité carte** » est construit dynamiquement en fonction des authentifications réussies et des canaux de confiances établis. Lors de la mise sous tension de la carte Morpho-Citiz 32, l'**état sécurité carte** est à « tous non-authentifié » et« pas de SM ouvert »

FMT_MSA.3.2 La TSF doit permettre à **[affectation : aucun rôle]** de spécifier des valeurs initiales alternatives pour remplacer les valeurs par défaut lorsqu'un objet ou une information est créé.

Itération SSCD

FMT_MSA.3.1 /SFP d'initialisation La TSF doit mettre en œuvre **[SFP d'initialisation]** et **[SFP de création de signature]** afin de fournir des valeurs par défaut **[restrictives]** pour les attributs de sécurité qui sont utilisés pour appliquer la SFP.

Raffinement L'attribut de sécurité des SCD **« SCD opérationnelles »** est défini à Non après la génération du SCD.

FMT_MSA.3.2 /SFP d'initialisation La TSF doit permettre à **[l'Administrateur]** de spécifier des valeurs initiales alternatives pour remplacer les valeurs par défaut lorsqu'un objet ou une information est créé.

Itération SSCD

FMT_MSA.3.1 /SFP Importation de SCD La TSF doit mettre en œuvre **[SFP Importation de SCD]** et **[SFP de création de signature]** afin de fournir des valeurs par défaut **[restrictives]** pour les attributs de sécurité qui sont utilisés pour appliquer la SFP.

Raffinement L'attribut de sécurité des SCD **« SCD opérationnelles »** est défini à Non après l'importation du SCD.

FMT_MSA.3.2 /SFP Importation de SCD La TSF doit permettre à **[l'Administrateur]** de spécifier des valeurs initiales alternatives pour remplacer les valeurs par défaut lorsqu'un objet ou une information est créé.

FMT_MTD.1 Gestion des données de la TSF

Itération

FMT_MTD.1.1 La TSF doit restreindre la possibilité de **[sélection : changer une valeur par défaut,**

interroger, modifier, supprimer, effacer [affectation : autres opérations]] les **[affectation : liste des données de la TSF]** aux **[affectation : les rôles autorisés identifiés]**.

Affectation **Gestion des données de la TSF :**

- Modifier la valeur du code PIN par l'émetteur ou par le porteur ;
- Modifier la valeur d'une clé cryptographique par l'émetteur ou l'autorité de domaine ;
- Créer un secret par l'émetteur ou l'autorité de domaine ;
- Bloquer/Débloquer une clé cryptographique par l'émetteur ou l'autorité de domaine ;
- Débloquer un code PIN par l'émetteur ;
- Bloquer/Débloquer une application par l'émetteur ;

Itération SSCD

FMT_MTD.1.1 La TSF doit restreindre la possibilité de **[modifier [affectation : sans objet]]** les **[RAD]** aux **[Signataire]**.

FMT_SMF.1 Spécification des fonctions de management

FMT_SMF.1.1 *La TSF doit être capable de mettre en œuvre les fonctions de gestion de la sécurité suivantes* ***[affectation : FS_GESTION, FS_SEC]***

FMT_SMR.1 Rôles de sécurité

Itération

FMT_SMR.1.1 La TSF doit tenir à jour les rôles **[affectation : les rôles autorisés identifiés]**.

Affectation **Rôles autorisés :**

- Voir Tableau 14

FMT_SMR.1.2 La TSF doit être capable d'associer les utilisateurs aux rôles.

Itération SSCD

FMT_SMR.1.1 La TSF doit tenir à jour les rôles **[Administrateur]** et **[Signataire]**.

FMT_SMR.1.2 La TSF doit être capable d'associer les utilisateurs aux rôles.

Cycle de vie	Rôles	Description
Initialisation (Phase 4 et 5)	Pré-personnalisateur (Administrateur)	Après réussite de l'authentification de l'utilisateur, ce rôle autorise, dans un environnement sécurisé, à initialiser la carte Morpho-Citiz 32.
Personnalisation (Phase 6)	Personnalisateur (Administrateur)	Après réussite de l'authentification de l'utilisateur, ce rôle autorise à personnaliser la TOE, dans un environnement sécurisé. Cet administrateur a la possibilité de : – Créer des objets fichiers ; – Charger et de mettre à jour les données utilisateur et TSF ;
Utilisateur final (Phase 7)	Émetteur (Administrateur)	Après réussite de l'authentification de l'émetteur, l'utilisateur peut : – Bloquer / Débloquer une application (ADF) ; – Créer un secret ; – Modifier le l'état d'un secret dans son cycle de vie ; – Bloquer / Débloquer un secret ; – Charger la valeur d'un secret ; – Créer et supprimer des fichiers / répertoires ;
Utilisateur final (Phase 7)	Autorité de domaine (Administrateur)	Après réussite de l'authentification de l'administrateur, l'émetteur peut : – Modifier le l'état d'un secret dans son cycle de vie ; – Bloquer / Débloquer un secret ; – Créer un secret ; – Modifier le l'état d'un secret dans son cycle de vie ;

		– Bloquer / Débloquer un secret ; – Charger la valeur d'un secret ; – Créer et supprimer des fichiers / répertoires (domaines) sous une application ;
Utilisateur final (Phase 7)	Porteur (Utilisateur)	Ce rôle a des possibilités définies par les fonctionnalités de la carte Morpho-Citiz 32. Les possibilités accessibles au porteur dépendent des options d'initialisation et de personnalisation.

