orange™ Business Services

Cardlet Mobile Connect

mobile connect

Cible de sécurité

Référence : MOB001-CDS01-1.5.0
Date : 13/11/2016
Interne Orange Applications for Business

Description du document

Propriété	Orange Applications for Business			
Titre projet	Cardlet Mobile Connect			
Titre document	Cible de sécurité			
Référence	MOB001-CDS01			
Version	1.5.0			
Classification	Interne Orange Applications for Business			
Rédacteur	C. Bergeon			
Statut	☐ En cours	☐ Relu	☒ Validé	☐ Approuvé
approbation (nom et signature)				
Date	13/11/2016			

Diffusion

société	**Nom**	**Fonction**	**Diffusion**
ANSSI		Certificateur	validation
Laboratoire TCS		Évaluateur	information
FIME		Développeur	information
Orange Applications for Business	C. Bergeon	Consultant SSI	rédaction
		Commanditaire	validation

Historique des versions

Version	**Opération**	**Nom**	**Date**
1.0	création	C. Bergeon	19/05/2015
1.10	Prise en compte des remarques de FIME	C. Bergeon	03/06/2015
1.20	Prise en compte des remarques orales de l'ANSSI lors de la réunion du 16/06/2015	C. Bergeon	25/06/2015
1.21	Prise en compte des remarques suite aux relectures internes	C. Bergeon	08/07/2015
1.3.0	Ajout exemple d'utilisation, le service Mobile Connect (§ 2.2.3), Ajout du périmètre d'évaluation (§ 8) H_SIM : restriction aux SIM EAL4+	C. Bergeon	10/11/2015

1.4.0	Prise en compte des remarques de l'ANSSI du 24/11/2015 : Modification de la catégorie du produit (§ 1.1) Ajout des interfaces avec la SIM (§ 3.2.2) Ajout de la configuration de la Cardlet dans les biens sensibles (§ 4.2) Ajout de la menace M_MOD-CONF-NAUTO (§ 5) Ajout de la fonction de sécurité F_STOCK-CONF (§ 6)	C. Bergeon	04/12/2015
1.5.0	Prise en compte des remarques du laboratoire TCS : Ajout hypothèse H_DEBLOC-PC (§ 3.5) Ajout tableau menace/mode de fonctionnement (§ 5.2) Modification et renommage de la menace M_ECOUTE_DAUTH (§ 5.1)	C. Bergeon	13/11/2016

Table des matières

Liste des figures

Liste des tableaux

1. Introduction

1.1. Identification

Organisation éditrice	Orange Applications for Business
Lien vers l'organisation	http://www.orange-business.com/fr/applications-for-business
Nom commercial du produit	Cardlet Mobile Connect
Identification du produit	MC23 FR
Numéro de la version évaluée	1.8
Catégorie de produit	Identification, authentification et contrôle d'accès

1.2. Documents de référence

Référence	Titre du document
[RFC4226] Décembre 2005	HOTP: An HMAC-Based One-Time Password Algorithm http://www.ietf.org/rfc/rfc4226.txt
[RFC6267] Juin 2011	OCRA: OATH Challenge-Response Algorithm https://tools.ietf.org/rfc/rfc6267.txt
[ETSI TS 102.225] v9.0.0 (2010-04)	Smart Cards Secured packet structure for UICC based applications http://www.etsi.org/deliver/etsi_ts/102200_102299/102225/11.00.00_60/ts_102225v110000p.pdf
[ETSI TS 131.115] v11.0.1 (2013-08) [3GPP TS 31.115] version 11.0.1	Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS) Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications http://www.etsi.org/deliver/etsi_ts/131100_131199/131115/11.00.01_60/ts_131115v110001p.pdf
[GPCS] v2.1.1	GlobalPlatform Card Specification http://www.globalplatform.org/specificationscard.asp
[RGS] v2.0	Référentiel Général de Sécurité – version 2.0 http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/liste-des-documents-constitutifs-du-rgs-v-2-0.html
[Java Card] v2.2.1	Java Card Specification http://download.oracle.com/otndocs/jcp/java_card_kit-2.2.1-fr-oth-JSpec
[SIM R6]	3rd Generation Partnership Project - (U)SIM API for Java™ Card 3GPP TS 31.130 v6.6.0 (juin 2007) http://www.qtc.jp/3GPP/Specs/31130-660.pdf Smart cards - UICC Application Programming Interface (UICC API) for Java Card (TM) – Release 6 ETSI TS 102 241 v6.4.0 (juin 2004) http://www.etsi.org/deliver/etsi_TS/102200_102299/102241/06.04.00_60/ts_102241v060400p.pdf
[CPAS8]	SIM Applet Authentication Specification – version 1.10
[PPUSIMB]	(U)SIM Java Card Platform Protection Profile Basic and SCWS Configurations (Basic configuration) Référence PU-2009-RT-79, version 2.0.2, 17 juin 2010. Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/04. http://www.ssi.gouv.fr/uploads/IMG/certificat/ANSSI-CC-cible_PP-2010-04en.pdf

Tableau n°1 : Documents de référence

1.3. Glossaire

3GPP	3rd Generation Partnership Project
CBC	Cipher Block Chaining
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile Communications
GSMA	GSM Association
HOTP	HMAC-Based One-Time Password
ISD	Issuer Security Domain
JCVM	Java Card Virtual Machine
LoA	Level of Assurance
MASP	Mobile Authentication Service Provider
MNO	Mobile Network Operator
OATH	Open AuTHentication
OCRA	OATH Challenge-Response Algorithm
OTA	Over The Air
RGS	Référentiel Général de Sécurité
SIM	Subscriber Identity Module
SMS	Short Message Service
SSD	Supplementary Security Domain
SAT	SIM Application Toolkit (= STK)
STK	SIM ToolKit
UICC	Universal Integrated Circuit Card
USAT	USIM Application Toolkit
USIM	Universal Subscriber Identity Module

2. Description du produit

2.1. Présentation générale

Le produit « **Cardlet Mobile Connect** » est une application Java Card téléchargeable sur une carte SIM d'un équipement de téléphonie mobile.

