Securicam

Atos Origin

Smart
Public Key Solution

Plan de la présentation

La carte Securicam

La protection des accès

La protection des données

La protection des échanges

Conclusions

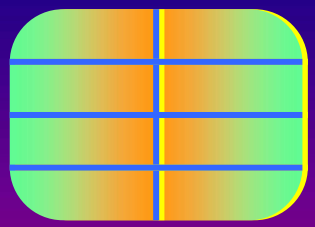
La carte Securicam

- **Un concept AtosOrigin**
- **Sur une carte Payflex de Schlumberger**
- **Pour sécuriser**
  - **Les accès**
  - **Les données**
  - **Les échanges**
  - **Des plate formes Windows NT et 2000 (95 ; 98 ; XP)**
- **Sur une logique « clés publiques »**

- **Au cœur de l'offre Securicam d'AtosOrigin**

- **Projet labellisé OPPIDUM par le Minefi**

les fonctions de la carte Securicam



Securicam

1. Calcul & Certification des clés
2. Signe des données
3. Vérifie une signature
4. Chiffre des données
5. Déchiffre des données

et plus encore...

La carte Securicam

- **Auto-certification = autonomie de l ’utilisateur**
- **Pas de gestion de clés**
  - **Clé publique à usage unique**
  - **Pas d’annuaires de certificats**
- **Approche techno-crypto**
  - **Légèreté et puissance SKI (3DES 128)**
  - **Réduction de la consommation bande passante**
  - **Composant simple, robuste, économique (Payflex)**
- **Réduction des coûts technologiques**

Des fonctions innovantes

- **Permises par :**
  - **l 'approche « fonctionnelle »**
  - **La protection des processus par la carte**

- **Les fonctions de chronologie**
- **Les fonctions de justification**
- **Les fonctions de délégation**
- **Les fonctions de Télé administration**

Les fonctions de Chronologie

- **Un compteur géré par la carte et intégré au certificat**
  - **garantit l ’ordre d ’émission**
  - **permet une meilleure traçabilité (absence de « trous »)**
- **Une date de dernière utilisation interdit la régression (mécanismes de gestion des révocations)**

Les fonctions de Télé Administration

- **Pilotage d ’une carte Securicam à distance**
  - **Inscription ; remplacement (postes nomades)**
  - **changements des « droits » (nombre de signatures autorisées, droit à déléguer…)**
  - **…**
- **Par l ’administrateur**
- **Sans possibilité de « rejeu »**
- **Messages traités par la carte elle même :**
  - **Pas de possibilités de détournement**

Plan de la présentation

La carte Securicam

La protection des accès

- **Notions de justificatifs**
- **Accès au poste de travail**
- **Accès à un serveur Web**

Conclusions

Atos Origin

Les Justificatifs

- **Un justificatif c ’est un ensemble de données ayant un sens vis à vis d’une application**
- **Son intégrité est garantie par une signature**
- **Sa confidentialité est assurée par chiffrement. Il est stocké dans la carte ou sur le poste de travail**
- **Utilisé par des mécanismes de gestion de « droits » d ’accès application ou serveur**
- **Exemple : stockage Login NT**

Accès au poste de travail

- **Protection des accès aux postes Windows NT ; 2000 ; XP**
- **Intégré à Winlogon (Gina)**
- **Sans « certificats »**
- **L'utilisateur choisit un justificatifs chargé dans la carte pour ouvrir une session :**
  - **Plusieurs justificatifs dans une même carte : Un seul mot de passe (la carte) pour tous ses comptes**
  - **Les passwords session peuvent être générés sur demande**
  - **Ils sont inconnus de l'utilisateur (anti Post It)**
  - **Et sont plus « durs » (14 digits aléatoires 1/255)**
  - **la mémorisation n'est plus un frein à leur renouvellement**
- **La confidentialité des mots de passe est assurée**

Accès à un serveur Web

- **Liaison HTPPS**
  - **Serveur authentifié par son certificat (X509)**
  - **Le serveur s'appuie sur un serveur d'authentification Securicam pour authentifier le client**
- **Accès client impossible par construction aux espaces Securicam Serveur sans la carte Ad Hoc**
- **Possibilité de signer ou chiffrer des formulaires sur le poste client (applet ou ActiveX)**
- **Ouverture vers des mécanismes d'accréditation complémentaires**
  - **Via annuaire LDAP**
  - **Via justificatifs**
  - **…**

