MARET Consulting | Boulevard Georges Favon 43 | CH 1204 Genève | Tél +41 22 575 30 35 | info@maret-consulting.ch | www.maret-consulting.ch

Retour d'expérience sur le déploiement de biométrie à grande échelle

Sylvain Maret
sylvain@maret-consulting.ch

Mardi 13 octobre 2009 / Mines ParisTech

Agenda

- Objectifs du projet
- Choix technologique
- Concept et design technique
- Mise en œuvre
- Processus humain
- Formation
- Difficultés rencontrées

Qui suis-je ?

- Architecte Sécurité
  - 15 ans d'expérience en Sécurité des Systèmes d'Information
  - Fondateur e-Xpert Solutions SA et MARET Consulting
  - Expert école ingénieur Yverdon & Université de Genève
  - Responsable OpenID Suisse Romande
  - Auteur Blog: la Citadelle Electronique
- Domaine de prédilection
  - Digital Identity Security

Le projet de gestion électronique des documents

- Mise en place d'une solution de GED
  - Accès à des informations très sensibles
  - Classification de l'information: Niveau A = Secret
  - Chiffrement des données
  - Contrôle des accès
- Projet pour une banque privée
  - Début du projet: 2005
- Population concernée
  - 500 personnes (Phase I)
  - A termes: 3000 personnes (Phase II)


(Classification Data: Secret)
Mise en place d'une technologie permettant d'identifier de façon forte
– via un mécanisme de preuve irréfutable –
les utilisateurs accédant au système d'information de la banque
Qui accède à quoi, quand et comment !

Les contraintes techniques du projet d'authentification forte

Obligatoires

- Intégration avec les applications existantes
  - Web
  - « Legacy »
  - Microsoft Smart Card Logon
- Séparation des rôles
  - Quatre yeux
- Signature numérique
- Auditing, Preuve
- Gestion des preuves

souhaitées

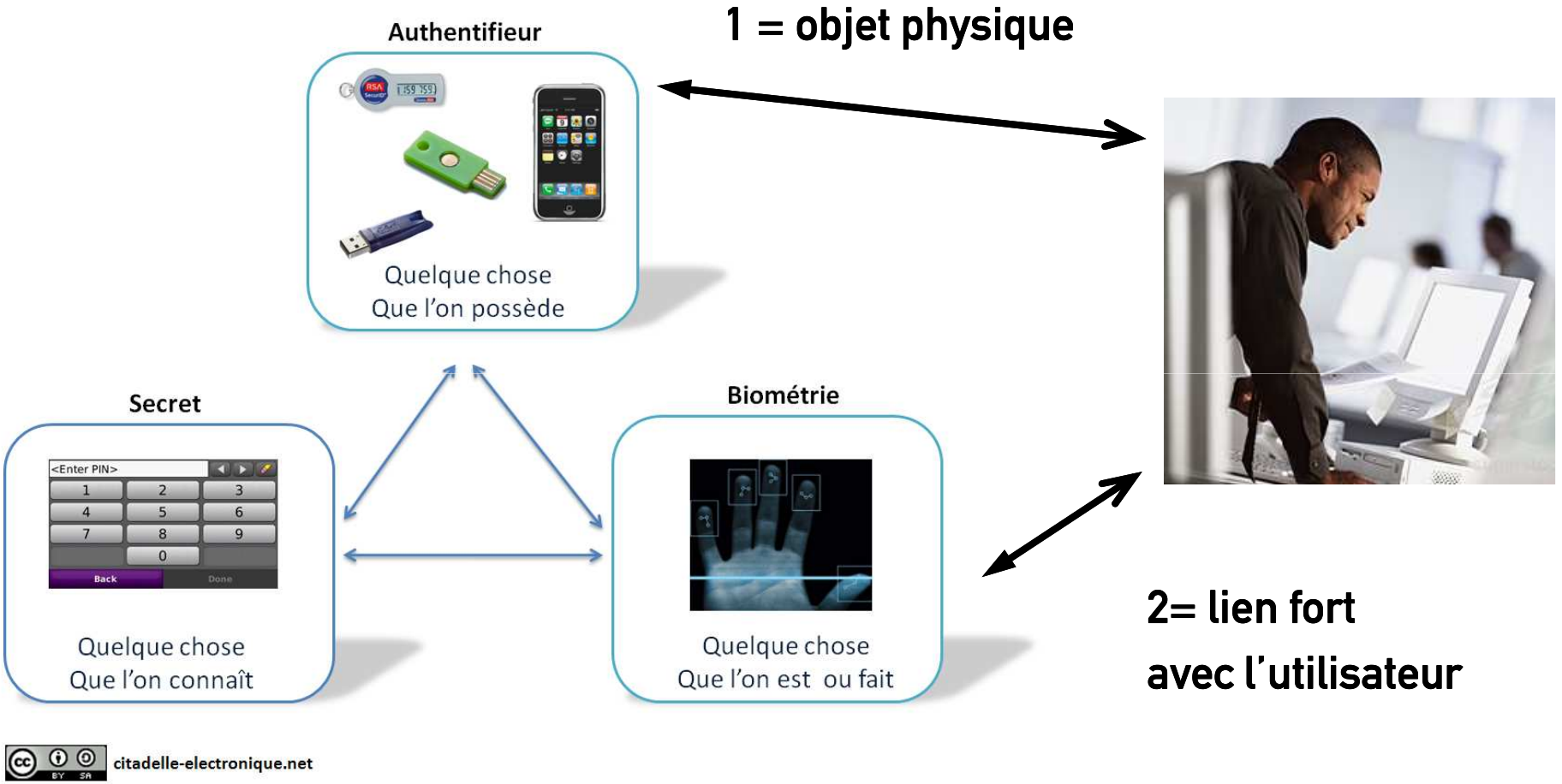
- Intégration avec sécurité des bâtiments
- Chiffrement des données
- Postes nomades
- Applications futures
  - Réseau et systèmes
  - Authentification forte
- Support impression
  - Accès aux imprimantes


