Architect of an Open World™

Cible de Sécurité CSPN

# Cible de sécurité CSPN - CRYPT2Protect

Date du document : 30 mars 2012

Référence du document : C2P/LP59035/FR

Version : 1.4

# Mises à jour

| Date | N° Ver. | Auteur | Motif révision | Parties Modifiées |
|---|---|---|---|---|
| 10/06/11 | 0.1 | JLC | Création du document | Toutes |
| 20/06/11 | 0.2 | JLC | Relecture interne | Toutes |
| 22/06/11 | 0.3 | JLC | Préparation réunion de lancement | Toutes |
| 28/06/11 | '1.0 | JLC | Prise en compte des remarques de la réunion de lancement | Toutes |
| 06/07/11 | '1.1 | JLC | Prise en compte des remarques de l'ANSSI | §2.1.1,§2.4, |
| 26/10/11 | '1.2 | JLC | Version du firmware.<br>Le niveau de sécurité de CHR n'est pas une hypothèse mais est précisé dans le périmètre de l'évaluation,<br>Les options MULTI_C et FULL_IP peuvent être activées. | §1.2<br>§2.4, §2.7<br><br><br><br>§2.7, §3 |
| 20/01/12 | '1.3 | JLC | Version du firmware.<br>Support des courbes brainpool et ANSSI<br>Option SAM_Manage renommée SEC_CHAN, et intègre les cartes MIFARE AES<br>L'option ENCRYPT peut aussi être activée pour le Centre de Gestion des Clés<br>Ajout de la commande de déchiffrement dans l'option SEC_CHAN | §1.2, §3<br>§2.1.1<br><br>§2.1.1, §2.7, §3<br><br><br>§2.7, §3<br><br><br>§2.1.1, §2.7, §4.3 |
| 30/03/12 | '1.4 | JLC | Version du firmware | §1.2, §3 |

# Table des Matières



# Index des Figures

# 1 Synthèse

## 1.1 Identification de la cible de sécurité

Cette cible de sécurité a été élaborée en vue d'une évaluation CSPN.

## 1.2 Identification du produit

| Catégorie | Identification |
|---|---|
| Organisation éditrice | Bull S.A.S. |
| Lien vers l'organisation | http://www.bull.com/ |
| Nom commercial du produit | CRYPT2Protect HR |
| Numéro de version évaluée | 8.04-03I |
| Catégorie du produit | Logiciel embarqué dans une enceinte cryptographique |

Références

| Code | Référence | Nom |
|---|---|---|
| CSPN | N°915/SGDN/DCSSI/SDR du 25 avril 2008 | Certification de sécurité de premier niveau des technologies de l'information. |
| PKCS11 | PKCS#11 v2.20 | Cryptographic Token Interface Standard<br>RSA Laboratories<br>28 June 2004 |
| IAS-ECC | IAS ECC, revision 1.01 | European Card for e-Services and National e-ID applications – Technical Specifications |
| ANSI X9.62 | ANSI X9.62 (2005) | Public Key Cryptography for the Financial Services Industry<br>The Elliptic Curve Digital Signature Algorithm (ECDSA)<br>November 16, 2005<br>American National Standards Institute |

.

# 2 Argumentaire (description) du produit

## 2.1 Description générale du produit

### 2.1.1 Présentation

Le produit **CRYPT2Protect HR** est une enceinte cryptographique autonome (Hardware Security Module - HSM) qui offre ses services cryptographiques à un serveur ou a un réseau complet (LAN) via TCP/IP pour effectuer la cryptographie symétrique et asymétrique. Toutes les données critiques de sécurité sont manipulées uniquement dans l'enceinte sécurisée du HSM et ne sont jamais exposées dans l'environnement non sécurisé des serveurs, pour en garantir la non compromission.

Le produit **CRYPT2Protect HR** est composé d'une enceinte cryptographique **CHR** dans laquelle est embarquée le logiciel **CRYPT2Protect**.

**CRYPT2Protect** est utilisé pour fournir des services cryptographiques pour le chiffrement de données, l'intégrité de messages, l'authentification d'utilisateurs ou de données, le stockage sécurisé des clés et des informations de sécurité, la signature, à des applications de gestion de titres électroniques sécurisées, des applications de eServices ou des applications d'infrastructures de gestion de clés publiques (IGC).

Le boîtier sécurisé "Tamper Resistant" **CHR** dispose de circuits de détection d'attaques qui provoquent l'effacement des données critiques de sécurité en cas d'alerte.

**CRYPT2Protect HR** dispose de deux connexions Ethernet pour la connexion sur un réseau local avec

- le serveur applicatif, qui se connecte sur un port TCP/IP configuré pour accéder aux services cryptographiques de **CRYPT2Protect**,
- le poste d'administration, équipé d'un navigateur, nécessaire uniquement pour des opérations ponctuelles d'initialisation et de configuration de **CRYPT2Protect**.

Des listes d'accès sont configurées par les administrateurs pour contrôler l'accès réseau aux services de **CRYPT2Protect** aux seuls serveurs applicatifs et postes d'administration autorisés.

Les connexions vers les services de **CRYPT2Protect** sont sécurisée en SSL, avec authentification mutuelle entre **CRYPT2Protect** agissant en tant que serveur et l'application ou l'utilisateur agissant en tant que client.

Les services cryptographiques offerts par **CRYPT2Protect** sont activés ou désactivés par un mécanisme d'options permettant de contrôler les fonctions disponibles pour l'application cliente :

- Fonctions de cryptographie générique (mécanismes PKCS#11),
- Fonctions de cryptographie dédiées à un cas d'utilisation particulier (par exemple gestion des transactions avec une carte e-Services)
- Fonctions de gestion des clés statiques

Ce mécanisme d'options permet de cloisonner les utilisations du produit : L'ensemble des options activées permet de limiter les fonctions disponibles aux seules fonctions utiles pour la production.

