CLUSIR Rhône Alpes

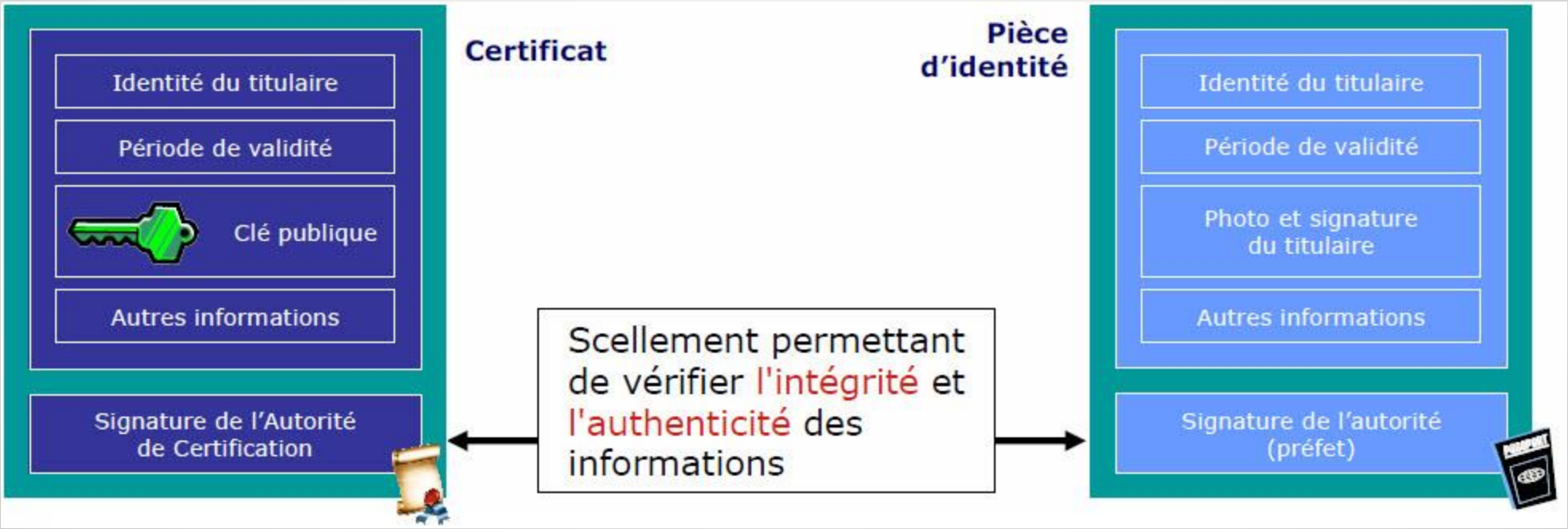
Services de confiance numériques :