Tableau 14 : Rôles autorisés

5.2.6 Protection de la vie privée (FPR)

FPR_UNO.1 Non observabilité

Itération

FPR_UNO.1.1 La TSF doit garantir que **[affectation : tous les utilisateurs]** ne peuvent pas observer l'exécution de **[affectation : liste des opérations]** sur **[affectation : liste des objets]** par **[affectation : liste d'utilisateurs ou de sujets protégés]**

Affectation **Rôles autorisés :**

- Voir Tableau 15

Itération SSCD

FPR_UNO.1.1 La TSF doit garantir que **[affectation : tous les utilisateurs]** ne peuvent pas observer l'exécution de **[affectation : liste des opérations]** sur **[affectation : liste des objets]** par **[affectation : liste d'utilisateurs ou de sujets protégés]**

Affectation **Rôles autorisés :**

- Voir Tableau 16

Opérations	Liste des objets	Liste d'utilisateurs ou sujets
Mise à jour	OB_SECRET	SUB_GS
Utilisation	OB_SECRET	SUB_CRYPTO

Tableau 15 : Protection de la vie privée

Opérations	Liste des objets	Liste d'utilisateurs ou sujets
Génération	SCD/SVD	Signataire, Administrateur
Utilisation	SCD	Signataire
Mise à jour	RAD	Administrateur

Tableau 16 : Protection de la vie privée – SSCD

5.2.7 Protection des fonctions de sécurité de la TOE (FPT)

FPT_AMT.1 Test de la machine abstraite

FPT_AMT.1.1 La TSF doit effectuer une suite de tests **[au cours du démarrage initial]** pour prouver le fonctionnement correct des hypothèses de sécurité fournies par la machine abstraite qui est à la base des TSF.

FPT_EMSEC.1 Emanation de la TOE

Cette exigence est une extension à la partie 2 des CC **[R1 – CC]** et provient des PP **[R3 – SSCD T2]** et **[R4 – SSCD T3]**.

FPT_EMSEC.1.1 La TOE ne doit pas émettre **[de canaux cachés]** en excès des **[limites de l'état de l'art]** permettant l'accès aux **[RAD et aux SCD]**.

Raffinement Les limites de l'état de l'art sont les limites actuellement attendues pour les évaluations de sécurité de produits « carte à puce » au niveau d'assurance EAL 4+.

FPT_EMSEC.1.2 La TSF doit garantir que **[tout utilisateur]** sont incapables d'utiliser l'interface suivante **[affectation: interface externe]** pour obtenir l'accès aux **[RAD]** et aux **[SCD]**.

FPT_FLS.1 Défaillance avec préservation d'un état sûr

FPT_FLS.1.1 La TSF doit préserver un état sûr quand les types de défaillances suivants se produisent :**[Liste des défaillances]**

Affectation **Liste des défaillances :**

- Interruption imprévue de l'exécution de la TSF en raison d'événements extérieurs (alimentation, extraction) ;
- Défaillance d'intégrité mémoires ;
- Défaillance d'intégrité sur applications propriétaires ;
- Défaillances de programmation E²PROM ;

FPT_PHP.1 Détection passive d'une attaque physique

FPT_PHP.1.1 La TSF doit détecter sans ambiguïté une l'intrusion physique qui pourrait compromettre les TSF.

FPT_PHP.1.2 La TSF doit pouvoir déterminer si une intrusion physique dans les dispositifs de la TSF ou dans les éléments de la TSF a eu lieu.

FPT_PHP.3 Résistance à une attaque physique

FPT_PHP.3.1 La TSF doit résister à **[affectation : scénarios d'intrusions physiques]** dans les **[affectation : Liste des dispositifs ou des éléments de la TSF]** en répondant automatiquement de telle façon que la TSP ne soit pas violée.

Affectation **Scénarios d'intrusion physique sur les éléments suivants :**

- Réduction de la fréquence d'horloge pour stopper la TOE durant une opération spécifique
- Elévation de la fréquence d'horloge pour corrompre la TOE,
- Modification de la température en vue de corrompre des opérations de la TOE,
- Modification de la tension en vue de corrompre des opérations de la TOE

FPT_SEP.1 Séparation de domaines pour la TSF

FPT_SEP.1.1 La TSF doit maintenir un domaine de sécurité pour sa propre exécution, qui la protège des interférences et des intrusions par des sujets non sûrs.