Choix technologique
authentification forte

Quelle technologie d'authentification forte ?

	OTP	PKI （HW）	Biométrie
Authentification forte	■	■	■ *
Chiffrement	■	■	■
Signature numérique	■	■	■
Non répudiation	■	■	■
Lien fort avec l'utilisateur	■	■	■

* Biométrie type Fingerprinting


Authentifieur
1 = objet physique
Quelque chose
Que l'on possède
Secret
<Enter PIN>
1
2
3
4
5
6
7
8
9
0
Back
Done
Quelque chose
Que l'on connaît
Biométrie
Quelque chose
Que l'on est ou fait
2= lien fort
avec l'utilisateur
citadelle-electronique.net

La technologie d'authentification forte pour ce projet

- Utilisation certificat numérique
  - PKI (X509)
- Biométrie
  - Lecture des empreintes
- Match on Card
  - Carte à puce
  - Crypto Processeur

Match On Card: c'est quoi ?

Your personnal reference template never goes out of the card!

1. Host Application Request

2. Reader captures the fingerprint

3. Reader extracts the template

4. Reader sends the template

5. Template Matching

6. Pass / Fail

7. Pass / Fail

Stockage des empreintes: que dit la loi ?

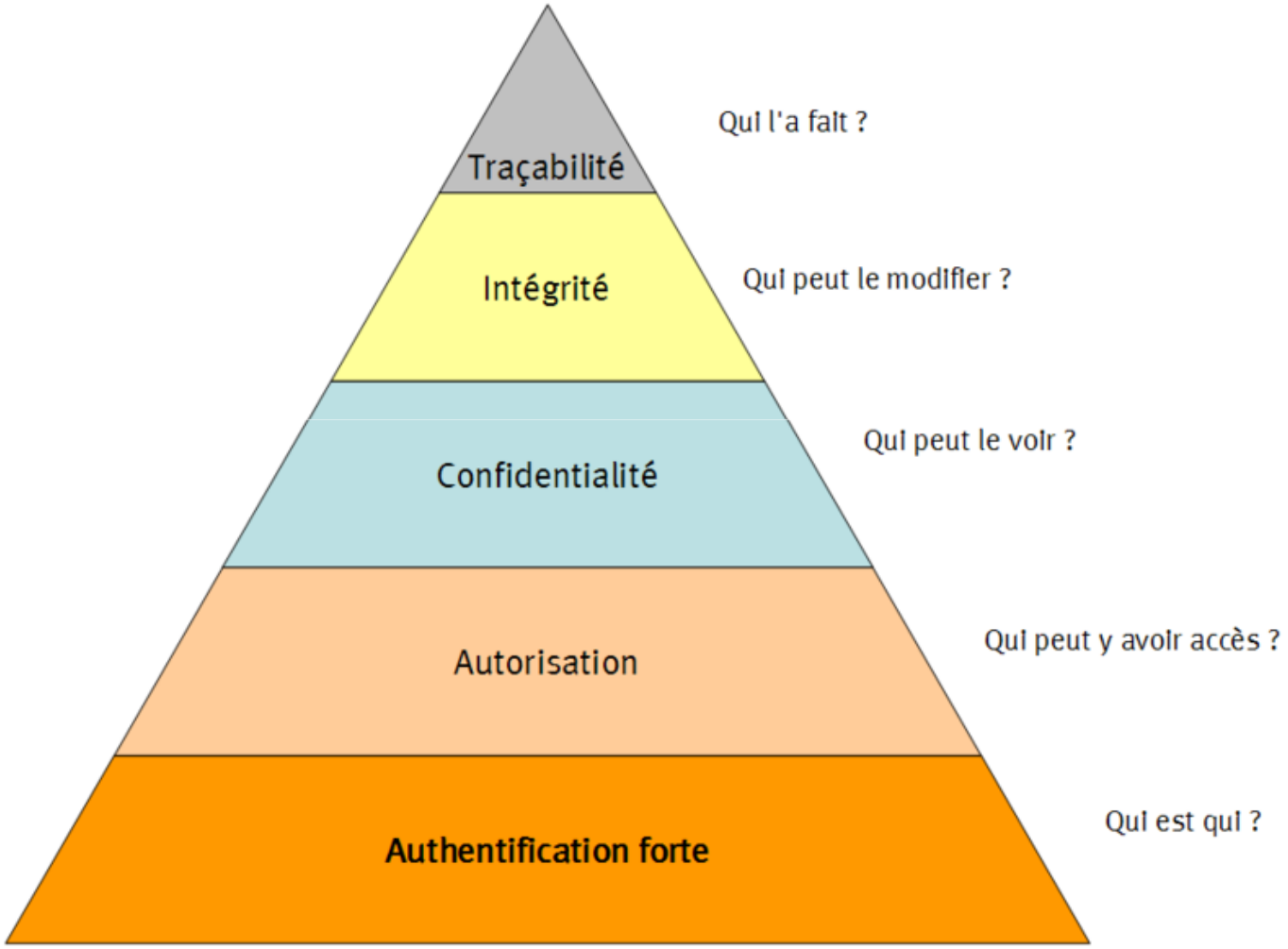
CNIL
Commission Nationale de l'Informatique et des Libertés