Les services cryptographiques offerts par CRYPT2Protect sont les suivants :

| Option | Services Cryptographiques | Algorithmes |
|---|---|---|
| BASIC | Génération de bi-clés asymétriques | RSA de 896 à 4098 bits par pas de 64 bits.<br>ECDSA : courbes nommées définies dans la table B1 de [ANSI X9.62], dans le RFC5639 (Brainpool) et dans le journal officiel 0241 du 16/10/2011 |
| | Signature et vérification de signature | RSA avec SHA-1 et SHA-256<br>ECDSA |
| | Génération de clé secrète | DES (64, 128 et 192 bits)<br>AES (128, 192 et 256 bits) |
| | Scellement de messages et vérification de sceaux | MAC ISO9797-1 algorithmes 1 et 3<br>CMAC |
| ENCRYPT | Chiffrement / déchiffrement par des clés secrètes | Mode ECB; CBC et CBC_PAD |
| PKCS11 | Dérivation de clés | Mécanismes définis dans [PKCS11] :<br>CONCATENATE_BASE_AND_KEY<br>XOR_BASE_AND_DATA<br>EXTRACT_KEY_FROM_KEY<br>CONCATENATE_BASE_AND_DATA<br>CONCATENATE_DATA_AND_BASE<br>ECB_DES3_ENCRYPT_DATA<br>ECB_AES_ENCRYPT_DATA<br>CBC_DES3_ENCRYPT_DATA<br>CBC_AES_ENCRYPT_DATA<br>SHA1_KEY_DERIVE<br>SHA256_KEY_DERIVE |
| | Import/export de clés secrètes et de clés RSA par des clés secrètes | Mode ECB; CBC et CBC_PAD |

| Option | Services Cryptographiques | Algorithmes |
|---|---|---|
| | Import/export de clés secrètes par des clés RSA | RSA |
| SECure_CHANnel | Gestion de canaux sécurisés avec des cartes IAS, Global Platform ou MIFARE<br>• Établissement des clés de canal sécurisé | Algorithmes [IAS-ECC] et Global Platform SCP 02 |
| | • Chiffrement des données vers la carte<br>• Déchiffrement de la réponse de la carte | DES3, AES |
| CGDC | Fonctions de gestion des clés | |

Les fonctions de gestion des clés permettent d'introduire les clés dans le système et de définir leur attributs, sous le contrôle mutuel de plusieurs porteurs de secrets :

- Identifiant unique de la clé dans le système,
- Type et usage de la clé, pour limiter l'usage de la clé aux seules fonctions autorisées,
- Dates de validité, pour définir la période d'utilisation de la clé,
- Identifiant de groupe, pour limiter l'utilisation de la clé aux seules applications authentifiées autorisées.

## 2.2 Description de l'environnement d'utilisation prévu

Le schéma suivant présente l'environnement d'utilisation du produit pour :

- La fourniture de services cryptographiques à un serveur applicatif,
- L'administration du **CRYPT2Protect HR** à partir d'un poste d'administration
- La gestion des clés sur le Centre de Gestion des Clés (CGDCng)

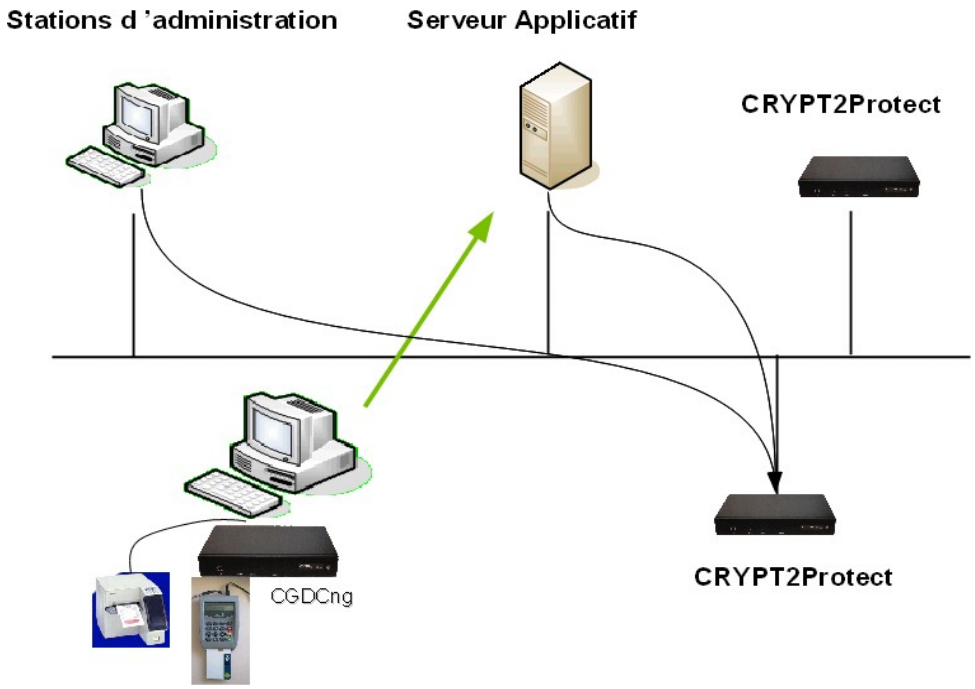


*Figure 1 Diagramme de connexion de CRYPT2Protect HR*

### 2.2.1 Accès aux services cryptographiques

L'application cliente établit une connexion réseau vers le service cryptographique de **CRYPT2Protect** et s'authentifie pour pouvoir utiliser les clés auxquelles elle a accès. L'application envoie des requêtes suivant un protocole spécifique au produit. Chaque requête, formatée en TLV (Type Longueur Valeur) fait l'objet d'une réponse, également formatée en TLV, de la part de **CRYPT2Protect**.

Pour permettre une montée en charge de la production, plusieurs HSM **CRYPT2Protect HR** peuvent être raccordées sur un segment Ethernet.

Le serveur applicatif peut ainsi :

- répartir la charge sur plusieurs HSMs,
- gérer les défaillances ou les mises en sécurité éventuelles d'un équipement.