FPT_SEP.1.2 La TSF doit appliquer une séparation entre les domaines de sécurité de sujets dans le TSC.

FPT_TDC.1 Cohérence élémentaire des données de la TSF inter TSF

Itération

FPT_TDC.1.1 La TSF doit offrir la capacité d'interpréter de façon cohérente **[affectation : Les clés des utilisateurs et le code du porteur]** quand elles sont partagées entre la TSF et un autre produit TI de confiance.

FPT_TDC.1.2 La TSF doit utiliser **[affectation : la spécification [R9 – E-ADMIN]]** pour interpréter les données de la TSF d'un autre produit TI de confiance.

Itération SSCD

FPT_TDC.1.1 La TSF doit offrir la capacité d'interpréter de façon cohérente **[affectation : Les SCD/SVD des utilisateurs et le code du Signataire]** quand elles sont partagées entre la TSF et un autre produit TI de confiance.

FPT_TDC.1.2 La TSF doit utiliser **[affectation : la spécification [R9 – E-ADMIN]]** pour interpréter les données de la TSF d'un autre produit TI de confiance.

FPT_TST.1 Test de la TSF

FPT_TST.1.1 La TSF doit exécuter une suite d'autotests **[pendant le démarrage initial]** pour démontrer le fonctionnement correct de la TSF.

FPT_TST.1.2 La TSF doit fournir aux utilisateurs autorisés la possibilité de contrôler l'intégrité de données de la TSF.

FPT_TST.1.3 La TSF doit fournir aux utilisateurs autorisés la possibilité de contrôler l'intégrité du code exécutable de la TSF mis en mémoire.

5.2.8 Chemin et Canaux de confiance (FTP)

FTP_ITC.1 Canal de confiance inter-TSF

	Itération SSCD
FTP_ITC.1.1 /Transfert de SVD	La TSF doit fournir un canal de communication sécurisé entre elle-même et un produit TI distant **CGA**, qui est distinct logiquement des autres canaux de communication et qui fournit une identification assurée de ses terminaisons ainsi qu'une protection contre une modification ou une divulgation des données sur le canal.
FTP_ITC.1.2 /Transfert de SVD	Les TSF doivent permettre **[le produit TI distant sécurisé]** de démarrer la communication par le canal de confiance.
FTP_ITC.1.3 /Transfert de SVD	La TSF **ou la CGA** doivent démarrer la communication par le canal de confiance pour **[le transfert de SVD]**.
	Itération SSCD
FTP_ITC.1.1 /Importation de DTBS	La TSF doit fournir un canal de communication sécurisé entre elle-même et un produit TI distant, qui est distinct logiquement des autres canaux de communication et qui fournit une identification assurée de ses terminaisons ainsi qu'une protection contre une modification ou une divulgation des données sur le canal.
FTP_ITC.1.2 /Importation de DTBS	La TSF doit autoriser la **CGA** à démarrer la communication par le canal de confiance.
FTP_ITC.1.3 /Importation de DTBS	La TSF **ou la SGA** doivent démarrer la communication par le canal de confiance pour la signature de la représentation des DTBS.
	Itération SSCD
FTP_ITC.1.1 /Importation de SCD	La TSF doit fournir un canal de communication sécurisé entre elle-même et un produit TI distant, qui est distinct logiquement des autres canaux de communication et qui fournit une identification assurée de ses terminaisons ainsi qu'une protection contre une modification ou une divulgation des données sur le canal.
FTP_ITC.1.2 /Importation de SCD	Les TSF doivent permettre **[le produit TI distant sécurisé]** de démarrer la communication par le canal de confiance.
FTP_ITC.1.3 /Importation de SCD	La TSF doit démarrer la communication par le canal de confiance pour **[l'importation de SCD]**.
Raffinement SSCD	Le « produit TI distant sécurisé » mentionné est un SSCD Type 1.

FTP_TRP.1 Chemin de confiance

FTP_TRP.1.1 /TOE La TSF doit fournir un chemin de communication entre elle-même et un utilisateur local qui soit logiquement distinct des autres chemins de communication et qui garantisse l'identification de ses extrémités et la protection des données transférées contre une modification ou une divulgation.

FTP_TRP.1.2 /TOE La TSF doit permettre **[aux utilisateurs locaux]** de démarrer la communication par le chemin de confiance.

FTP_TRP.1.3 /TOE La TSF exige l'utilisation d'un chemin de confiance pour **[l'authentification initiale de l'utilisateur][affectation: pas d'autres services]**.