Atos Origin

Plan de la présentation

La carte Securicam

La protection des accès

La protection des données

- **Depuis l'explorateur Windows**
- **Dans l'espace Securicam**
- **L'utilisation de délégations**

Atos Origin

Depuis l'explorateur

- **Signature de fichiers (Intégrité)**
- **Chiffrement de fichiers (Confidentialité)**
  - **3DES 128 dans la carte**
- **Chiffrement étendu par rapport à EFS**
  - **Chiffrement pour soi (comme EFS)**
  - **Chiffrement pour plusieurs destinataires**
  - **Pas d'annuaires de clés**
  - **Données chiffrées accessibles en cas de remplacement de la carte**
- **Pas de gestion de certificats**

L'Espace Securicam

- **Pour définir les zones Securicam**
  - **Choix d'un répertoire standard**
  - **Définition des « abonnés »**
  - **Transformation immédiate en zone Securicam**
  - **Opération réversible**
- **Pour gérer les justificatifs**
  - **Création ; modification; suppression ; export ; import**
  - **Chargement / déchargement dans carte**
- **Pour gérer les délégations**
  - **Création ; modification; suppression ; export ; import**
  - **Chargement dans carte**

Les Zones Securicam

- Sont des répertoires accessibles
  - Après authentification Securicam
  - Aux seules personnes « abonnées »
- Les fichiers y sont chiffrés
- Ils peuvent être sauvegardés sans droits d'accès au contenu
- La liste des « abonnés » peut être modifiée à tout moment
- Peuvent être sur un répertoire réseau (partage)
- Protection / extraction par simple glisser
- Accès direct à l'application par double clic (déchiffrement dans répertoire temporaire ; mise à jour à la fermeture de l'application)

Les délégations

- **Transmettre (temporairement) ses pouvoirs sans transmettre ses secrets**
  - **signature**
  - **déchiffrement**
- **De façon explicite (signature « p/o »)**
  3 Niveaux :
  - **Donner délégation**
  - **Utiliser délégation**
  - **Limiter usage**

non traité en approche cryptologique PKI

Administration simplifiée

- **Une plate forme autonome pour inscrire et révoquer les membres de la communauté**
- **Le remplacement d'une carte est transparent**
  - **La carte précédente est révoquée (inutilisable)**
  - **La carte de remplacement permet de déchiffrer les fichiers existants**
- **Différenciation claire des rôles :**
  - **Administrateur système**
  - **Administrateur sécurité**

Plan de la présentation

La carte Securicam

La protection des accès

La protection des données

La protection des échanges

Conclusions

Atos Origin

Intégration messagerie

- **Outlook / Notes**
- **Possibilité de signer ou chiffrer un message**
- **Chiffrement pour plusieurs destinataires**
- **Transformation de la note en pièce jointe attachée**
- **Chiffrement des pièces jointes**

Atos Origin

Plan de la présentation

La carte Securicam

La protection des accès

La protection des données

La protection des échanges

Conclusions

Atos Origin

Conclusions

Securicam l'offre sécurité clés en mains

- Une plate-forme d'administration évoluée
- La sécurité « carte »
  - Des accès
  - Des données
  - Des échanges
- L'autonomie de la confiance pour des groupes

Contacts : securicam@atosorigin.com

Securicam pour qui ?

- Les intranet et extranet « Corporate »,
- Les communautés EDI
- Les ASP (Application Service Provider) PME Intégré à la carte
- Les e.business communautaires :
  - banque à domicile,
  - courtiers d ’assurances,…
- Les municipalités : carte Ville =
  - PME +
  - Authentification
- Les universités
- …

Atos Origin

Securicam

a été labellisé
« Programme Société de l ’Information »
par le MEFI sur les critères :

- **Degré d ’innovation technique, industrielle, d ’usage ou de contenu**
- **Réalisme technique, industriel et économique**
- **Intérêt pour la société**
- **Partenariat**
  - **Atos**
  - **Schlumberger**
  - **Scort**