Diverses API sont proposées pour permettre aux éditeurs et aux intégrateurs de logiciels d'intégrer aisément la cryptographie à leur application en gérant tout ou partie du protocole d'échange avec **CRYPT2Protect**. Le portefeuille comprend une implémentation d'une API Java et une API PKCS#11. Des extensions de l'API PKCS#11 permettent d'accéder à toutes les fonctions cryptographiques de haut niveau offertes par **CRYPT2Protect** en plus des fonctions standard PKCS#11.

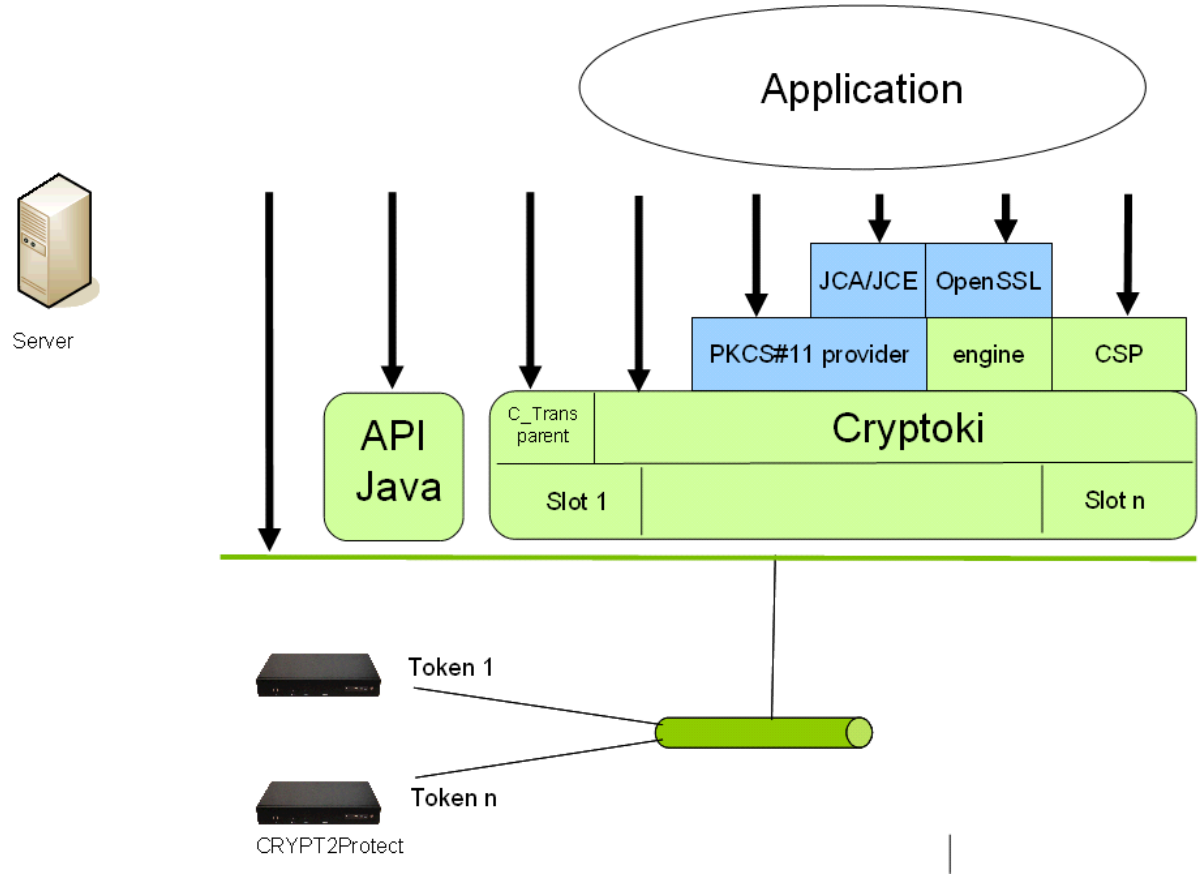


*Figure 2 : Services cryptographiques de CRYPT2Protect*

L'interface cryptoki (PKCS#11) peut être utilisée directement par l'application, ou peut être accédée au travers d'interfaces de niveau supérieur :

- Un fournisseur PKCS#11 (PKCS#11 Provider) permet à une application Java d'accéder aux services de l'API PKCS#11
- Le fournisseur PKCS#11 peut lui-même être utilisé par un fournisseur JCA/JCE pour offrir une interface standard JCA/JCE à l'application.
- Bull fournit un moteur (engine) pour connecter les commandes OpenSSL à l'API PKCS#11 pour les opérations de cryptographie RSA et de Génération de nombres aléatoires.
- Bull fournit un CSP (Cryptographic Service Provider) offrant une interface MS CAPI (Microsoft Cryptographic API).

### 2.2.2 Accès à l'administration

L'application d'administration de **CRYPT2Protect** est accessible à partir d'un navigateur en se connectant sur le serveur WEB intégré de **CRYPT2Protect.**

La connexion au serveur d'administration peut être sécurisée en SSL (obligatoire pour les accès distants, en dehors du sous réseau local).

Les administrateurs sont authentifiés par **CRYPT2Protect**.

L'application d'administration fournit des informations sur l'état du HSM **CRYPT2Protect** :

- État des applications et options chargées
- État du système (interfaces réseau, processus, occupation de la mémoire)
- Statistiques concernant les vérifications de code
- Utilisateurs définis
- Configuration de la sécurité réseau.

Les principales fonctions offertes par le service d'administration sont les suivantes :

- Visualisation des versions logicielles des logiciels chargés dans **CRYPT2Protect HR**,
- Chargement de nouvelles versions de logiciel ou de nouvelles options,
- Redémarrage (reboot) à distance de **CRYPT2Protect HR**,
- Configuration de la date et de l'heure.
- Configuration des couches réseau TCP/IP,
- Configuration du port série,
- Paramétrage et visualisation des traces des opérations d'administration et des commandes et réponses échangées avec le serveur applicatif.
- Vérification du KCV (Key Check Value) des clés chargées dans **CRYPT2Protect**.
- Gestion des administrateurs et de leur mot de passe.
- Gestion de la sécurité d'accès à **CRYPT2Protect** à partir du réseau : configuration des listes d'accès, gestion des clés et certificats SSL.