5.3 EXIGENCES D'ASSURANCE SECURITE POUR LA TOE

Les exigences d'assurance sécurité sélectionnées correspondent au niveau d'évaluation EAL4 augmenté des composants ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4.

ADV_IMP.2 Implémentation de la TSF

Tâches du développeur

ADV_IMP.2.1D Le développeur doit fournir une représentation de l'implémentation d l'ensemble de la TSF.

Contenu et présentation des éléments de preuve

ADV_IMP.2.1C La représentation de l'implémentation doit définir la TSF d'une façon non ambiguë avec un niveau de détail suffisant pour qu'elle puisse être générée sans décision de conception supplémentaire.

ADV_IMP.2.2C La représentation de l'implémentation doit avoir une cohérence interne.

ADV_IMP.2.3C La représentation de l'implémentation doit décrire les relations entre toutes **les parties de l'implémentation.**

Tâches de l'évaluateur

ADV_IMP.2.1E L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.

ADV_IMP.2.2E L'évaluateur doit déterminer que la **représentation de l'implémentation** est une instanciation correcte et complète des exigences fonctionnelles de sécurité de la TOE.

Dépendances **Liste des dépendances**

- ADV_LLD.1, ADV_RCR.1, ALC_TAT.1 ;

ALC_DVS.2 Caractère suffisant des mesures de sécurité

Tâches du développeur

ALC_DVS.2.1D Le développeur doit produire la documentation relative à la sécurité du développement.

Contenu et présentation des éléments de preuve

ALC_DVS.2.1C La documentation relative à la sécurité du développement doit décrire toutes les mesures de sécurité physiques, organisationnelles, touchant au personnel et autres qui sont nécessaires pour protéger la confidentialité et l'intégrité de la conception et de l'implémentation de la TOE dans son environnement de développement.

ALC_DVS.2.2C La documentation relative à la sécurité du développement doit fournir des éléments de preuve indiquant que ces mesures de sécurité sont appliquées au cours du développement et de la maintenance de la TOE.

ALC_DVS.2.3C Les éléments de preuve doivent justifier que les mesures de sécurité fournissent le niveau de protection nécessaire pour maintenir la confidentialité et l'intégrité de la TOE.

Tâches de l'évaluateur

ALC_DVS.2.1E L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.

ALC_DVS.2.2E L'évaluateur doit confirmer que les mesures de sécurité sont appliquées.

Dépendances **Pas de dépendances**

AVA_MSU.3 Analyse et test des états non sûrs

Tâches du développeur

AVA_MSU.3.1D Le développeur doit fournir une documentation d'information.

AVA_MSU.3.2D Le développeur doit documenter une analyse de la documentation d'information.

Contenu et présentation des éléments de preuve

AVA_MSU.3.1C La documentation d'information doit identifier tous les modes possibles de fonctionnement de la TOE (y compris le fonctionnement suite à un panne ou à une erreur opérationnelle), leurs conséquences et implications pour le maintien d'un fonctionnement sécurisé.

AVA_MSU.3.2C La documentation d'information doit être complète, claire, cohérente et raisonnable.

AVA_MSU.3.3C La documentation d'information doit lister toutes les hypothèses sur l'environnement attendu.

AVA_MSU.3.4C La documentation d'information doit lister toutes les exigences pour les mesures de sécurité externes (y compris les contrôles externes procéduriers, physiques et personnels).

AVA_MSU.4.5C La documentation d'analyse doit prouver que la documentation d'information est complète.

Tâches de l'évaluateur

AVA_MSU.3.1E L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.

AVA_MSU.3.2E L'évaluateur doit appliquer à nouveau toutes les procédures de configuration, d'installation et sélectivement d'autres procédures, afin de confirmer que la TOE peut être configurée et utilisée de manière sûre en utilisant seulement les guides fournis.

AVA_MSU.3.3E L'évaluateur doit déterminer si l'utilisation des guides permet de détecter tous les états non sûrs.

AVA_MSU.3.4E L'évaluateur doit confirmer que la documentation d'analyse montre que sont donnés des conseils pour une exploitation sûre de la TOE dans tous les modes d'exploitation.

AVA_MSU.3.5E L'évaluateur doit effectuer des tests indépendants afin de déterminer si un administrateur ou un utilisateur, ayant acquis une bonne compréhension des guides, serait raisonnablement capable de déterminer si la TOE est configurée et exploitée d'une manière non sûre.

Dépendances: **Liste des dépendances**

- ADV_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD, USR.1 ;

AVA_VLA.4 Résistance élevée

Tâches du développeur

AVA_VLA.4.1D Le développeur doit réaliser une analyse de vulnérabilité.

AVA_VLA.4.2D Le développeur doit produire la documentation relative à l'analyse de vulnérabilité.

Contenu et présentation des éléments de preuve

AVA_VLA.4.1C La documentation relative à l'analyse de vulnérabilité doit décrire l'analyse des livrables de la TOE pour rechercher les chemins par lesquels l'utilisateur peut violer la TSP.