Sa fonction principale est la validation sûre (acceptation ou refus) de demandes émises par un système tiers au moyen de SMS échangés au travers du réseau de téléphonie mobile.

Dans toute la suite du document, l'application Java Card constituant le produit sera appelée la « **Cardlet** ».

2.2. Exemples d'utilisation

2.2.1. Authentification forte

Une application tierce sur Internet nécessitant une authentification forte à 2 facteurs (application du monde bancaire, application du monde la santé, …) transmet une demande à la Cardlet de l'utilisateur pour que ce dernier confirme sur son équipement de téléphonie mobile le fait qu'il est bien la personne qui souhaite se connecter à l'application tierce.

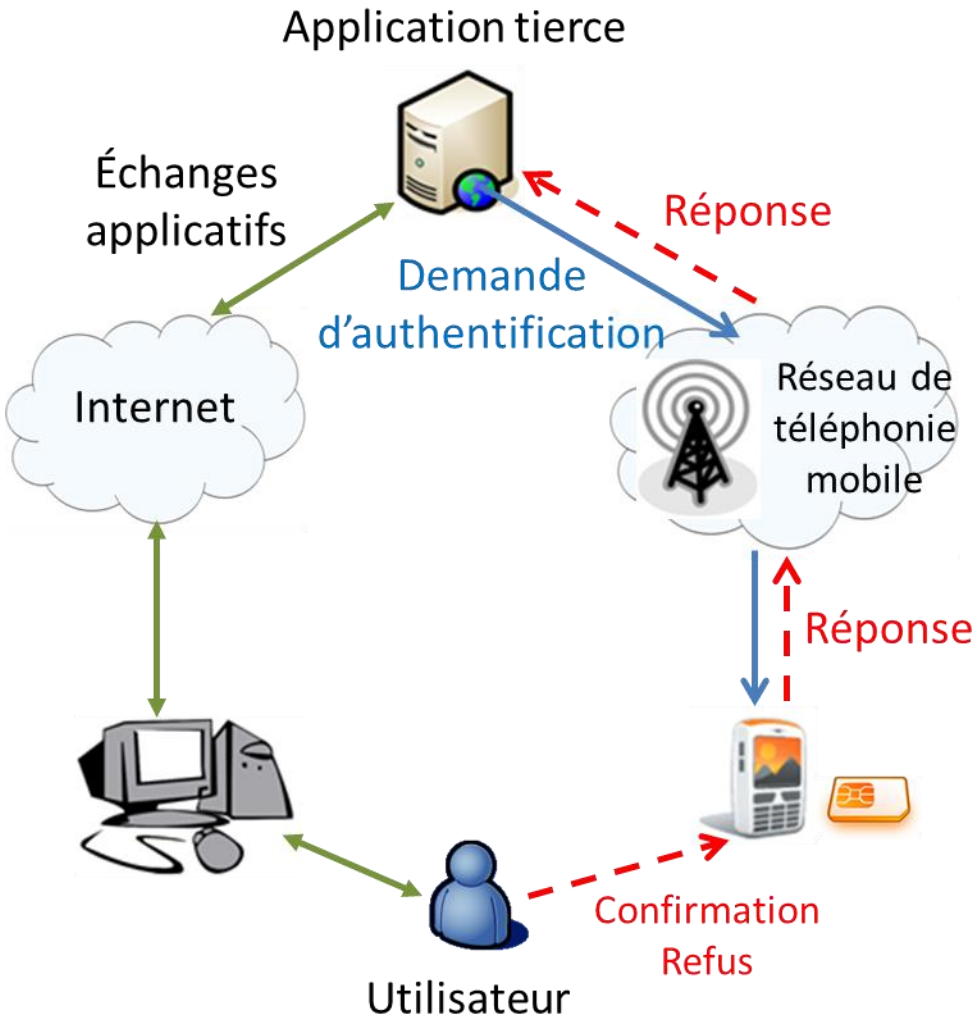

Figure 1 : Exemple d'utilisation : authentification forte

2.2.2. Validation d'une opération

Une application tierce sur Internet nécessitant d'avoir l'accord et la validation de l'utilisateur avant d'effectuer une opération importante (transaction bancaire, passage d'une commande, …) transmet une demande à la Cardlet de l'utilisateur pour que ce dernier valide l'opération sur son équipement de téléphonie mobile personnel.

