Faut-il brûler vos certificats ?

JRES 2003

Serge Aumont

- Motivation
- https : illusion de sécurité ?
- Protection des clés privées
- Mobilité
- Les AC de confiance
- La révocation
- Exploiter une IGC
- L'interopérabilité
- Signature : la loi
- Signature : la techno
- Dématérialisation
- Faut-il brûler vos certificats ?

Motivations

- Un certificat c’est magique.

Le discours ambiant :

- certificats=protection maximale et universelle

Parfois de la techno béatitude :

- C’est nouveau donc c’est un progrès
- C’est complexe donc cela permet de résoudre des problèmes complexes.

Motivations

- Techno ancienne dont l'avènement tarde (X509 : 1988, SSL 1994)
- Concepts sophistiqués / usages basiques
- Les implémentations très éloignées du modèle (surtout les navigateurs)
- Critiques radicales des IGC depuis au moins 3 ans :
  - « ten risks of PKI »,
  - « to late for digital certificates »,
  - « Only Mostly Dead RIP PKI », …

- Motivation
- https : illusion de sécurité ?
- Protection des clés privées
- Mobilité
- Les AC de confiance
- La révocation
- Exploiter une IGC
- L'interopérabilité
- Signature : la loi
- Signature : la techno
- Dématérialisation
- Faut-il brûler vos certificats ?

https : une illusion de sécurité ?

- 3 préoccupations :

« Sniff » des mots de passe	Un certificat auto signé est suffisant
Faux serveurs	Menace théorique imparfaitement contrée par https (serveur/service)
Identification des utilisateurs et contrôle d'accès	Attention : distribuer des certificats personnels est difficile.

HTTPS : illusion de sécurité ?

- HTTPS souvent brandi comme l'argument de sécurité absolu.
- Amalgame entre serveur sécurisé et session sécurisée.
- Sauf HSM (hardware security module), clés privées en clair sur le disque !
- SSL en dehors d'une politique de sécurité cohérente : un gadget ?

- Motivation
- https : illusion de sécurité ?
- Protection des clés privées
- Mobilité
- Les AC de confiance
- La révocation
- Exploiter une IGC
- L'interopérabilité
- Signature : la loi
- Signature : la techno
- Dématérialisation
- Faut-il brûler vos certificats ?

Protection des clés privées

- Un point critique de la politique de certification
- Mozilla, IE, Netscape : stockage de la clé sur le disque dur.
- Chiffrement (3DES) avec une passphrase

Protection des clés privées

- Ce qu'on peut imaginer de pire dans ce domaine : IE
  - Par défaut l'usage du certificat ne requiert pas de passphrase !
  - Par défaut les clés sont exportables !

Protection des clés privées

- Aucune administration des *passphrase* possible (ce que l'on sait faire avec des mots de passe classiques : complexité minimum, test de dictionnaire, changements périodiques,recouvrement,...)
- En cas de copie : attaque possible offline avec beaucoup de temps et aucune trace dans aucun log.

Protection des clés privées

- La solution cryptokey (PKCS#11) permet la génération du bi-clé sur un support USB ou carte à puce.
- API PKCS#11 = accès au service de chiffrement asymétrique sans accéder à la clé privée elle-même.
- «ce que l'on a» + «ce que l'on sait»
- Niveau de protection des clés très élevé

Protection des clés privées

- Les marchands de token USB ont 2 arguments :
  1. pas de lecteur spécifique
  2. la carte à puce recule
- Il faut cependant :
  - un driver = obstacle à la mobilité
  - configurer les applications
- connectique USB limite les usages

Protection des clés privées

- caractère impersonnel du support en complète contradiction avec sa vocation
- références culturelles : on se prête facilement des gadgets USB, on ne prête pas sa carte bancaire.

Protection des clés privées

- Matérialiser le support de clés implique :
  1. initialiser électriquement le support
  2. s'assurer que la demande de certificat est faite sur le support
  3. déployer les pilotes
  4. gérer les pertes de code pin
  5. gérer les pertes du support
  6. gérer la récupération des supports
- Tentative de solution : un serveur de tokens virtuels (*cryptolog*)

- Motivation
- https : illusion de sécurité ?
- Protection des clés privées
- Mobilité
- Les AC de confiance
- La révocation
- Exploiter une IGC
- L'interopérabilité
- Signature : la loi
- Signature : la techno
- Dématérialisation
- Faut-il brûler vos certificats ?

