Cryptographie

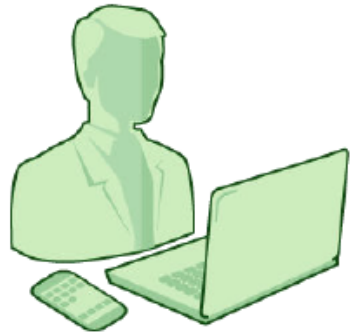
Signature numérique, authentification et chiffrement

- Signature numérique, authentification et chiffrement

- Signature numérique, authentification et chiffrement

Alice

1. Transmet clé publique
2. Transmet clé publique
3. Crée un message , son haché et une clé de session
4. Chiffre message (clé de session)
5. Chiffre haché (clé privée Alice)
6. Chiffre la clé de session
7. Transmet + + → Bob
8. Déchiffre la clé de session ( ) =
9. Déchiffre le message ( ) =
10. Déchiffre haché ( ) =
11. Compare le haché calculé et le haché reçu



Authentification émetteur	Confidentialité	Intégrité	Authentification destinataire	Vitesse de traitement
✓	✓	✓	✓	✓

Cryptographie

Signature numérique, authentification et chiffrement

- Signature numérique
  - Chiffrer le haché d'un message
  - Avec sa clé privée
  - -> authentification et intégrité du message

Cryptographie

Signature numérique, authentification et chiffrement

- Signature numérique et chiffrement
  - Authentification émetteur :
    - Déchiffrement du haché avec la clé publique de l'émetteur
  - Confidentialité :
    - Chiffrement du message avec la clé de session
  - Intégrité :
    - Comparaison haché reçu et haché calculé
  - Authentification du destinataire :
    - Déchiffrement de la clé de session avec la clé privée du destinataire

CEJMA

Sécuriser les communications et les documents

- Autorité de certification de confiance
  - Tiers de confiance dans un domaine défini (entreprise, Agence, continent, etc.)
  - Gère les certificats et les identités numériques
  - Signe les certificats émis -> garant de leur authenticité

CEJMA

Sécuriser les communications et les documents

- Création identité numérique
  - Création bi-clé asymétrique
  - Renseignement de l'identité de l'utilisateur
  - Création de l'identité numérique :
    - Identité + clé publique + clé privée
  - Création du certificat public signé et limité dans le temps:
    - identité + clé publique

CEJMA

Sécuriser les communications et les documents

- Vérifications :
  - Deux conditions pour la preuve électronique :
    - Signataire identifié : nom, adresse, etc.
    - Lien entre le document et l'identité
    - -> non-répudiation par le signataire du document signé

CEJMA

Sécuriser les communications et les documents

- Vérifications :
  - Certificat électronique délivré par une CA de confiance
    - -> vérifier l'identité de l'auteur du document
  - Clé publique :
    - -> vérifier la signature électronique
  - Empreinte électronique :
    - -> Intégrité