### 2.2.3 Le Centre de Gestion des Clés

Le Centre de Gestion et de Distribution des Clés (CGDCng) est utilisé pour préparer les magasins de clés des serveurs applicatifs cibles :

- Initialisation des clés de chiffrement des clés applicatives,
- Gestion des clés de confiance (TRUSTED) pour le token PKSC#11,
- Gestion des clés maîtres mises en œuvre dans les services dédiés à un cas d'utilisation particulier, par exemple les clés maîtres des cartes IAS-ECC ou Global Platform.

Le Centre de Gestion des Clés (CGDCng) permet d'effectuer la gestion des clés et de leurs attributs dans le cadre de Cérémonies de Clés, indépendamment des systèmes de production. L' interface graphique de l'application CGDCng facilite le déroulement des Cérémonies de Clés. La gestion centralisée des clés sur le CGDCng permet de garantir un niveau de sécurité maximal, limite les coûts annexes et élimine les opérations de gestion des clés sur les serveurs de production. L'utilisation de cartes à puce offre la plus grande sécurité et la commodité pour une sauvegarde sécurisée, la valorisation et le transfert de clés cryptographiques. Le dispositif sécurisé d'introduction des clés est relié directement au HSM du CGDCng pour la saisie des codes PIN et des composantes clés, offrant un chemin de confiance pour l'introduction des secrets.

## 2.3 Description de l'utilisation du produit

### 2.3.1 Utilisation de CRYPT2Protect dans des infrastructures de Gestion de Clés publiques (IGC)

**CRYPT2Protect** offre des fonctions cryptographiques standard (PKCS#11) qui peuvent être utilisées par des Autorités de Certification dans une Infrastructure de Gestion de Clés publiques (IGC).

Les IGC sont des ensembles de composants, fonctions et procédures dédiés à la gestion de clés cryptographiques asymétriques et des certificats associés. Une IGC peut être composée d'un service de génération de certificats, d'un service d'enregistrement, d'un service de publication....

Une IGC peut utiliser le HSM **CRYPT2Protect HR** pour couvrir ses besoins de cryptographie, en particulier :

- génération de la paire de clés d'AC (Autorité de Certification) au cours du processus de Cérémonie de clés,
- stockage sécurisé et utilisation contrôlée des clés de l'AC,
- génération de bi-clés qui peuvent ensuite être chargées sur des cartes remises aux porteurs,
- Chiffrement des données secrètes : les clés, les données d'authentification (par exemple pour le séquestre et le recouvrement des paires de clés des utilisateurs)
- Génération de paires de clés utilisées pour le chiffrement, de certificats de logiciels et de composants d'infrastructure
- Signature de certificats électroniques, de CRLs et de jetons OCSP.

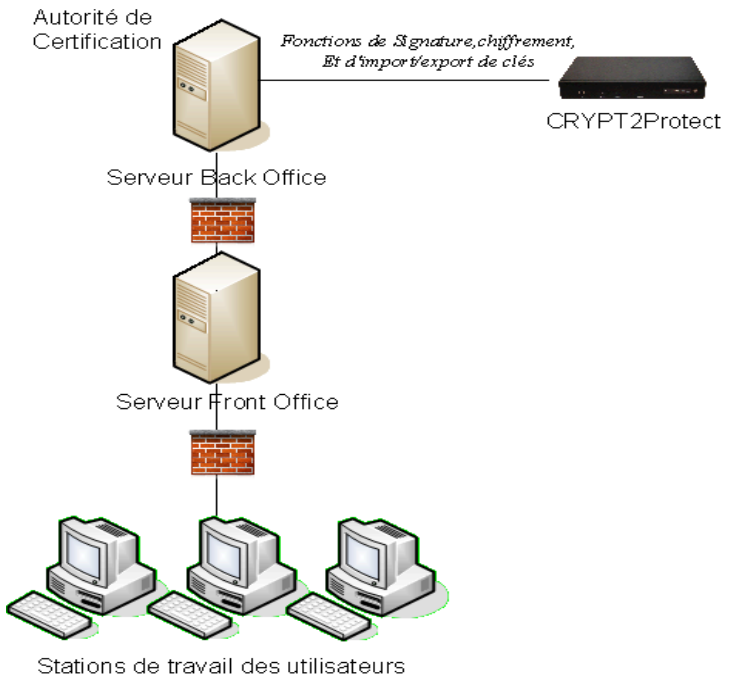


*Figure 3: Intégration de CRYPT2Protect dans une Autorité de Certification*

Une Autorité d'Horodatage (TSA - Time Stamping Authority) est une tierce partie fiable qui utilise également des fonctions de gestion de clés privées.

La TSA prend les mesures appropriées pour s'assurer que le temps est exact et fiable. La TSA associe l'empreinte des données (le hash) avec l'heure exacte de la signature électronique. Ceci est fait en utilisant la clé privée de la TSA (preuve de l'origine de l'horodatage).

La TSA utilise un HSM **CRYPT2Protect HR** pour confiner sa clé privée et signer le cachet d'horodatage.

