cyberens
Technologies & Services

Comment protéger vos données ?

15 novembre 2018

Marion CANDAU

embarcadero MVP

@marioncandau

marion.candau@cyberens.fr

radstudio.cyberens.fr

Tour 6
74, rue Georges Bonnac
33000 Bordeaux

Plan de la présentation

- Qui suis-je ?

- Comment protéger vos données ?
  1. Comment garder vos données confidentielles ?
  2. Comment gérer les mots de passe de vos applications ?
  3. Comment prouver votre identité ?
  4. Comment assurer l'intégrité de vos données ?

- Notre bibliothèque TMS Cryptography Pack

Qui suis-je ?

- Docteure en communications numériques
- Ingénieure en cryptographie chez Cyberens depuis 2015
  - TMS Cryptography Pack
  - Applications à base de cryptographie
    - Chiffrement de SMS
    - Chiffrement d'emails
  - Conseil (analyse de risques, ingénierie de sécurité)
  - MVP Embarcadero depuis septembre 2017

Comment protéger vos données ?

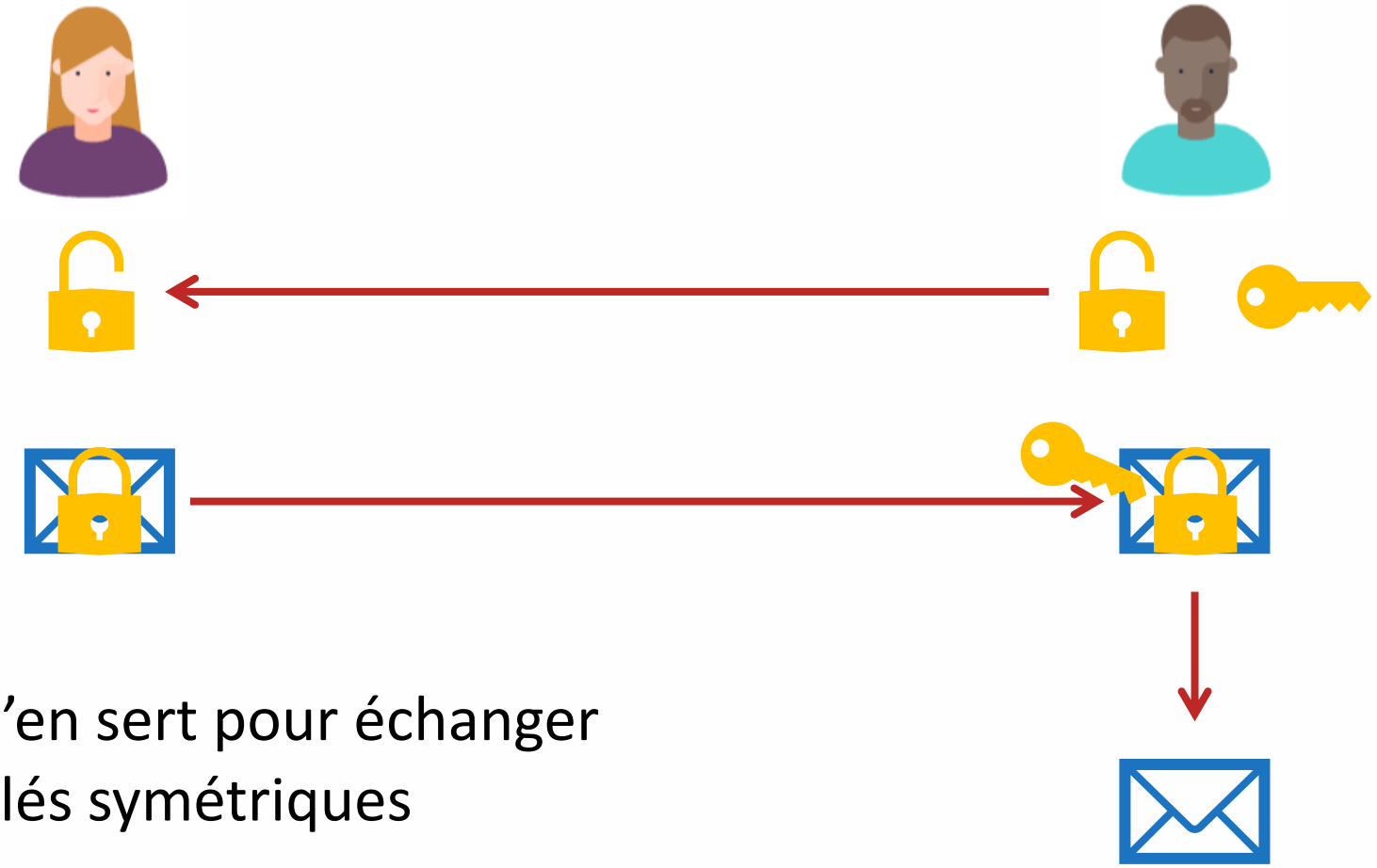
1. Comment garder vos données confidentielles ?
2. Comment gérer les mots de passe de vos applications ?
3. Comment prouver votre identité ?
4. Comment assurer l'intégrité de vos données ?

