LA SIGNATURE NUMÉRIQUE

Exposés de Système/Réseaux – 2006

Benoît DEPAIL - IR3

Sommaire

I. Présentation

- Le problème
  - Assurer l'intégrité
  - Authentifier l'auteur

I. Présentation

- Le problème
  - Assurer l'intégrité
  - Authentifier l'auteur
- Technologies
  - Somme de contrôle (MD5, SHA, ...)
  - Cryptographie asymétrique

I. Présentation

Rappel sur les sommes de contrôle

- Un fichier = Une somme de contrôle unique

I. Présentation

Rappel sur les sommes de contrôle

- Un fichier = Une somme de contrôle unique
- Un seul sens à l'opération

I. Présentation

Rappel sur les sommes de contrôle

- Un fichier = Une somme de contrôle unique
- Un seul sens à l'opération
- Algorithme utilisés :
  - MD5
  - SHA

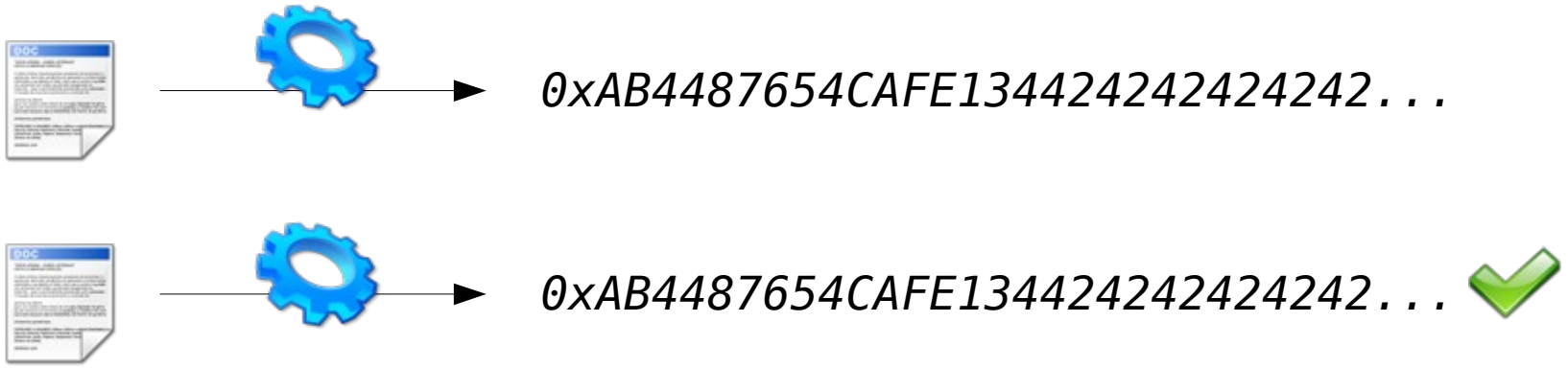
I. Présentation

Rappel sur les sommes de contrôle

0xAB4487654CAFE134424242424242...