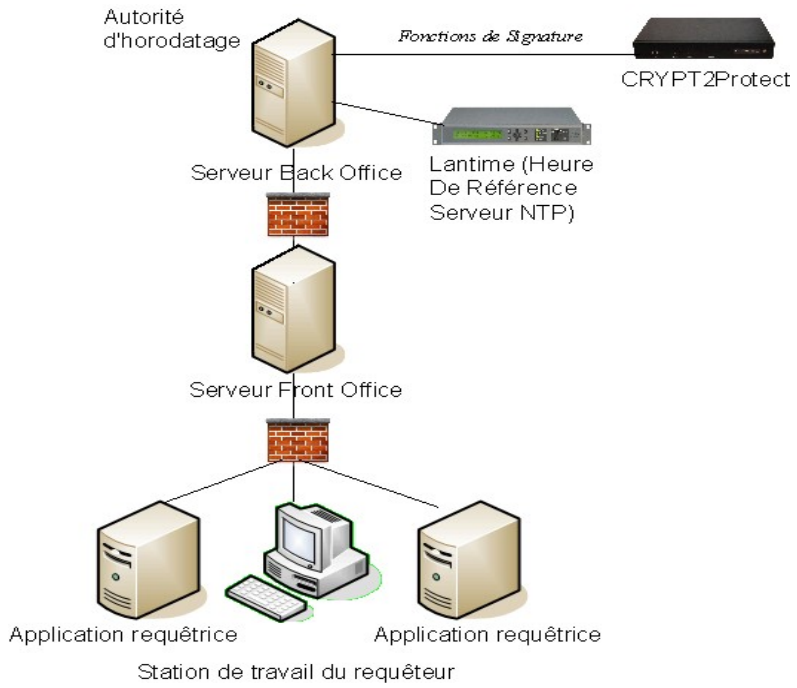


*Figure 4: Intégration de CRYPT2Protect par une autorité d'horodatage*

### 2.3.2 Intégration de CRYPT2Protect dans applications des cartes e-Services

La norme [IAS-ECC] (Identification-Authentification-Signature European-Citizen-Card) permet l'interopérabilité des cartes e-Services au niveau européen.

La fonctionnalité de Secure Messaging des cartes IAS-ECC permet la mise en place de fonctionnalités telles que :

- le déploiement à distance de données sensibles dans le domaine des IGC (Infrastructures de Gestion de Clés), comme par exemple le déploiement de clés privées et de certificats de chiffrement depuis une IGC jusqu'à la carte.
- l'administration à distance d'une carte IAS-ECC, dans le domaine des systèmes de gestion de cartes, comprenant par exemple,
  - le verrouillage / déverrouillage de fonctionnalités ou de données sur la carte,
  - le déblocage à distance du code PIN entre un système de gestion de cartes et la carte elle-même.
- la lecture et/ou l'écriture sur la carte de données privées du porteur, dans le cadre d'un fournisseur d'identités.

Les mécanismes de Secure Messaging IAS-ECC prévoient ainsi l'établissement d'un canal sécurisé avec la carte. Les clés de sessions établies pour le canal sécurisé permettent de protéger les données échangées avec la carte en intégrité et en confidentialité, les données sensibles ne devant pas être exposées en clair en dehors de l'enceinte sécurisée d'un HSM.

La figure 5, ci-dessous, présente une architecture type où un tiers de confiance (Serveur d'intermédiation) met en relation le porteur d'une carte avec un fournisseur de service en ligne.
Dans cette architecture, les composants « serveur d'authentification » et « serveur d'attributs » supportent les interfaces hautes exposées vers des fournisseurs de services souhaitant exploiter les cartes pour réaliser différentes fonctions comme l'authentification ou la transmission de données stockées sur la carte ; ces deux composants peuvent intégrer des boitiers CRYPT2Protect pour signer et chiffrer les assertions SAML et les données transmises au fournisseur de service.
Le composant « serveur 'dialogue carte' », lui, prend en charge les communications effectives avec les cartes en mode Secure Messaging. Ce protocole peut être implanté dans le serveur en utilisant les fonctions du boitier **CRYPT2Protect** permettant l'établissement de clés de canal sécurisé ainsi que leur utilisation.

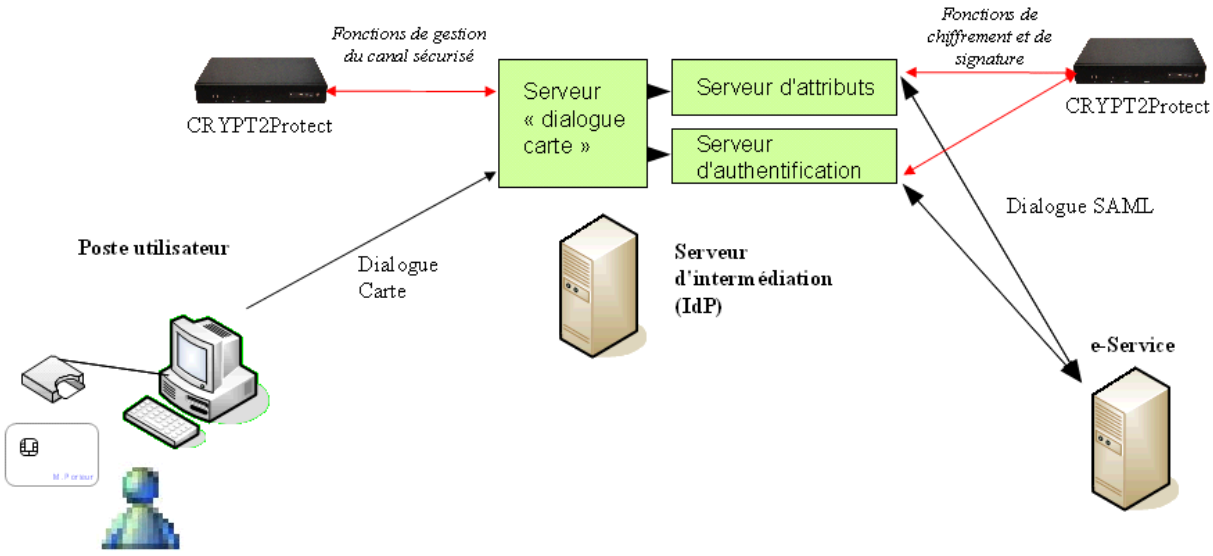


*Figure 5 : Intégration de CRYPT2Protect dans les solutions d'utilisation des cartes IAS-EC*

**Note** : en outre, **CRYPT2Protect** supporte aussi les protocoles GlobalPlatform SCP02 et MIFARE AES assurant ainsi la sécurisation des transferts de données sur les chaines de personnalisation de cartes à puce ou sans contact.

## 2.4 Description des hypothèses sur l'environnement

Il est considéré pour l'évaluation que les administrateurs sont de confiance.

