[Introduction aux concepts de PKI]

Février 2001

http://securit.free.fr

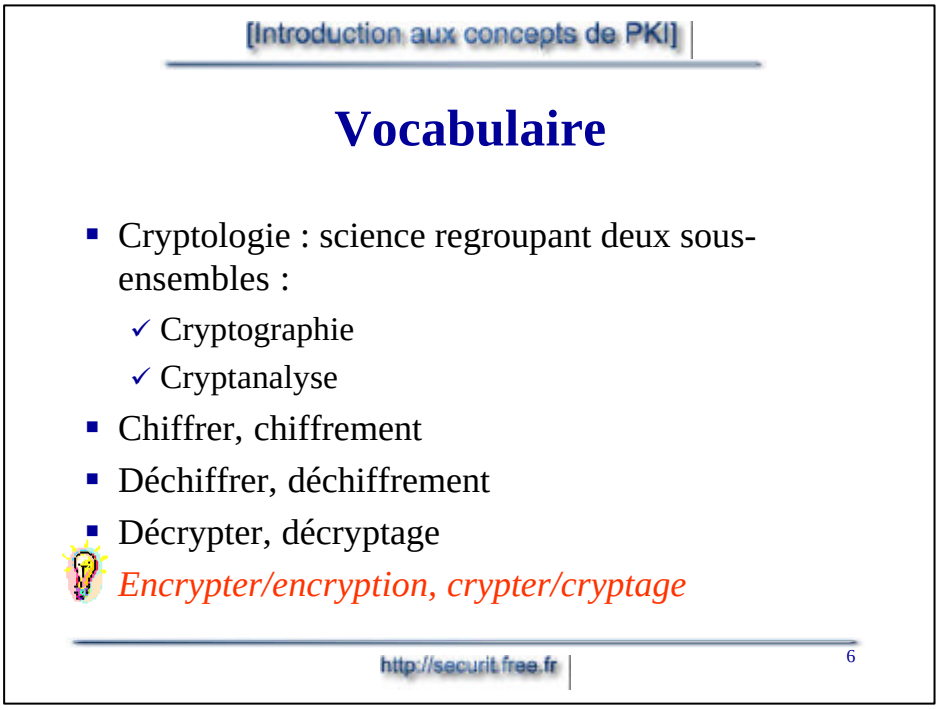
Sommaire

I. Introduction

Introduction

- Public Key Infrastructure
  - ✓ Infrastructure à clés publiques
  - ✓ Désigne l'ensemble des solutions techniques basées sur la cryptographie à clés publiques
- Objectifs de la présentation
  - ✓ Maîtriser les concepts de base de la cryptographie
  - ✓ Comprendre les éléments essentiels d'une PKI
  - ✓ Appréhender les modèles de certification

I. Les bases de la cryptographie



Cryptologie

Étude des procédés de chiffrement Ensemble de la **cryptanalyse** et de la **cryptographie**.

Cryptanalyse

La **cryptanalyse** consiste à déchiffrer un message dont on connaît généralement le procédé de chiffrement, mais pas les clés (le code est considéré comme cassé sans que tout le message soit nécessairement déchiffré).

Cryptographie

Ensemble des techniques permettant le **chiffrement** ou **cryptage** d'un message pour en assurer la confidentialité (et/ou l'authenticité) puis le déchiffrement et/ou la vérification par le récepteur habilité (à qui des clés de déchiffrement ont été données).

Chiffrer, chiffrement

Application d'un code secret à un ensemble de données pour en assurer la confidentialité et/ou l'authenticité.

Décrypter, décryptage

Action consistant à retrouver un texte en clair à partir du texte chiffré, sans connaître la clé de déchiffrement.

Autres termes == anglicismes !! (ex. : la chaîne cryptée !)