1. Comment garder vos données confidentielles ?

- Problème : comment s'échanger la clé ?

1. Comment garder vos données confidentielles ?

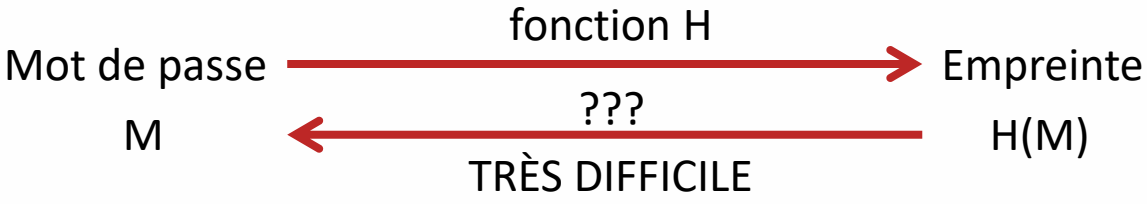
- Solution : cryptographie asymétrique



- On s'en sert pour échanger les clés symétriques

2. Comment gérer les mots de passe de vos applications ?

- Un utilisateur entre son mot de passe, comment je vérifie que c'est le bon ?
- PAS DE MOTS DE PASSE STOCKÉS EN CLAIR !!!
- On utilise une **fonction de hachage**

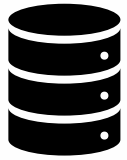


2. Comment gérer les mots de passe de vos applications ?

Identifiant I
Mot de passe M

H

$(I, H(M))$



(I_j, E_j)

$(I, H(M))$

On cherche j
tel que $I = I_j$

si $E_j = H(M)$ alors $R = 1$
sinon $R = 0$

R

2. Comment gérer les mots de passe de vos applications ?

- Problème : si un attaquant connait H
  - Il peut précalculer les H(M) sur une liste de mots de passe
  - En déduire M en fonction de H(M)

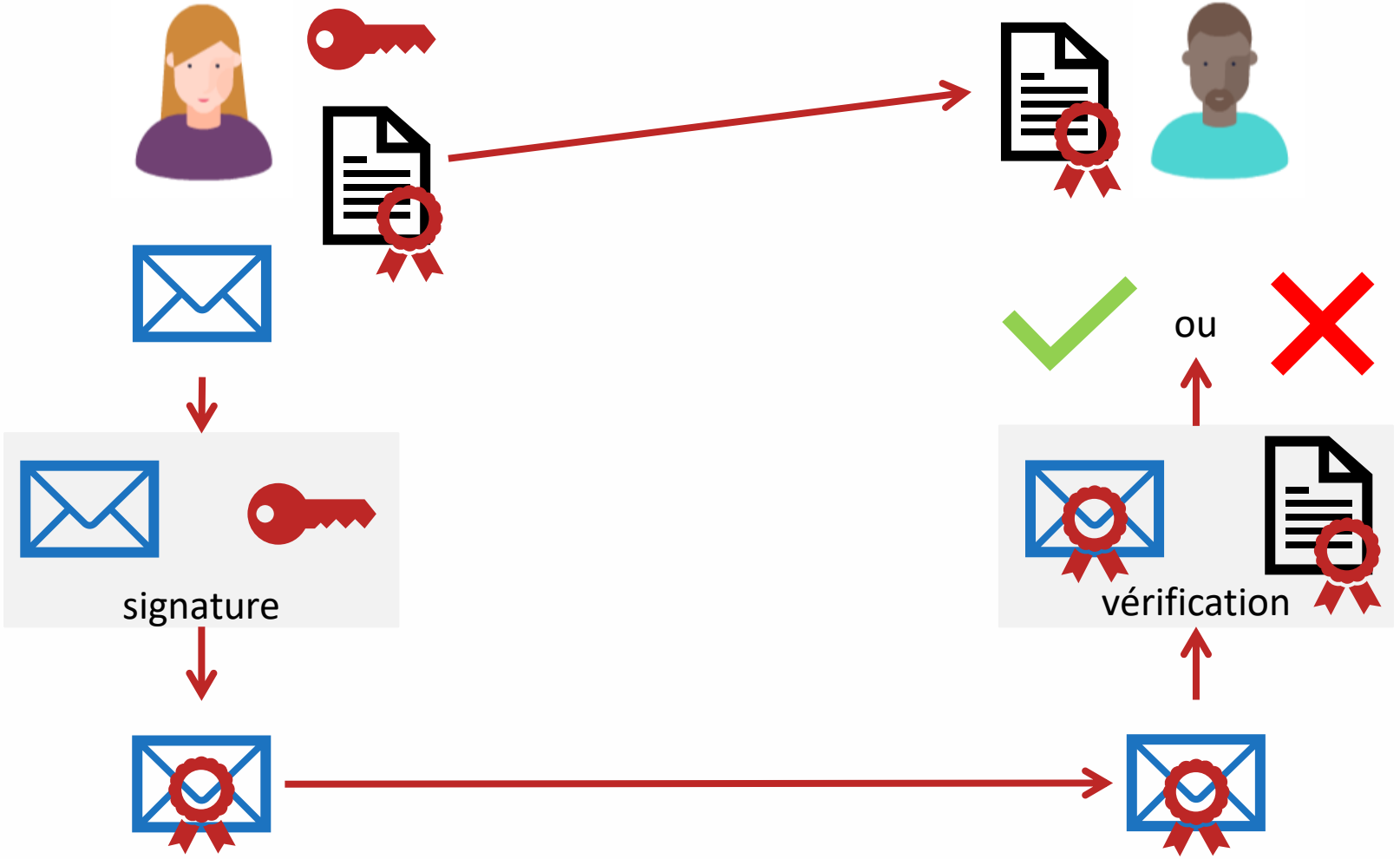
- Solutions :
  - Mots de passe avec des règles difficiles
  - Mots de passe longs
  - On ajoute du « sel » : on calcule H(M + S)
    - Salage statique: le même sel pour tous (dépassé)
    - Salage dynamique: le mot de passe est envoyé via un canal sécurisé et la base contient $(I_j, E_j = H(M_j + S_j), S_j)$