Il est considéré pour l'évaluation que l'accès physique aux équipements techniques composant la plate forme cible ainsi que les consoles d'administration est contrôlé de manière à prévenir toute altération par ce biais. Les administrateurs systèmes en charge du maintien en condition opérationnelle des serveurs et des CRYPT2Protect sont sensibilisés à la SSI, compétents et de confiance.

Il est considéré pour l'évaluation que les applications clientes de CRYPT2Protect sont sûres. Ces applications doivent effectuer les contrôles nécessaires sur les données envoyées à CRYPT2Protect. Elles doivent également authentifier de façon robuste les personnes qui s'y connectent et leur donner les bons droits d'accès.

## 2.5 Description de dépendances

### 2.5.1 Réseau

En matière d'environnement réseau, le boitier **CRYPT2Protect HR** doit disposer d'un lien physique pour les flux applicatifs (service crypto) et les flux d'administration (service http). Il doit :

- être accessible par les serveurs en liste blanche sur le port crypto (2001/tcp) ou cryptos (3001/tcp).
- Être accessible par les postes d'administration en liste blanche sur le port http (80/tcp) ou https (443/tcp).

A l'exception de ces besoins, tous les autres ports d'accès TCP/IP peuvent être fermés ce qui par là même va permettre de limiter les risques d'intrusion sur la plate forme.

### 2.5.2 Bibliothèques d'interface

Si l'application utilise la bibliothèque PKCS#11 pour accéder aux services cryptographiques de **CRYPT2Protect**, cette bibliothèque doit être installée sur le serveur.

La bibliothèque PKCS#11 fournie par Bull est compatible avec les environnements suivants :

- Microsoft Windows (32 ou 64 bits)
- Linux (32 ou 64 bits)

### 2.5.3 Gestion des clés

Une cérémonie de personnalisation client des HSM **CRYPT2Protect HR** doit être réalisée avant leur mise en production. Cette cérémonie permet l'introduction de la clé maitre dans la mémoire sécurisée et sauvegardée du boîtier. La clé maître est également partagée sur des cartes à puce détenues par des porteurs de secrets de confiance (au moins deux).

Une cérémonie d'initialisation des clés de stockage doit être réalisée sur le Centre de Gestion des Clés. Cette cérémonie permet l'initialisation de la base de clés du CGDCng :

- Génération de clés maîtres de stockage des arborescences des clés et partage de ces clés sur cartes à puce détenues par des porteurs de confiance (au moins trois)
- Génération éventuelle et introduction dans cette base des clés maîtres des boîtiers **CRYPT2Protect HR** cibles,
- Génération des clés de stockage assurant la sécurité des magasins de clés et distribution de ces clés vers les serveurs cibles (chiffrées par les clés maîtres des boîtiers cibles).

### 2.5.4 Authentification des applications

Une cérémonie de clés doit être réalisées sur le Centre de Gestion des Clés pour préparer les objets de sécurité nécessaires au contrôle d'accès aux services de **CRYPT2Protect** et aux clés :

- Bi-clé RSA d'authentification de **CRYPT2Protect** (en tant que serveur SSL),
- Certificat serveur du boîtier et certificats auto-signés des autorités de certification de confiance,
- Liste blanche des applications autorisées, avec leurs droits d'accès (liste des groupes de clés).

Les clés, certificats et cartes à puce des applications clientes doivent également être préparés, sur le Centre de Gestion des Clés ou sur une autre IGC.

## 2.6 Description des utilisateurs typiques

Le présent paragraphe présente la liste des rôles qui interviennent dans la mise en place et l'utilisation de **CRYPT2Protect**. Certains utilisateurs peuvent assurer plusieurs rôles.

**Les administrateurs** de **CRYPT2Protect** assurent la gestion de l'ensemble des **CRYPT2Protect** gérés depuis un même centre de gestion des clés.

Les administrateurs **CRYPT2Protect** effectuent des opérations comportant la saisie et/ou le transfert de secrets (saisie de mot de passe). En particulier, ils ont pour rôle de :

- Configurer les interfaces réseau et les listes d'accès,
- Charger les objets de sécurisation des connexions préparés sur le Centre de Gestion des Clés,
- Charger les mises à jour de logiciel et les options (signées par Bull),

**Les opérateurs** de **CRYPT2Protect** assurent les opérations d'exploitation de **CRYPT2Protect**.

Les opérateurs **CRYPT2Protect** effectuent des opérations comportant la saisie et/ou le transfert de secrets (saisie de mot de passe). En particulier, ils ont pour rôle de :

- Redémarrer le boîtier,
- Consulter les journaux.

**Les porteurs de demi-secret** ont en charge la gestion des clés maître KM2bntx des **CRYPT2Protect** et de la clé maître KDKM de protection des clés dans la base de clés du Centre de Gestion des Clés

En particulier, ils ont pour rôle de garder le support cryptographique contenant les composantes de clés maître sous contrôle, ainsi que le code PIN associé.

**L'opérateur du CGDCng** a pour rôle l'assistance lors de la réalisation des opérations techniques à effectuer sur le centre de gestion des clés CGDCng. L'opérateur du CGDCng est authentifié (client SSL) par le **CRYPT2Protect** du Centre de Gestion des Clés.

**L'application cliente** utilise les services cryptographiques de **CRYPT2Protect** en mettant en œuvre les clés qui ont été préparées lors des cérémonies de clés sur le Centre de Gestion des Clés. L'application cliente est authentifiée (client SSL) par **CRYPT2Protect**

## 2.7 Description du périmètre de l'évaluation

Le périmètre d'évaluation est constitué du logiciel **CRYPT2Protect** embarqué dans l'enceinte cryptographique CHR et sur lequel sont activés les ensembles d'options permettant son utilisation dans le cadre des configurations évaluées suivantes :

- Infrastructures de Gestion de Clés publiques (IGC),
- Applications de cartes e-Services,
- Centre de Gestion des Clés (CGDCng).