Services de sécurité

- Fonctions et objectifs de sécurité
  - ✓ Principaux
    - *Confidentialité* *(confidentiality)*
    - *Intégrité des données* *(data integrity)*
    - *Authentification* *(authentication)*
    - *Non-répudiation* *(non-repudiation)*
  - ✓ Alternatifs
    - *Horodatage* *(timestamping)*
    - *Témoignage* *(witnessing)*
    - *Accusé de réception* *(receipt)*
    - *Révocation* *(revocation)*
    - …

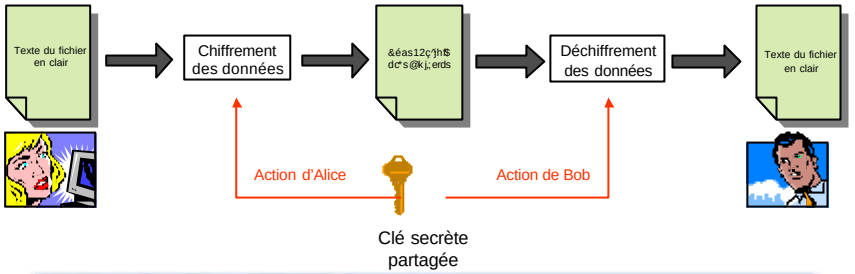
Personnalités célèbres

Alice

Bob

Cryptographie symétrique

- Cryptographie à clé secrète
  (clé de chiffrement == clé de déchiffrement)
- Confidentialité : Alice écrit un message à Bob

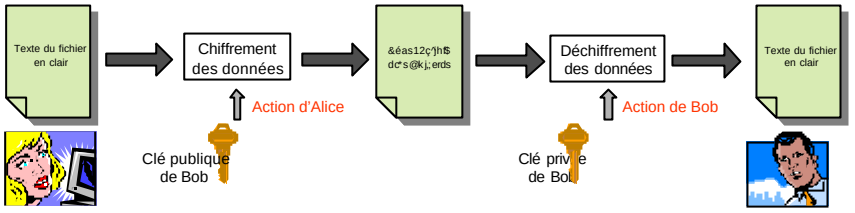


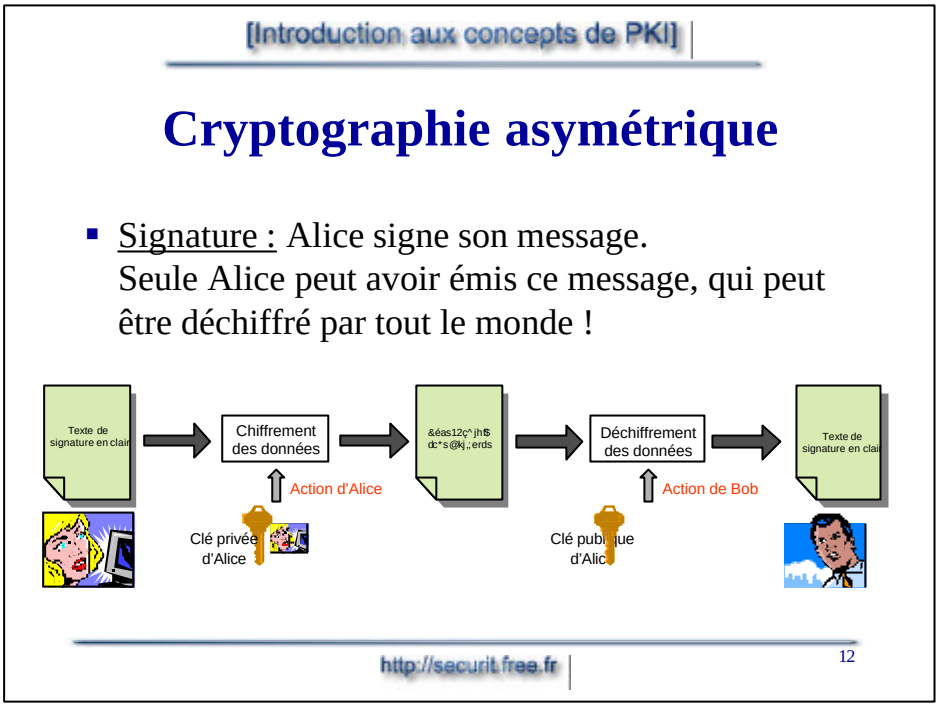
Cryptographie symétrique

- Algorithmes
  - Chiffrement par blocs (*block ciphers*)
    - ✓ *Le texte est découpé en blocs, puis chiffré de bloc en bloc*
    - ✓ *Principaux algorithmes :*
      - 3-DES (112 ou 168 bits), AES (128, 192 ou 256 bits), DES (56 bits)
      - FEAL, IDEA, CAST, Blowfish…
  - Chiffrement par flux (*stream ciphers*)
    - ✓ *Traitement des données par unité de bit, à partir d'un vecteur d'initialisation*
    - ✓ *Principaux algorithmes :*
      - RC4 (largement utilisé par Microsoft)
      - Tout algorithme de chiffrement par bloc, avec un bloc de 1 bit !