AVA_VLA.4.2C La documentation relative à l'analyse de vulnérabilité doit décrire la disposition des vulnérabilités identifiées.

AVA_VLA.4.3C La documentation relative à l'analyse de vulnérabilité doit montrer pour toutes les vulnérabilités identifiées que la vulnérabilité ne peut pas être exploitée dans l'environnement voulu de la TOE.

AVA_VLA.4.4C La documentation relative à l'analyse de vulnérabilité doit justifier que, avec les vulnérabilités identifiées, la TOE est résistante aux attaques évidentes en pénétration.

AVA_VLA.4.5C La documentation relative à l'analyse de vulnérabilité doit montrer que la recherche des vulnérabilités est systématique.

AVA_VLA.4.6C La documentation relative à l'analyse de vulnérabilité doit fournir une justification que l'analyse prend en compte complètement les fournitures de la TOE.

Tâches de l'évaluateur

AVA_VLA.4.1E L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.

AVA_VLA.4.2E L'évaluateur doit conduire des tests en pénétration, construits sur l'analyse en vulnérabilité du développeur, pour garantir que les vulnérabilités identifiées ont été adressées.

AVA_VLA.4.3E L'évaluateur doit réaliser une analyse en vulnérabilité indépendante.

AVA_VLA.4.4E L'évaluateur doit réaliser des tests en pénétration indépendants, basés sur l'analyse en vulnérabilité indépendante, pour déterminer si les vulnérabilités additionnelles identifiées sont exploitables dans l'environnement voulu.

AVA_VLA.4.5E L'évaluateur doit déterminer que la TOE est résistante aux attaques en pénétration réalisées par un attaquant possédant un haut potentiel d'attaque.

Dépendances: **Liste des dépendances**

- ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1 ;

5.4 EXTENSION DES EXIGENCES FONCTIONNELLES DE SECURITE

La famille additionnelle FPT_EMSEC (Emanation de la TOE) de la classe FPT (protection de la TSF) est définie ici pour décrire les exigences fonctionnelles de sécurité TI de la TOE. La TOE doit prévenir d'attaques contre la SCD et les autres données secrètes quand l'attaque est basée sur l'observation externe de phénomènes physiques de la TOE. Par exemple, de telles attaques correspondent à l'évaluation de la radiation électromagnétique de la TOE, de l'analyse en puissance simple (SPA), de l'analyse en puissance différentielle (DPA), du timing attack, etc. Cette famille décrit les exigences fonctionnelles pour limiter les émanations exploitables. La description de cette famille est celle présentée dans les PP **[R3 – SSCD T2]** et **[R4 – SSCD T3]**.

5.5 EXIGENCES DE SECURITE DE L'ENVIRONNEMENT TI

5.5.1 Génération de la clé de signature (SSCD Type 1)

FCS_CKM.1 Génération de clés cryptographiques

FCS_CKM.1.1 La TSF doit générer des clés cryptographiques conformément à l'algorithme de génération de clé cryptographique **[affectation: Liste des algorithmes de génération de clés]** et aux tailles spécifiées de clés cryptographiques **[affectation: Tailles de clés associées]** respectant la **[Liste des normes]**.

Affectation **Voir Tableau 17**

Liste des algorithmes de génération de clés	Tailles de clé	Liste des normes
Génération de clé RSA	1024 à 2048 bits	AREA-K **[R10 – AREAK1]**, **[R11 – AREAK2]**

Tableau 17 : Génération de clés cryptographiques

FCS_CKM.4 Destruction de clés cryptographiques

FCS_CKM.4.1 /Type 1 La TSF doit détruire les clés cryptographiques conformément à **[affectation : une méthode de destruction de clés cryptographiques]** spécifiée qui satisfait aux normes suivantes : **[effacement de la mémoire contenant la clé]**

FCS_COP.1 Opération cryptographique

FCS_COP.1.1 /CORRESP La TSF doit exécuter **[affectation : vérification de correspondance SCD/SVD]** conformément à un algorithme cryptographique **[affectation :** Calcul de clé RSA**]** et avec des tailles de clés cryptographiques **[affectation : de 1024 à 2048 bits]** spécifiés qui satisfont à ce qui suit : **[affectation : Signature PKCS#1 V2.1 – padding v 1.5]**.

FDP_ACC.1 Contrôle d'accès partiel

FDP_ACC.1.1 /SFP Exportation de SCD La TSF doit appliquer la **[SFP exportation de SCD]** lors de **[l'exportation de SCD par l'administrateur]**.

FDP_UCT.1 Confidentialité élémentaire des données échangées

FDP_UCT.1.1 /Exportation La TSF doit appliquer la **[SFP Exportation de SCD]** pour pouvoir **[transmettre]** les objets de manière à les protéger de toute divulgation non autorisée.