Mobilité et certificats

- VPN : l'espoir de prolonger le réseau local privé jusque sur le PC nomade.
- SSL dans les applications : objectif plus limité mais un atout important pour la mobilité (ex:IMAPS, POPS).
- Relais de messagerie en SMTP/TLS si distribution de certificats sur les postes clients
- Mon certificat dans le cyber café des JRES ?

- Motivation
- https : illusion de sécurité ?
- Protection des clés privées
- Mobilité
- Les AC de confiance
- La révocation
- Exploiter une IGC
- L'interopérabilité
- Signature : la loi
- Signature : la techno
- Dématérialisation
- Faut-il brûler vos certificats ?

Les AC de confiance

- Netscape, Mozilla, IE =~ 100% ?
- Pré configurées avec des listes d'autorités de certification commerciales (AC).
- Choix opaque qu'on ne peut pas vraiment modifier

Les AC de confiance

- Les AC toutes sur le même plan :
  - Quel que soit « la qualité » de l'AC
  - Quel que soit les usages
- On peut distribuer des navigateurs +/- pré configurés mais pas verrouiller cette config
- RFC3095 : serveur de validation permettant une administration centralisée de cette fonction.

- Motivation
- https : illusion de sécurité ?
- Protection des clés privées
- Mobilité
- Les AC de confiance

- La révocation
- Exploiter une IGC
- L'interopérabilité
- Signature : la loi
- Signature : la techno
- Dématérialisation
- Faut-il brûler vos certificats ?

La révocation

- Des difficultés théoriques très connues qu'on ne peut balayer en arguant du caractère exceptionnel de la révocation.
- En évaluant les conséquences d'une compromission de clé on conclut toujours sur la nécessité d'un système de révocation.

La révocation

- Fenêtre de vulnérabilité : temps entre la compromission et le moment où l'exploitation du certificat révoqué est impossible (idem anti-virus)
- Minimiser la fenêtre de vulnérabilité
  1. Capacité à détecter la corruption
  2. Réactivité de l'IGC
  3. Diffusion de l'info jusqu'aux applications

La révocation : détection

- Comment détecter qu'une clé a été compromise ? Une question sous estimée.
- On révoque toujours en cas de vol du support physique
- On ne révoque pas chaque fois qu'une faille est détectée dans IE ☺
- Que faire si j'ai laissé mon navigateur ouvert le temps de la pause café ?

La révocation : réactivité de l'IGC

- Une très forte contrainte d'exploitation pour l'IGC (révoquer impose l'utilisation de la clé privée de l'AC)
- Réponse pas si simple surtout si critères de vérification élevés des demandes de révocation.
- Fort impact sur l'organisation et donc les coûts de l'IGC.

La révocation : propager l'info

- Le modèle des CRLs est un non sens pour la propagation de l'info de révocation :
  - La CRL est diffusée en pull (et non push)
  - La validité de la CRL est déterminée a priori sans moyen de forcer une mise à jour des utilisateurs en cas d'avalanche de révocation
- Validité de la CRL = compromis entre
  1. fenêtre de vulnérabilité
  2. Charge réseau et serveur

La révocation : alternatives aux CRLs

- Online Certificat Status Protocol (OCSP RFC 2560). L'application interroge un serveur pour connaître la validité d'un certificat.
- C'est une solution pour un des trois facteurs de la fenêtre de vulnérabilité
- C'est une garantie que le traitement de la révocation est fait selon la politique de l'IGC

La révocation

Clients	CRL	OCSP
Netscape 4	Mauvaise config par défaut, pas de mise à jour	Non
N7 et Mozilla	Mauvaise config par défaut	Oui !
IE	Mauvaise config par défaut	Non
Apache(modssl)	A coup de crontab !	Non
IIS	Oui !	?

- Motivation
- https : illusion de sécurité ?
- Protection des clés privées
- Mobilité
- Les AC de confiance
- La révocation
- Exploiter une IGC
- L'interopérabilité
- Signature : la loi
- Signature : la techno
- Dématérialisation
- Faut-il brûler vos certificats ?

