Certificats (électroniques) : Pourquoi ? Comment ?

CA CNRS-Test et CNRS

Nicole Dausque CNRS/UREC
CNRS/UREC
IN2P3 – Cargèse
23-27/07/2001

http://www.urec.cnrs.fr/securite/articles/certificats.kezako.pdf
http://www.urec.cnrs.fr/securite/articles/PC.CNRS.pdf
http://www.urec.cnrs.fr/securite/articles/CA.CNRS-Test.pdf
http://www.urec.cnrs.fr/securite/articles/IGC.pdf

Sommaire

- Rappel des services de base en sécurité
- Lacunes des applications réseau actuelles
- Principes : chiffrement, empreinte, signature, certificats
- Autorité de Certification
- Infrastructure de Gestion de Clés
- Quelques applications et standards
- Exemple de client : Netscape
- Autorité de certification CNRS
- Comment combler les lacunes des applications
- Bilan des certificats

Rappel des services de base en sécurité (1)

urec

- Authentification
  - Assurance de l'identité d'une personne, d'un objet
  - Carte nationale d'identité, passeport
- Intégrité
  - Garantie de non modification par un tiers
  - Document manuscrit : simple
- Confidentialité
  - Protection contre la « lecture » non autorisée par un tiers
  - Coffre-fort, pli cacheté

Rappel des services de base en sécurité (2)

- Non-répudiation
  - Pour que l'émetteur ne puisse pas nier l'envoi
  - Et le récepteur ne puisse pas nier la réception
  - Transactions financières – commerciales

- Contrôle d'accès
  - Autorisations ou non d'accès à des objets

Lacunes des applications réseau actuelles (1)

urec

- Pourquoi cette nouvelle problématique ?
  - Documents électroniques : modifications difficilement détectables
  - Réseaux informatiques : confidentialité, intégrité, … : mécanismes à mettre en place
- Pas d'authentification dans la messagerie électronique :
  - Notes officielles sous forme papier
- Pas de confidentialité dans la messagerie électronique :
  - Élections, notations, gestion personnel, financière, … : courrier postal
- Applications de gestion :
  - Plusieurs administrations de comptes avec mots de passe

Lacunes des applications réseau actuelles (2)

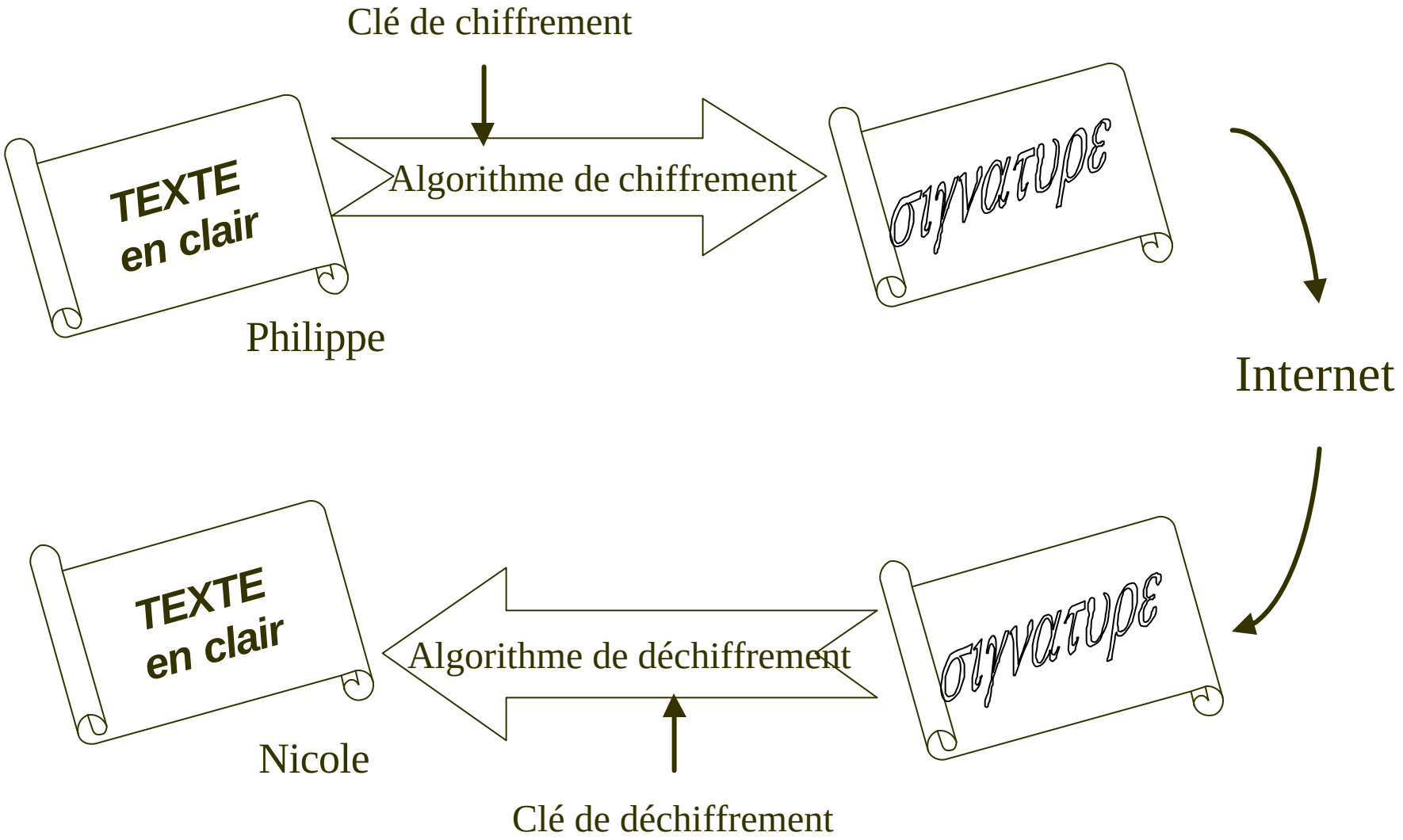
urec

- CNRS : pas d'Intranet. D'où des difficultés pour :
  - Mettre sur un serveur Web des informations réservées aux agents CNRS
  - Diffuser des logiciels avec des contrats de licences « organisme »
  - Respecter les contrôles d'accès à des bases de données payantes (contrat organisme)
  - Créer des espaces de libre échange pour des groupes de travail ou des communautés
- Accès à distance : mot de passe en clair sur le réseau
- Authentification dans les projets de calcul distribués (grilles)