L'enceinte cryptographique CHR a subi une analyse dans le cadre des évaluations MEPS pour le Groupement des Cartes Bancaires et FIPS pour le NIST (National Institute of Standards and Technology) et répond aux exigences des niveaux 3 et 3+EFT/EFP de ces évaluations respectives.

Configuration évaluée pour une Infrastructure de Gestion de Clés publiques ou une application de cartes e-Services :

| **Options pour la production** | **Services Cryptographiques** |
|---|---|
| BASIC | Signature et vérification de signature<br>Scellement de messages et vérification de sceaux |
| **pour une IGC** | |
| ENCRYPT | Chiffrement / déchiffrement par des clés secrètes |
| PKCS11 | Dérivation de clés<br>Import/export de clés |
| **pour une application e-Services** | |
| SECure_CHANnel | Gestion de canaux sécurisés avec des cartes IAS (ou Global Platform ou MIFARE)<br>• Établissement des clés de canal sécurisé<br>• Chiffrement des données vers la carte<br>• Déchiffrement des réponses de la carte |

Note : Les options MULTI_C et FULL_IP peuvent également être activées pour autoriser plusieurs connexions simultanées sur le service cryptographique et pour activer la gestion de la passerelle réseau par défaut.

Configuration évaluée pour le Centre de Gestion des Clés :

| Options pour le Centre de Gestion des Clés | Services Cryptographiques |
|---|---|
| BASIC | Signature et vérification de signature<br>Scellement de messages et vérification de sceaux |
| CGDC | Commandes de génération, importation/exportation, sortie/introduction par composantes des clés statiques. |
| ENCRYPT | Chiffrement / déchiffrement par des clés secrètes |
| PKCS11 | Dérivation de clés<br>Import/export de clés |

# 3 Description de l'environnement technique de fonctionnement

Le produit **CRYPT2Protect** offre deux services au travers de deux interfaces Ethernet :

- Service cryptographique pour l'application cliente,
- Service d'administration au travers d'un navigateur.

L'environnement réseau est défini au §2.5.1. « Réseau »

Des bibliothèques d'interface peuvent être utilisées par les applications (Voir les §2.2.1 « Accès aux services cryptographiques » et §2.5.2 « Bibliothèques d'interface »).

Un PIN PAD peut être connecté sur le port série en face avant du boîtier pour les opérations de personnalisation et pour les cérémonies de clés (XiMax avec application XiPass 2.4 de Xiring).

Une imprimante peut être connectée sur le port série en face arrière pour l'impression des demi-secrets lors des opérations de cérémonie de clés (Imprimante EPSON TMJ7000).

CRYPT2Protect est évaluée dans l'architecture suivante :

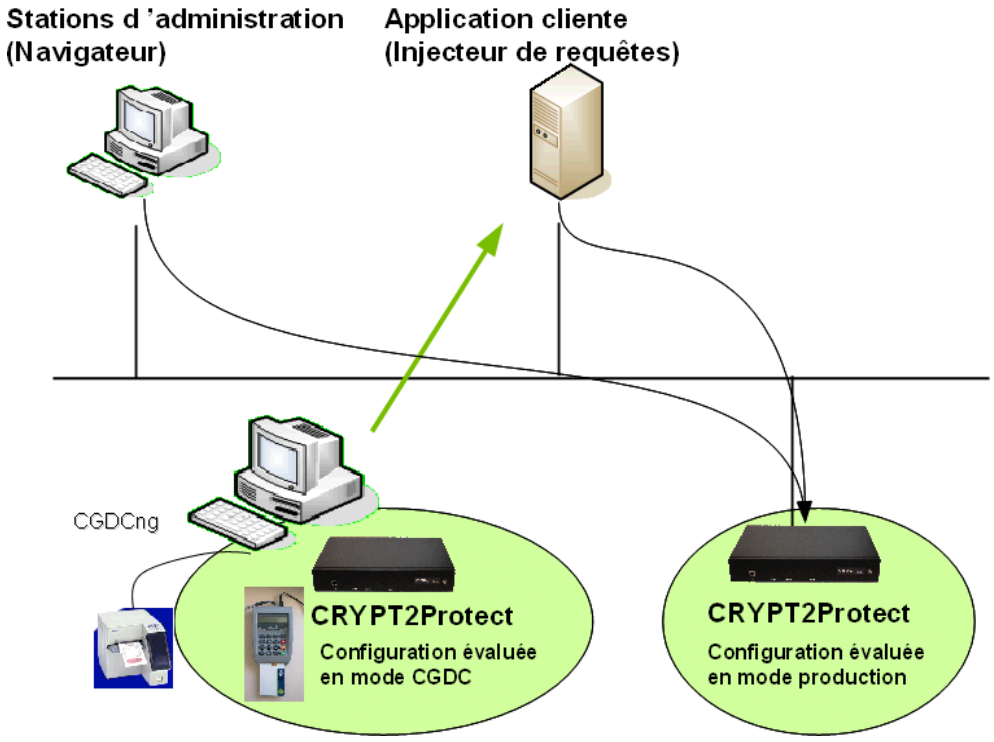


*Figure 6 : Architecture d'évaluation*

**La configuration évaluée en mode CGDC** est composée du firmware CRYPT2Protect V8.04-03I avec les options BASIC, CGDC, ENCRYPT et PKCS11 actives. Un PIN PAD XiMax est utilisé pour l'introduction des secrets.

L'application CGDCng version 4.7.1 est utilisée pour activer les services cryptographiques du CRYPT2protect et préparer les environnements de clés nécessaires à l'évaluation de la configuration de production.

**La configuration évaluée en mode production** est composée du firmware CRYPT2Protect V8.04-03I avec les options BASIC, ENCRYPT, PKCS11 et SECure_CHANnel actives.

Les options MULTI_C et FULL_IP peuvent également être activées pour autoriser plusieurs connexions simultanées sur le service cryptographique et pour activer la gestion de la passerelle réseau par défaut.

Un navigateur WEB est utilisé pour accéder aux services d'administration du boîtier.

