Carte TOOAL v1.0

Fonctions de sécurité

Mediscs

- Société créée : 2004
- Labellisée OSEO-ANVAR -> DMP
  - Stockage des données sur une CD-RW
  - Brevet d'auto-gravure
- Vers les systèmes d'authentification
  - Dispositif d'authentification (CD, DVD, Clé USB, Portable)
  - SSO
  - Fédération des identités
- 13 personnes (10 R&D et Production)

La carte TOOAL ?

- La carte TOOAL est un mini CD (RW), au format carte Bancaire.
- Ce CD contient les données nécessaires pour permettre l'authentification de son propriétaire sur des services internet ou intranet sécurisés.

Caractéristiques générales

- Aucun lecteur spécifique à installer,
- Aucun logiciel à installer sur le poste client
- Aucun impact sur l'architecture du service
- Aucune trace sur le poste client
- Pré-requis :
  - Lecteur CD / Graveur CD (Administration)
  - OS : Windows XP SP2 et au delà.
  - Navigateur : Internet Explorer 6 et au-delà.
  - Sécurisation minimale de l'OS avec antivirus et firewall (tout mises à jour).

Caractéristiques de sécurité

- Coffre-fort électronique sur la carte TOOAL
  - Chiffrement AES 256.
  - Brevet MEDISCS pour cacher les données dans le CD.
  - Paramétrage de l'algorithme de génération de la clé secrète unique pour chaque CD (PKCS#5 v2.1 PBKDF2 + NIST SP800-90).
  - Exécutable signé et compressé
- Authentification par code PIN + défi du support
- Installation du certificat dans le Keystore de Microsoft avec une protection renforcée de la clé privée (niveau de sécurité haut)
  - Clé de session connue seulement par la CD Carte