Fondation commune pour couvrir ces besoins

les certificats

Chiffrement : confidentialité



Chiffrement : algorithmes symétriques

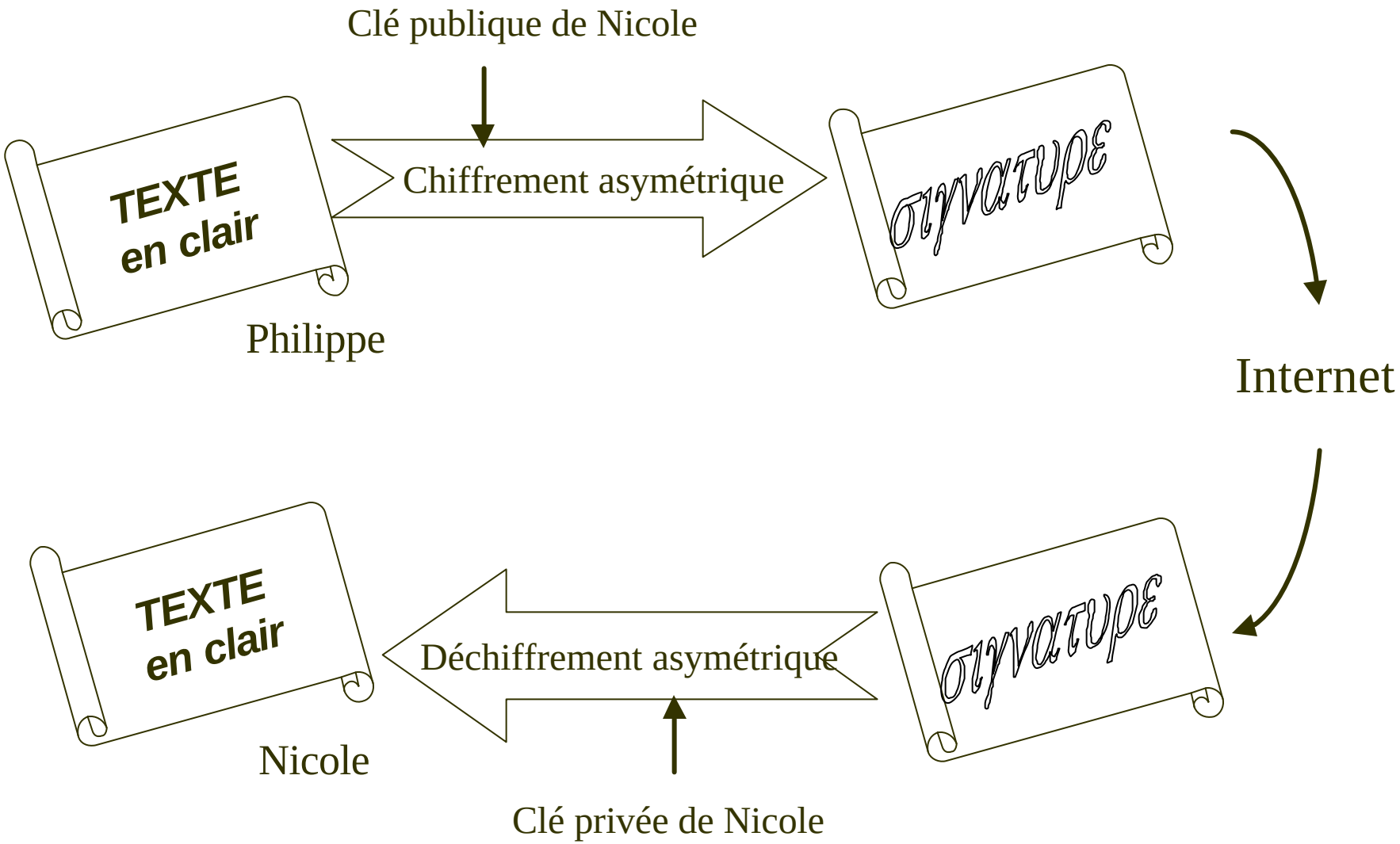
- Clé de chiffrement = clé de déchiffrement
  - D'où : clé secrète
- DES (Data Encryption Standard) : 56 bits
- Triple DES : 112 bits
- AES (Advanced Encryption Standard)
- Chiffrement et déchiffrement rapides
- Problème de gestion des clés
  - Nombre de clés très élevé
  - Besoin de canal sécurisé pour les échanges de clés

Chiffrement: algorithmes asymétriques

urec

- Clé de chiffrement ≠ clé de déchiffrement
- Couple de clés (créées ensemble)
- Impossible de découvrir une clé à partir de l'autre
- Tout texte chiffré avec une clé est déchiffré avec l'autre et uniquement avec celle-ci
- Concrètement :
  - 1 couple de clés / utilisateur ou machine ou application
  - Créé par l'utilisateur sur son poste ou …
  - 1 clé publique : que l'on rend publique (annuaire)
  - 1 clé privée : que le propriétaire est le seul à connaître

Chiffrement asymétrique



Chiffrement : algorithmes asymétriques

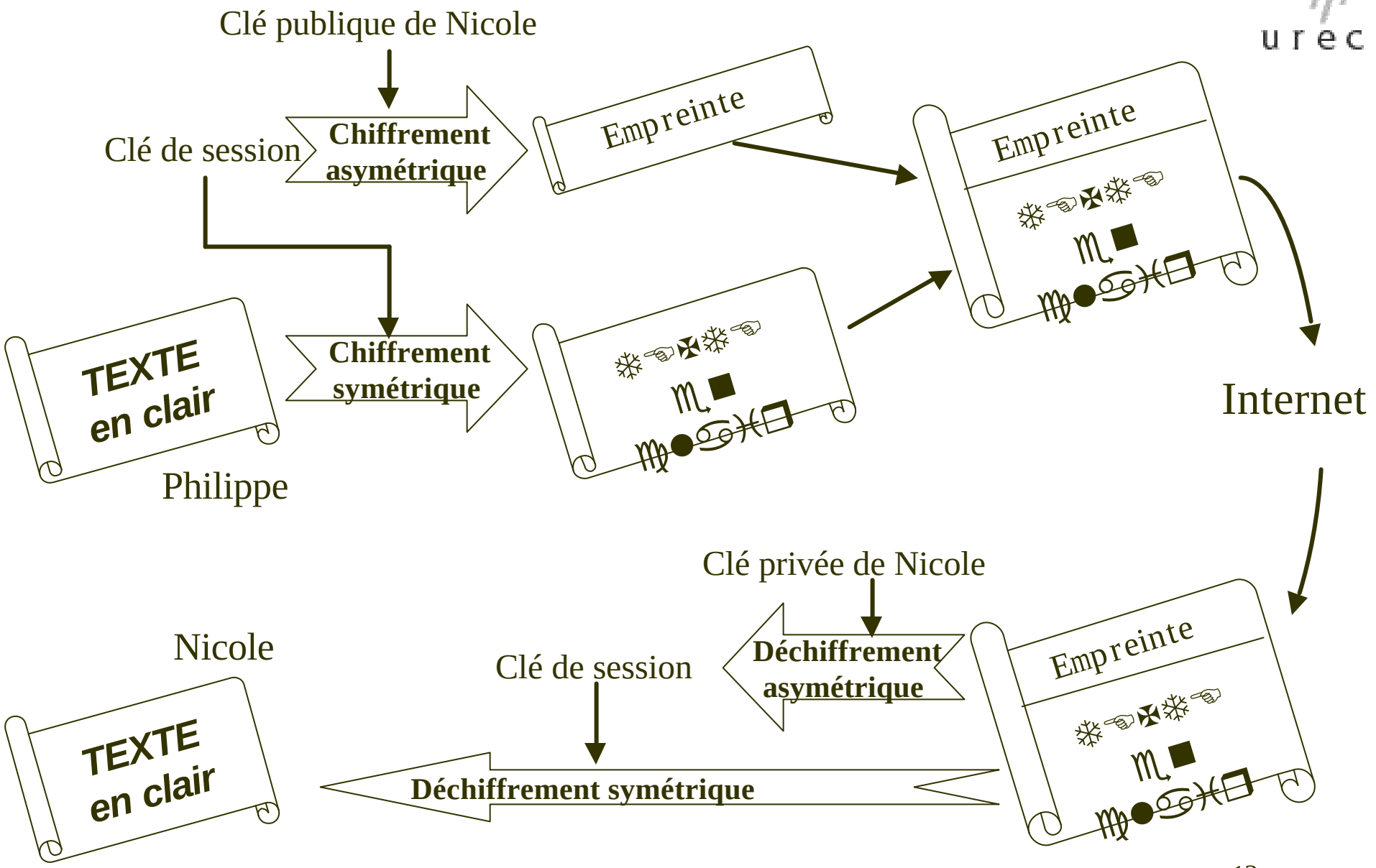
- RSA (Rivest, Shamir, Adelman)
- Si annuaire des clés publiques : permet une utilisation du chiffrement de manière planétaire
- Problème : temps de chiffrement et de déchiffrement
  - RSA : 1000 fois plus lent que Triple DES