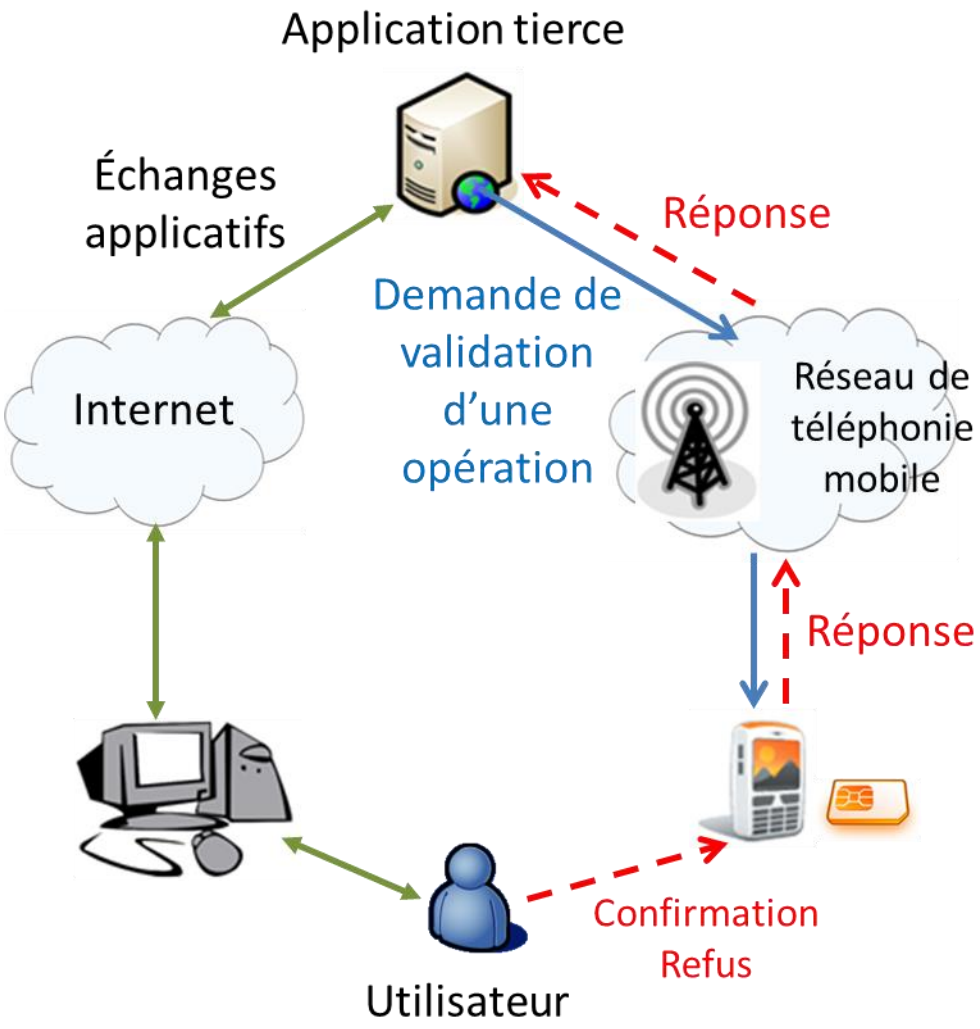

Figure 2 : Exemple d'utilisation : validation d'une opération

2.2.3. Fournisseur de services

Un fournisseur de services (Exemple : Service Mobile Connect) peut assurer pour le compte des applications tierces, l'interface entre ces dernières et la Cardlet des différents utilisateurs, dans le cas des exemples d'utilisation présentés précédemment.