Préposé fédéral à la protection des données et à la transparence

- Biométrie : l'autorisation de la CNIL est obligatoire !
- Pour la biométrie basée sur les empreintes digital, obligation de stocker les données sur un support physique
- Forte recommandation d'utiliser un support physique tel que carte à puce, clé USB, etc.

Concept et design technique

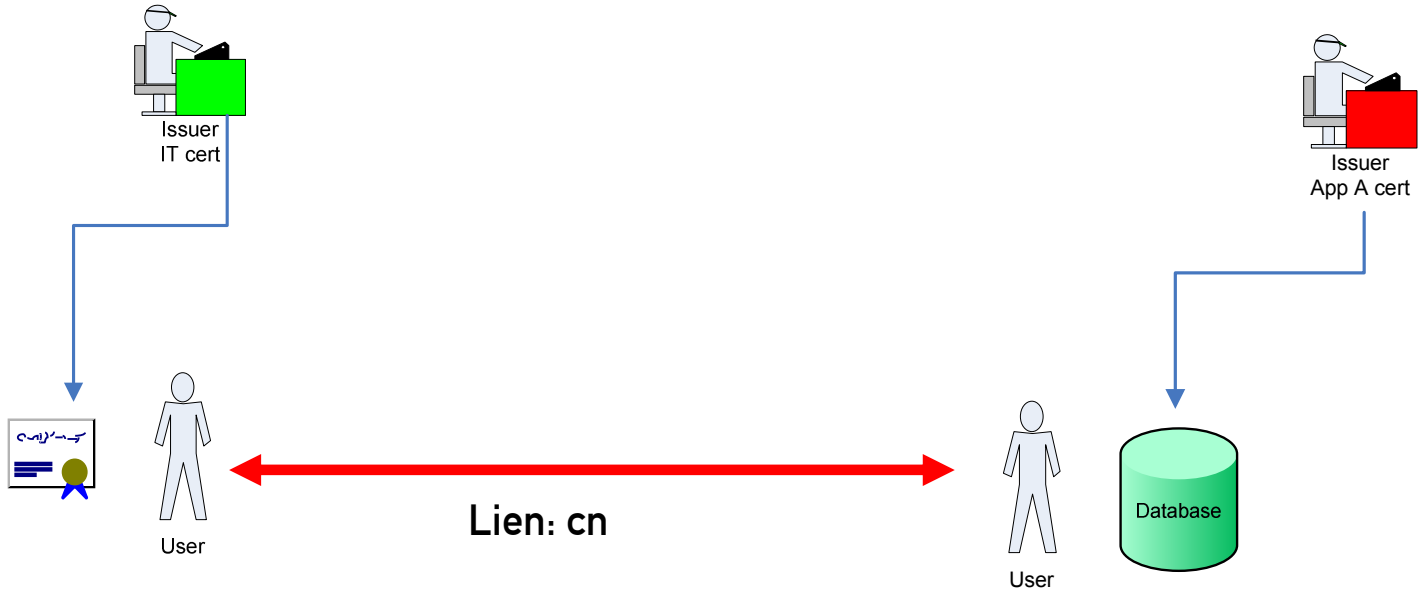
Pyramide de l'authentification forte



Concept de base: un lien unique

Gestion des identités

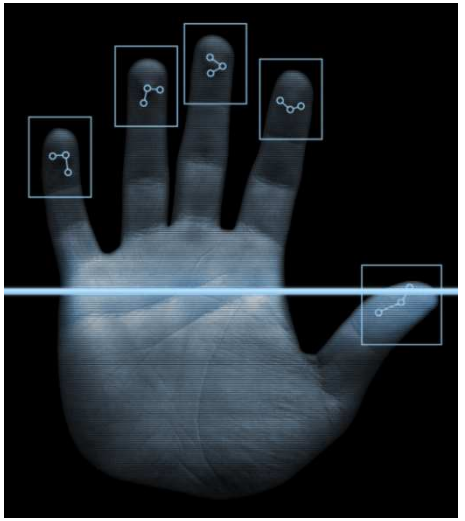
Gestion des accès



PHASE 1
Authentification forte

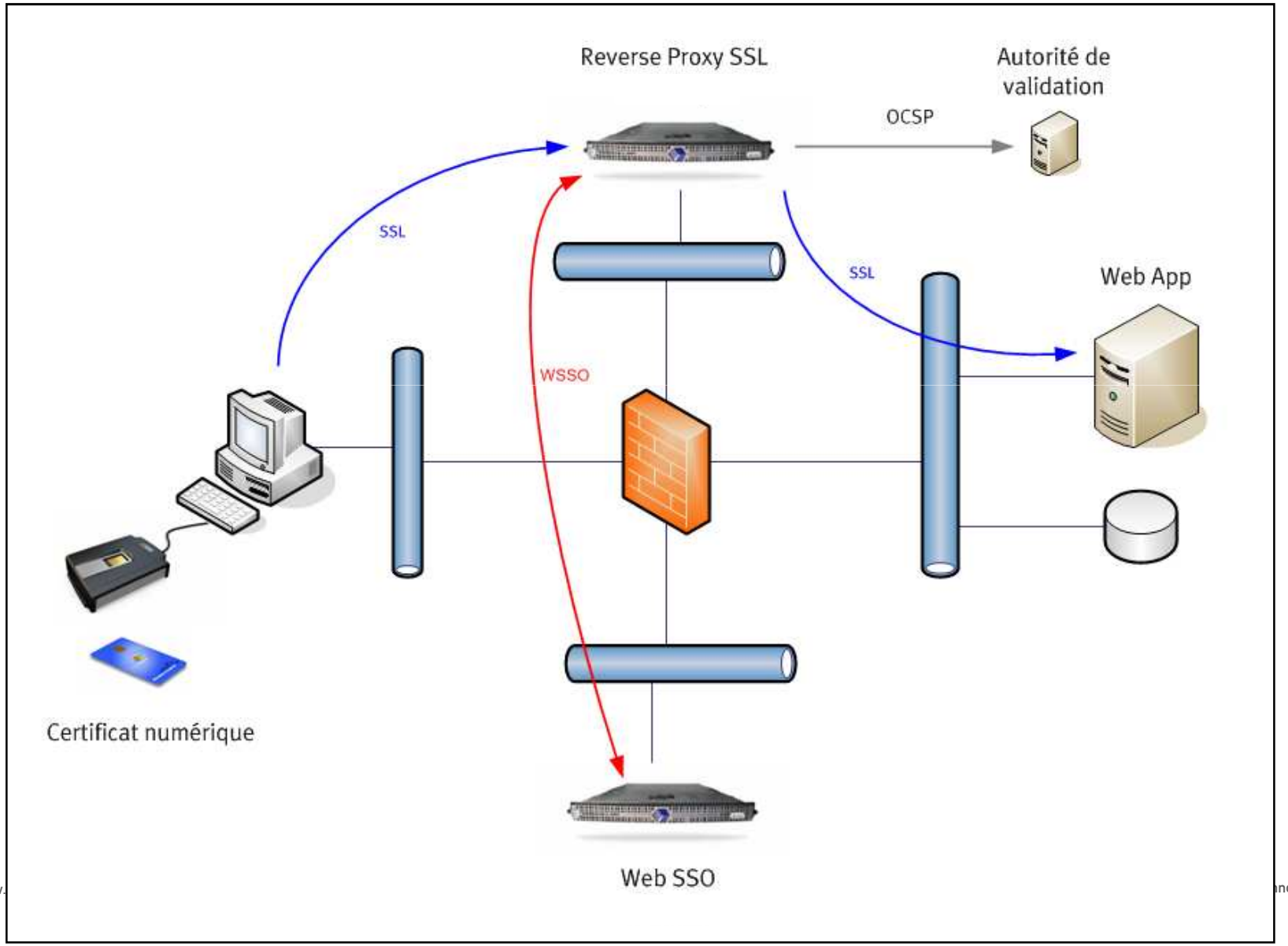
PHASE 2
Autorisation

Composants de l'architecture technique



- Mise en place d'une PKI « intra muros »
  - Non Microsoft (Séparation des pouvoirs)
- Mise en place de la révocation Online
  - Protocole OCSP
- Utilisation d'un Hardware Security Module
- Sécurisation de l'architecture PKI
  - OS « Hardening »
  - Firewall interne
  - SSH pour le « remote » management
  - Auditing

Concept pour la sécurisation de l'application GED



La mire d'authentification biométrique

Authentification d'un utilisateur avec PKINIT

Poste Client

GINA

1

SSP Kerberos

(TGT)TGS_key
C-T_key
U_Cert

3

4

6

CSP

2

5

Driver Athena

2

5

U_Cert

7

AS Req: U_Cert + [Authenticator]Sing_U_priv_key

AS Res: [((TGT)TGS_key + C-T_key + KCA_Cert)Rdm_key