- Algorithmes de chiffrement : publics
  Secret : certaines clés

Chiffrement : clé de session (1)

- Pour contourner les mauvaises performances des traitements avec les algorithmes asymétriques
- Durant une session (courte dans le temps) :
  - Choix d'une clé (de session) par un des interlocuteurs
  - Transfert de cette clé chiffrée de manière asymétrique à l'autre interlocuteur
  - Ensuite, utilisation de cette clé pour chiffrer de manière symétrique le texte
- Nombre de bytes chiffrés en asymétrique (clé de session) très petit / nombre de bytes chiffrés en symétrique (le texte)

Chiffrement : clé de session (2)



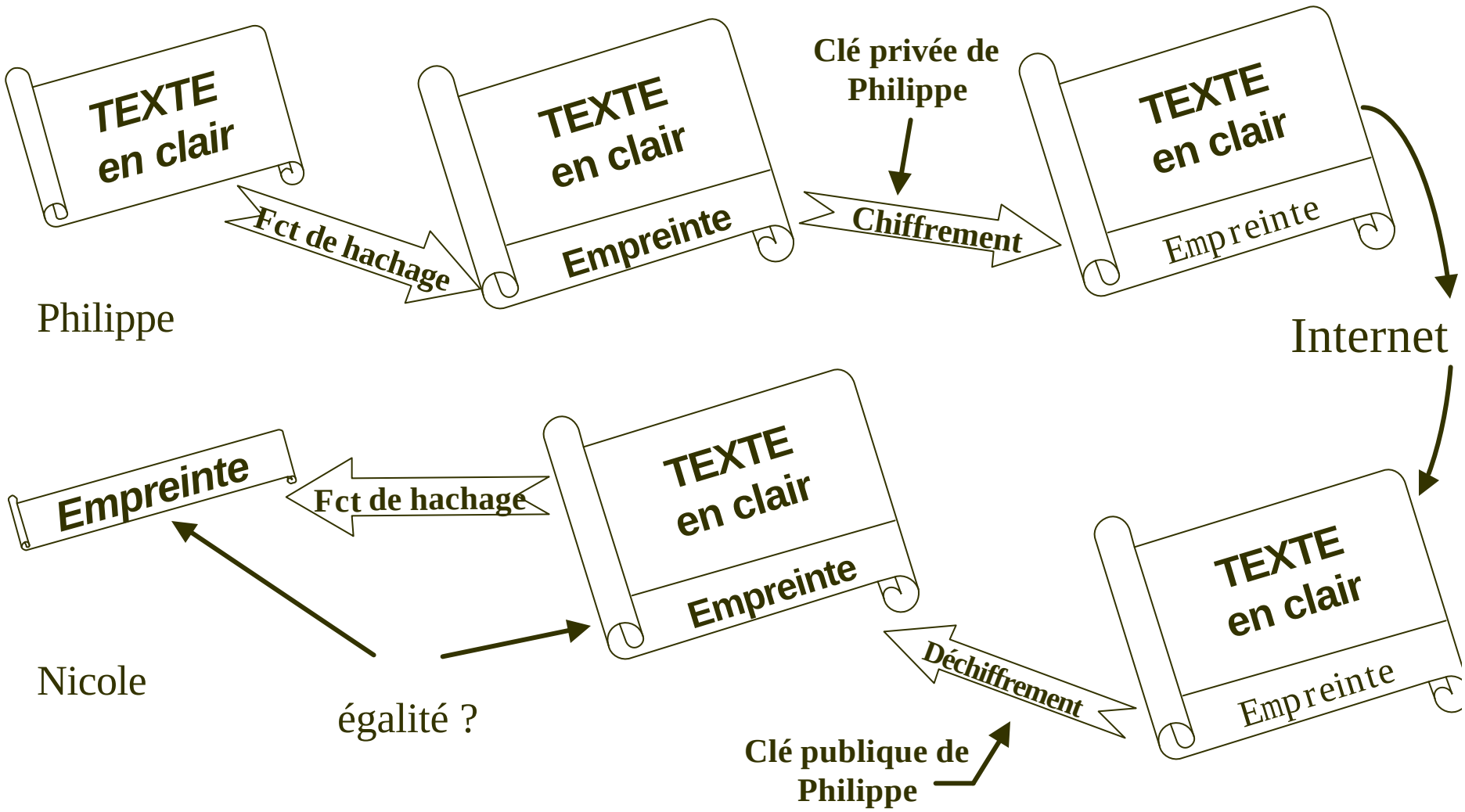
Chiffrement : longueur des clés

- Décrypter
  - Déchiffrer sans posséder la clé de déchiffrement
  - Nombreuses méthodes. Limite : rapidité des calculateurs (Ouf !)
- Plus la clé est longue (nombre de bits), plus il est difficile de décrypter
  - Avec un algorithme de chiffrement solide (bon mathématiquement)
- La puissance des machines augmente
  - La taille des clés utilisées doit augmenter
  - La législation s'adapte :
    Utilisation des produits de chiffrement en France :
    - Avant 1999 : libre pour des clés jusqu'à 40 bits
    - Après 1999 : libre pour des clés jusqu'à 128 bits

Signature électronique

- Un mécanisme pour l'authentification et l'intégrité
- Utilise une fonction de hachage (appliquée sur le document)
  - Génère une suite de bits de taille fixe (très petite)
  - Empreinte ou condensé
  - Un bit du texte initial modifié ⇒ Empreinte différente
  - MD5 (Message Digest) : empreinte de 128 bits
  - SHA (Secure Hash Algorithm) : empreinte de 160 bits
- Outils courants : permettent de signer et de chiffrer

