

# **Les services de confiance**

**[pierre.chassigneux@certplus.com](mailto:pierre.chassigneux@certplus.com)**

## **Plan de l'exposé**

- Deux mots sur Certplus
- Etat des lieux
- Rôle et responsabilité de :
  - l'autorité de certification;
  - l'autorité d'enregistrement;
  - l'opérateur de certification.
- Gestion du cycle de vie des certificats:
  - Révocation des certificats;
  - Validation des certificats.
- Recouvrement des clés privées

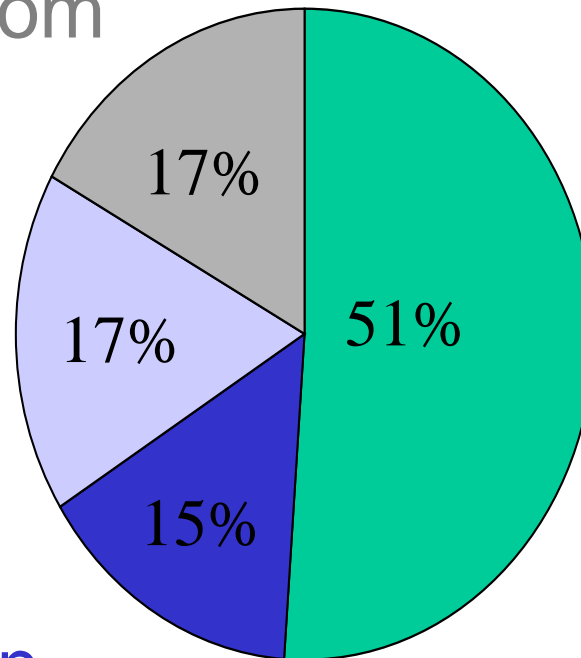
# Certplus : Opérateur français de services de confiance

France Telecom

Matra

Verisign

Gemplus



## **Current Context**

- **A worldwide Public Key Infrastructure that supports international, government, and state policies and regulations will not be available until the new century.**
- **In the mean time, corporations like banking, trade and administration sectors can utilize this new technology to satisfy their security requirements in accordance with their business needs.**
- **Companies chose to manage their own certificate authority (CA) instead of outsourcing the totality or a part of the CA functions to a third party. This choice has to be thought-full according to objective criterias.**
- **Boundaries between CA, registration authority (RA) and certificate processor (CP) are not yet well delimited.**

# **Corporate Public Key Infrastructure**

- **When companies chose to manage their own PKI, It means that they are at the same time: certificate authority, registration authority, certificate processor and trusted third party if needed.**
- **This can be accomplished with turn key solutions.**
- **This choice implicates large investments if these companies want to have a high level of security :**
  - **This level depends on the PKI security policies that are derived from the existing set of corporate security policies.**
- **Before setting up a corporate PKI with or without outsourced components it is fundamental to examine the PKI component security requirements.**

# Components security requirements

- **Each component has a security criterion based on the level of protection necessary to perform the business objectives within the acceptable level of risk.**
- **Certificate server:**
  - A security policy must exist for each CA function (enrollment, certificate generation, issuance, revocation ...  
nota: certificate policies for corporate security needs can be more lenient than commerce related ones.
  - A CPS (certificate practice statement must exist to allow the subscribers to be well aware of these practices before trusting the CA. The CPS deals also with CA liabilities.
  - Must provide for the adequate protection of the private key that it uses to sign certificates. The information system must be protected from network and physical intrusion.

# Components security requirements

- **Directory server:**
  - Must support network authentication through IP address/DNS name, and user authentication through LDAP user name and password, or a X509 version 3 public-key certificate.
  - Must control the users ' ability to perform read, write, search, or compare operations down to the attribute level. Directory administrators must be able to restrict particular users from performing specific directory operations.
  - Must provide privacy (SSL) and message integrity for all communications.

## Components security requirements

- **PKI clients ( Web browser, secure e-mail...) must be able to:**
  - generate digital signatures and manage certificates;
  - generate a public/private key pair: the software or hardware used to generate the key pair must use a non-deterministic algorithm;
  - create a certificate request;
  - display certificate;
  - delete certificates;
  - secure storage of private keys (e.g., password, and hardware).
  - configure security options;
  - control which cryptographic algorithm, modes and key length they use to protect their data
  - ...