3. Comment prouver votre identité ?

- Certificats électroniques
- Norme X509
  - Une clé publique
  - Des informations d'identité
  - Une période de validité
  - Signé par une autorité de certification
  - Exemple : certificat de Cyberens
- Certificat associé à une clé privée

4. Comment assurer l'intégrité de vos données ?

- Signature électronique



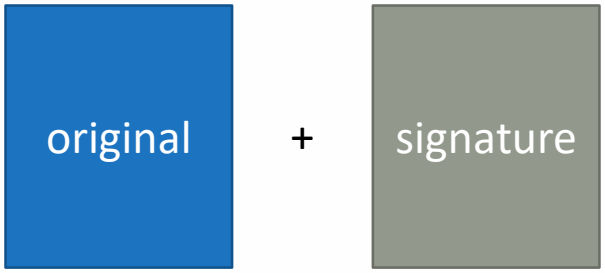
4. Comment assurer l'intégrité de vos données ?

- Formats de signature avancés
  - CAdES (CMS Advanced Electronic Signatures)
    - Format binaire (ASN.1)
    - Signe tout type de fichier
  - XAdES (XML Advanced Electronic Signatures)
    - Format XML
    - Signe tout type de fichier
  - PAdES (PDF Advanced Electronic Signatures)
    - Format PDF
    - Ne signe que les PDF

- Conformes au règlement européen eIDAS

4. Comment assurer l'intégrité de vos données ?

- 3 modes:
  - Détachée
    - CAdES
    - XAdES



  - Enveloppante
    - CAdES
    - XAdES

  - Enveloppée
    - XAdES
    - PAdES

Notre bibliothèque TMS Cryptography Pack

- Algorithmes standards forts
- Multi plateforme
- Composants graphiques
- Version 1.0 en juin 2016, version 3.3 aujourd'hui
  - Chiffrement symétrique
    - AES, SPECK, Salsa
  - Chiffrement asymétrique
    - RSA, ECIES
  - Fonctions de hachage
    - SHA-2, SHA-3, RIPEMD, Blake2B
  - Fonctions de dérivations de clés
    - Argon2, PBKDF2
  - Certificats X509
  - Signature électronique brute
    - RSA, EdDSA, ECDSA
  - Formats de signature
    - CAdES, XAdES, PAdES
  - Nouveauté 3.3
    - TLockFile : exécutable auto-déchiffrant

Notre bibliothèque TMS Cryptography Pack

Démo

Conclusion

- Penser sécurité dès la phase de conception

- RGPD, NF525, eIDAS, …
  - Obligation de protéger les données
  - Obligation de ne pas stocker les mots de passe en clair
  - Obligation d'authentifier des documents