Etat des lieux

Gilles DEFER

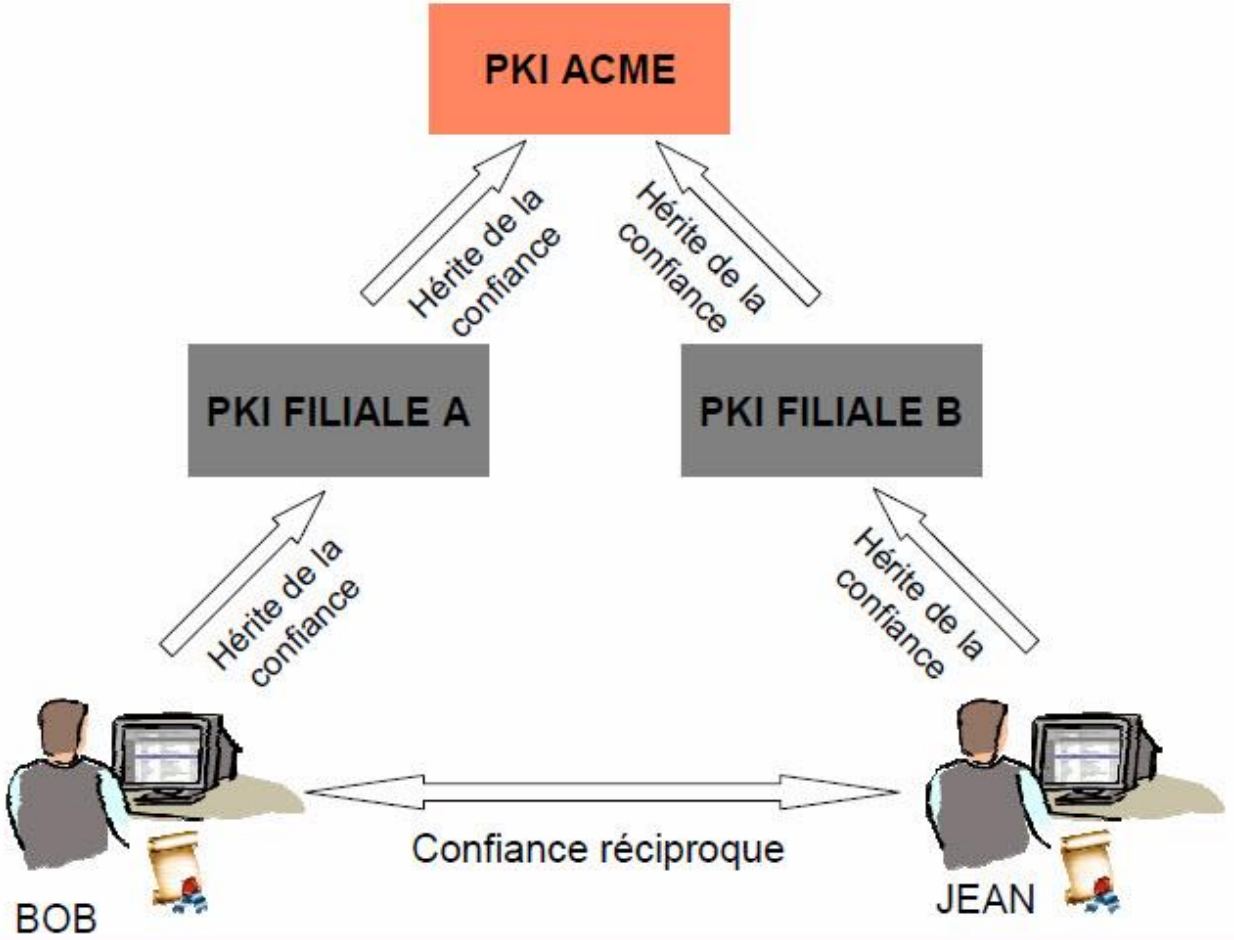
Février 2011

Les bases de la confiance numérique



Les bases de la confiance numérique

Exemple de hiérarchie de confiance



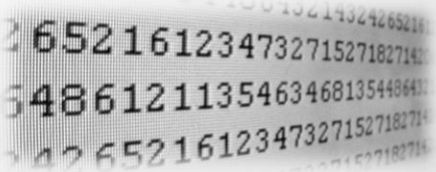
Différentes authentifications fortes

Quelle différence entre un token OTP/SSO et un support cryptographique ?

→ Le secret partagé…ou non

→ Fournir la non-répudiation : seul le porteur possède la clé privée

Services de confiance numérique : quick wins



- Chiffrement/signature Outlook

- Smart Card Logon Microsoft

- Chiffrement de fichier

- Wifi

- Terminaux mobiles

Services avancés de confiance numérique

- SCCM
- Dématérialisation des workflows
- Dématérialisation des documents
- Archivage numérique
- Carte multi service
- Horodatage

Services de confiance numériques : Remarques

- Une PKI ne sert à rien sans les applications utilisatrices
- Différence entre le certificat et son utilisation

  → l'exemple d'Outlook
- Non maturité des outils
- Introduction d'une durée de vie / expiration