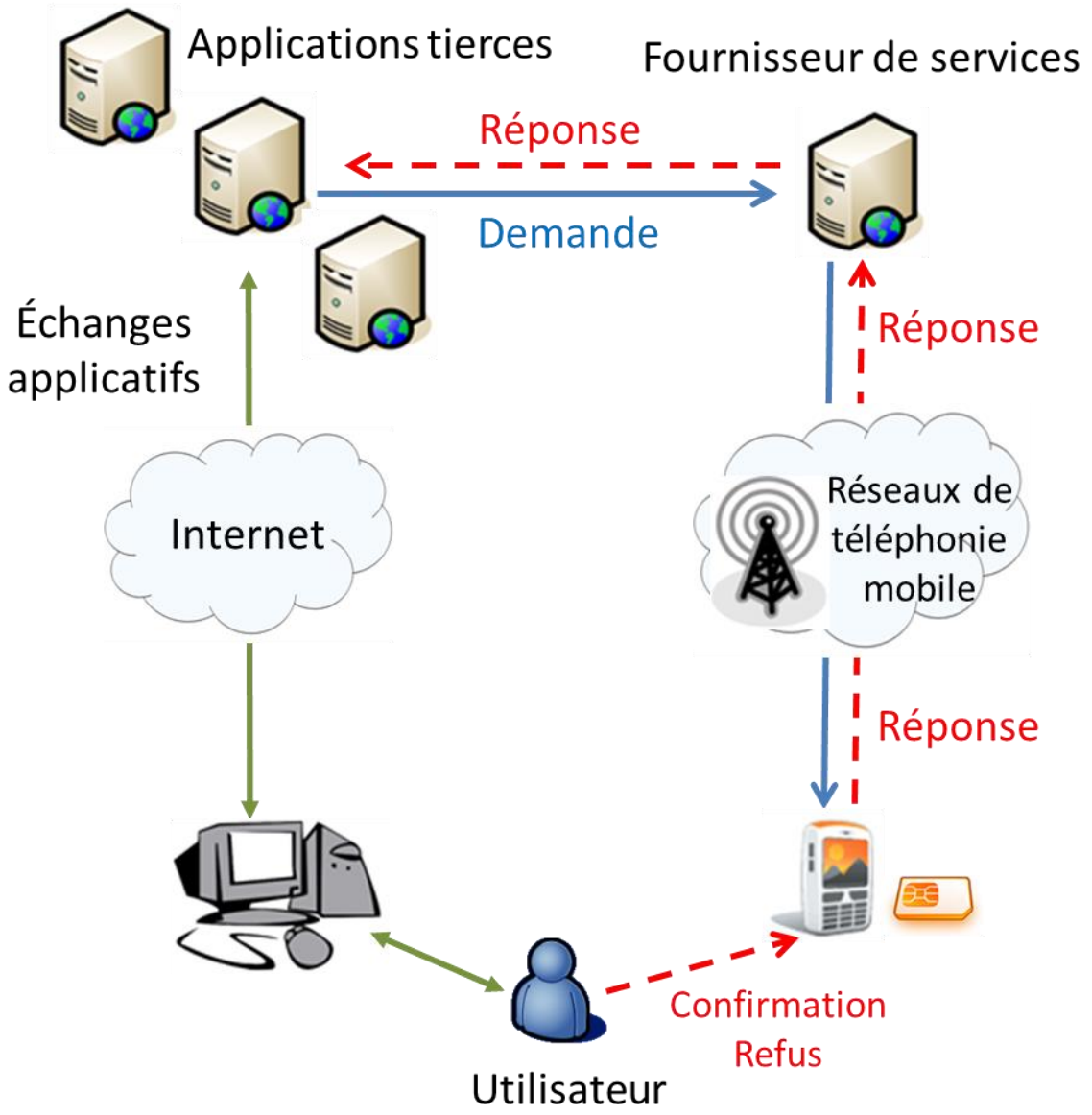

Figure 3 : Exemple d'utilisation : fournisseur de services

Note : le fournisseur de services s'interface avec les réseaux de téléphonie mobile des différents opérateurs.

Exemple : Le service Mobile Connect

Le service **Mobile Connect proposé par Orange** met en œuvre le mode de fonctionnement décrit ci-dessus.

Lors d'une opération nécessitant une validation de la part de l'utilisateur, l'application tierce transmet au service Mobile Connect une demande de validation.

De manière sécurisée, le service Mobile Connect se charge alors de :

- **transférer la demande** jusqu'à l'équipement de téléphonie mobile de l'utilisateur concerné, via le réseau de son opérateur (MNO),
- à l'aide de la Cardlet Mobile Connect embarquée dans la carte SIM de l'équipement de téléphonie mobile de l'utilisateur :
  - **afficher la demande** sur l'équipement de téléphonie mobile,
  - le cas échéant, contrôler le code personnel saisi par utilisateur,
  - **récupérer la réponse de l'utilisateur** (acceptation/refus de la demande),
- **remonter la réponse** de l'utilisateur à l'application tierce.

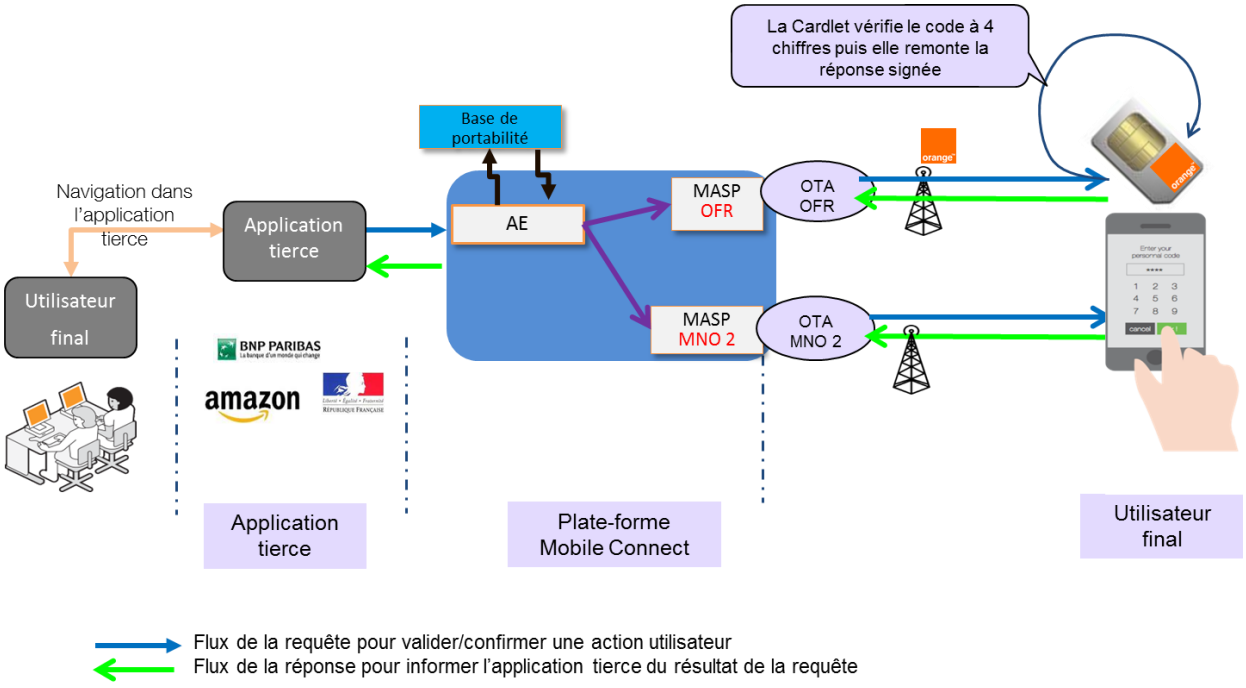

Figure 4 : Exemple d'utilisation : le service Mobile Connect

2.3. Fonctionnement du produit

La Cardlet offre deux modes fonctionnement en fonction du niveau de sécurité (LoA) choisi par l'application tierce initiatrice de la demande.