# La certification: des métiers et des responsabilités différents

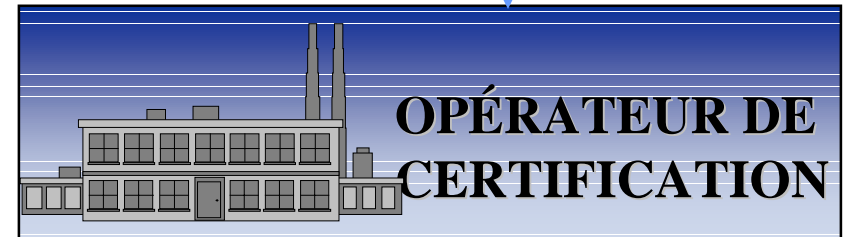
Est responsable vis à vis des utilisateurs du niveau de confiance qui est associé aux différentes classes de certificats émis



Approuve les pratiques de l'opérateur de certification



AC définit les règles d'attribution des certificats et le niveau de garantie aux utilisateurs

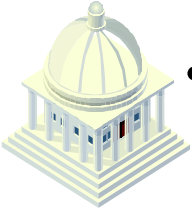


OC signe les demandes et revoie les certificats à leurs destinataires- Gère les CRLs

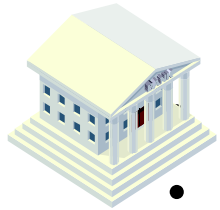
AE s'assure que le demandeur de certificat vérifie les conditions d'attribution du certificat



# Le rôle d'une Autorité Certifiante



- L 'autorité certifiante a un rôle essentiellement ' politique ', en définissant les procédures et principes de certification
- Approuve et éventuellement définit les procédures qui devront être appliquées par les autorités d 'enregistrement et les opérateurs de certification
- Est responsable vis à vis des utilisateurs du niveau de confiance qui est associé aux différentes classes de certificats émis
- Différentes Autorités certifiantes :
  - Le secteur bancaire (GIE Carte Bancaire, Visa, Mastercard)
  - Le GIP CPS aujourd'hui dans le secteur Santé/social
  - Le Ministère des Finances
  - Les Chambres de Commerce et d 'Industrie
  - Les notaires
  - La DG d 'une entreprise
  - ....

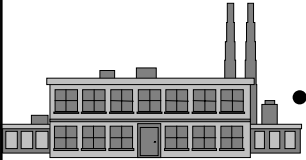


# Le rôle de l'Autorité d'Enregistrement

Définit les procédures d'enregistrement

- Travaille par délégation pour le compte de l'Autorité certifiante
- Pour enregistrer un utilisateur et lui émettre un certificat, l'Autorité d'Enregistrement doit :
  - Obtenir toutes les informations qui seront contenues dans le certificat (l'utilisateur doit fournir les éléments de preuve d'identité requis). En fonction des besoins, plusieurs procédures d'enregistrement avec des niveaux d'assurance d'identification différents peuvent coexister : procédure on-line, off-line (présence physique de l'utilisateur)....
  - Mettre ces informations dans un message appelé ' Demande de Signature de Certificat ' (CSR)
  - Signer ce message pour permettre à l'Opérateur de Certification d'authentifier la demande
  - Le transmettre pour signature à l'Opérateur de Certification