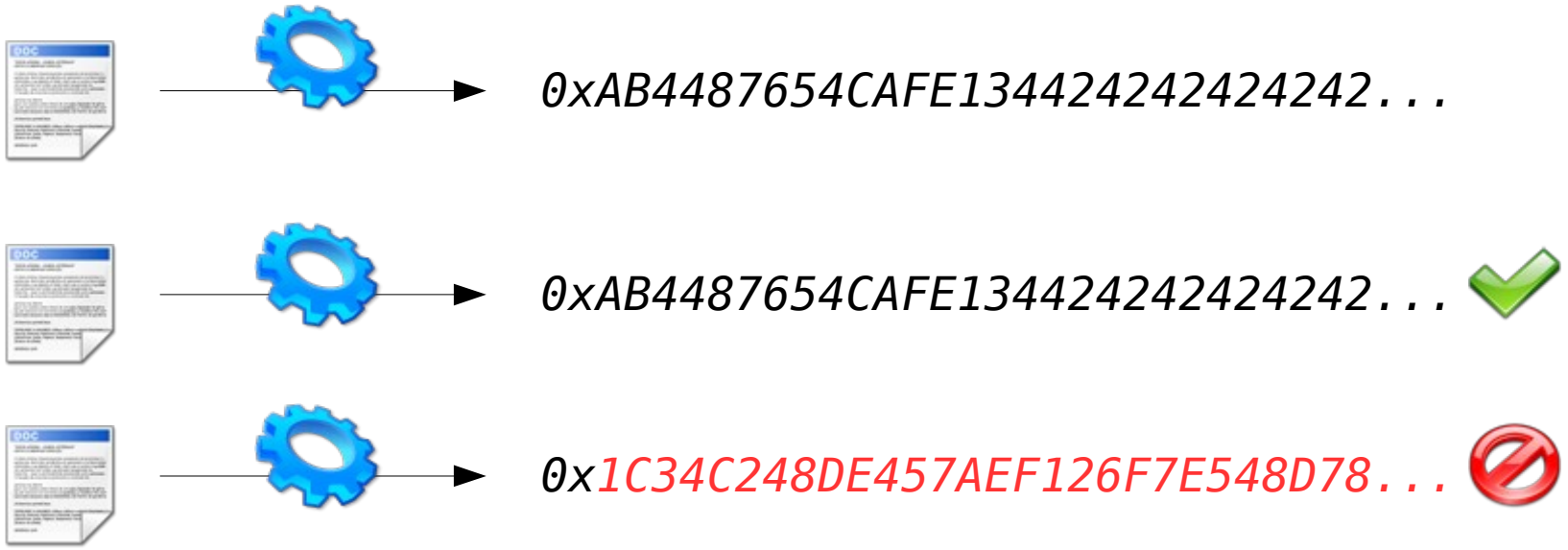
I. Présentation

Rappel sur les sommes de contrôle



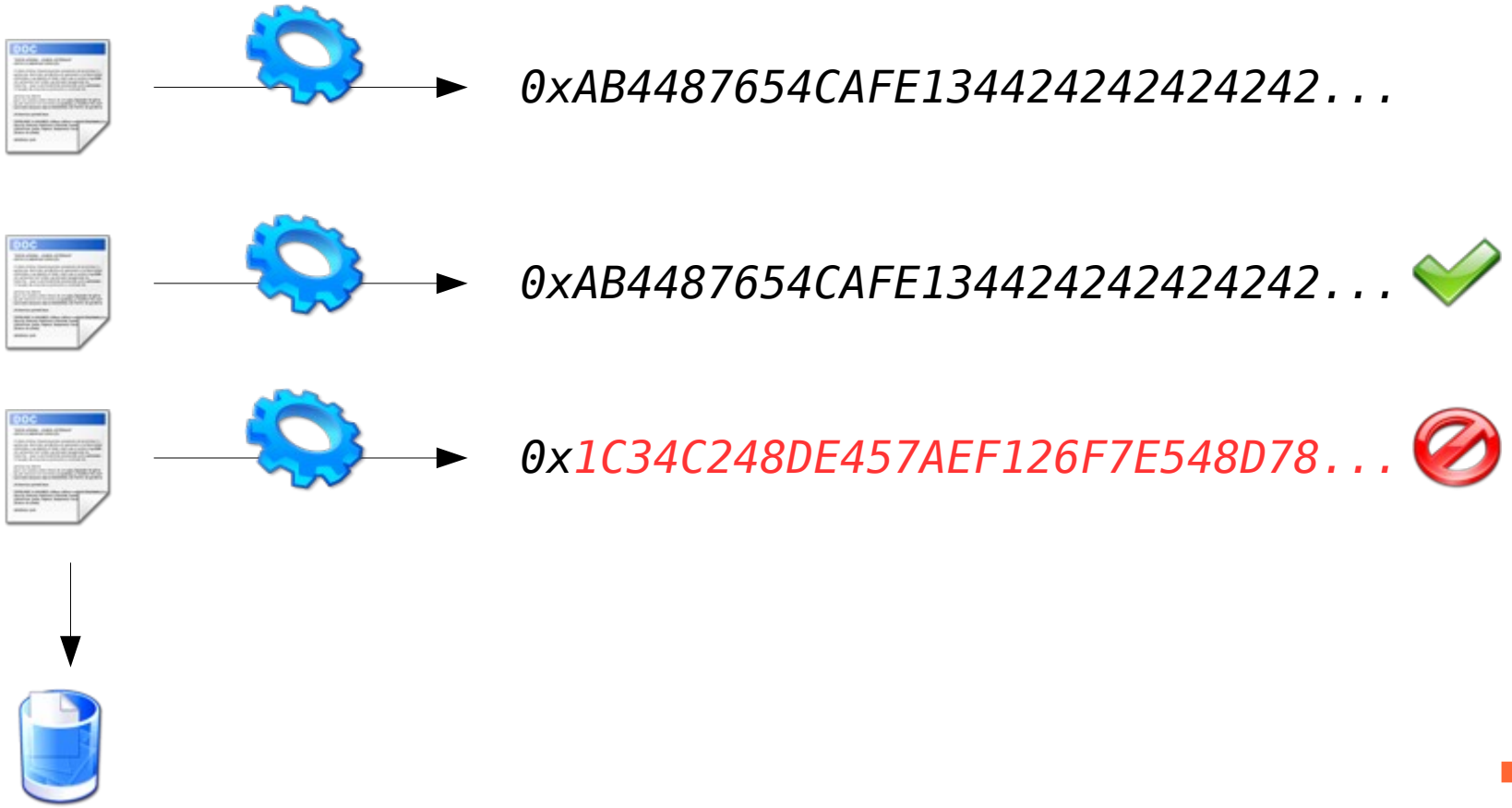
I. Présentation

Rappel sur les sommes de contrôle



I. Présentation

Rappel sur les sommes de contrôle



I. Présentation

Rappel sur la cryptographie asymétrique

- Clé publique, clé privée

I. Présentation

Rappel sur la cryptographie asymétrique

- Clé publique, clé privée
- Jeu de clés sécurisable, révoquable, certifiable

I. Présentation

Rappel sur la cryptographie asymétrique

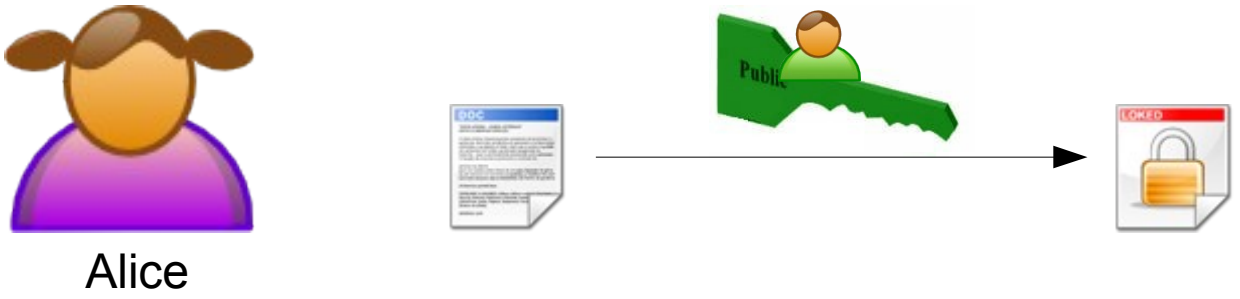
- Clé publique, clé privée
- Jeu de clés sécurisable, révoquable, certifiable
- Hiérarchies de jeux de clés

I. Présentation

Rappel sur la cryptographie asymétrique

I. Présentation

Rappel sur la cryptographie asymétrique



I. Présentation

Fonctionnement détaillé

- Générer une paire de clés

I. Présentation

Fonctionnement détaillé

- Générer une paire de clés
- Rendre accessible la clé publique

I. Présentation

Fonctionnement détaillé

- Générer une paire de clés
- Rendre accessible la clé publique
- Signer le message/document

I. Présentation

Fonctionnement détaillé

- Générer une paire de clés
- Rendre accessible la clé publique
- Signer le message/document
- Envoyer au destinataire