Signature électronique (2)

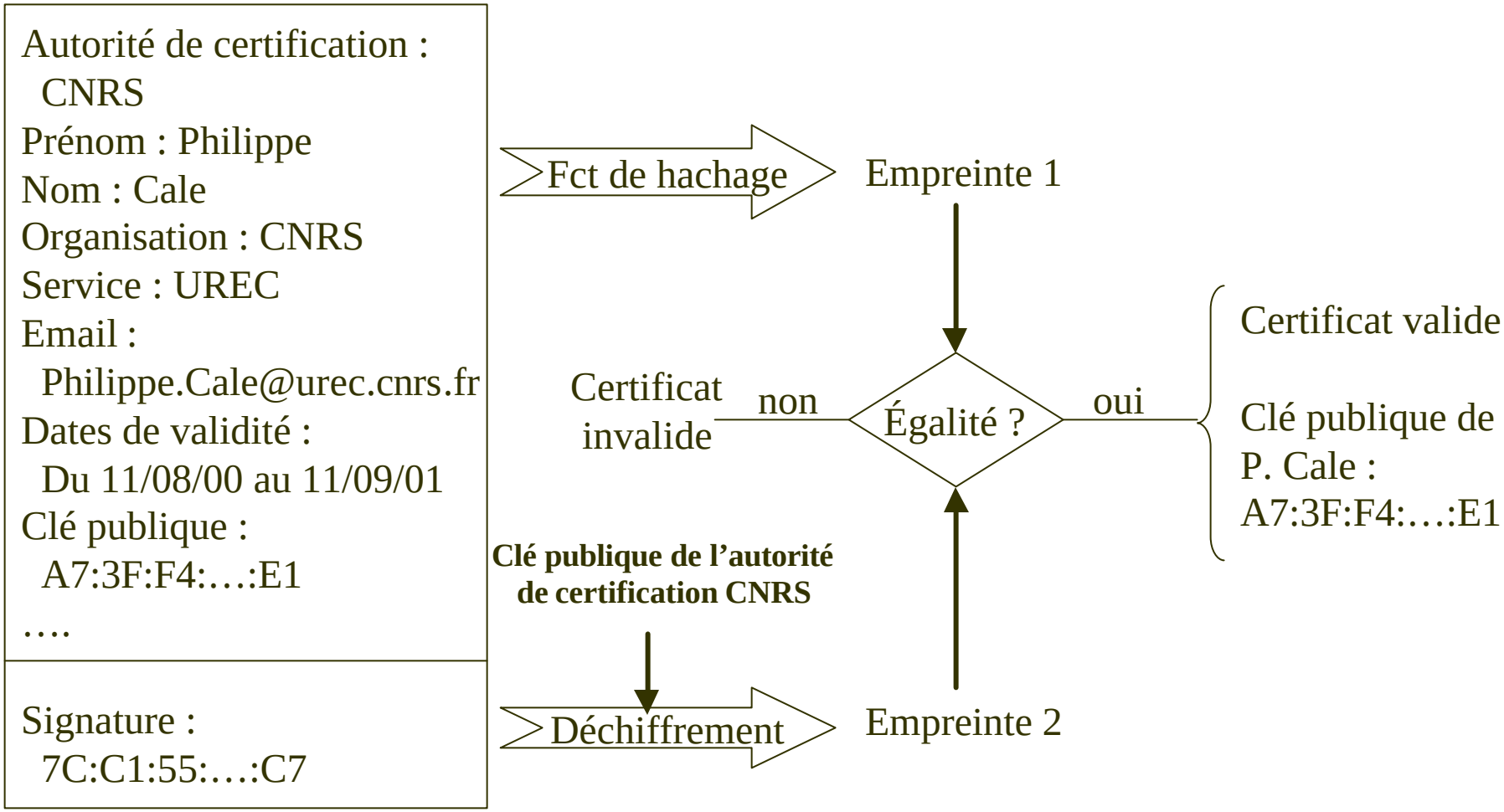


Certificats : principes

- Pb : comment être sûr de la clé publique d'une personne ?
- Solution : certificat : carte d'identité ou passeport
- Fichier, créé et délivré par une autorité de certification
  - Exemple : CNRS
- Contient :
  - Nom de l'autorité (CNRS par exemple)
  - Nom, prénom, email, infos diverses (numéro d'agent, unité, …)
  - Clé publique de la personne
  - Signature de l'autorité de certification (CNRS par exemple)
- Vérification d'un certificat (qui garantit la clé publique)
  - Avec la clé publique de l'autorité de certification
  - Et la date de validité
- Toute personne voulant vérifier un certificat CNRS doit connaître la clé publique de l'autorité de certification CNRS

Certificats : vérification

Certificat de P. Cale



Autorité de certification

- Techniquement, une autorité de certification peut être n'importe qui
- Quelle autorité ? Exemple : 3 choix pour le CNRS
  - Société commerciale
    - La plupart sont américaines (France : CERT-Plus et Poste)
    - Coût d'un certificat : 200 F / pers / an
  - Attendre une autorité de certification ministère(s)
  - Décider de mettre en place ce service
- Décision stratégique pour une entreprise, organisme, …

Infrastructure de gestion de clés : IGC (1)

urec

- Certificat = Carte d'identité ou passeport
  - Il faut : mairies, préfectures, agents de mairie, éditeurs, tampons, formulaires, fichiers, …
- IGC : Infrastructures de Gestion de Clés
  - ICP : Infrastructures à Clés Publiques
  - PKI : Public Key Infrastructure
- 3 éléments :
  - Autorités d'enregistrement
  - Autorité(s) de certification
  - Service(s) de publication
- Certificats pour des personnes, des applications, des matériels