+ (Rdm_key)U_pub_key]Sign_KCA_priv_key

10

Sing_U_priv_key

DC (KCA)

Active Directory

8

9

KCA_Cert

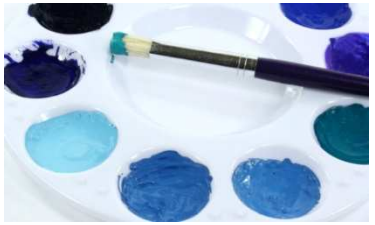
AS

TGS

TGS_key
C-T_key


Mise en œuvre

Quelques dates clé du projet (1/3)



- Décembre 2005: démarrage du projet Authentification Forte
- Avril 2006: Finalisation de l'étude Technologie
- Novembre 2006: Lettre de cadrage
- Décembre 2006: Audit du projet par un Cabinet d'audit
- Janvier 2007: Intégration de la solution
- Juin 2007: Cérémonie de génération des Clés
- Juillet 2007: Mesure de recettes solution technique

Quelques dates clé du projet (2/3)

- Octobre 2007: Finalisation des procédures d'exploitation
  - Processus
- Novembre 2007: Formation team gestion des identités
- Début 2008: Déploiement
  - Enrôlement de 500 personnes
  - Installation des lecteurs
- Mi 2008: Blocage du projet
  - Pas de déploiement dans les succursales
  - Mise en conformité de la PKI avec le principe des quatre yeux
    - Circulaire CFB 06/6 – contrôle interne, séparation des rôles / tâches

Quelques dates clé du projet (3/3)

- Fin 2008: Rédaction CP & CPS pour la PKI
- Début 2009: Changement des processus de génération des identités
- Février 2009: Cérémonie pour le partage des secrets
- Mars 2009: démarrage d'un nouveau projet pour la mobilité
- Avril 2009: Déploiement dans les succursales