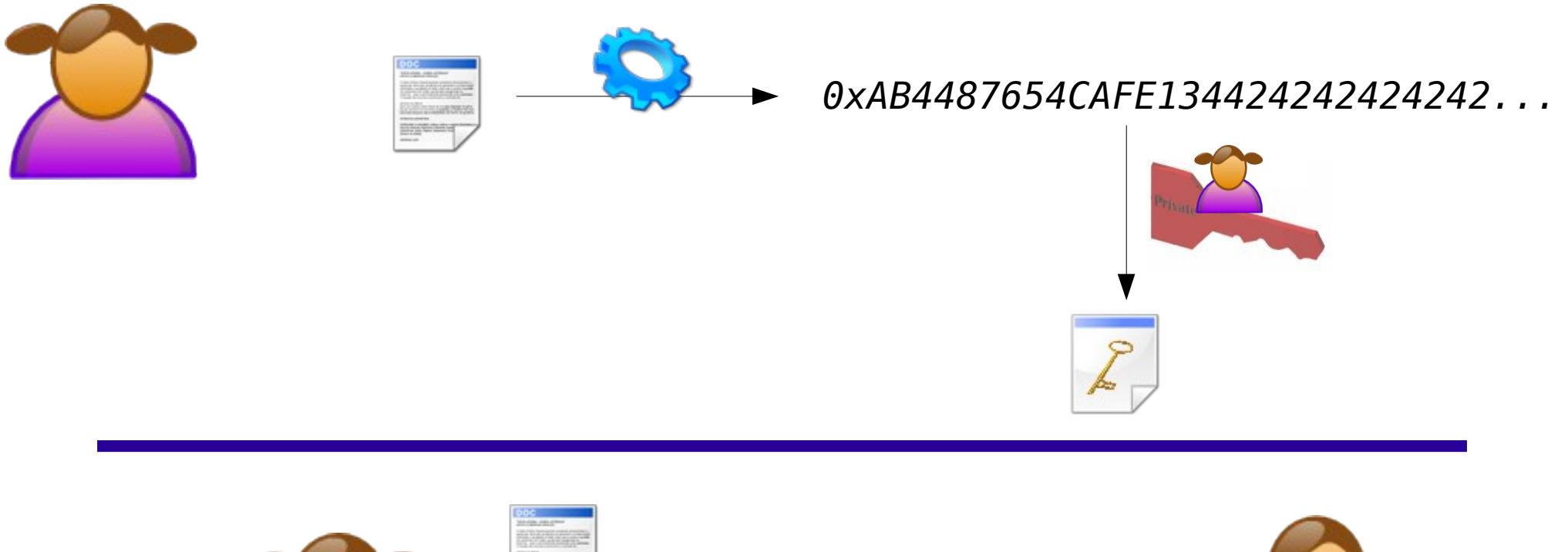
I. Présentation

Fonctionnement détaillé

- Générer une paire de clés
- Rendre accessible la clé publique
- Signer le message/document
- Envoyer au destinataire
- Vérifier la signature