Cryptographie asymétrique

- Cryptographie à clé publique
  (clé de chiffrement != clé de déchiffrement)
- Confidentialité : Alice écrit à Bob, Bob est le seul à pouvoir déchiffrer le message émis par Alice !





Algorithmes (confidentialité)

- Diffie-Hellman – 1976
  - Basé sur la difficulté du calcul du logarithme discret dans un corps fini
- RSA – 1978
  - Basé sur la difficulté de décomposer un grand nombre en ses facteurs premiers
- Courbes elliptiques – 1980
  - Basé sur la résolution d'une équation de courbe elliptique dans un ensemble discret
- Autres : ex. El Gamal

Algorithmes (signature)

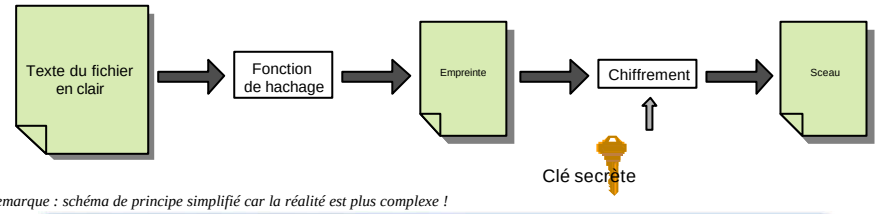
- DSA
- RSA, ElGamal, Rabin (confidentialité et signature)

Cryptographie asymétrique

- Algorithmes (confidentialité)
  - Diffie-Hellman – 1976
    - ✓ *Basé sur la difficulté du calcul du logarithme discret dans un corps fini*
  - RSA – 1978
    - ✓ *Basé sur la difficulté de décomposer un grand nombre en ses facteurs premiers*
  - Courbes elliptiques – 1980
    - ✓ *Basé sur la résolution d'une équation de courbe elliptique dans un ensemble discret*
  - Autres : ex. El Gamal
- Algorithmes (signature)
  - DSA
  - RSA, ElGamal, Rabin (confidentialité et signature)

Fonction de hachage et scellement de données

- Objectifs et services de sécurité
  - ✓ Assurer l'authenticité d'un message
    - *Intégrité des données lors de leur transport*
    - *Authentification du message (authentification de l'origine des données)*
  - ✓ Remarque : la non-répudiation (de la part de l'émetteur) n'est pas assurée (c'est le rôle du service de signature)



Remarque : schéma de principe simplifié car la réalité est plus complexe !

Protocoles

- Quelques protocoles utilisant les services de cryptographie
  - ✓ S/MIME
  - ✓ SSL/TLS
  - ✓ S/WAN
  - ✓ SSH
  - ✓ Kerberos

Comparaison

- Cryptographie symétrique
  - ✓ Avantages
    - *Simple et facile à implémenter*
    - *Traitement CPU rapide*
    - *Adapter aux grands flux de données à chiffrer*
  - ✓ Inconvénients
    - *Absence de certains services de sécurité*
    - *Distribution des secrets partagés (complexité en n^2)*
- Cryptographie asymétrique
  - ✓ Avantages
    - *Distribution des secrets*
    - *Multiples services (confidentialité, signature)*
  - ✓ Inconvénients
    - *Consommation importante en ressources CPU*
    - *Non-adapté pour le chiffrement de flots de données importants*
    - *Publication et cycle de vie des certificats*

↳ Solution : combinaison des deux méthodes (clé de session symétrique chiffrée par un système asymétrique). Exemple : SSL

II. Les bases d'une infrastructure à clés publiques

Composants

- Définition
  - ✓ « Une infrastructure de gestion de clés offre un environnement de confiance, ainsi qu'un ensemble de garanties et services relatifs aux certificats de clés publiques », SCSSI – PC² v2.0, 10/05/199
- Composants essentiels
  - ✓ Objets
    - *Bi-clés*
    - *Certificats*
  - ✓ Éléments
    - *Autorité de certification*
    - *Autorité d'enregistrement*
    - *Autorité d'horodatage*
    - *Système de publication/distribution de certificats (annuaire)*
    - *Applications compatibles avec la PKI*