- Juin 2009 : Mise en place Smart Card Logon


Processus Humain

Le maillon faible ? Plus important que la technique…

- Définition des rôles
  - Tâches et responsabilités
  - Objectif: séparation des pouvoirs
    - Quatre yeux
- Mise en place des processus pour la gestion des identités
- Mise en place des procédures d'exploitation

Mise en place des processus pour la gestion des identités

- Processus pour le team gestion des identités
  - Enrôlement des utilisateurs
  - Révocation
  - Gestion des incidents
    - Perte, vol, oublie de la carte
  - Renouvellement
  - Etc.
- Processus pour le Help Desk
- Processus pour les Auditeurs
- Processus pour le RSSI
- Etc.

Le résultat

- Une série de documents initiaux
  - Procédures d'exploitation
  - Description des processus
  - Charte d'utilisation
  - Définition des rôles et responsabilités
  - Partage des secret (Quatre yeux)
  - Etc.
- Adaptation des documents


Formation

- Un élément très important !
  - Formation du team gestion des identités
  - Formation des utilisateurs
  - Formation Help Desk
  - Formation aux technologies
    - PKI
    - Biométrie

Formation du team gestion des identités

- Un long travail à ne pas négliger
  - Technique de prise d'empreinte
  - Comment expliquer la technologie
  - Gestion des problèmes
    - Technique
    - Humain
  - Coaching les 1ere semaines