FTP_ITC.1 Canal de confiance inter-TSF

FTP_ITC.1.1 /Exportation de SCD La TSF doit fournir un canal de communication sécurisé entre elle-même et un produit TI distant, qui est distinct logiquement des autres canaux de communication et qui fournit une identification assurée de ses terminaisons ainsi qu'une protection contre une modification ou une divulgation des données sur le canal.

FTP_ITC.1.2 /Exportation de SCD Les TSF doivent permettre **[le produit TI distant sécurisé]** de démarrer la communication par le canal de confiance.

FTP_ITC.1.3 /Exportation de SCD La TSF doit démarrer la communication par le canal de confiance pour **[l'exportation de SCD]**.

Raffinement SSCD Le « produit TI distant sécurisé » mentionné est un SSCD Type 2.

5.5.2 Application de génération de certificats (CGA)

FCS_CKM.2 Distribution des clés cryptographiques

FCS_CKM.2.1 /CGA La TSF doit distribuer des clés cryptographiques selon une méthode de distribution de clés cryptographiques conforme aux certificats qualifiés et respectant les règles suivantes : **[affectation : [R10 – AREAK1], [R11 – AREAK2]]**.

FCS_CKM.3 Accès aux clés cryptographiques

FCS_CKM.3.1 /CGA La TSF doit effectuer **[l'importation des SVD]** conformément à une méthode d'accès aux clés cryptographiques, **[d'importation des clés cryptographiques au travers d'un canal de confiance]** respectant les règles suivantes : **[affectation: [R10 – AREAK1], [R11 – AREAK2]]**.

FDP_UIT.1 Intégrité de l'échange de données

FDP_UIT.1.1 /Importation de SVD La TSF doit appliquer la **[SFP d'importation de SVD]** pour pouvoir recevoir des données de l'utilisateur protégées contre les erreurs **[de modification]** et **[d'insertion]**.

FDP_UIT.1.2 /Importation de SVD La TSF doit pouvoir déterminer lors de la réception des données de l'utilisateur si une **[modification]** ou une **[insertion]** a eu lieu.

FTP_ITC.1 Canal de confiance inter-TSF (FTP_ITC.1)

FTP_ITC.1.1 /Importation des SVD La TSF doit fournir un canal de communication sécurisé entre elle-même et un produit TI distant, distinct logiquement des autres canaux de communication et qui fournit une identification assurée de ses terminaisons ainsi qu'une protection contre une modification ou une divulgation des données sur le canal.

FTP_ITC.1.2 /Importation des SVD La TSF doit permettre **[la TSF]** de démarrer la communication par le canal de confiance.

FTP_ITC.1.3 /Importation des SVD La TSF **ou la TOE** doivent démarrer la communication par le canal de confiance pour **[l'importation de SVD]**.

5.5.3 Application de création de signature (SCA)

FCS_COP.1 Opération cryptographique

FCS_COP.1.1 /Hash de la SCA La TSF doit exécuter **[le calcul de Hash des DTBS]** conformément à un algorithme cryptographique spécifié **[affectation: dans [R10 – AREAK1], [R11 – AREAK2] et [R13 – ERRATUM]]** et des tailles de clés cryptographiques respectant les règles suivantes : **[affectation: [R10 – AREAK1], [R11 – AREAK2]]**.

FDP_UIT.1 Intégrité de l'échange de données

FDP_UIT.1.1 /DTBS de la SCA La TSF doit appliquer la **[SFP de création de signature]** pour pouvoir transmettre des données de l'utilisateur de façon à éviter les erreurs de **[modification]**, de **[suppression]** et **[d'insertion]**.

FDP_UIT.1.2 /DTBS de la SCA La TSF doit pouvoir déterminer lors de la réception des données de l'utilisateur si une **[modification]**, une **[suppression]** ou une **[insertion]** a eu lieu.

FTP_ITC.1 Canal de confiance inter-TSF

FTP_ITC.1.1 /DTBS de la SCA La TSF doit fournir un canal de communication sécurisé entre elle-même et un produit TI distant, distinct logiquement des autres canaux de communication et qui fournit une identification assurée de ses terminaisons ainsi qu'une protection contre une modification ou une divulgation des données sur le canal.

FTP_ITC.1.2 /DTBS de la SCA La TSF doivent autoriser **[la TSF]** à démarrer la communication par le canal de confiance.

FTP_ITC.1.3 /DTBS de la SCA La TSF **ou la TOE** doivent démarrer la communication par le canal de confiance pour **[la signature de la représentation des DTBS au moyen du SSCD]**.

FTP_TRP.1 Chemin de confiance

FTP_TRP.1.1 /SCA La TSF doit fournir un chemin de communication entre elle-même et un utilisateur local distinct logiquement des autres chemins de communication et qui fournit une identification assurée de ses terminaisons ainsi qu'une protection contre une modification ou une divulgation des données.