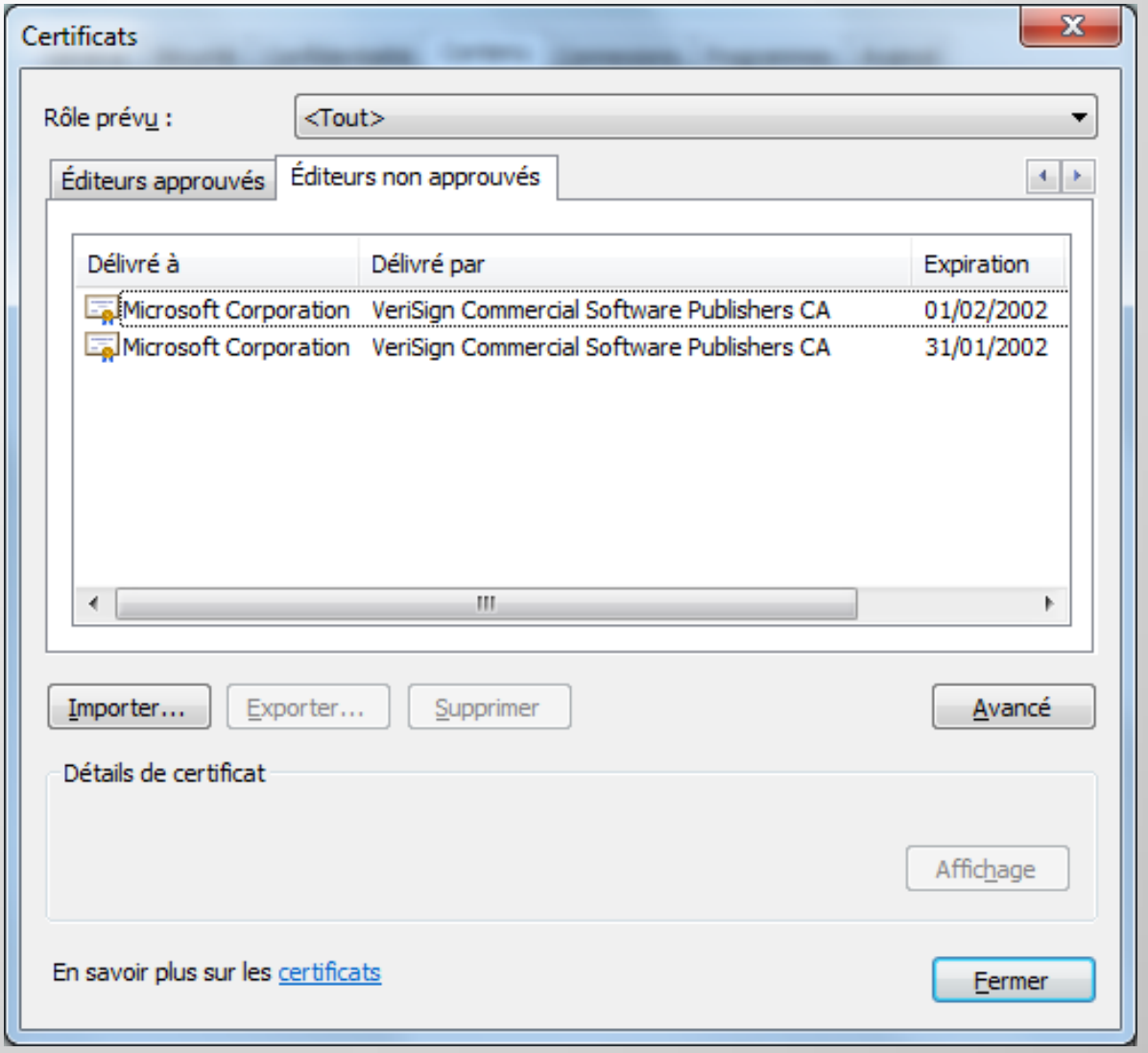
Services de confiance numériques : attaques

- ISC2 Amazon
- Attention aux CRLs
- Mise en œuvre faible : cas du BlackBerry
- Algorithmes trop robustes : attaque des workflows
- Révocations illégitimes
- Impacts Wikileaks, Renault...

Services de confiance numériques

Attaques sur les processus :