Formation des utilisateurs

- Environ 30 minutes par utilisateur lors de l'enrôlement
  - Explication de la technologie
    - Match on Card
  - Positionnement des doigts
    - Essais
  - Remise d'une brochure explicative
  - Signature de la charte d'utilisation


Difficultés
rencontrées

Quelques exemples…

- Enrôlement de certains utilisateurs
- Problème pour la convocation des gestionnaires
- Problème technique sur le système de validation Online

Enrôlement de certains utilisateurs

- **Problème**
  - Capture des empreintes sur certaines personnes
    - Entre 1 à 2% des personnes présentent des problèmes pour l'enrôlement
- **La solution**
  - Utilisation de capteur de meilleur qualité
  - Création d'un profil avec un FAR plus faible

Problème pour la convocation des gestionnaires

- Problème
  - Convocation pour la prise d'empreinte
    - Pas de succès
    - Peu de réponse !
- La solution
  - Passage par la direction de l'entreprise (CEO)

Problème technique sur le système de validation Online

- **Problème**
  - Instabilité du système de révocation
  - Impossible de reproduire le Bug avec le support de l'éditeur
  - Elément très critique de l'architecture
- **Solution**
  - 1 année de « debugging » au labo
  - Trouvé le problème
    - Trop de mémoire sur les serveur de validation
    - Limitation de la mémoire


Retour
d'expérience

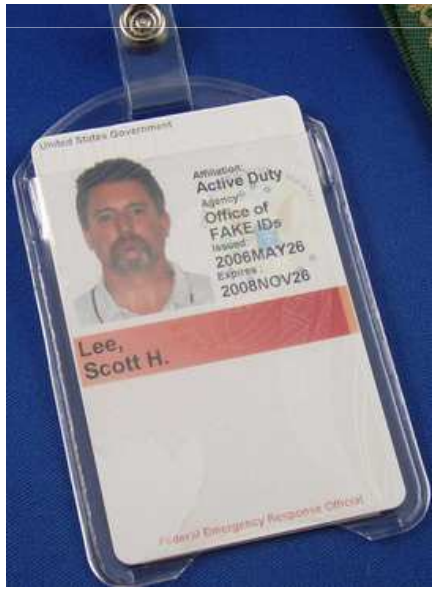
Conclusion (1/2)

- La technique est un aspect mineur pour la réussite d'un projet de cette ampleur
- Ne pas sous estimer la rédaction des processus
  - CP / CPS pour la PKI
  - Processus de gestion
- Ne pas sous estimer la séparation des pouvoirs
- Demander un appuis de la direction

Conclusion (2/2)

- L'auditing est très important
  - Contrôle de la gestion des identités
  - Gestion de la fraude
- La Biométrie est une technologie mature
- Technologie PKI
  - Offre un noyau de sécurité pour le futur
  - Chiffrement, signature
  - Information Rights Management
  - Sécurité de la donnée
- Un pas vers la convergence
  - Sécurité physique et logique

La suite du projet: la convergence ?



Quelques liens

- MARET Consulting
  - http://maret-consulting.ch/
- La Citadelle Electronique (le blog)
  - http://www.citadelle-electronique.net/
- Article banque et finance:
  - Usurper une identité? Impossible avec la biométrie!
    - http://www.banque-finance.ch/numeros/88/59.pdf
  - Biométrie et Mobilité
    - http://www.banque-finance.ch/numeros/97/62.pdf