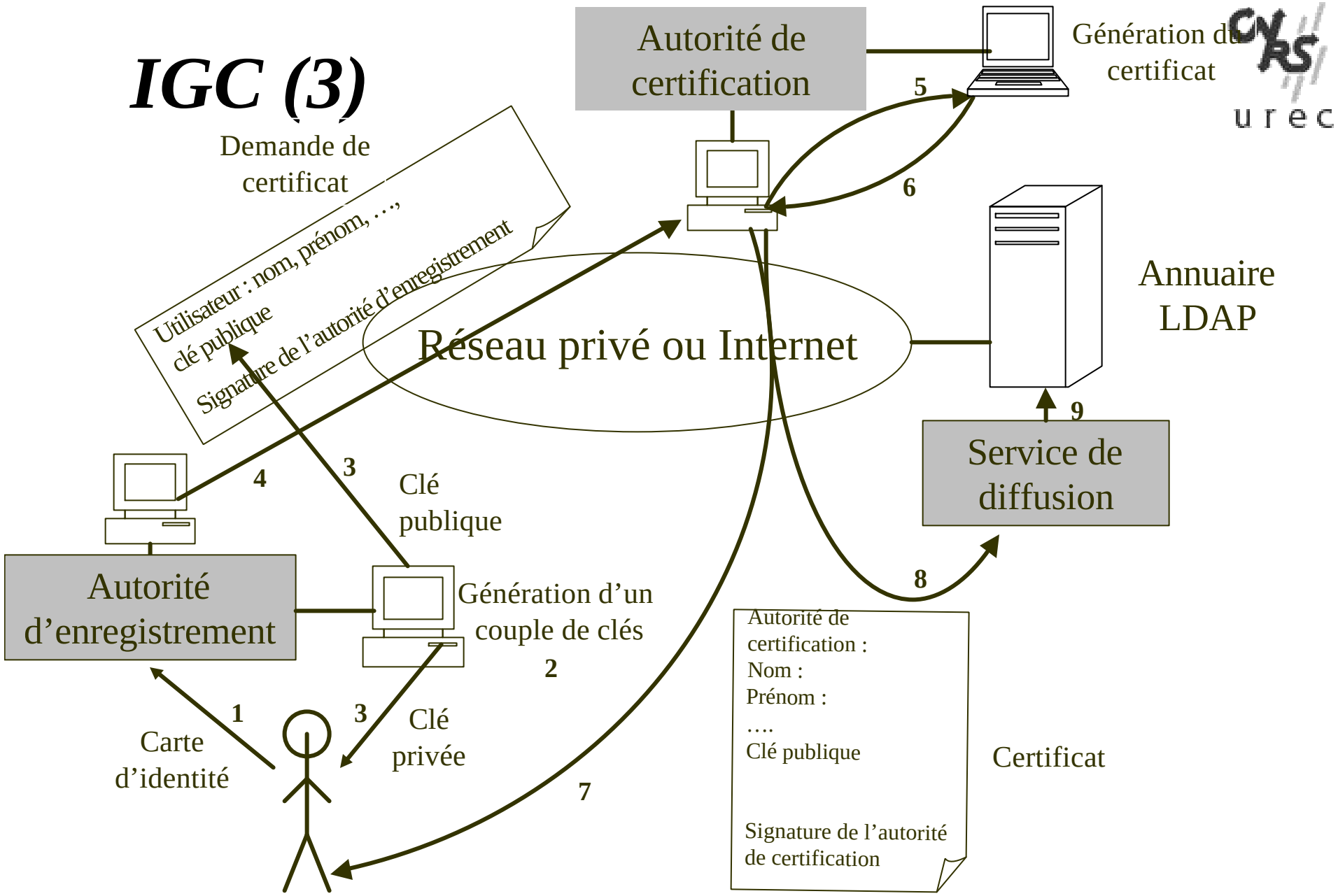
IGC (2)

- Autorités d'enregistrement
  - Guichets auxquels s'adressent les utilisateurs demandeurs de certificat
  - Vérification de l'identité de l'utilisateur
  - Récupération (éventuellement génération) de la clé publique de l'utilisateur
  - Transmission de demandes (signées) de création de certificat à l'autorité de certification

IGC (3)

- Autorité de certification
  - Reçoit les demandes de créations de certificats
  - Crée les certificats
  - Signe les certificats
  - Transmet les certificats aux utilisateurs et au service de publication
  - Possède un certificat avec sa clé publique auto-signé ou signé par une autorité « supérieure »
- Service de publication
  - Rend accessible les certificats : annuaire LDAP
  - Publie une liste des certificats révoqués

IGC (3)


Autorité de certification
Génération du certificat
5
6
Demande de certificat
Utilisateur : nom, prénom, …,
clé publique
Signature de l'autorité d'enregistrement
Réseau privé ou Internet
Annuaire LDAP
9
Service de diffusion
4
3
Clé publique
Autorité d'enregistrement
Génération d'un couple de clés
2
8
Autorité de certification :
Nom :
Prénom :
….
Clé publique
Signature de l'autorité de certification
1
3
Carte d'identité
Clé privée
7
Certificat

IGC CNRS : points d'interrogation

- Quelle durée de validité d'un certificat ?
  - Lors de la création
  - Liste de révocation (périodicité de publication)
- Des certificats CNRS pour qui ?
- Certificat pour signer et/ou pour chiffrer ?
- Séquestre et sauvegarde des clés privées ?
  - En cas de perte
  - En cas de requête de la justice

IGC CNRS : points d'interrogation (2)

- Stockage du certificat et de la clé privée
  - Disquette, carte à puce
- Signature de l'autorité de certification CNRS
- Quelle sous-traitance ?
- Utilisation de logiciels libres ou commerciaux ?
- Besoin de recommandations
  - Synchronisation des horloges : NTP
  - Adresses électroniques canoniques
- . . .

Quelques applications et standards

- S/MIME : standard messagerie
  - Authentification, intégrité (signature)
  - Confidentialité (chiffrement)
  - Supporté par Netscape et Internet Explorer (Outlook)
- HTTPS et SSL : communications Web
  - Supporté par Netscape et Internet Explorer
- IPSec : communications entre équipements réseau ou ordinateurs
- Ces 3 applications sont complémentaires
- Autres : IMAPS, POPS, Stelnet (?), SFTP (?),...utilisent les certificats

S/MIME : message non sécurisé

From : Philippe.Cale@urec.cnrs.fr

To : Serge.Montau@cru.fr

Date : 18 septembre 2000

Subject : CR réunion Paris

****

Je te joins le compte-rendu de la dernière réunion.

Philippe

****

Type de fichier : Word

Nom du fichier : CR.doc

<Fichier Word contenant le compte-rendu>

****

S/MIME : message signé

From : Philippe.Cale@urec.cnrs.fr
To : Serge.Montau@cru.fr
Date : 18 septembre 2000
Subject : CR réunion Paris
Type de message : Signé au format PKCS7
****