Dans les deux modes de fonctionnement, l'utilisateur confirme ou refuse la demande reçue sur son équipement de téléphonie mobile sur la base des informations affichées en relation avec les opérations qu'il est en train d'effectuer simultanément en ligne sur l'application tierce.

2.3.1. Mode « Click OK » ou validation

Dans ce premier mode de fonctionnement (LoA2), l'acceptation/confirmation ou le refus se font respectivement via deux touches distinctes sur l'écran de l'équipement de téléphonie mobile.

Figure 5 : Exemple d'utilisation du mode de fonctionnement "Click OK"

2.3.2. Mode « Code personnel » ou authentification

Dans ce second mode de fonctionnement (LoA3), l'acceptation/confirmation nécessite la saisie préalable d'un code personnel à partir de l'équipement de téléphonie mobile.

Figure 6 : Exemple d'utilisation du mode de fonctionnement "Code personnel"

2.4. Services offerts par le produit

Les services offerts par la Cardlet sont accessibles par l'intermédiaire d'un jeu de commandes conforme à la spécification de la GSMA [CPAS8] (SIM Applet Authentication Specification). Ces commandes sont fournies à la Cardlet par la carte SIM qui les a elle-même reçues sous la forme de SMS binaires (Cf. Figure 7 : Interfaces réseau).

2.4.1. Traitement des demandes de validation

Suite à la réception d'une demande transmise par l'application tierce distante, la Cardlet :

- génère via le SIM ToolKit, l'affichage sur l'écran de l'équipement de téléphonie mobile des informations associées à la demande, transmises par l'application tierce distante et ce dans la limite de la taille d'un SMS,
- dans le cas d'une demande avec authentification, vérifie le code personnel saisi par l'utilisateur,
- transmet la réponse de l'utilisateur (acceptation ou refus) à l'application tierce distante.

2.4.2. Personnalisation

Lors de la première utilisation de la Cardlet ou suite à une réinitialisation de celle-ci, la personnalisation de la Cardlet consiste pour l'utilisateur à créer son code personnel à partir de son équipement de téléphonie mobile.

Le code personnel est créé via une double saisie.

Le code personnel de l'utilisateur n'est connu que de l'utilisateur.

2.4.3. Administration

La Cardlet est administrée à distance.

Chaque mode de fonctionnement de la Cardlet (validation par « click OK » ou par saisie d'un code personnel) peut être indépendamment activé/désactivé.

Pour le mode de fonctionnement avec code personnel :

- le code personnel de l'utilisateur peut être réinitialisé (l'utilisateur devra alors en définir un nouveau),
- la Cardlet peut être débloquée suite au dépassement du seuil de tentatives infructueuses de saisie du code personnel.

Note : A l'installation de la Cardlet, ses 2 modes de fonctionnement sont désactivés par défaut.

2.4.4. Supervision

La Cardlet peut être supervisée à distance.

Elle remonte à la demande des informations d'état sur ses deux modes de fonctionnement.

3. Description de l'environnement

3.1. Plate-forme d'exécution

3.1.1. Cartes SIM

La Cardlet fonctionne avec des cartes SIM au standard 3GPP Release 6 (R6).

	3GPP Release 6
Global Platform	2.1.1 - March 2003
Java Card	2.2.1
3GPP	TS 31.130 **R6** v6.2
ETSI	TS 102.241 **R6** v6.7.0

Tableau n°2 : Types de carte SIM supportés

3.1.2. Équipements de téléphonie mobile

La Cardlet fonctionne avec tous les téléphones mobiles équipés d'une carte SIM compatible (Cf. ci-dessus les types de carte SIM supportés).

3.2. Interfaces externes de la Cardlet

3.2.1. Interfaces réseau

La figure ci-dessous schématise les interfaces réseau de la Cardlet.

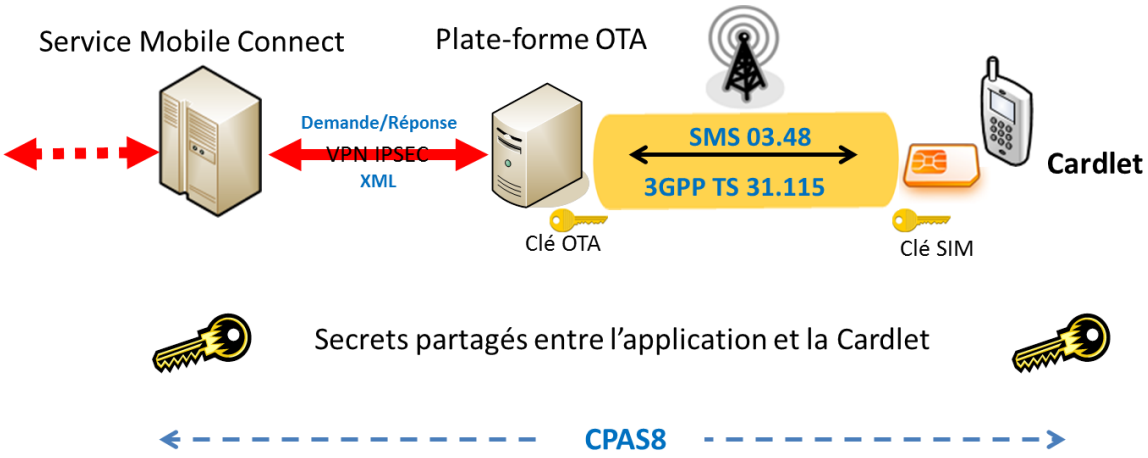

Figure 7 : Interfaces réseau

Les échanges applicatifs avec la Cardlet suivent la spécification de la GSMA CPAS8.
Certains de ces échanges applicatifs s'appuient des secrets partagés.

