Travail collaboratif
et
signature électronique

Michel.Miqueu@Cert-IST.com

Agenda

- Contexte
- Besoins
- Solutions
- Limites
- Autres solutions
- Discussion

Contexte

Un projet Européen : EISPP

- Sous contrat PCRD N°5
- Avec la Commission Européenne comme client
  - ➔Unité Trust et Security de la "DG" IST
  - ➔A l'origine de la directive signature électronique

Un projet en coopération multi-nationale

- Cert-IST (coordinateur)
- Siemens CERT (Allemagne)
- esCERT et InetSecur (Espagne)
- CLUSIT et I.Net (Italie)
- Callineb (Suède)

Objectifs et événements du projet

- www.eispp.org

Besoins

Contexte du projet

- Plusieurs lots
- Un responsable technique par lot
  - ➔ Responsable de la livraison au coordinateur
  - ➔ Après procédures d'approbation/revue

Approbation des dé livrables

- Format électronique
- Avant livraison
- Par les "responsables" de chaque contractant
- Après approbation interne par responsable technique

Délai minimal

Solution

- **Signature PGP**
- **Mécanisme**
  - Le fichier livré par le responsable technique
    - ➔ est signé par le coordinateur
    - ➔ En "signature détachée"
  - Les responsables des co-contractants
    - ➔ Signent le fichier de signature du coordinateur
    - ➔ Et le lui retournent
- **Avantages**
  - Parallélisme
  - Pas de circulation…
  - Besoin de délai minimal couvert

Limites

- **Le client n'est pas partie prenante du schéma**
  - Pour des raisons "structurelles/bureaucratiques"
- **Conséquences**
  - Le fichier livré au client
    - ➔Contient la date et le nom des approbateurs contractants
    - ➔Il est donc différent de celui approuvé
- **Le schéma inter-contractants**
  - N'est pas adaptable pour l'extérieur
- **Limites de PGP en tant que "standard"**

Autres solutions

Clé PGP partagée (key share)

- Avantage
  - ➔Une clé pour le projet
  - ➔Garantie que tous ont signé avant signature effective
- Inconvénient
  - ➔Génération ? (id PGP signing parties)
- Non testée

Certificats X-500

- S-Mime adapté au mail, pas à signer des fichiers ?
- UAs (outlook par ex) causent pb
  - ➔Signature attachée/ détachée
  - ➔Pièces jointes modifient la signature.
- MTAs et passerelles peuvent aussi poser pbs
  - ➔Exchange…

Discussion

- **Autres expériences ?**
- **Questions**