Je te joins le compte-rendu de la dernière réunion.
Philippe
****

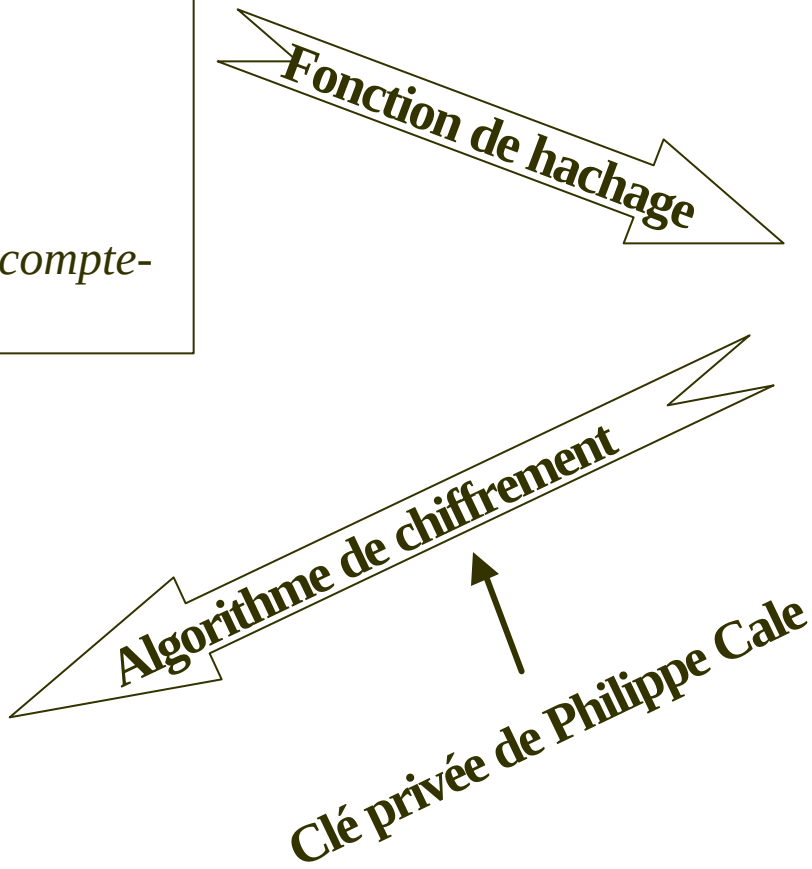
Type de fichier : Word
Nom du fichier : CR.doc
<Fichier Word contenant le compte-rendu>
****

Signature :
MIIFsgYJKoZIhvc …
….JTMQsCQYqsdQ
****

S/MIME : génération de la signature

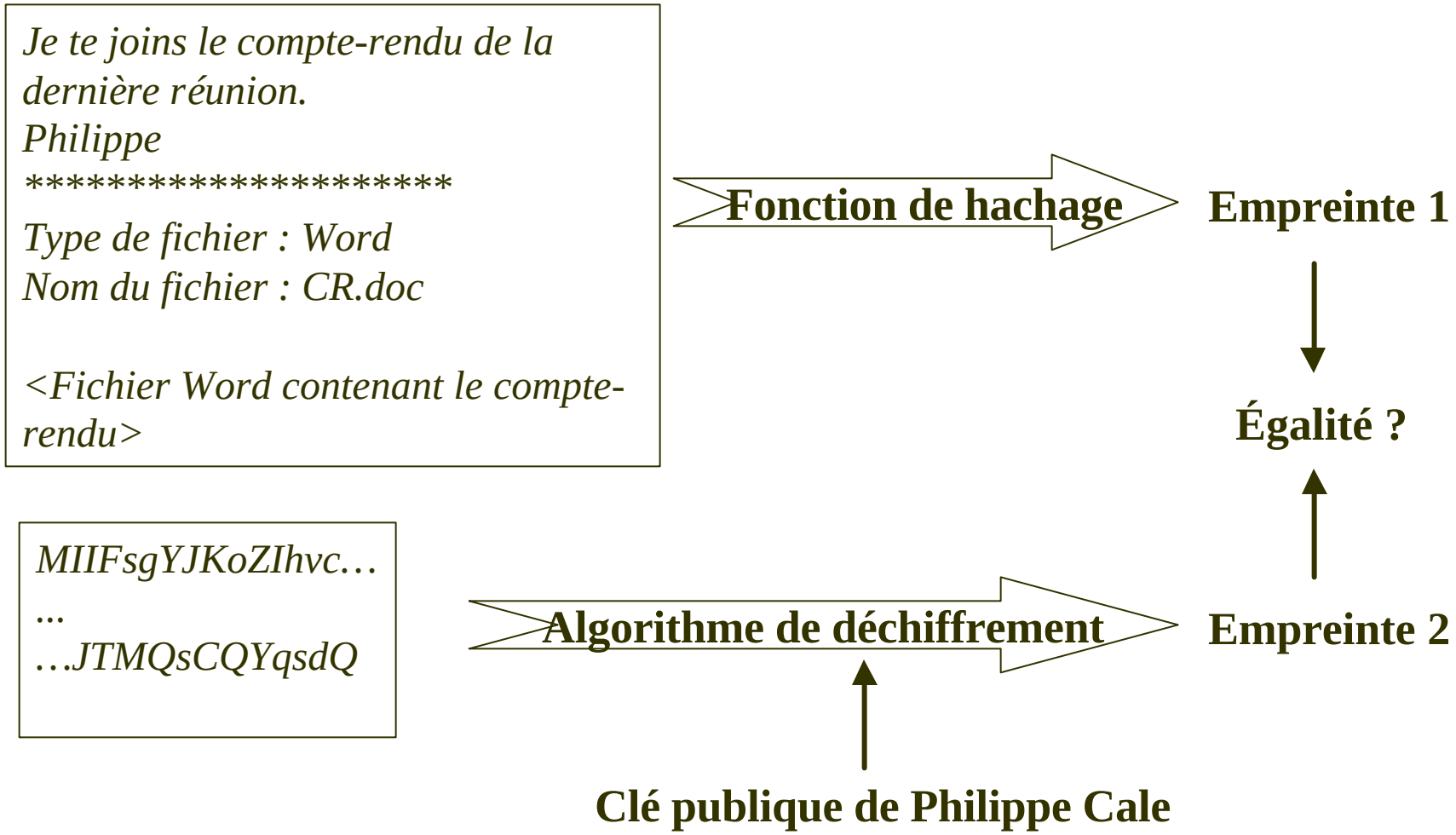
Je te joins le compte-rendu de la dernière réunion.
Philippe
****
Type de fichier : Word
Nom du fichier : CR.doc

<Fichier Word contenant le compte-rendu>



MIIFsgYJKoZIhvc…
…
…JTMQsCQYqsdQ

S/MIME : vérification de la signature



S/MIME : message chiffré

From : Philippe.Cale@urec.cnrs.fr

To : Serge.Montau@cru.fr

Date : 18 septembre 2000

Subject : CR réunion Paris

Type de message : chiffré au format PKCS7

MIAGCSqGSIb3DQEHA6CAMIACA …

…

… g+h7gBDhCfCAAAAAAAAAAAAA=

S/MIME : chiffrement

Je te joins le compte-rendu de la dernière réunion.
Philippe
****
Type de fichier : Word
Nom du fichier : CR.doc