Un canal de communication entre la plate-forme OTA de l'opérateur de téléphonie mobile et la carte SIM assure par le biais de SMS binaires, le transport des informations destinées à la Cardlet.
Ce canal de communication respecte les spécifications techniques :

- ETSI TS 131.115/3GPP TS 31.115 (Secure packets over SMS)
- ETSI TS 102.225/3GPP TS 03.48 (Secure packets structure for UICC based applications).

3.2.2. Interfaces avec la SIM

La Cardlet est installée dans l'ISD (Issuer Security Domain) de la carte SIM.
Elle s'interface avec cette dernière pour :

- effectuer tous les échanges avec :
  - l'application distante sous la forme de SMS binaires, comme décrits ci-dessus,
  - l'utilisateur (affichage et saisie) via le STK (SIM ToolKit) de la carte SIM,
- sauvegarder ses données de configuration via la JCVM.

Note : STK (SIM ToolKit) aussi appelé SAT (SIM Application Toolkit) pour les SIM 2G et USAT (USIM Application Toolkit) pour les SIM 3G.

3.3. Utilisateurs et rôles

U_UTILISATEUR : Utilisateur

L'utilisateur de la Cardlet est le propriétaire de l'équipement de téléphonie mobile équipé de la carte SIM hébergeant la Cardlet. Il est également titulaire d'un abonnement auprès d'un opérateur de téléphonie mobile.

Il utilise la Cardlet pour accepter ou refuser les demandes de validation reçues du demandeur (U_DEMANDEUR).

U_DEMANDEUR : Demandeur

Le demandeur s'adresse à l'utilisateur (U_UTILISATEUR) pour obtenir la validation de ses demandes.

U_ADMINISTRATEUR : Administrateur

L'administrateur administre et supervise à distance la Cardlet.

U_MNO : Opérateur de téléphonie mobile

L'opérateur de téléphonique mobile est propriétaire de la carte SIM fournie à l'utilisateur (U_UTILISATEUR).

Il fournit la Cardlet à l'utilisateur, soit préinstallée dans la carte SIM, soit par téléchargement à partir de sa plate-forme OTA.

Il assure également les échanges de SMS binaires avec la carte SIM via sa plate-forme OTA.

3.4. Dépendances

La mise en œuvre de la Cardlet nécessite un équipement de téléphonie mobile (téléphone, tablette, …) équipé d'une carte SIM (Cf. Tableau n°2 : Types de carte SIM supporté) fournie par un opérateur de téléphonie mobile dans le cadre d'un abonnement incluant l'échange de SMS.

3.5. Hypothèses de sécurité sur l'environnement

H_MOBILE : Équipement de téléphonie mobile de confiance

L'équipement de téléphonie mobile utilisé est supposé :

- ne jamais avoir été déplombé (rooté ou jailbreaké),
- posséder un OS à jour en termes de correctifs de sécurité,
- disposer d'un verrouillage automatique de l'écran au bout d'une minute d'inactivité basé sur : un code, un motif, etc.

H_SIM : SIM de confiance

La carte SIM utilisée est certifiée EAL4+ selon les Critères Communs avec une conformité au profil de protection « (U)SIM Java Card Platform – Basic configuration » [PPUSIMB].

H_INSTAL : Installation de la Cardlet

La Cardlet est installée dans l'ISD (Issuer Security Domain) de la carte SIM, conformément à sa procédure d'installation via des moyens sûrs qui garantissent d'une part, son installation intègre et d'autre part, la protection de ses biens sensibles via les mécanismes de sécurité intrinsèques de la carte SIM.

H_CANAL : Canal sécurisé

Toutes les commandes externes destinées à la Cardlet se font via un canal sécurisé (SMS-MT binaires chiffrés et signés) établi entre la carte SIM et l'interface OTA de l'opérateur de téléphonie mobile conformément aux spécifications techniques ETSI TS 131.115/3GPP TS 31.115 (Secure packets over SMS) et ETSI TS 102.225/3GPP TS 03.48 (Secure packets structure for UICC based applications).

H_QUAL-SECRET : Qualité des secrets

Les secrets partagés utilisés par la Cardlet pour garantir l'intégrité et l'authenticité des réponses aux demandes de validation sont uniques et de qualité.

H_IMP-SECRET : Importation des secrets partagés

Les secrets partagés utilisés par la Cardlet lui sont fournis lors de son initialisation, via des moyens sûrs (i.e. H_CANAL).

H_DEBLOC-PC : Déblocage du code personnel

Avant de transmettre une demande de déblocage ou de réinitialisation du code personnel à la Cardlet, le service distant s'assure au préalable de l'identité du détenteur du téléphone.

4. Description des biens sensibles

4.1. Biens sensibles protégés par la Cardlet

Ce sont les biens essentiels que la Cardlet doit protéger pour assurer ses services.