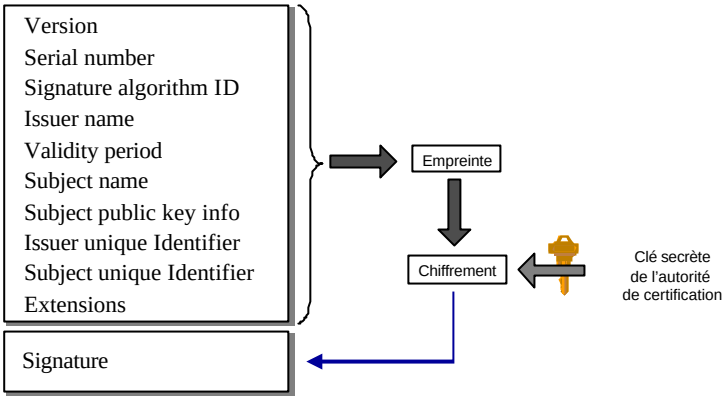
Bi-clés

- Couple composé d'une clé privée et d'une clé publique permettant la mise en œuvre d'algorithmes de chiffrement asymétriques
- On distingue classiquement 4 différents bi-clés (SCSSI-PC[2]):
  - ✓ Bi-clés de confidentialité
    - *Utilisés pour chiffrer des messages de petite taille*
  - ✓ Bi-clés de signature
    - *La clé privée est utilisée pour signer des messages*
    - *La clé publique est utilisée pour vérifier les signatures*
  - ✓ Bi-clés de certification
    - *Utilisés par l'autorité de certification pour signer des certificats ou des messages de révocation*
  - ✓ Bi-clés d'échange/transport de clés
    - *Permet le transport des clés symétriques utilisées pour sécuriser les communications*

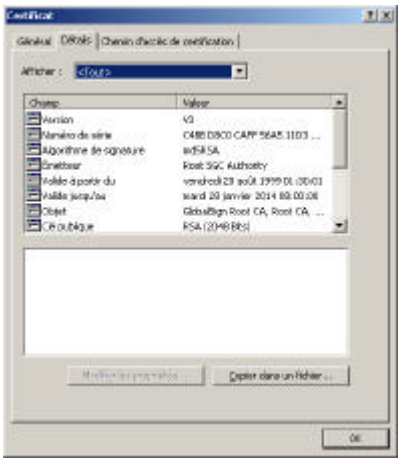
Certificats

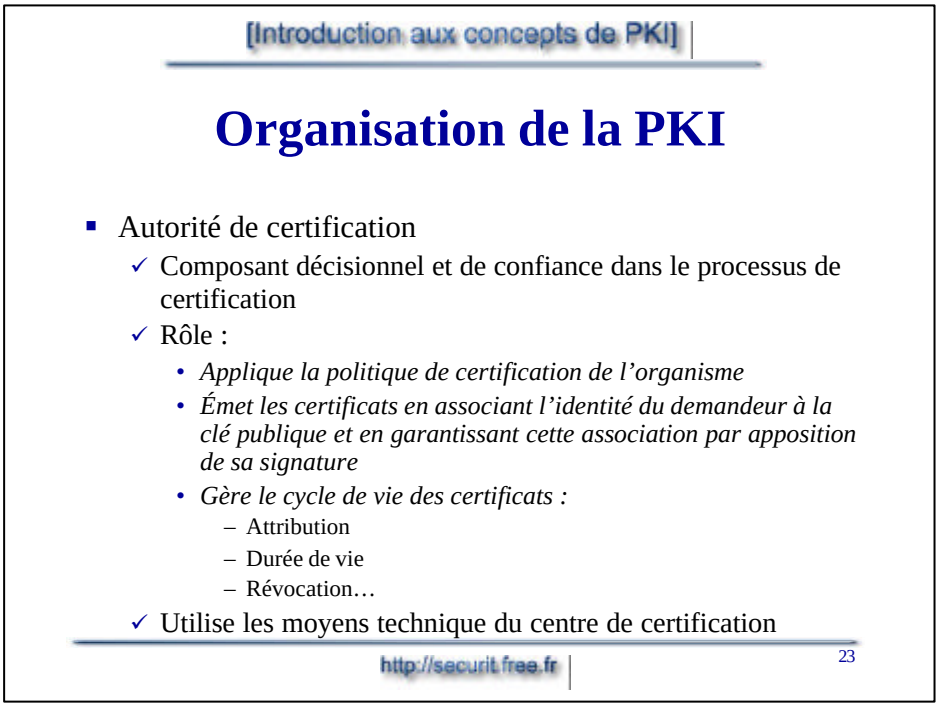
- Définition
  - ✓ « Clé publique d'un utilisateur, ainsi que certaines autres informations, rendue infalsifiable par chiffrement avec la clé secrète de l'autorité de certification qui l'a délivré. » [ISO 9594-8]
  - ✓ Format standard : X.509 v3 (norme PKI-X)
  - ✓ Informations certifiées (non-exhaustif)
    - *Identité du porteur*
    - *Clé publique du porteur*
    - *Durée de vie du certificat*
    - *Identité de l'autorité de certification émettrice*
    - *Signature de l'autorité de certification émettrice*