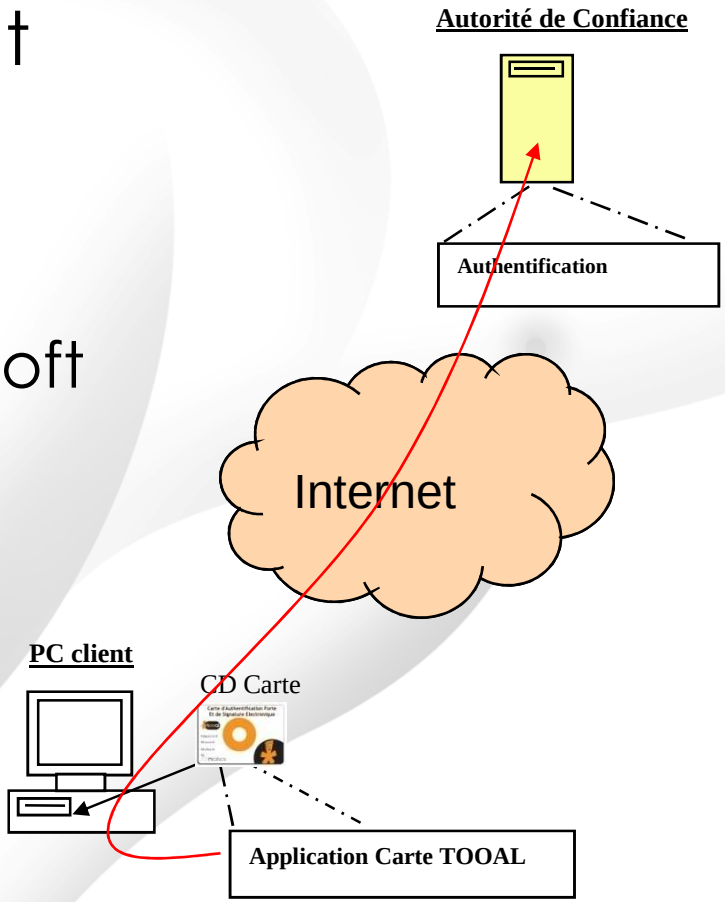
Les fonctionnalités

Certificat X.509 logiciel

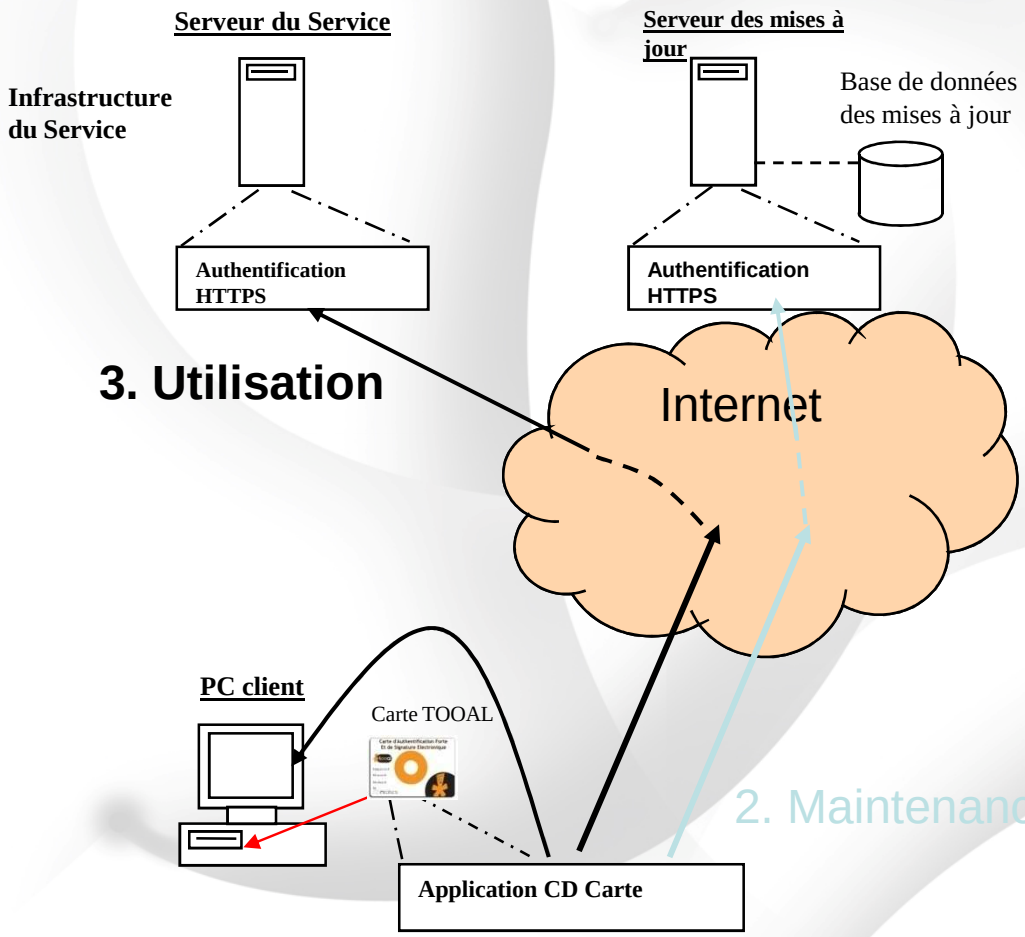
- **Confinement**
  Dispositif du porteur
- **Utilisation**
  Simplification de la démarche

Confinement du Certificat

1. Retrait du certificat
   - Site web
2. Importation
   - Keystore de Microsoft
   - Fichier PKCS#12
3. …



Utilisation du certificat



Utilisation :

- Authentification HTTPS
- Signature électronique
- Chiffrement des données
- Exportation du certificat

1. Installation automatique du certificat
4. Suppression automatique du certificat

Biens à protéger

- D.CLE_PRIVEE & D.CERTIFICAT
- D.RAD
- D.VAD
- D.RAD_DEBLOCAGE
- D.APPLICATION
- D.SAUVEGARDE

Fonctions de sécurité

- SF.Initialisation
- SF.Authentification
- SF.Certificat & SF.Clé privée
- SF.Administration
- SF.Protections

SF.Initialisation

- L'initialisation consiste à initialiser la carte TOOAL avec un code PIN aléatoire et à lui faire générer des données secrètes nécessaires à sa future utilisation

SF.Authentification

- SF.Authentification.Utilisateur
- SF.Authentification.Accès
- SF.Authentification.Changement du code PIN
- SF.Authentification.Déblocage du code PIN

SF.Certificat & SF.Clé privée

- SF.Certificat.Import & SF.Clé privée.Import
- SF.Certificat.Export & SF.Clé privée.Export
- SF.Certificat.Suppression & SF.Clé_privée.Suppression