Exploiter une IGC

- L'exploitation d'une IGC est assujettie à la *politique de certification.*
- La PC stipule le domaine d'application de l'IGC, le niveau de sécurité dans la mise en œuvre, la responsabilité financière de l'autorité administrative,...
- Exemples de contraintes :
  - Délai de prise en compte d'une demande de révocation 6h 365 jours / an
  - Entraînement des personnels : 2 crash-tests par an

Exploiter une IGC

- Des contraintes fortes et contradictoires. Exemple :

Assurer la protection de la clé privée	Un seul exemplaire, accessible par un seul opérateur
Assurer la disponibilité de la clé privée	Multiplier les copies, les lieux de stockage et les personnes ayant les droits d'accès

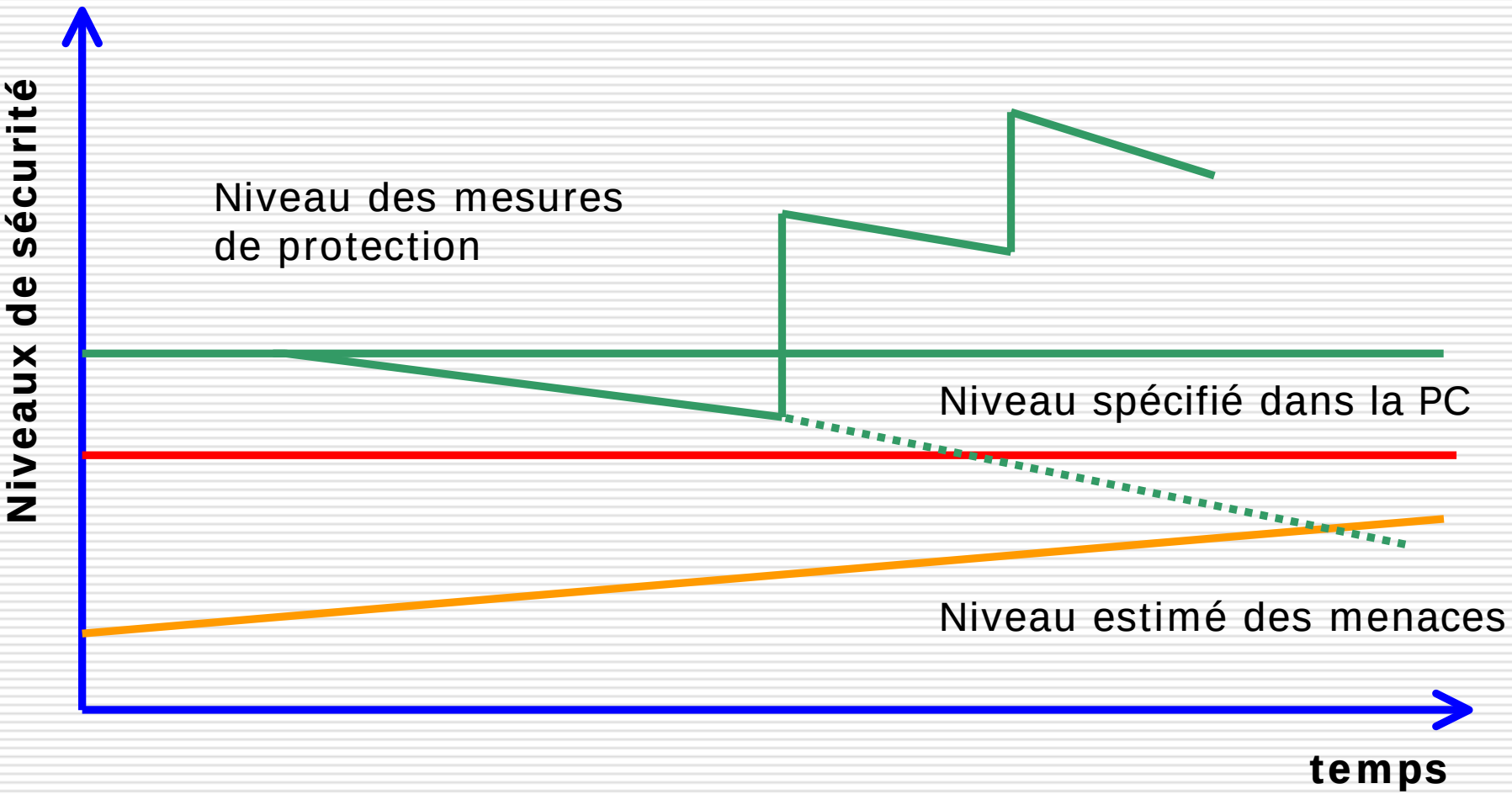
Exploiter une IGC

- Elément de solution « n parmi m »
- n est augmenté pour se protéger des opérateurs indélicats
- m est augmenté pour maintenir la disponibilité pendant les absences de certains opérateurs
- n/m : fort impact organisationnel