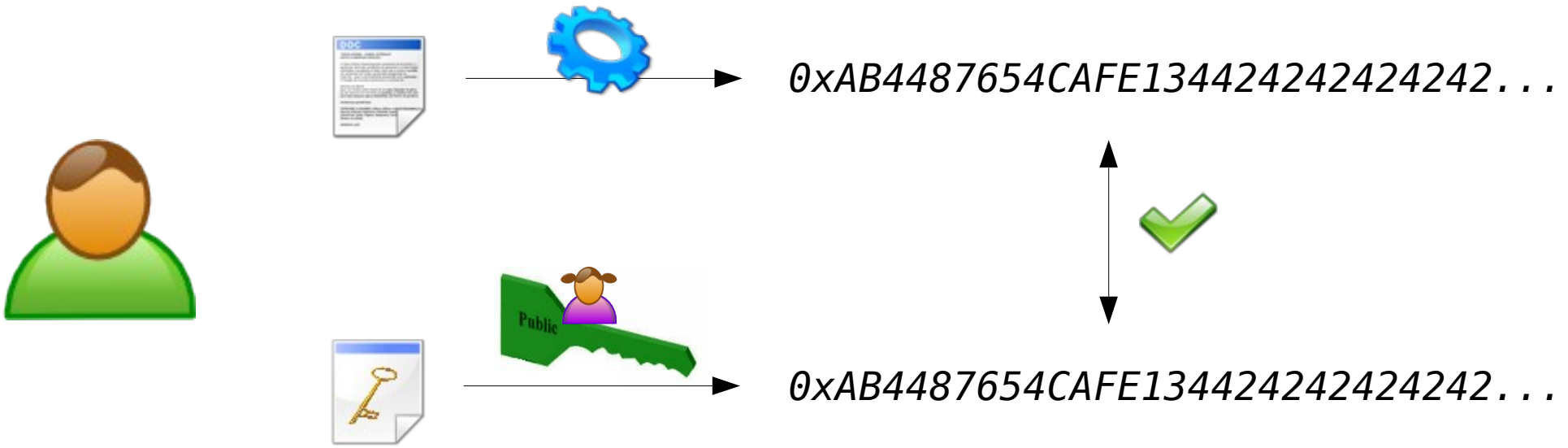
I. Présentation

Fonctionnement : Signer un document



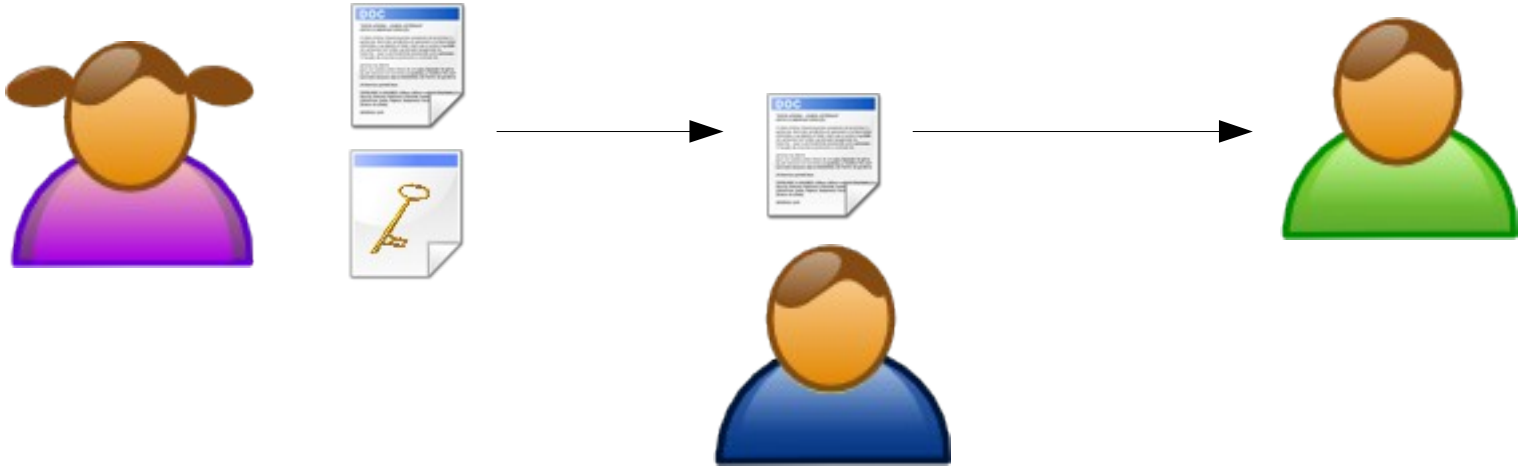
I. Présentation

Fonctionnement : Vérifier un document (1)