Ces biens sensibles sont les suivants :

- La réponse de l'utilisateur à une demande de validation (intégrité),
- Le code personnel de l'utilisateur (intégrité et confidentialité).

4.2. Biens sensibles protégés par l'environnement de la Cardlet

Ce sont les biens essentiels qui doivent être protégés par l'environnement de mise en œuvre de la Cardlet pour que cette dernière puisse assurer ses services.

Ces biens sensibles sont les suivants :

- Le logiciel de la Cardlet (intégrité),
- La configuration de la Cardlet (intégrité et confidentialité) comprenant pour chacun de ses 2 modes de fonctionnement :
  - l'état du dit mode de fonctionnement (activé/désactivé),
  - le secret partagé utilisé pour garantir l'intégrité et l'authenticité des réponses aux demandes de validation,
  - le compteur de demandes (anti-rejeu),
  - pour le mode fonctionnement avec code personnel :
    - le nombre maximum d'essais autorisés,
    - le nombre d'essais courant,
    - l'état (verrouillé ou pas),
- Le code personnel de l'utilisateur (intégrité et confidentialité).

5. Description des menaces

5.1. Menaces

M_FALSI-VALID : Falsification des demandes/réponses de validation

Une personne pourrait intercepter et falsifier les demandes de validation transmises à la Cardlet et/ou leur réponse afin de rejouer une réponse valide ou de forger de fausses réponses pour mystifier l'entité distante à l'origine de ces demandes.

M_UTIL-NAUTO : Utilisation non autorisée de la Cardlet

Suite au vol de l'équipement de téléphonie mobile, une personne non autorisée pourrait tenter d'utiliser la Cardlet à l'insu de l'utilisateur pour valider des demandes d'authentification/validation auprès d'un service applicatif tiers auprès duquel elle se ferait passer pour l'utilisateur légitime.

M_ACC-PC-NAUTO : Accès non autorisé au code personnel

Une personne pourrait récupérer (application malveillante au niveau de l'équipement de téléphonie mobile, par exemple) le code personnel de l'utilisateur, pour ensuite s'en resservir à ses propres fins après avoir volé l'équipement de téléphonie mobile.

M_MOD-CONF-NAUTO : Modification non autorisée de la configuration de la Cardlet

Une personne pourrait modifier la configuration de la Cardlet (Application malveillante au niveau de l'équipement de téléphonie mobile, par exemple) pour ensuite s'en resservir à ses propres fins (attaque en force brute du code personnel) après avoir volé l'équipement de téléphonie mobile.

5.2. Menaces/Modes de fonctionnement

Le tableau ci-dessous donne pour les 2 modes de fonctionnement possibles de la Cardlet, les menaces couvertes.

Menace	LoA 2 (Click OK)	LoA 3 (Code Personnel)
M_FALSI-VALID	Oui	Oui
M_UTIL-NAUTO	Non	Oui
M_ACC-PC-NAUTO	Sans objet	Oui
M_MOD-CONF-NAUTO	Sans objet	Oui

Tableau n°3 : Relation menaces/modes de fonctionnement

Note : Le mode « Click OK » doit être réservé aux opérations les moins sensibles, voire en second niveau de validation.

6. Description des fonctions de sécurité

Les fonctions de sécurité mises en œuvre dans la Cardlet sont les suivantes :

F_CREAT-PC : Création du code personnel

Cette fonction de sécurité permet à l'utilisateur de définir son code personnel lors des opérations de personnalisation de la Cardlet ou suite à une demande de réinitialisation du code personnel.

Elle s'effectue via une double saisie (combinaison de 4 chiffres, différente d'une suite de 4 chiffres identiques).

Elle intègre une détection d'inactivité (30 secondes) qui déclenche l'abandon de l'opération sur time-out.

Elle s'appuie sur le STK (SIM ToolKit) de la carte SIM de l'équipement de téléphonie mobile.

F_ENTRE-PC : Saisie du code personnel

Cette fonction de sécurité permet à l'utilisateur de saisir son code personnel avant chaque demande de validation nécessitant la saisie du code personnel (Cf. § 2.3.2 Mode « Code personnel » ou authentification).

Elle bloque l'accès à la fonctionnalité de validation LoA3 (validation avec code personnel) de la Cardlet, tant que l'utilisateur n'a pas saisi un code correct, correspondant à celui qu'il a défini (Cf. F_CREAT-PC).

Elle intègre une détection d'inactivité (30 secondes) qui déclenche l'abandon de la demande de validation sur time-out.

Elle s'appuie sur le STK (SIM ToolKit) de la carte SIM de l'équipement de téléphonie mobile.

F_BLOC-PC : Blocage du code personnel

Cette fonction de sécurité bloque la fonctionnalité de validation LoA3 (validation avec code personnel) de la Cardlet, suite au dépassement du nombre maximum de tentatives infructueuses défini, lors de la saisie du code personnel de l'utilisateur. Le nombre maximum d'essais est de 3 par défaut, mais peut être ajusté entre 1 et 15 lors de la phase de configuration de la Cardlet. Seule une demande de déblocage ou de réinitialisation du code personnel permet alors de débloquer la fonctionnalité de validation LoA3 de la Cardlet.

F_STOCK-PC : Stockage du code personnel

Cette fonction de sécurité assure le stockage du code personnel de l'utilisateur via la JCVM de la carte SIM.

Les mécanismes de sécurité de la carte SIM assurent sa protection contre un accès non autorisé.