# Le rôle de l'opérateur de certification

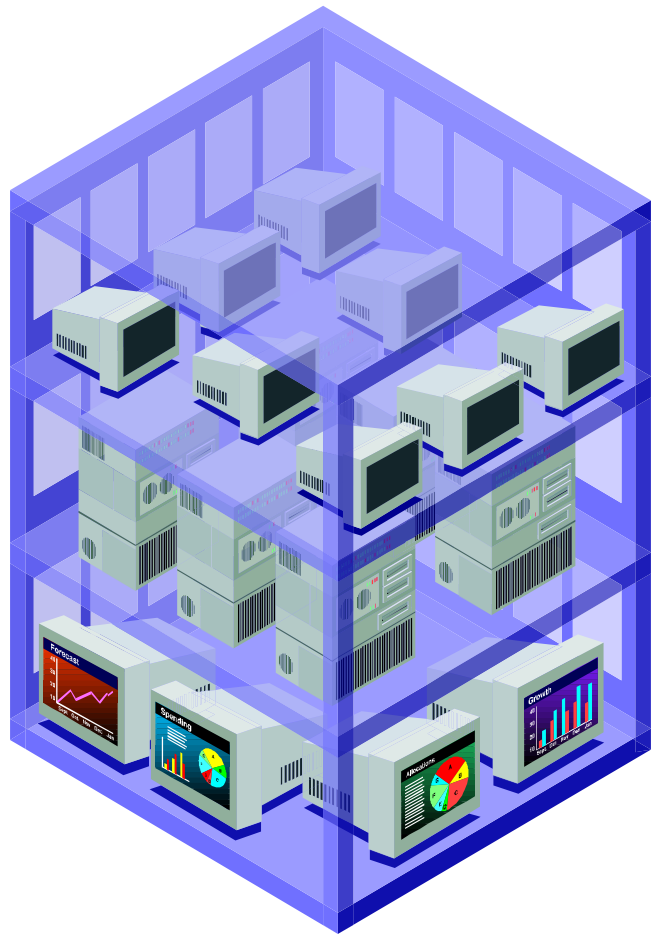


- Signe les demandes de signature de certificats et de révocation de certificats émise par l'Autorité d'enregistrement selon des procédures approuvées par l'Autorité certifiante.
- Effectue dans certains cas toute ou partie des fonctions suivantes
  - Génération de bi-clés RSA
  - Personnalisation des cartes (key management)
  - Gestion des certificats pour le compte du CA (annuaire, listes de révocation...)
  - Distribution des certificats via Internet, par transporteurs pour les certificats stockés sur cartes selon des procédures déjà existantes dans les centres de personnalisation.
  - Peut être Autorité d'enregistrement pour le compte de l'Autorité certifiante dans le cas d'identification de bas niveau des utilisateurs
- L'opérateur de certification est un industriel qui s'appuie sur une infrastructure très fiable et performante

## Remarques

- Il est relativement facile de devenir un opérateur de certification
- Il est très difficile de devenir un opérateur de certification de confiance, avec la technologie, l'infrastructure et les pratiques méthodologiques nécessaires pour apporter la confiance indispensable à cette activité.
- On appelle « insourcing » une solution PKI dont toutes les composantes sont gérées par l'organisme utilisateur.
- On appelle « outsourcing » une solution PKI dont la fonction d'opérateur de certification est assurée par un tiers.

# Outsourcing: les avantages



- Un très haut niveau de sécurité (physique et logique)
- Performance, fiabilité
- Des centres de traitement en haute disponibilité avec des opérations 24/24, 7/7j.
- Offre de support et d'assistance
- Des infrastructures flexibles
- Du personnel qualifié
- Le respect de procédures strictes
- Des pratiques reconnues, auditables
- Participer à la mise en place des infrastructures PKI public ou d'entreprises

## Les activités connexes

- Le service de certification peut être considéré comme le service de base de Certplus
- Il sera progressivement complété par :
  - **Un service de « tiers de séquestre » pour répondre aux besoins de confidentialité élevée, dans le cadre de la réglementation française actuelle**
  - **Des services de notarisation (par délégation d 'Autorités Morales)**
  - **Des services de gestion de droits ( ' copyrights ' )**
  - **Des services d 'horodatage (timestamping)**
  - **Des services de validation des certificats**

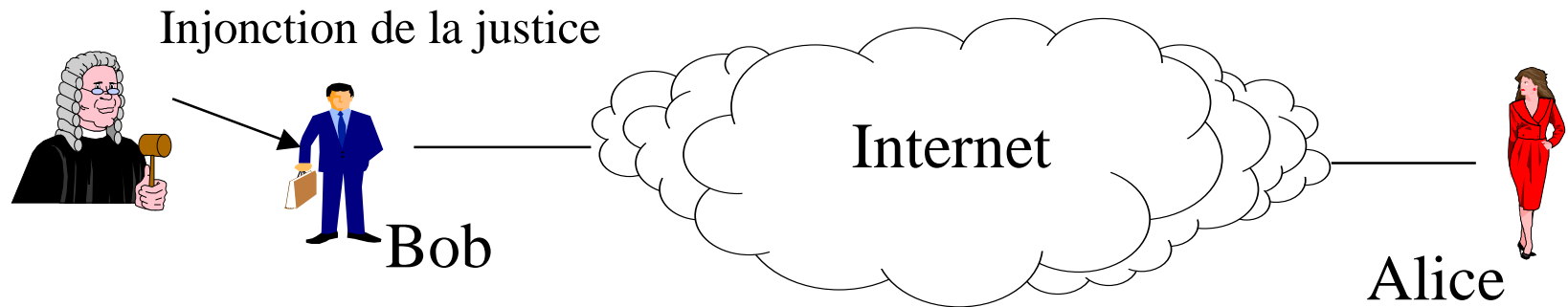
# **Gestion du cycle de vie des certificats**