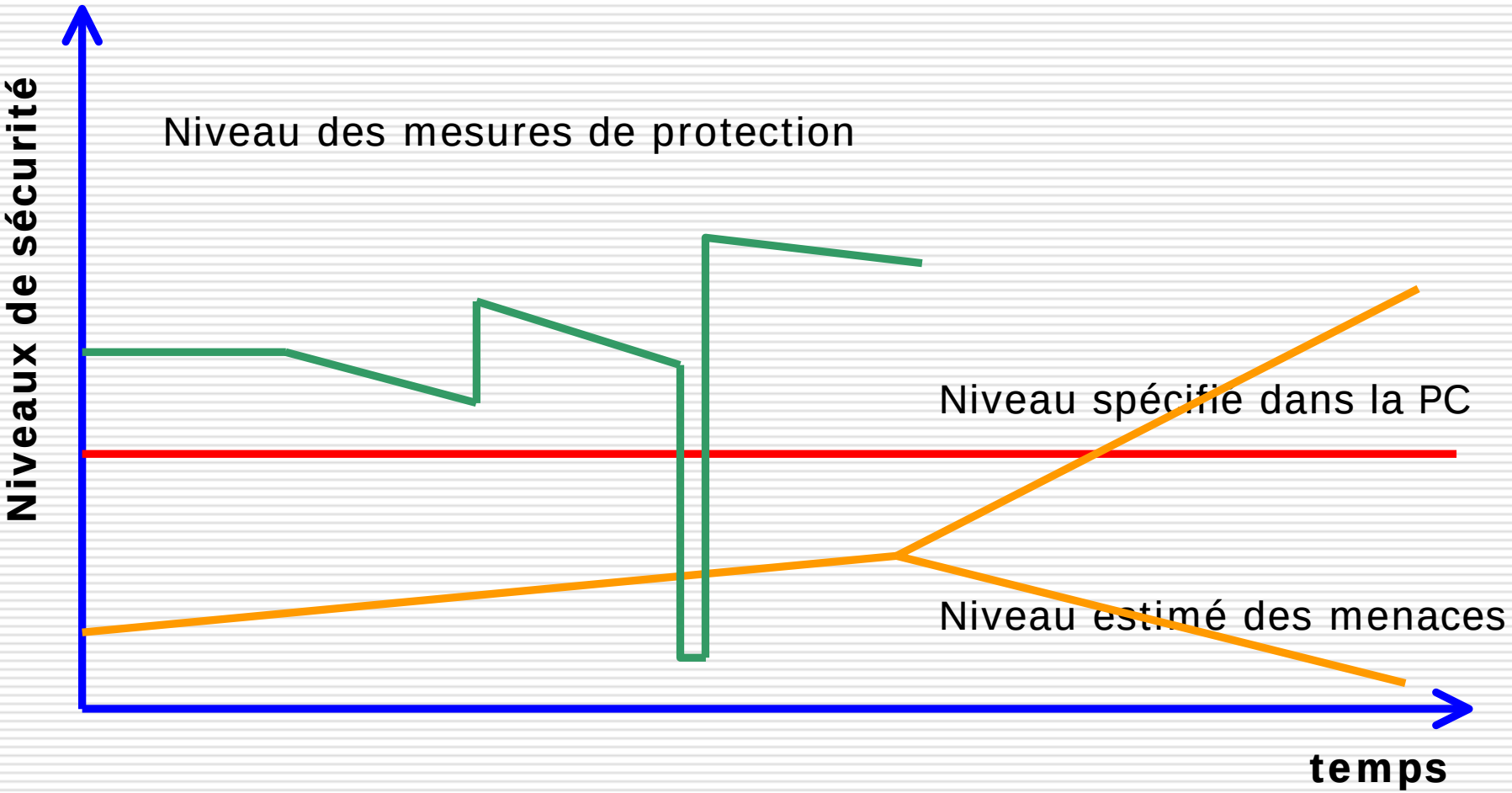
Exploiter une IGC

- Un pari de longue durée
- Changer les clefs du certificat racine est-t-il possible ?
- Validité du certificat racine : plusieurs décennies
- AC des impôts 2013
- Certiposte 2018
- Verisign 2028