F_STOCK-CONF : Stockage de la configuration de la Cardlet

Cette fonction de sécurité assure le stockage de la configuration de Cardlet via la JCVM de la carte SIM.

Les mécanismes de sécurité de la carte SIM assurent sa protection contre un accès non autorisé.

F_REP-VALID : Réponse à une demande de validation

Cette fonction de sécurité est appelée lors de l'envoi de la réponse de l'utilisateur (acceptation ou refus) suite à une demande de validation, par « click OK » ou « code personnel ».

Elle génère un HOTP (HMAC-Based One-Time Password) en utilisant les mécanismes cryptographiques de la carte SIM.

Ce HOTP est construit à partir des informations contenues dans la demande, de celles contenues dans la réponse associée et du secret partagé associé au mode de fonctionnement utilisé (« click OK » ou « code personnel »).

Le format de l'HOTP est conforme aux spécifications RFC 6287 :

OCRA (OATH Challenge-Response Algorithm) SHA1 – 8.

7. Couverture des menaces

La matrice ci-dessous donne la couverture des menaces identifiées au chapitre 5 par les fonctions de sécurité de la Cardlet décrites au chapitre 6 renforcées par les hypothèses de sécurité sur l'environnement posées au § 3.5.

	M_FALSI-VALID	M_UTIL-NAUTO	M_ACC-PC-NAUTO	M_MOD-CONF-NAUTO
F_CREAT-PC		X		
F_ENTRE-PC		X		
F_BLOC-PC		X		
F_STOCK-PC		X	X	
F_STOCK-CONF	X			X
F_REP-VALID	X			
H_MOBILE		X	X	X
H_SIM	X	X	X	X
H_INSTAL	X		X	X
H_CANAL	X			X
H_QUAL-SECRET	X			
H_IMP-SECRET	X			
H_DEBLOC-PC		X		X

Tableau n°4 : Couverture des menaces

La fonction de sécurité « **F_CREAT-PC** » protège contre les erreurs de saisie (double saisie) lors de la création ou de la réinitialisation du code personnel de l'utilisateur et interdit certains codes trop simples (exemple : 0000), réduisant le risque d'une utilisation non autorisée de la Cardlet.

La fonction de sécurité « **F_ENTRE-PC** » bloque l'accès à la fonctionnalité de validation de la Cardlet en l'absence de saisie d'un code correct, empêchant ainsi une utilisation non autorisée de la Cardlet.

La fonction de sécurité « **F_BLOC-PC** » verrouille automatiquement la fonctionnalité de validation de la Cardlet, suite au dépassement du nombre maximum de tentatives infructueuses défini lors de la saisie du code personnel, empêchant ainsi une utilisation non autorisée de la Cardlet.

La fonction de sécurité « **F_STOCK-PC** » garantit la protection du code personnel lors de son stockage, empêchant ainsi une utilisation non autorisée de la Cardlet.

La fonction de sécurité « **F_STOCK-CONF** » garantit la protection de la configuration de la Cardlet (Cf. § 4.2) lors de son stockage, empêchant ainsi une modification non autorisée de la Cardlet.

La fonction de sécurité « **F_REP-VALID** » garantit l'intégrité et l'authenticité de la réponse retournée par la Cardlet (indirectement par l'utilisateur) suite à une demande, empêchant ainsi une falsification ou un rejeu de cette réponse.

Les hypothèses « **H_CANAL** », « **H_QUAL-SECRET** », « **H_IMP-SECRET** » et « **H_SIM** » viennent renforcer la garantie de l'authenticité de la réponse apportée par la fonction de sécurité « F_REP-VALID » en assurant respectivement :

- la protection en confidentialité et en intégrité de toutes les commandes transmises à la Cardlet,
- l'utilisation d'un secret de qualité pour la fonction de sécurité « F_REP-VALID »,
- la fourniture à la Cardlet de ce dit secret via des moyens sûrs,
- la protection d'accès aux secrets par les mécanismes de sécurité de la carte SIM.

L'hypothèse « **H_INSTAL** » garantit d'une part, que la Cardlet est intègre et qu'elle est correctement installée dans l'ISD de la carte SIM et d'autre part, que ses biens sensibles seront ainsi protégés contre un accès non autorisé, par les mécanismes de sécurité intrinsèques de la carte SIM.

Les hypothèses « **H_MOBILE** » et « **H_SIM** » sont des prérequis pour la mise en œuvre sûre des fonctions de sécurité et la protection des biens sensibles.

L'hypothèse « **H_DEBLOC-PC** » est une recommandation pour le service distant afin d'éviter d'effectuer le déblocage ou la réinitialisation du code personnel de la Cardlet détenue par une personne non autorisée, suite à un vol ou une perte de la carte SIM.

8. Périmètre d'évaluation

L'évaluation porte sur la Cardlet (MC23 FR) destinée aux cartes SIM 3GPP R6.

La plate-forme d'évaluation est constituée de :

- 1 téléphone mobile Apple iPhone 6S,
- 1 carte SIM Gemalto NFC N9 - Profil 162 Orange.

La carte SIM Gemalto N9 est une SIM NFC V2 G1 évaluée EAL4+.

Cible de sécurité :

http://www.ssi.gouv.fr/uploads/IMG/certificat/ANSSI-CC-cible_2012-48en.pdf

Rapport de certification :

http://www.ssi.gouv.fr/uploads/IMG/certificat/ANSSI-CC_2012-48fr.pdf