FTP_TRP.1.2 /SCA La TSF doit permettre à **[la TSF]** de démarrer la communication par le chemin de confiance.

FTP_TRP.1.3 /SCA La TSF nécessite l'utilisation d'un chemin de confiance pour **[l'authentification initiale de l'utilisateur][affectation: pas d'autres services]**.

5.6 EXIGENCES DE SECURITE DE L'ENVIRONNEMENT NON TI

R.Administrator_Guide *Application des informations de l'administrateur*
La mise en œuvre des exigences de la Directive, ANNEXE II « Exigences concernant les prestataires de service de certification délivrant des certificats qualifiés », stipule alinéa (e) que les employés des CSP ou d'autres entités correspondantes doivent respecter les informations de l'administrateur fournies par la TOE. Un contrôle adapté des CSP ou des autres entités correspondantes doit garantir la conformité actuelle.

R.Sigy_Guide *Application des informations de l'utilisateur*
La mise en œuvre du SCP selon les exigences de la Directive, ANNEXE II « Exigences concernant les prestataires de service de certification délivrant des certificats qualifiés », stipule alinéa (k) que le signataire doit respecter les informations de l'utilisateur pour la TOE.

R.Sigy_Name *Nom du signataire dans le Certificat qualifié*

La CSP doit vérifier l'identité de la personne à laquelle un certificat qualifié est délivré conformément à la Directive [1], ANNEXE II « Exigences concernant les prestataires de service de certification délivrant des certificats qualifiés », alinéa (d). Le CSP doit vérifier que cette personne détient le SSCD qui met en œuvre les SCD correspondant aux SVD à inclure dans le certificat qualifié.

6. SPECIFICATIONS GENERALES DE LA TOE

6.1 FONCTIONS DE SECURITE DE LA TOE

6.1.1 Spécifications des fonctions de sécurité de la TOE

6.1.1.1 Fonctions de sécurité de bas niveau

FS_CHECKSUM
Génération d'un checksum afin d'assurer les contrôles d'intégrité.
FS_CHECKSUM a un SOF élevé.

FS_PHYS
Protections physiques contre les attaques extérieures de type intrusion.

FS_RANDOM
Fonction de génération d'un nombre aléatoire de longueur n octets.

FS_CAPTEUR
Gestion des capteurs du composant AT90SC12836RCT :

- Surveillance tension ;
- Surveillance fréquence ;
- Surveillance température ;
- Surveillance instruction invalide.

6.1.1.2 Fonctions de sécurité de niveau OS

FS_CHECK
Test l'intégrité :

- D'un entête de fichier ;
- D'un enregistrement de fichier ;
- De la zone OTP ;
- D'un objet TLV ;
- Des secrets (PIN et Clés) ;
- Des buffers d'I/O.

FS_TEST
Les éléments suivants sont testés au démarrage :

- La mémoire ROM ;
- La mémoire E²PROM ;
- La mémoire RAM ;
- Le générateur de nombre aléatoire ;
- Bloc matériel de DES ;
- Le crypto processeur ;

FS_MEMOIRE
Fonction gérant l'effacement de la mémoire E²PROM et/ou RAM.

FS_INIT

Fonction appelée après chaque reset et réalisant :

- Le test de la TOE par appel de la fonction FS_TEST ;
- L'émission d'ATR ;
- L'initialisation de tous les modules logiciels et l'initialisation des applications.

FS_BACKUP
Afin d'avoir une E²PROM toujours intègre, toute opération d'écriture correspond à un cycle d'écriture indivisible.

FS_OTP
Gestion de la zone OTP en mémoire E²PROM. Gestion notamment du paramètre « cycle de vie » de la TOE.

FS_ACCES
Cette fonction gère l'accès aux fichiers, aux répertoires, aux données propriétaires (TLV) et aux clés stockées en E²PROM.

FS_AUDIT
La fonction FS_AUDIT permet de réagir à une anomalie ou un défaut détecté.

6.1.1.3 Fonctions de sécurité au niveau du gestionnaire d'application

FS_GESTION
Au démarrage de la carte, cette fonction appelle FS_INIT puis attend une commande du terminal. Cette commande est soit traitée, soit redirigée vers un autre élément.
La fonction gère notamment :

- La sélection d'une application ;
- Gestion de l'état de sécurité carte ;
- La gestion des applications (étanchéité).

6.1.1.4 Fonctions de sécurité de niveau applicatif

FS_AUTH
Cette fonction gère les authentifications des différents utilisateurs de la TOE sur la base des secrets d'authentification associés aux différents utilisateurs (appel à FS_CRYPTO).
FS_AUTH a un SOF élevé.