- **Révocation des certificats**
- **Validation des certificats**

# Components security requirements

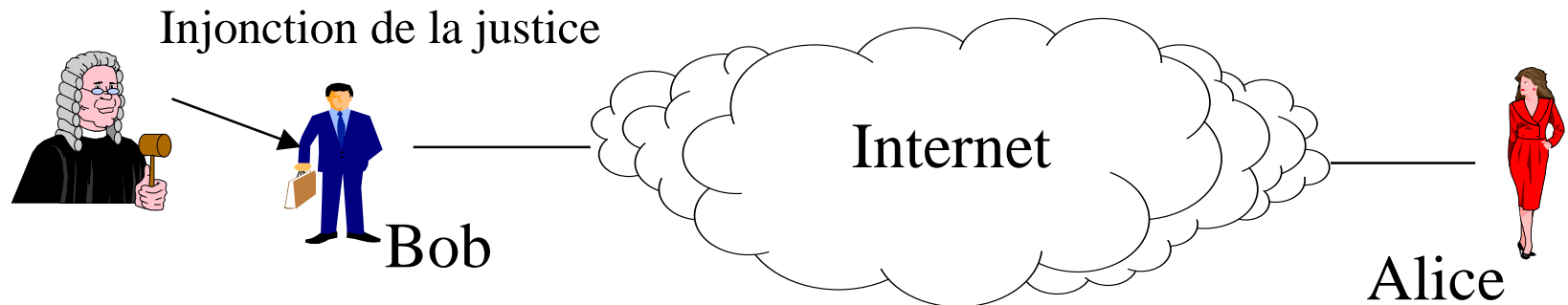
- **Key recovery or key escrow system:**
  - For internal recovery needs in case of private keys loss
    - Secure storage of all key material
  - For external recovery needs in accordance with the national regulations ( trusted third party)
    - The system has to fulfill the government requirements:
      - - very secure dedicated area with access control;
      - - personal clearance;
      - -...

## Recouvrement de clé (Key recovery)



- Toutes les informations reçues ou émises par Bob contiennent un champ supplémentaire (LEAF: *law enforcement access field*) qui contient :
  - La clé de session chiffrée par une clé publique dont la clé privée correspondante est détenue par un organisme agréé
  - Des informations qui permettent d'identifier l'organisme agréé et la clé privée de recouvrement de clés
- **La clé privée de recouvrement de clés est partagée par plusieurs utilisateurs**

## Séquestre de clé (Key escrow)



- Toutes les informations transmises ou reçues par Bob ne contiennent pas de champ de recouvrement de clés supplémentaires :
  - La clé de session est chiffrée avec la clé publique de l'émetteur et du destinataire
  - Dans ces conditions, les clés privées correspondantes doivent être détenues par un organisme agréé.
- **Il est impératif que les certificats des usagers contiennent des informations sur l'organisme agréé qui gère les clés privées.**

## Activité « tiers de séquestre »

Pourquoi Investir dans une telle activité?

Liminaire : de nombreux experts considèrent que ce type d'activité ne sera jamais rentable pour les raisons suivantes:

- **Les investissements tant humains que matériels à faire pour satisfaire au cahier des charges du SCSSI sont très importants**
- **Le prix payé par l'Administration pour gérer ou mettre en œuvre les conventions secrètes ne permettra jamais d'amortir ces dépenses**
- **La France ne sera-t-elle pas contrainte à « lâcher du lest » au sein d'une communauté internationale où certains acteurs et non des moindres prônent plutôt des régimes de libre utilisation de la cryptologie forte ?**
- ...

## **Pourquoi Certplus a investi dans cette activité ?**

- Raisons légales (à suivre...)
  - **La déclaration du Premier Ministre du mois de janvier dernier prévoit « l'instauration d'obligations, assorties de sanctions pénales, concernant la remise aux autorités judiciaires, de la transcription en clair des documents chiffrés.**
  - **De notre point de vue un régime volontariste pour recourir à des tiers de séquestre est préférable à un régime obligatoire. De nombreuses sociétés choisiront d'y recourir car ce n'est pas leur cœur de métier.**
- Raisons stratégiques
  - **L'activité « tiers de séquestre » est complémentaire de l'activité de certification**
  - **Cette activité est nécessaire pour permettre d'offrir à nos clients des solutions de recouvrement de clés pour des besoins internes (perte, destruction des clés par nos clients...).**

# Conclusion

- L'explosion des échanges numériques dans tous les secteurs d'activité et la nécessité de sécuriser ces échanges (authentification, intégrité, confidentialité) imposent inévitablement de recourir aux procédés de cryptologie dits à clé publique.
- L'usage des certificats est indissociable de cette technologie.
- Les certificats doivent être émis par des organismes de confiance, apportant aux utilisateurs une garantie suffisante sur la pérennité de leurs services et la qualité de leurs prestations.
- Il n'y a pas un seul type de certificats mais des certificats adaptés aux besoins exprimés et aux garanties exigées.
- Les activités (tiers de séquestre - «notarisation» -horodatage - archivage) sont complémentaires de l'activité de certification.

## Conclusion: suite et fin

Un certain nombre de question se posent:

- Quelles seront les conditions minimales requises pour qu'une signature numérique ait valeur de preuve? (En France, dans l'union européenne, au niveau international)
- Les autorités de certification se « cross-certifieront »-elles selon leurs propres critères (auto-régulation)? Ou s'appuieront-elles sur des opérateurs de certification reconnus (cf. schéma d'accréditation des opérateurs de certification);
- Quelles seront les obligations minimales à imposer aux opérateurs de certification pour notamment protéger les utilisateurs de certificats en cas de cessation de leur activité?
- ...