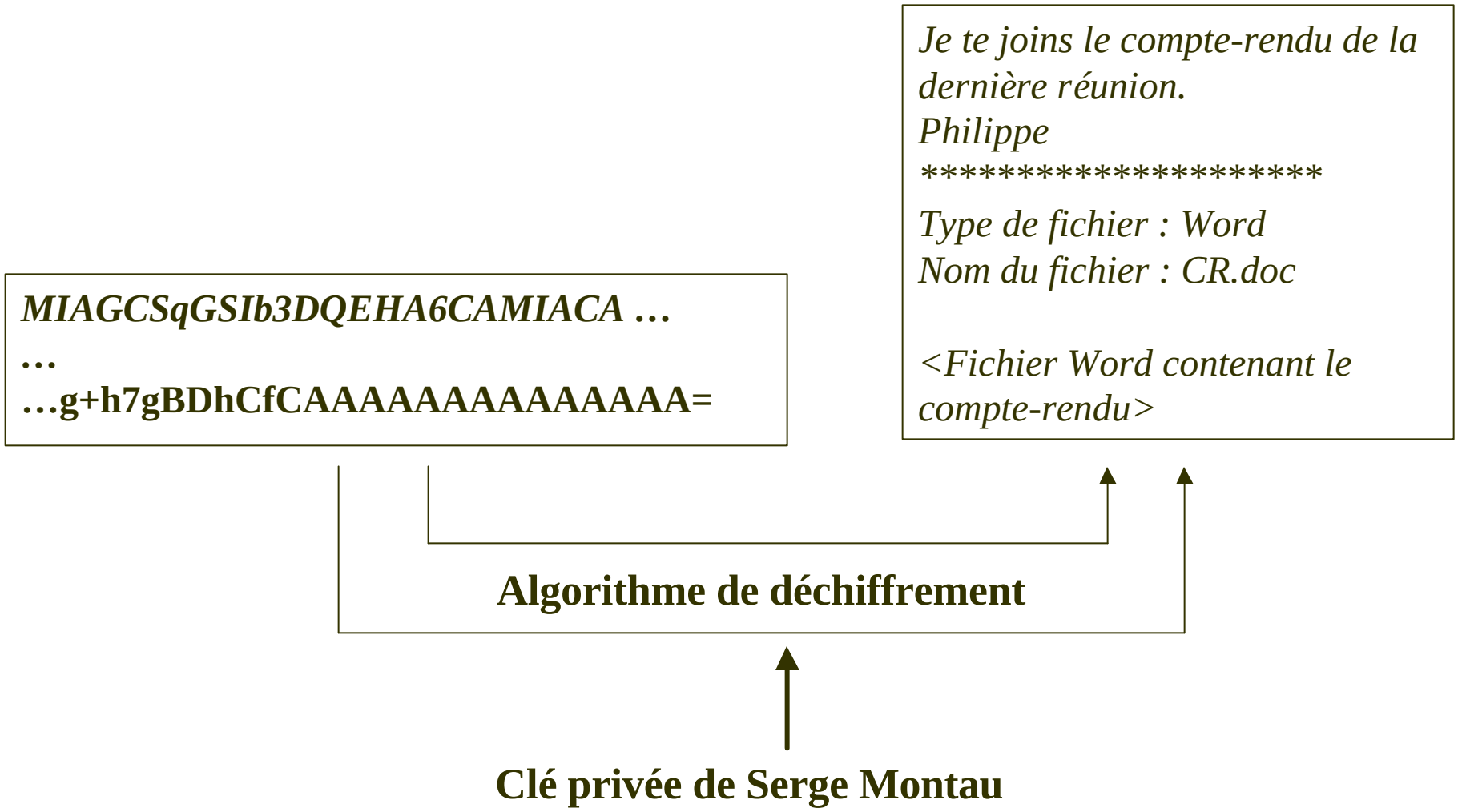
<Fichier Word contenant le compte-rendu>

MIAGCSqGSIb3DQEHA6CAMIACA …
…
…g+h7gBDhCfCAAAAAAAAAAAAA=

Algorithme de chiffrement

Clé publique de Serge Montau

S/MIME : déchiffrement



SSL et HTTPS

- SSL (Secure Socket Layer)
  - Pour applications en mode client-serveur sur TCP
  - Authentification des extrémités, confidentialité et intégrité des échanges
  - Utilisation de certificats et de clés de session
  - Flot de données découpé en paquets signés et chiffrés
- HTTPS = HTTP sur SSL
  - URL : https://www.services.cnrs.fr/csec/
- Utilisation courante : seul le serveur possède un certificat
  - Serveur Web sécurisé
  - Authentification du serveur
  - Chiffrement des échanges : transmission numéro carte bancaire, authentification des utilisateurs avec mot de passe sans risque d'écoute

IPSec

- Chaque datagramme IP peut être signé (authentification et intégrité) et chiffré (confidentialité) : entêtes IP (v4 et v6) spécifiques
- Utilisation de certificats possible
- Entre équipements IP
  - Routeurs
  - Stations

Client Netscape et les certificats (1)

- Fonctions sur le poste utilisateur
  - Générer un couple de clés privée-publique
  - Stocker la clé privée, protégée par un mot de passe
  - Exporter la clé privée et le certificat dans un fichier (avec mot de passe) qui pourra être copié sur une disquette pour être utilisé sur un autre poste, avec IE, …
  - Récupérer le certificat (donc la clé publique) et la liste de révocation d'une autorité de certification

Client Netscape et les certificats (2)

- Fonctions sur le poste utilisateur (suite)
  - Signer et chiffrer un message avant l'envoi
    - Pour signer : mot de passe pour accéder à la clé privée
    - Pour chiffrer : certificat du destinataire nécessaire
  - Vérifier la signature d'un message reçu
  - Déchiffrer un message reçu
  - Passer en mode HTTPS-SSL (piloté par le serveur)
  - Pour mettre à jour les tables suivantes

Client Netscape et les certificats (3)

- Tables de certificats
  - Chemin : Navigator-Security-Certificates
  - Des autorités de certification auxquelles Netscape fait confiance (signers) : il faudra ajouter CNRS
  - Des utilisateurs (people): récupérés dans un annuaire LDAP ou dans des messages signés reçus
  - Des serveurs Web
  - De l'utilisateur
    - Un utilisateur peut avoir plusieurs certificats
    - Un utilisateur peut utiliser un certificat différent pour la messagerie et pour accéder à un site Web
  - Listes de révocation : une par autorité de certification

Autorité de certification CNRS : chronologie

- 1999 : travail stagiaire UREC sur S/MIME et les certificats
- Février 2000 : plate-forme de tests CNRS-Test
- Juin 2000 : décision de créer une autorité de certification CNRS et d'en confier la mise en place à l'UREC
- Depuis septembre 2000 : comités
  - de pilotage animé par C. Michau
  - technique animé par JL. Archimbaud
  - travail : définition de la politique de certification et des procédures
- Depuis septembre 2000 : développement du logiciel IGC
  - C. Gross et Ph. Leca
  - OpenSSL et OpenCA avec des adaptations
  - 1ère version opérationnelle début mai 2001
- Début mai 2001 : sites pilotes

Autorité de certification CNRS : CNRS-Test

- Autorité de certification : plate-forme de tests administrée par l'UREC
- Se mettre dans des conditions de production
  - Guide utilisateur en ligne, …
- Acquérir un savoir faire
  - Voir les options possibles, les problèmes, les avantages, …

http://www.urec.cnrs.fr/securite/articles/CA .CNRS-Test.pdf

http://www.services.cnrs.fr/ca/

Autorité de certification CNRS : CNRS-Test : utilisation

urec

- Environ 100 certificats délivrés
  - Aux coordinateurs sécurité et quelques correspondants, utilisateurs Globus (Datagrid)
  - Principalement sous Netscape
- Utilisations
  - Messagerie
    - Signature des avis CERT et autres messages
    - Chiffrement lors de l'envoi de la liste de contrôles, rapport d'incidents, …
  - Accès Web (contrôle d'accès selon le certificat)
    - Documents réservés aux coordinateurs sécurité (accès lecture)
    - Préparation du cours national SIARS (accès lecture et écriture)
  - Calcul distribué : globus