Une application cliente soumet des requêtes cryptographiques au boitier CRYPT2Protect en utilisant les jetons de clés préparés sur le CGDCng. La connexion entre l'application cliente et le boitier est sécurisée en SSL (les clés et certificats nécessaires sont préparés sur le CGDCng).

# 4 Description des biens sensibles que le produit doit protéger

## 4.1 Description des biens sensibles

Le tableau suivant présente la liste des biens sensibles principaux :

| Bien sensible | Description |
|---|---|
| CLE_APP_PRI | Clé privée d'une application (Clé d'Autorité de certification,...) |
| CLE_APP_SEC | Clé secrète d'une application (Clé Maitre émetteur d'une carte IAS-ECC...) |

Pour assurer la protection des biens sensibles principaux, des objets de sécurité intermédiaires sont gérés par **CRYPT2Protect** :

| Bien sensible | Description |
|---|---|
| KM2bntx | Clé Maître de **CRYPT2Protect**, introduite dans le boîtier lors de la personnalisation. |
| KDKM | Clé Maître de stockage des clés sur le Centre de Gestion des Clés |
| KC2P | Bi-Clé RSA d'authentification de **CRYPT2Protect** pour l'authentification mutuelle avec les applications clientes.<br>Le jeton sécurisé sous la clé KM2bntx est préparé sur le Centre de Gestion des Clés et chargé dans le boîtier cible par l'administrateur. |
| USER | Élément de la liste blanche des applications autorisées à accéder aux services de **CRYPT2Protect**.<br>Le jeton sécurisé sous la clé KM2bntx est préparé sur le Centre de Gestion des Clés et chargé dans le boîtier cible par l'administrateur. |

## 4.2 Description des menaces

Les menaces directes sur les biens sensibles principaux sont les suivantes :

| Menace | Description | Bien sensible |
|---|---|---|
| MD_DIVUL | Divulgation de la valeur d'une clé secrète ou privée | CLE_APP_PRI, CLE_APP_SEC |
| MD_DETOUR | Détournement de l'utilisation d'une clé | CLE_APP_PRI, CLE_APP_SEC |
| MD_AUTO | Utilisation d'une clé par une entité non autorisée | CLE_APP_PRI, CLE_APP_SEC |

Les menaces indirectes sur les biens sensibles sont les suivantes :

| Menace | Description | Bien sensible |
|---|---|---|
| MI_INTRO | Introduction d'une clé dans le système | |
| MI_MOD_ACC | Modification de la configuration des listes d'accès réseau | |
| MI_COM_KM | Compromission de la clé maître du boîtier | KM2bntx |
| MI_MOD_ATT | Modification des attributs des clés | CLE_APP_PRI, CLE_APP_SEC |
| MI_MOD_FIRM | Modification du logiciel embarqué pour y introduire des fonctions malveillantes | |
| MI_MOD_OPT | Activation de fonctions non autorisées dans la configuration évaluée | |

## 4.3 Description des fonctions de sécurité du produit

Le tableau suivant précise les fonctions de sécurité internes aux produit et mises en place pour contrer les menaces.

| Fonction | Description | Menace |
|---|---|---|
| F_AUT_ADM | Authentification des administrateurs | M_MOD_ACC<br>M_MOD_FIRM<br>M_MOD_OPT |
| F_AUT_OPE | Authentification des opérateurs | |
| F_AUT_APP | Authentification des applications clientes | MD_AUTO |
| F_PERSO | Personnalisation du boitier (introduction de la clé maitre sous dual control) | MI_COM_KM |
| F_JETONS | Protection des jetons de clés (confidentialité et intégrité) | MI_MOD_ATT |
| F_SIG_FIRM | Signature des logiciels embarqués et chargement par l'administrateur authentifié. | MI_MOD_FIRM |
| F_SIG_OPT | Signature des fichiers d'option (contrôle des services offerts et en particulier désactivation des fonctions de gestion des clés sur le HSM de production) et chargement par l'administrateur authentifié. | MI_MOD_OPT |
| F_TYPE | Typage des clés (cloisonnement des clés entre les différents configurations évaluées) | MD_DETOUR |
| F_GID | Contrôle d'accès aux clés (liés à l'authentification) | MD_AUTO |

| Fonction | Description | Menace |
|---|---|---|
| F_USAGE | Contrôle de l'usage des clés (et en particulier clés CKA_TRUSTED seulement sur le CGDCng) | MD_DETOUR |
| F_CONT_MUT | Gestion des clés sous contrôle mutuel sur le Centre de Gestion des Clés (introduction des secrets KDKM) avec des privilèges (droit d'exporter les clés quel que soit les attributs PKCS#11) | MD_DIVUL<br>MD_DETOUR |
| F_AUT_OPC | Authentification de l'opérateur du CGDCng par le boîtier **CRYPT2Protect** du CGDCng | MI_INTRO |
| F_ACC_LIST | Définition des listes d'accès au travers de l'administration (services TCP ouverts en fonction des adresses appelantes). | M_MOD_ACC |

Le tableau suivant précise les fonctions de sécurité offertes aux applications clientes :

| Fonction | Description |
|---|---|
| FC_GenKeyPair | Génération de bi-clés d'autorité de certification ou d'utilisateur |
| FC_GenKey | Génération de clé secrète |
| FC_Sign | Signature de certificats électroniques, de CRLs, de jetons OCSP, de contremarques de temps...<br>Calcul de sceau avec une clé secrète |
| FC_Verify | Vérification de signature<br>Vérification de sceau avec une clé secrète |
| FC_Encrypt | Chiffrement de données |
| FC_Decrypt | Déchiffrement de données. |
| FC_Derive | Dérivation de clé. |
| FC_Wrap | Exportation de clé chiffrée |
| FC_Unwrap | Importation de clé chiffrée. |
| FC_SC_Key | Établissement de clé de canal sécurisé IAS-ECC, MIFARE AES ou SCP02 |
| FC_SC_Enc | Chiffrement de données dans un canal sécurisé. |
| FC_SC_Dec | Déchiffrement d'une réponse carte dans un canal sécurisé |

**FIN DU DOCUMENT**