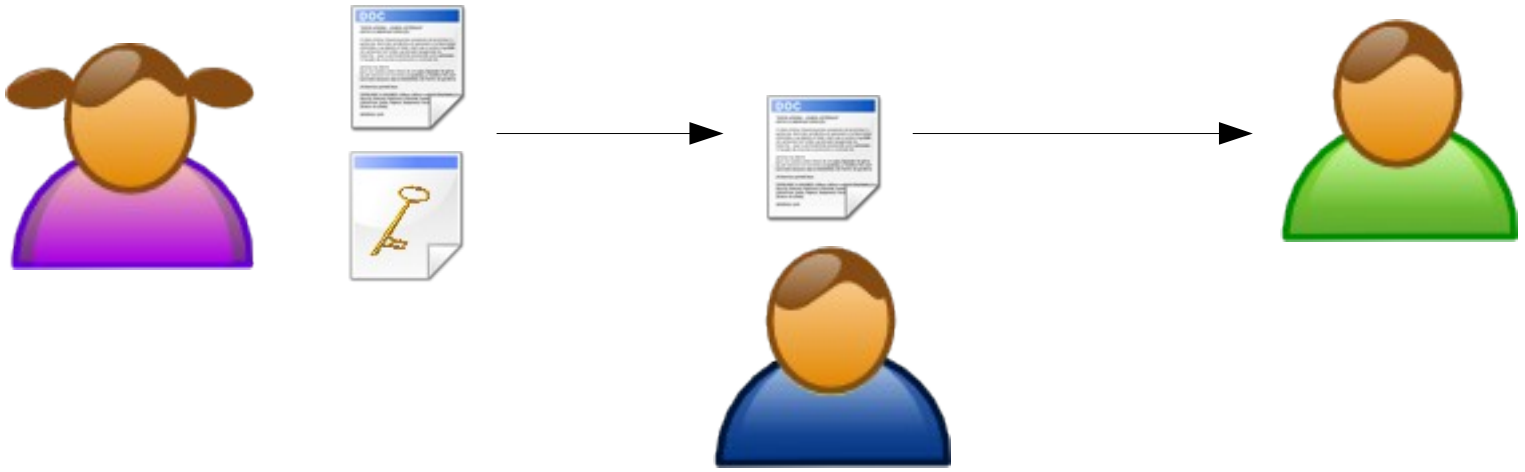
I. Présentation

Fonctionnement : Vérifier un document (2)



I. Présentation

Fonctionnement : Vérifier un document (2)