"Le conseil et l'expertise pour le choix et la mise

en oeuvre des technologies innovantes dans la sécurité

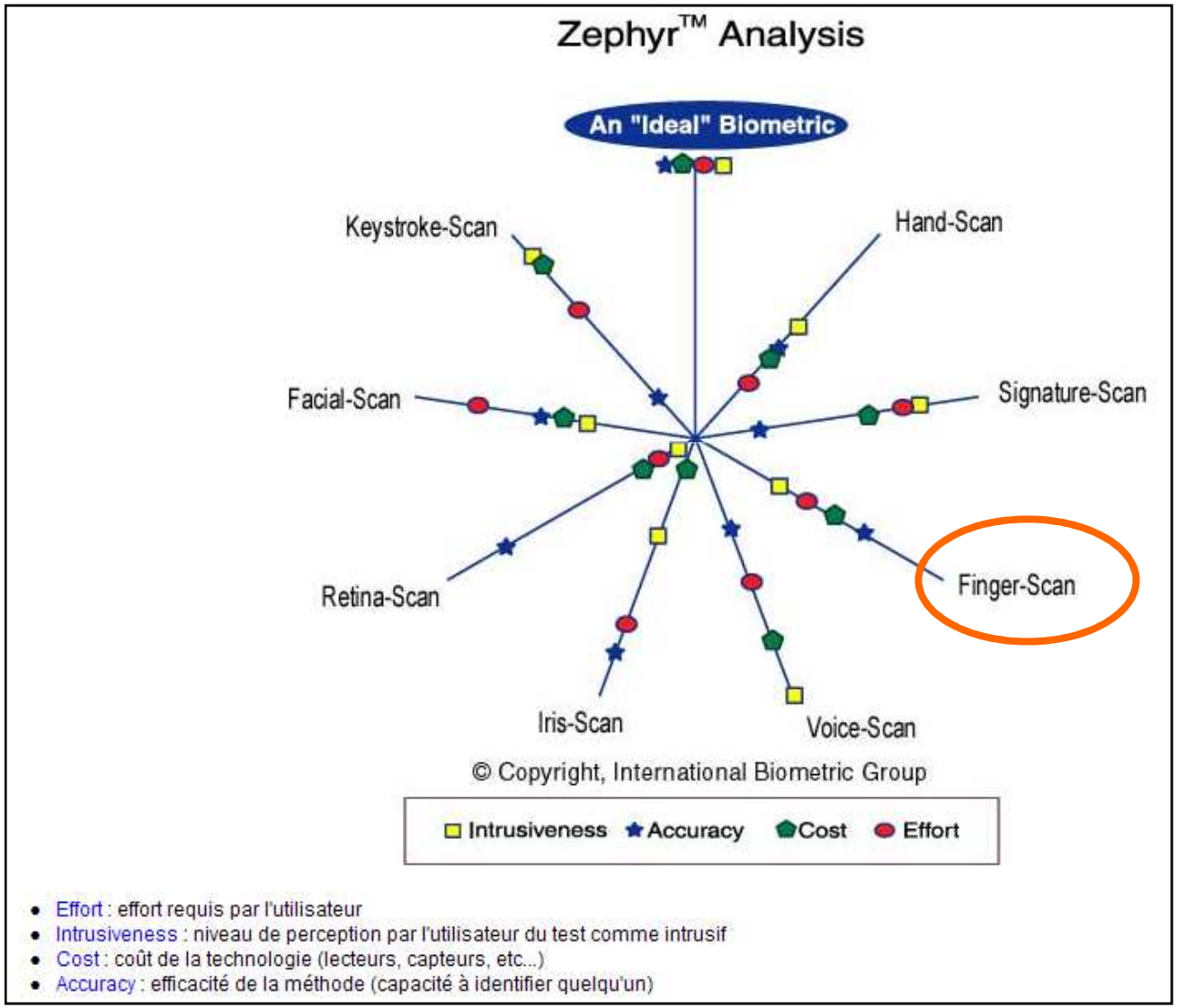
des systèmes d'information et de l'identité numérique"

MARET Consulting | Boulevard Georges Favon 43 | CH 1204 Genève | Tél +41 22 575 30 35 | info@maret-consulting.ch | www.maret-consulting.ch