Exploiter une IGC



Exploiter une IGC



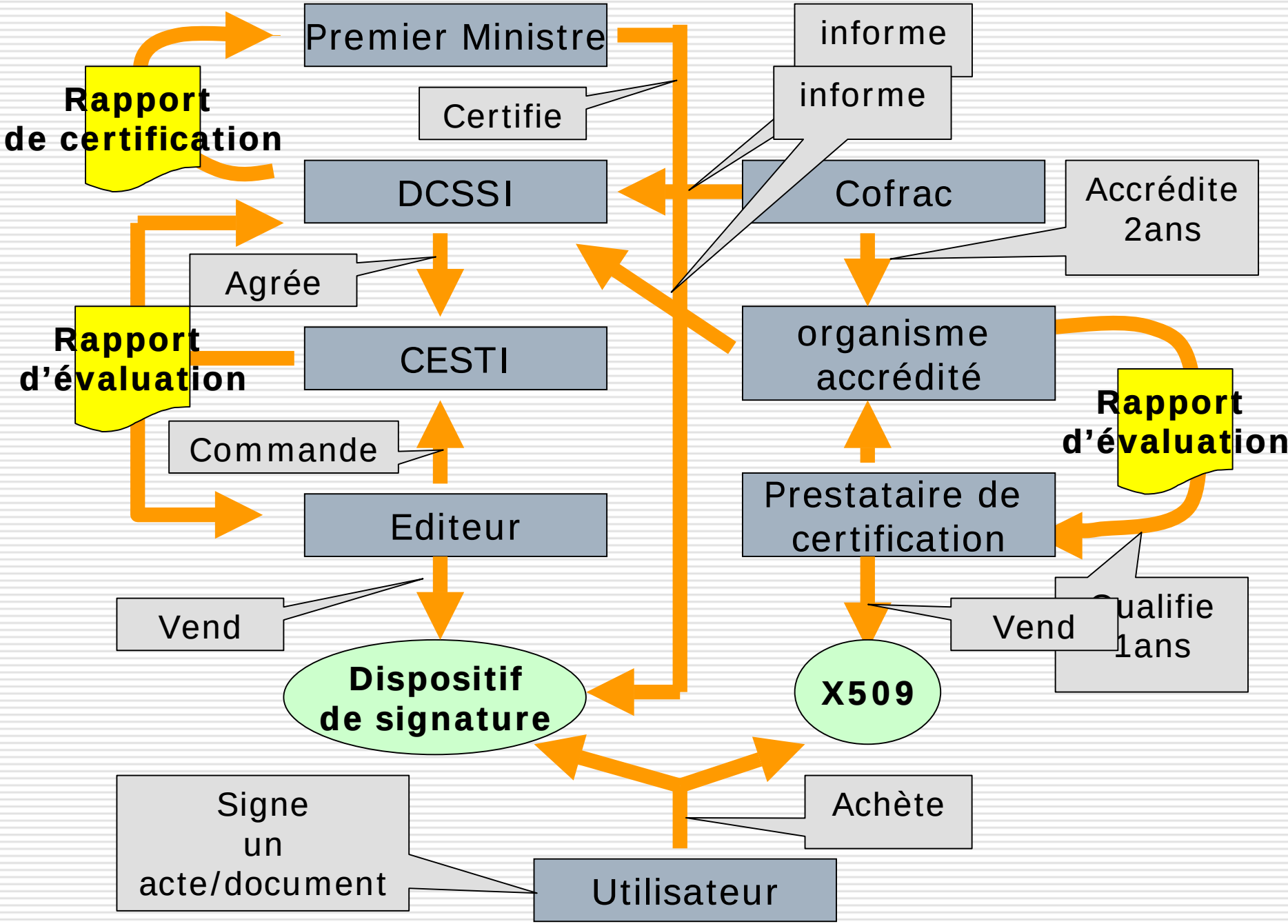
Peut-on faire évoluer la PC ?