Autorité de certification CNRS : CNRS-Test : bilan

- Navigateurs et outils de messagerie
  - OK avec les dernières versions des logiciels :
    - Netscape, Internet Explorer, Outlook Express
  - Plugin avec Eudora : il semble y avoir des produits (MSI …)
- Être prudent : technologies sont loin d'être mûres et rodées
  - Problème avec la liste de révocation, le renouvellement des certificats, le nom des certificats dans Netscape, opacité des « internes » de Netscape et IE
- Partie organisationnelle est très importante
  - 70 % du travail
- Une formation des administrateurs et des utilisateurs est obligatoire
- Mais les services rendus sont déjà très utiles et prometteurs

  ⇨ ***On continue***

Autorité de certification CNRS : Politique de certification

- http://www.urec.cnrs.fr/securite/articles/PC.CNRS.pdf
- Certificats
  - Pour les personnes
    - Pour authentification et signature : pas de séquestre de clés privées
    - Pour chiffrement : séquestre clés privées (non délivrés dans phase pilote)
  - Pour les services : Web, …
  - Pour les codes : applets, …
- Toute personne dans un laboratoire (ou dans un projet CNRS) pourra disposer d'un certificat
  - Personnel CNRS ou non, permanent ou non
- Applications :
  - Messagerie, contrôle d'accès à des pages Web, listes de diffusion, diffusion de notes officielles …
  - Outils utilisateurs : Netscape, IE (Outlook) au moins

Autorité de certification CNRS : Politique de certification (2)

- Certificat de l'autorité de certification CNRS auto-signé
- 3 sous-autorités
  - CNRS-Standard : utilisation courante
    - AE : directeur du laboratoire ou représentant
  - CNRS-Plus : actes avec une valeur administrative
    - AE : délégué ou représentant ?
  - CNRS-Projets : durée limitée, partenaires non CNRS
    - Une sous-autorité par projet
    - AE : responsable de projet ou représentant
- L'autorité CNRS-Test continue pour les tests
  - Mais avec le logiciel IGC développé et les nouvelles procédures
- Un annuaire LDAP contient les certificats

Autorité de certification CNRS : Politique de certification (3)

urec

- Certificats de personne
  - Format X509V3
  - Algorithme RSA 1024 bits (ou 512 ou 2048)
  - Durée de validité : 1 an par défaut
  - CN : prénom, nom, adresse électronique
  - DN pour personne qui travaille dans un labo CNRS
    - C=FR, O=CNRS, OU=Code unité
  - DN pour CNRS-Projets : dépend du projet
- Certificats de service
  - DN=nom de la machine (sous forme de domaines)
- Certificats signature et intégrité : clé privée de l'utilisateur
  - Générée par l'utilisateur sur son poste
  - Ni connue de l'UREC, ni stockée par l'UREC

Autorité de certification CNRS : Procédures

- Demande de certificat est faite par un formulaire web
  - Nom, prénom, téléphone, email, laboratoire
    - Création du couple de clefs privée-publique (en local)
  - Échange de message pour vérifier l'adresse électronique
  - AE reçoit un message l'avertissant d'une demande
  - Vérification des informations par AE
  - Transfert à AC
  - AC génère le certificat (mise à jour sur LDAP)
  - Utilisateur récupère son certificat
- Chaque AE a un certificat CNRS-Plus
- Révocation : par l'AE

Autorité de certification CNRS : Sites pilotes

urec

- CNRS-Plus
  - Pour les AE
- CNRS-Standard
  - http://igc.services.cnrs.fr/CNRS-Standard/
  - IMAG, LAAS
  - Laboratoires des délégations de Bordeaux et Toulouse
- CNRS-Projets
  - Datagrid-fr
  - SSI
  - JRES2001

Combler les lacunes des applications réseau actuelles (1)

urec

Principe : chaque personnel CNRS possède un certificat (ou plusieurs)

- Pb : pas d'authentification dans la messagerie électronique
  - (notes officielles sous forme papier)
  - Directeurs, délégués, … ont un certificat et signent leurs notes avant de les diffuser électroniquement
- Pb : pas de confidentialité dans la messagerie électronique
  - (Élections, notations, gestion personnel, gestion financière, … : courrier postal)
  - Toutes les personnes peuvent signer et chiffrer leurs messages

Combler les lacunes des applications réseau actuelles (2)

urec

- Pb : applications de gestion
  - (plusieurs administrations de comptes avec mots de passe)
  - Un agent a un certificat qui lui permet d'accéder à une ou plusieurs applications. Les applications se référent à des annuaires et aux certificats pour contrôler l'accès : pas de mot de passe
- Pb : CNRS : pas d'Intranet
  - On peut créer très facilement des Intranet « de personnes »
  - Les serveurs WWW se réfèrent au certificat du client et aux annuaires pour contrôler les accès aux pages Web
- Pb : Accès à distance : mot de passe en clair sur le réseau
  - Mot de passe local pour accéder à sa clé privée. Utilisation de celle-ci et du certificat pour s'authentifier : pas de transport de mot de passe.
- Pb : Projets de calculs distribués (grilles)
  - Globus (un des produits de metacomputing) utilise les certificats

Bilan des certificats : positif

- Un même certificat peut servir au :
  - Contrôle d'accès interactif : équivalent login-mot de passe (qui ne circule pas sur le réseau)
  - Contrôle d'accès à des pages Web (Intranet : lecture, écriture)
  - Authentification et intégrité de messages électroniques
  - Chiffrement session interactive, accès Web, transport de message
- Une base unique pour la sécurisation des applications courantes actuelles et futures

Bilan des certificats : bémols

- Lacunes techniques : liste de révocation …
- Le succès repose sur la confiance (apparence de sérieux)
  - Domaine totalement libéralisé = entreprises commerciales
    Choix : profit à court terme / sérieux des procédures
- La fiabilité du système repose encore et toujours sur l'utilisateur : protection de sa clé privée
- Il faut d'autres systèmes pour gérer les droits d'accès
- Ne résout pas les problèmes classiques :
  - Vols, attaques Internet (logiciels bogués, saturations, …), personnel mal intentionné, …
  - Il faudra toujours des serrures, une charte, une architecture sécurisée, une liste de contrôles, …

Bilan (avis personnel)

- Dans notre communauté, le succès des certificats va dépendre
  - Du sérieux des procédures que l'on mettra en place
  - De l'accompagnement des ingénieurs pour le déploiement
    - Connaissance, formation
  - De l'accompagnement des utilisateurs
    - Information, sensibilisation

- L'intérêt des certificats réside principalement dans les nouveaux services qu'il sera plus facile de mettre en place
  - Et pas dans une « reconversion » des anciennes procédures (papier) à l'identique