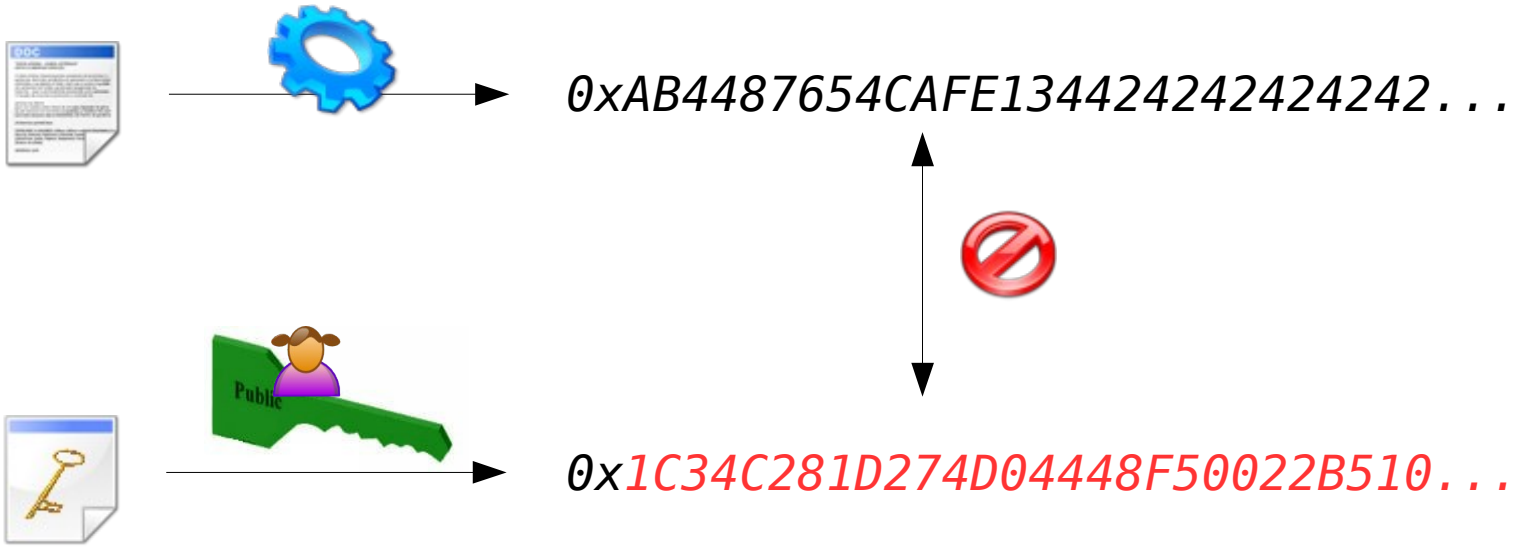


I. Présentation

Fonctionnement : Vérifier un document (3)

I. Présentation

Fonctionnement : Vérifier un document (3)



III. Les outils

Algorithmes

- Génération de clés et signature
  - RSA, DSA

III. Les outils

Algorithmes

- Génération de clés et signature
  - RSA, DSA
- Somme de contrôle
  - SHA, MD5

III. Les outils

Outils de signature/chiffrement (OpenPGP)

- Windows
  - PGPFreeware
  - WinPT (basé sur GnuPG)

III. Les outils

Outils de signature/chiffrement (OpenPGP)

- Windows
  - PGPFreeware
  - WinPT (basé sur GnuPG)
- Linux
  - GnuPG (ligne de commande)
  - GPA (frontend à GnuPG)

III. Les outils

Outils de signature/chiffrement (OpenPGP)

- Windows
  - PGPFreeware
  - WinPT (basé sur GnuPG)
- Linux
  - GnuPG (ligne de commande)
  - GPA (frontend à GnuPG)
- MAC
  - MacGPG
  - PGPFreeware

III. Les outils

Plugins pour client mail

- Windows
  - G-Data pour Outlook
  - WinPT pour Outlook Express

III. Les outils

Plugins pour client mail

- Windows
  - G-Data pour Outlook
  - WinPT pour Outlook Express
- Linux
  - Enigmail pour Thunderbird
  - Inclus dans Kmail et Evolution

III. Les outils

Plugins pour client mail

- Windows
  - G-Data pour Outlook
  - WinPT pour Outlook Express
- Linux
  - Enigmail pour Thunderbird
  - Inclus dans Kmail et Evolution
- MAC
  - Eudora-GPG pour Eudora
  - GPGMail for OSX pour Apple Mail

V. Valeur juridique

- Signature vaut preuve si :

« une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification »

N'atteint pas la valeur d'une signature manuscrite !!!

V. Valeur juridique

- L'équivalence est acquise si
  - Mise en oeuvre d'une signature avancée
    - Propre au signataire
    - Identifie le signataire
    - Moyens de création sous contrôle exclusif du signataire
    - Toute modification détectable

V. Valeur juridique

- L'équivalence est acquise si
  - Mise en oeuvre d'une signature avancée
    - Propre au signataire
    - Identifie le signataire
    - Moyens de création sous contrôle exclusif du signataire
    - Toute modification détectable
  - Utilisation d'un dispositif sécurisé
    - Données utilisées (clé) uniques et confidentielles
    - Données non déductibles et non falsifiables
    - Données protégeables (mot de passe)
    - Données à signer non modifiées

V. Valeur juridique

- L'équivalence est acquise si
  - Mise en oeuvre d'une signature avancée
    - Propre au signataire
    - Identifie le signataire
    - Moyens de création sous contrôle exclusif du signataire
    - Toute modification détectable
  - Utilisation d'un dispositif sécurisé
    - Données utilisées (clé) uniques et confidentielles
    - Données non déductibles et non falsifiables
    - Données protégeables (mot de passe)
    - Données à signer non modifiées
  - Utilisation d'un certificat pour vérifier la signature