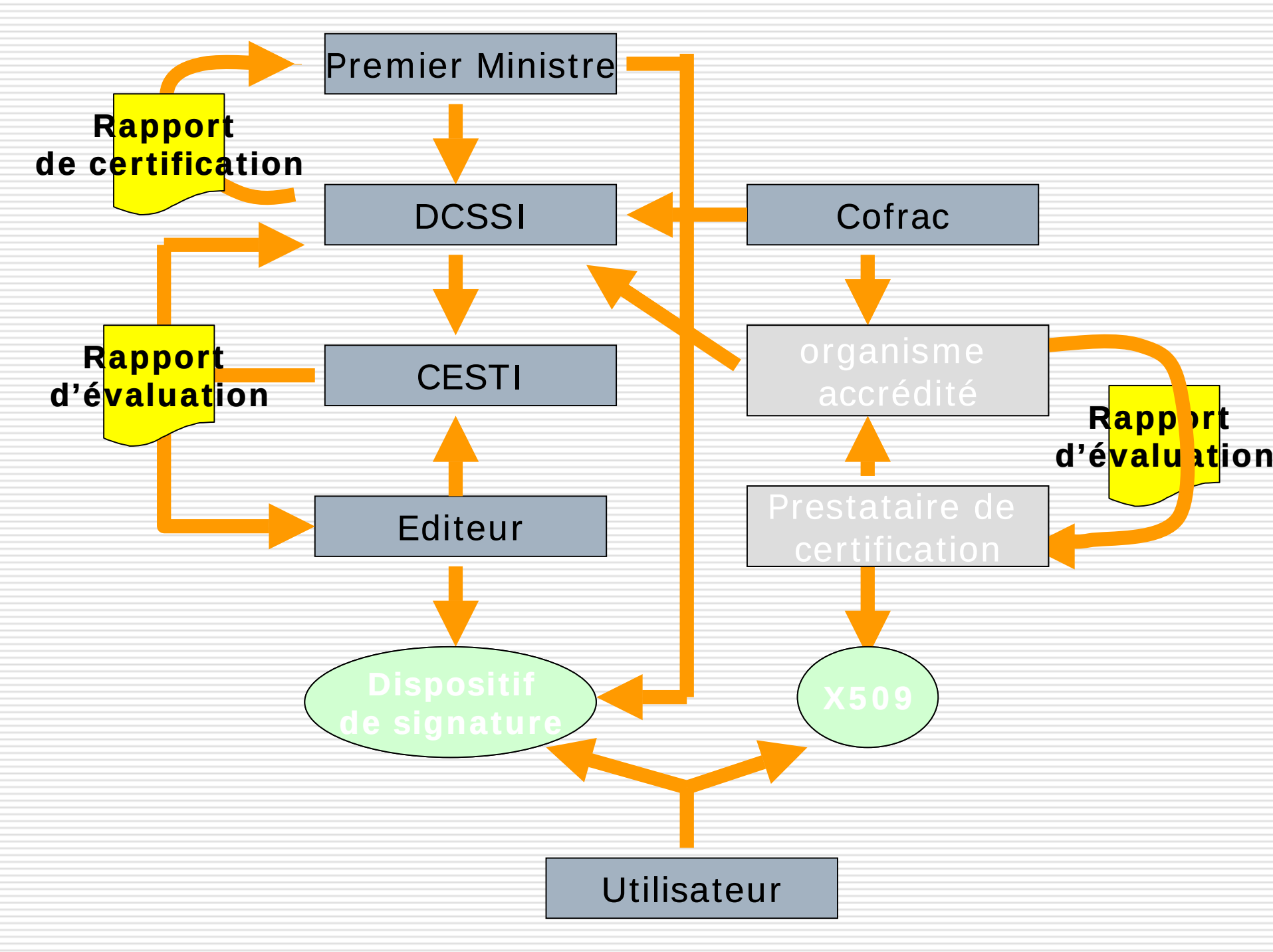
- Un ID de la PC doit figurer dans chaque certificat (attribut *certificat policies*)
- Il est donc possible de dériver plusieurs versions d'une PC
- on ne peut pas « rattraper » les certificats émis
- On se doit donc de respecter la PC jusqu'à expiration des certificats émis.

- Motivation
- https : illusion de sécurité ?
- Protection des clés privées
- Mobilité
- Les AC de confiance
- La révocation
- Exploiter une IGC
- L'interopérabilité
- Signature : la loi
- Signature : la techno
- Dématérialisation
- Faut-il brûler vos certificats ?

La signature

- La loi distingue trois types de signature :
  1. Signature électronique
  2. Signature électronique sécurisée
  3. Signature électronique sécurisée présumée fiable
- Vocabulaire destructeur
- Présomption de fiabilité : dispositif certifié + certificats qualifiés


Premier Ministre
Rapport de certification
Certifie
informe
informe
DCSSI
Cofrac
Accrédite 2ans
Agrée
Rapport d'évaluation
CESTI
organisme accrédité
Rapport d'évaluation
Commande
Editeur
Prestataire de certification
Vend
Vend
Qualifie 1ans
Dispositif de signature
X509
Signe un acte/document
Achète
Utilisateur


Premier Ministre
Rapport
de certification
DCSSI
Cofrac
Rapport
d'évaluation
CESTI
organisme
accrédité
Rapport
d'évaluation
Editeur
Prestataire de
certification
Dispositif
de signature
X509
Utilisateur

Un nouveau chantier juridique ?