→ Certificats illégitimes



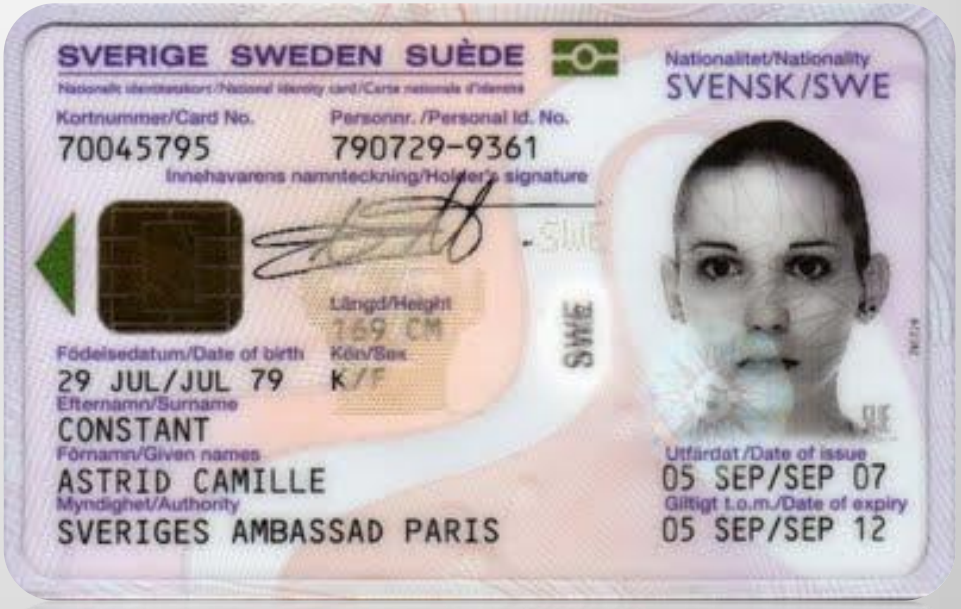
Services de confiance numériques

Exemple de mise en œuvre

Signature numérique d'emails pour personne morale

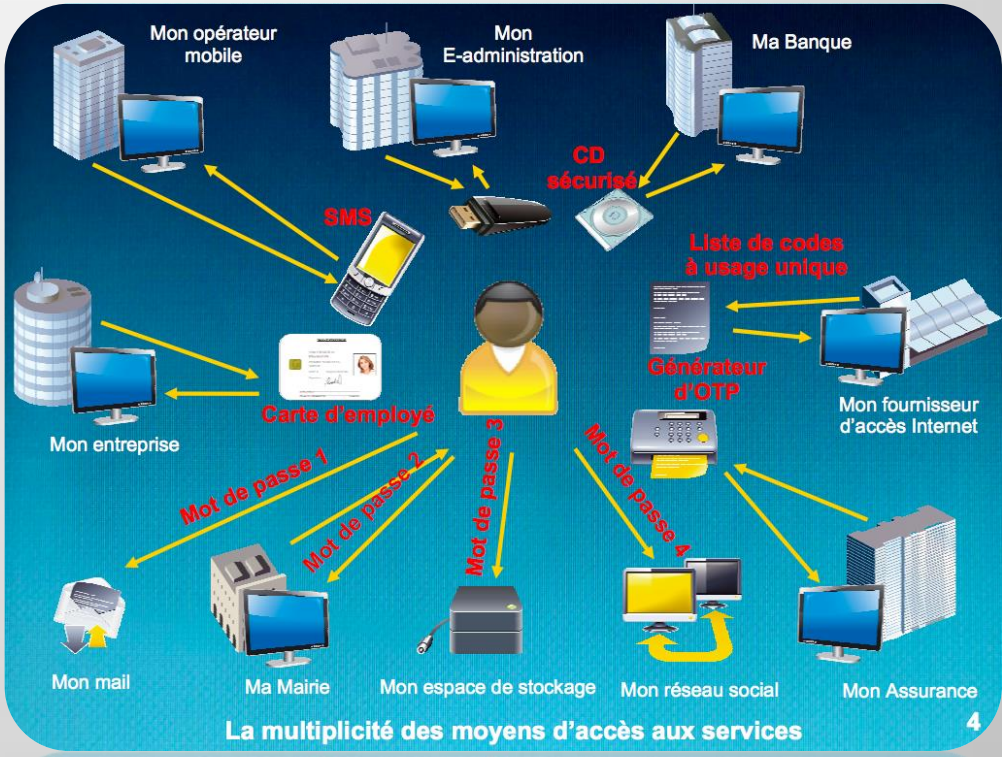
Services de confiance numériques : à l'étranger

Carte nationale d'identité numérique : l'exemple de la suède depuis 2005



Services de confiance numériques en France

- IDéNum + Carte Nationale D'Identité Electronique
- Guichet unique : service-public.fr
- DMP
- Permis de conduire électronique
- Lettre recommandée électronique
- Vers une carte universelle?



Services de confiance numériques : précautions

- Absence du S/MIME dans les webmails, Iphone…
- PKI Microsoft pour les environnements Microsoft
- Il n'y en a pas "juste pour une heure"
- Une PKI n'est valable que dans un périmètre de confiance donné. En dehors, des certificats publics sont utilisés
- **50 % d'organisationnel, 25% de juridique et "seulement" 25% de technique**

Best practices

- AES-256/SHA-256
- Ajuster en fonction du contexte : SHA1 peut suffire pour une validité pour une semaine
- Vérifier systématiquement les CRLs
- Attention au support et au paramétrage des applications
- Séparation des pouvoirs, saisie puis validation
- Utiliser des outils qualifiés/certifiés
- OCSP

Best practices

- Rigueur
- Documentation
- **Importance des workflows**
- Traitement juridique
- SLA
- Mettre en œuvre le RGS !

Services de confiance numériques

Questions ?