Certificats



Certificats





Centre de certification

Entité de l'autorité de certification

Rôle :

Fournit les moyens techniques pour la gestion des certificats et des bi-clés (modules cryptographiques spécifiques)

Stocke et protège la clé privée de l'autorité de certification (critique)

Gère le cycle de vie des certificats

Organisation de la PKI

- Autorité d'enregistrement
  - ✓ Interface entre l'utilisateur et l'autorité de certification
  - ✓ Rôle :
    - *Authentifie les demandeurs ou porteurs de certificats*
    - *Applique la politique de certification vis-à-vis des requêtes des utilisateurs*
    - *Récupère la clé publique du demandeur*
    - *Soumet les demandes de certificats à l'autorité de certification*

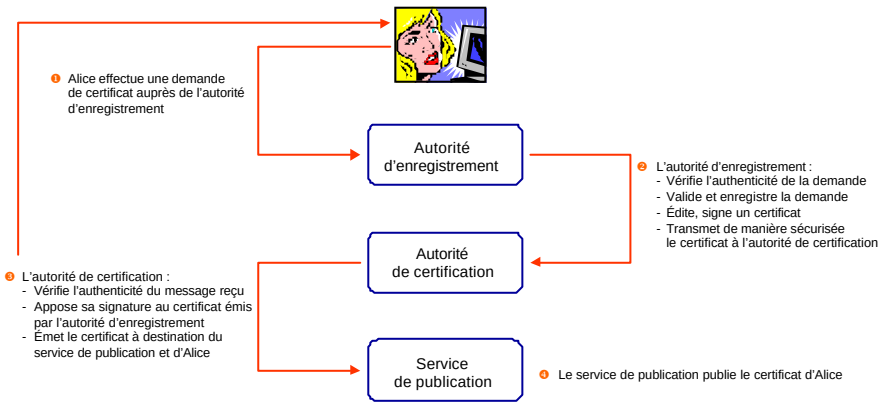
Organisation de la PKI

- Système de publication de certificats
  - ✓ Il s'agit en général d'un annuaire supportant le standard X.500/LDAP
  - ✓ Peut être implémenté dans un serveur Web, voire un système de messagerie, ou de fichiers…
  - ✓ Rôle :
    - *Rend disponible, à l'ensemble des utilisateurs, les certificats des clés publiques émis par une autorité de certification*
    - *Publie une liste de certificats valides et révoqués (CRL)*

Organisation de la PKI

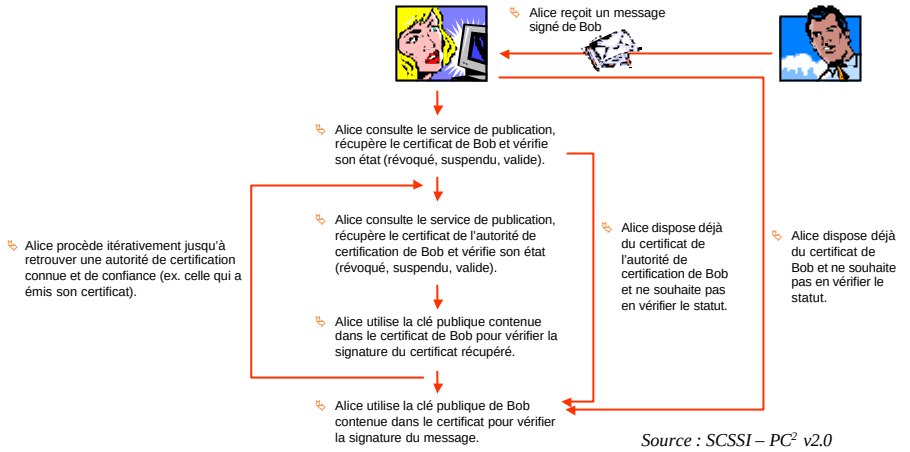
- Applications compatibles avec la PKI
  - ✓ Une PKI est une infrastructure fournissant des services de sécurité à des applications !
  - ✓ Applications « PKI-ready »
    - *Accès à un site Web*
    - *Messagerie sécurisée*
    - *VPN*