- Le marché est cadenassé
- La commission européenne pense assouplir le dispositif.
- Malgré la complexité de cette organisation, des experts juridiques estiment que le dernier mot reviendra à la jurisprudence.

- Motivation
- https : illusion de sécurité ?
- Protection des clés privées
- Mobilité
- Les AC de confiance
- La révocation
- Exploiter une IGC
- L'interopérabilité
- Signature : la loi
- Signature : la techno
- Dématérialisation
- Faut-il brûler vos certificats ?

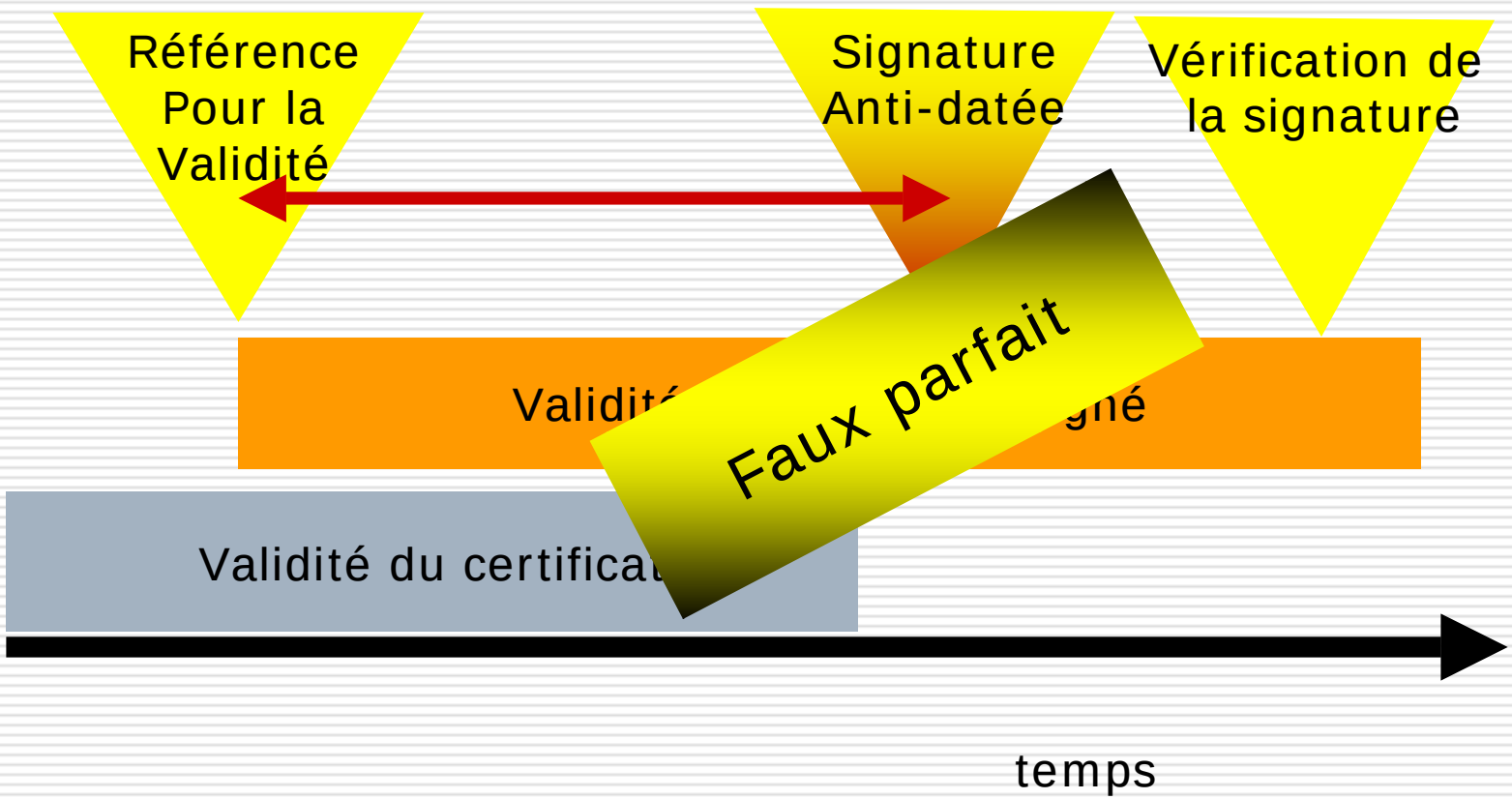
La signature : un concept complexe

- La notion de signature (manuscrite ou numérique) dépend des usages et de la culture.
- La transposition dans le monde numérique de la notion de fausse signature donne froid dans le dos.
- Il faut du solide