FS_RATIF
Au travers de l'identifiant du secret (Clé, PIN), une application peut gérer une structure contenant les compteurs de ratification associés à ce secret. La gestion de ces compteurs de ratification se fait par lecture / écriture avec contrôle du nombre maximum d'essai.

FS_CRYPTO
Cette fonction assure les opérations cryptographiques de haut niveau :

- Chiffrement/Déchiffrement de données ;
- Déchiffrement de secrets ;
- Production/vérification de cryptogrammes d'authentification ;
- Contrôle d'intégrité sur des clés cryptographiques et des données ;
- Génération de signature électronique sécurisée sur des données externes ;
- Calcul de valeur de hachage ;
- Vérification du code PIN.

FS_SEC
Cette fonction permet d'assurer la gestion des secrets. La gestion des secrets comprend les fonctions suivantes :

- Génération de bi-clé de signature électronique;
- Génération de clé de session ;
- Destruction de clé ;
- Modification d'un secret ;
- Transfert d'un secret ;

- Déblocage d'un secret.

FS_SEC a un SOF élevé.

FS_COMMANDE

Lorsque le gestionnaire reçoit une commande, il la dispatche à une application pour un traitement. La fonction FS_COMMANDE implémentée dans les applications, effectue alors les traitements suivants :

- Test de la validité d'une commande ;
- Tests concernant la sémantique de la commande ;

6.1.2 Correspondance fonctions de sécurité / SFR

	FAU_SAA.1	FCS_CKM.1	FCS_CKM.3	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACC.2	FDP_ACF.1	FDP_DAU.1	FDP_ETC.1	FDP_ITC.1	FDP_RIP.1	FDP_SDI.2	FDP_UCT.1	FDP_UIT.1	FIA_AFL.1	FIA_ATD.1	FIA_UAU.1	FIA_UAU.3	FIA_UAU.4	FIA_UID.1	FIA_USB.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	*FMT_SMF.1*	FMT_SMR.1	FPR_UNO.1	FPT_AMT.1	FPT_EMSEC.1	FPT_FLS.1	FPT_PHP.1	FPT_PHP.3	FPT_SEP.1	FPT_TDC.1	FPT_TST.1	FTP_ITC.1	FTP_TRP.1
FS_CHECKSUM									X						X																								
FS_PHYS	X																																	X					
FS_RANDOM		X																		X																			
FS_CAPTEUR	X																																X	X					
FS_CHECK	X								X				X																	X									
FS_TEST	X																													X							X		
FS_MEMOIRE				X								X																											
FS_INIT	X																																						
FS_BACKUP													X																			X							
FS_OTP																												X											
FS_ACCES	X		X	X		X	X	X		X	X			X			X	X						X		X	X		X						X		X	
FS_AUDIT													X																					X					
FS_GESTION						X	X	X									X	X			X	X			X	X		*X*								X		X	X
FS_AUTH																		X			X		X														X	X
FS_RATIF																X																							
FS_CRYPTO					X									X	X				X	X									X		X						X	X
FS_SEC		X	X			X	X				X			X													X	*X*		X		X				X		
FS_COMMANDE							X																																

7. ANNONCE DE CONFORMITE A UN PP

7.1 REFERENCE AUX PP

La présente cible de sécurité est conforme aux profils de protection **[R3 – SSCD T2]** et **[R4 – SSCD T3]** ainsi qu'au profil de protection **[R2 – 9911]**.

La répartition entre ces trois profils de protection pour les hypothèses, les menaces, les objectifs de sécurité de la TOE et de son environnement ainsi que pour les exigences fonctionnelles de sécurité pour la TOE est présentée dans les tableaux suivants :

- Tableau 5 : Correspondances ST/PP – hypothèses pour la TOE ;
- Tableau 6 : Correspondances ST/PP – menaces pour la TOE ;
- Tableau 8 : Correspondances ST/PP – objectifs de sécurité pour la TOE ;
- Tableau 9 : Correspondances ST/PP – objectifs de sécurité pour l'environnement de la TOE ;
- Tableau 10 : Correspondances ST/PP – exigences de sécurité pour la TOE.

7.2 AJOUTS AUX PP

Dans la présente cible de sécurité, les ajouts d'exigence de sécurité suivants ont été apportés aux exigences de sécurité des profils de protection **[R2 – 9911]**, **[R3 – SSCD T2]** et **[R4 – SSCD T3]** déjà présents dans la présente cible de sécurité :

- FMT_SMF : Spécification des fonctions de management

Les ajouts d'exigences de sécurité, sont présentés en « *italique* » dans les chapitres et les tableaux suivants :

- Chapitre 5.2.5 : Gestion de la sécurité (FMT)
- Chapitre 6.1.2 : Correspondance fonctions de sécurité / SFR
- Tableau 10 : Correspondances ST/PP – exigences de sécurité pour la TOE.

FIN DE DOCUMENT