Demande de certification



Source : SCSSI – PC² v2.0

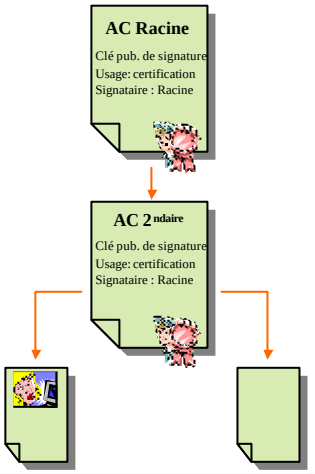
Vérification de signature



Source : SCSSI – PC² v2.0

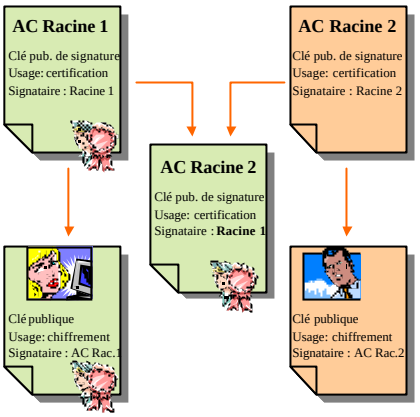
Certification hiérarchique

- L'autorité de certification racine est le point de confiance (reçu de manière sécurisée)
  - Le certificat de l'AC racine est auto-signé
- L'autorité de certification intermédiaire (ex. secondaire) délivre des certificats au plus près des utilisateurs
  - Le certificat de l'AC intermédiaire est signé par l'AC racine (publié en ligne)
- L'utilisateur reçoit son certificat de la part de l'autorité de certification intermédiaire
  - Le certificat utilisateur est signé par l'AC intermédiaire et peut contenir le chemin complet de certification (publié en ligne)



Certification croisée

- *Cross-certification*
- Problème : des utilisateurs disposant de certificats d'AC distinctes (ex. 2 entreprises) souhaitent communiquer de manière sécurisée.
- Question : comment faire confiance à des certificats émis par une AC extérieure ?
- Solutions : l'AC certifie la clé publique de l'AC extérieure (processus potentiellement bi-directionnel)
- Problématique : interopérabilité



III. Conclusions

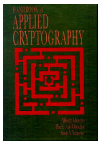
Conclusions

- La PKI est avant tout une infrastructure
  - ✓ Elle doit être pensée de manière transversale, comme une infrastructure de sécurité à part entière
  - ✓ Elle doit être modulaire et adaptée aux besoins, si nécessaire
- Attention à l'interopérabilité :
  - ✓ Avec d'autres solutions de PKI
  - ✓ Avec d'autres standards
  - ✓ Avec les applications
  - ✓ Cas de la certification croisée !
- Attention aux effets de mode et aux discours commerciaux : qui n'a pas sa PKI ?!?

V. Références

Références

- Handbook of Applied Cryptography
  - ✓ A. Menezes, P. Van Oorschot, S. Vanstone
    - *CRC Press, 1996*
    - *www.cacr.math.uwaterloo.ca/hac*
- Procédures et politiques de certification de clés
  - ✓ PC² Version 2.0, SCSSI, 1999
    - *www.scssi.gouv.fr*
- RSA FAQ v4.1
  - ✓ RSA Laboratories, mai 2000
    - *www.rsasecurity.com/rsalabs/faq*



Références

- Quelques éditeurs de solutions de PKI
  - ✓ Baltimore
  - ✓ Entrust
  - ✓ iD2 Technologies
  - ✓ CS
  - ✓ RSA Security
  - ✓ Microsoft ?!?