What you see is what you sign

- Une notion simple difficile à garantir !
- « Word » et « Word pad » peuvent donner des versions différentes du même document.
- Les macros et les includes peuvent affecter la vue du document sans affecter l'indicateur d'intégrité de la signature !
- Quelle *TOE* pour l'évaluation d'une application de signature ?

Horodatage


Référence
Pour la
Validité
Signature
Anti-datée
Vérification de
la signature
Faux parfait
temps

Horodatage

- Comment se protéger d'un faux anti-daté établi avec un certificat révoqué (ou expiré) ?
- Horodatage = signature par une autorité de datation de la date et de l'empreinte du document signé.

Rien sur l'horodatage dans le droit français.

- Motivation
- https : illusion de sécurité ?
- Protection des clés privées
- Mobilité
- Les AC de confiance
- La révocation
- Exploiter une IGC
- L'interopérabilité
- Signature : la loi
- Signature : la techno
- Dématérialisation
- Faut-il brûler vos certificats ?

La dématérialisation

- La dématérialisation de procédure est la principale justification de la notion de signature
- Les directives européennes imposent la dématérialisation pour créer le marché correspondant.
- Il y aurait des « gisements de productivité » dans la dématérialisation !

La dématérialisation

- Dématérialiser impose de formaliser complètement la procédure
- Beaucoup de procédures fonctionnent parce qu'elles ne sont pas complètement formelles : le facteur humain n'est pas seulement un facteur de lenteur, d'erreurs ou de coûts, c'est aussi un facteur de souplesse et d'intelligence.

La dématérialisation

- Les documents préparatoires du Plan Stratégique pour l'Administration Electronique (PSAE) reconnaissent 2 dangers :
  1. Les risques pour les libertés individuelles
  2. L'accroissement de la « fracture numérique »

Les libertés individuelles

- La CNIL nous a appris
  - qu'il convient de mettre des gardes fous pour prévenir les tentations abusives, en particulier celle de l'administration.
  - qu'un identifiant universel est un danger potentiel.
- Le PSAE crée un « dossier électronique personnel » centralisé

Accroissement des inégalités

- Les objectifs de productivité de l'administration et d'économies sont-ils compatibles avec les précautions indispensables pour limiter les inégalités d'accès dues aux disparités :
  - économiques
  - culturelles
  - géographiques

- Motivation
- https : illusion de sécurité ?
- Protection des clés privées
- Mobilité
- Les AC de confiance
- La révocation
- Exploiter une IGC
- L'interopérabilité
- Signature : la loi
- Signature : la techno
- Dématérialisation
- Faut-il brûler vos certificats ?

Faut-il brûler votre certificat ?

- Impossible de contrôler les éléments fondamentaux d'une PC avec les clients actuels
- pas de progrès sensibles sur ce plan depuis plusieurs années.

Faut-il brûler votre certificat ?

- Serveurs SSL : coût mesuré sans HSM mais, gain à vérifier
- Certificats commerciaux requis ?
- SSL avec authentification du client :
  - pour des populations limitées
  - avec support cryptokey
  - déploiement délicat : infrastructure, distribution, formation, renouvellement, etc
- Examiner les alternatives comme CAS qui offre un très bon niveau de sécurité.

Faut-il brûler votre certificat ?

- VPN avec certificats: oui, mais ne pas demander l'impossible : traverser le firewall avec du trafic chiffré

- S/MIME : ce n'est pas de la signature. Bonne réponse à la menace de diffusion de faux messages à condition d'être systématique pour créer les habitudes.

Faut-il brûler votre certificat ?

- pas d'alternative aux certificats pour la signature et la dématérialisation, oui mais il faut :
  - une implication de l'état (semble venir)
  - un cadre juridique plus abouti
  - archivage et horodatage
  - gestion des privilèges et autorisations
  - workflow complet à mettre en œuvre (serveur et client)