Annexes

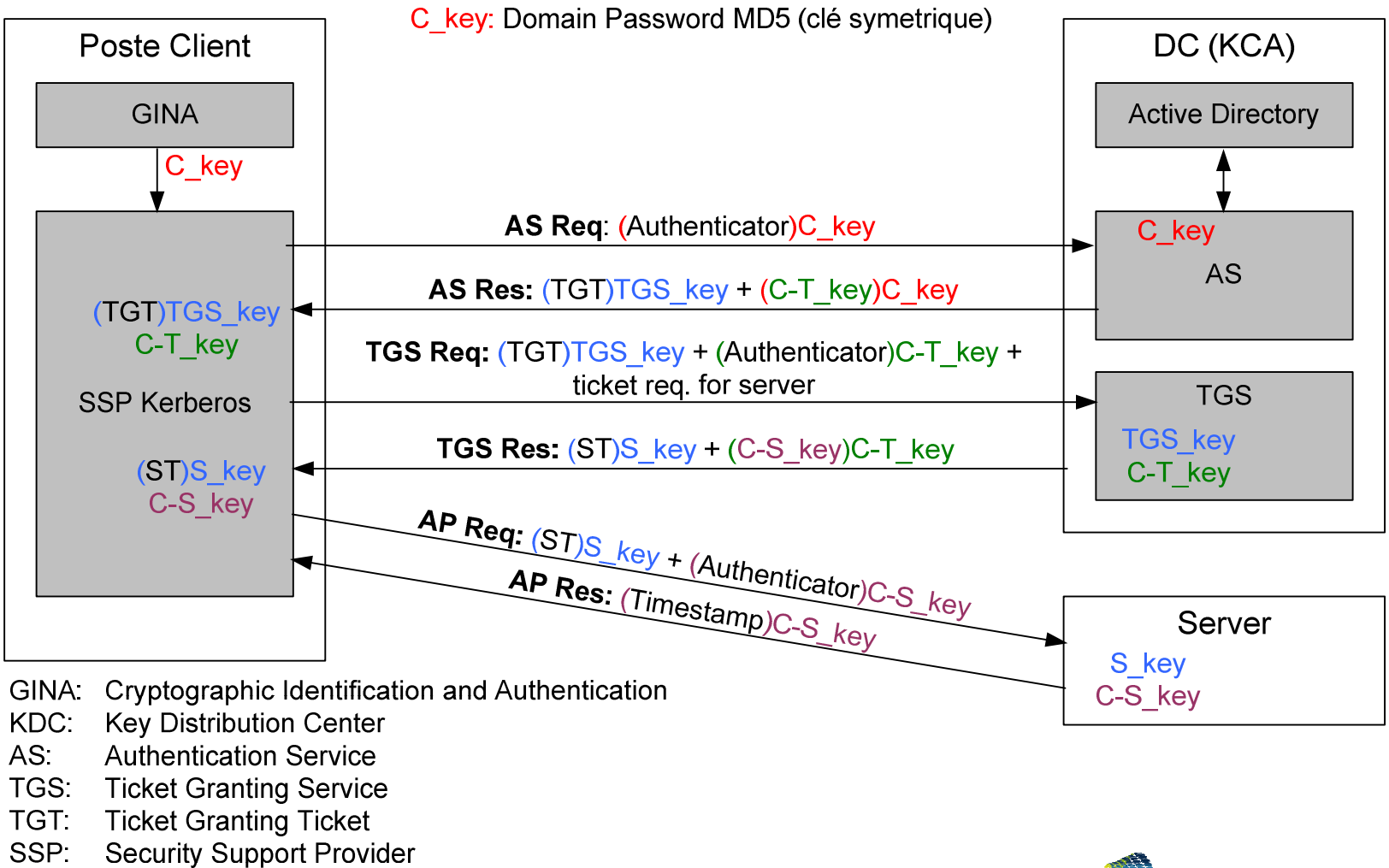
Sylvain Maret
MARET Consulting

Quelle technologie biométrique pour l'IT ?



- Effort : effort requis par l'utilisateur
- Intrusiveness : niveau de perception par l'utilisateur du test comme intrusif
- Cost : coût de la technologie (lecteurs, capteurs, etc...)
- Accuracy : efficacité de la méthode (capacité à identifier quelqu'un)

Authentification d'un utilisateur avec Kerberos



GINA: Cryptographic Identification and Authentication
KDC: Key Distribution Center
AS: Authentication Service
TGS: Ticket Granting Service
TGT: Ticket Granting Ticket
SSP: Security Support Provider

Authentification d'un utilisateur avec PKINIT

Poste Client

GINA

1

SSP Kerberos

(TGT)TGS_key
C-T_key
U_Cert

3

4

6

CSP

2

5

Driver Athena

2

5

U_Cert

7

AS Req: U_Cert + [Authenticator]Sing_U_priv_key

AS Res: [((TGT)TGS_key + C-T_key + KCA_Cert)Rdm_key
+ (Rdm_key)U_pub_key]Sign_KCA_priv_key

10

Sing_U_priv_key

DC (KCA)

Active Directory

8

9

KCA_Cert

AS

TGS

TGS_key
C-T_key

Authentification d'un utilisateur avec PKINIT (suite)

- 1. Saisie des empreintes dans *Winlogon* lors de l'insertion de la carte à puce dans le lecteur. Transmis au SSP Kerberos
- 2. Appel au driver d'*Athena*. Envoi des minutie biométrique pour accéder aux données contenues dans la carte à puce
- 3. Récupération du certificat utilisateur par le SSP
- 4. Génération, par le SSP, d'un authentifieur contenant un *Timestamp*. Transmis au CSP
- 5. Signature de l'authentifieur par le CSP (réalisé dans la carte à puce)

Authentification d'un utilisateur avec PKINIT (suite)

- 6. Signature retournée au SSP
- 7. Requête AS (*Authentication Service*) au KDC pour obtenir le TGT. Contient : certificat, authentifieur et signature
- 8. Vérification de la validité du certificat (*Certification Path*, CRL, *trust* CA). Vérification de la signature. Recherche des informations de l'utilisateur (user@domain)
- 9. Récupération des informations utilisateur (user SID (*Security Identifier*), group SID) pour construire le TGT
- 10. Réponse AS contenant le TGT. Chiffré avec la clé publique du client et signée par le KDC

[((TGT)TGS_key + C-T_key + KCA_Cert)Rdm_key + (Rdm_key)U_pub_key]Sign_KCA_priv_key

Démonstration: Microsoft Smart Card Logon (PKINIT)