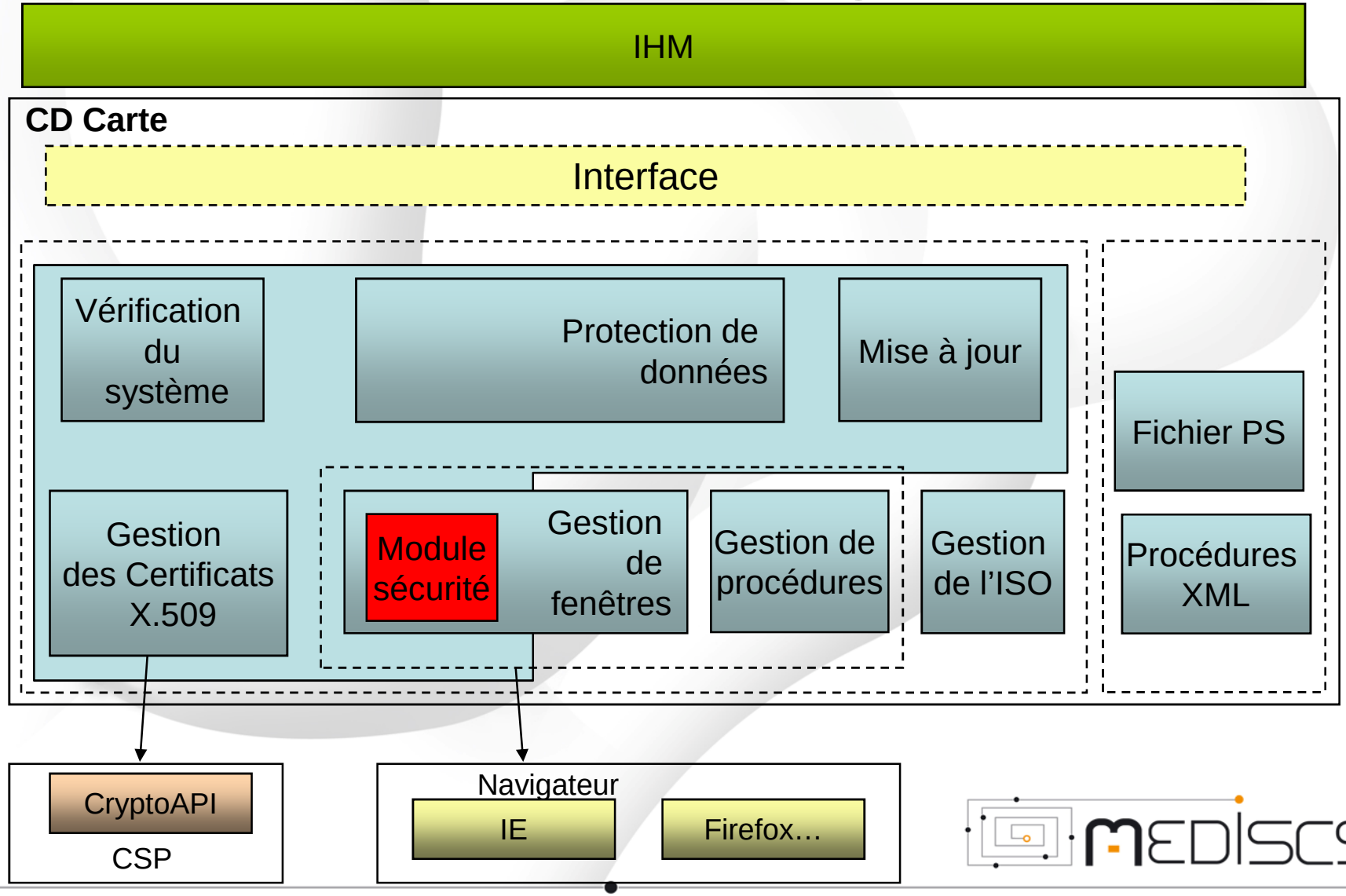
SF.Administration

- SF.Administration.Mise à jour
- SF.Administration.Sauvegarde

SF.Protections

- SF.Protections.Crypto
- SF.Protections.Tests

Architecture logicielle



Technologie utilisée

- Langage : C++
- Compilateur : Visual Studio 2005
- CSP : Technologies Microsoft
- Objet COM : IWebBrowser2
- Gravure : SPTI
- Implémentations cryptographiques Mediscs

Standards utilisés

- Manipulation du CD : ISO-9660, MMC-4
- Clé secrète : PKCS#5 v2.1 + NIST SP800-90
- Chiffrement des donnés : AES, Blowfish
- Empreintes : SHA256
- Format du certificat : X.509 (PKCS#12)

Future proche

- Certification Critères communs 3.1 (EAL 2+)
- Création de requêtes PKCS#10
- Token Virtuel
  - PKCS#11
  - PKCS#15

Merci

Paul FRAUSTO
rssi@mediscs.com