

Pas de mot de passe pour le passeport biométrique belge

G. Avoine, K. Kalach et J.-J. Quisquater

UCL Crypto Group

- ▷ ICAO (Chicago, 1944) standardise et émet des recommandations, sur sécurité (safety, security), protection de l'environnement, efficacité, etc. en particulier sur les passeports.
- ▷ DOC 9303 Part 1 (MAL98, 11 Sept 2002, Mai 2004-Oct 2004).
- ▷ Passeport électronique et biométrique.
- ▷ Puce interrogeable à distance (micro-circuit+antenne \approx RFID).

L'identification par radiofréquence (**RFID**) est une technique qui permet d'identifier à **distance** des objets ou des personnes munis d'un transpondeur (micro-circuit + antenne), appelé (**tags**).

Par extension, la RFID permet aussi de **recupérer des données** stockées sur le tag, éventuellement récupérer le **résultat d'un calcul** réalisé par le tag.

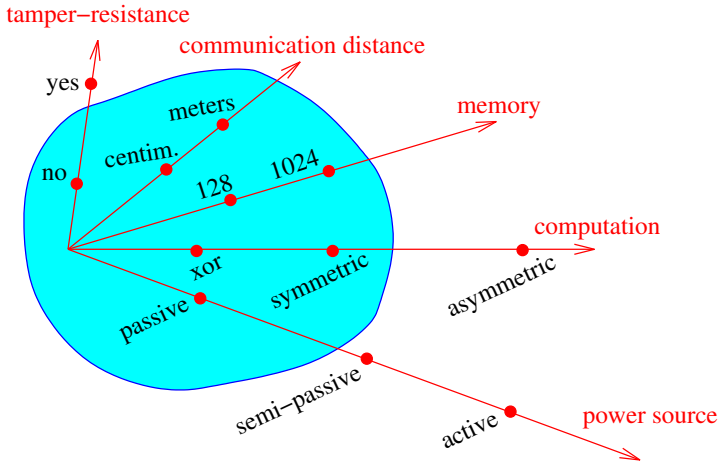
Quelques exemples d'applications



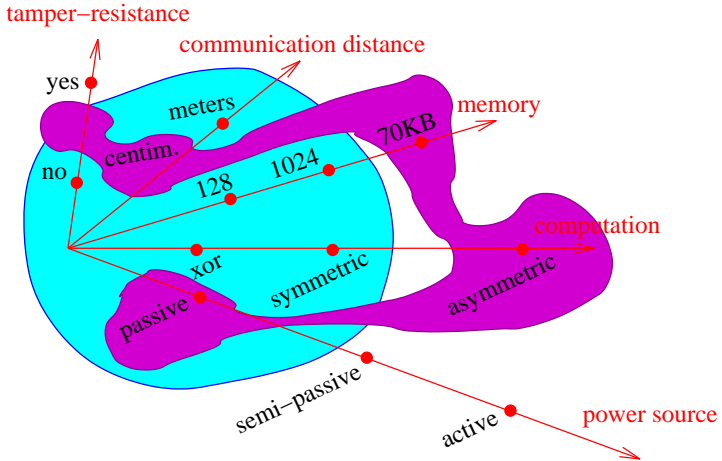
Quelques formats de tags



Caractéristiques des tags



Caractéristiques des tags



- ▶ Usurpation d'identité
- ▶ Fuite d'information (confidentialité)
- ▶ Traçabilité malicieuse

Protection de l'état :

- ▷ Modification du contenu d'un passeport (auth. passive)
- ▷ Fabrication d'un faux passeport (à partir d'un passeport vierge)
- ▷ Clonage d'un passeport existant (authentification active)

Protection de l'individu :

- ▷ Fuite info: Basic Access Control, Secure Messaging, Radio shield
- ▷ Traçabilité malicieuse: conception protocoles + UID random

Authentification passive

donnée

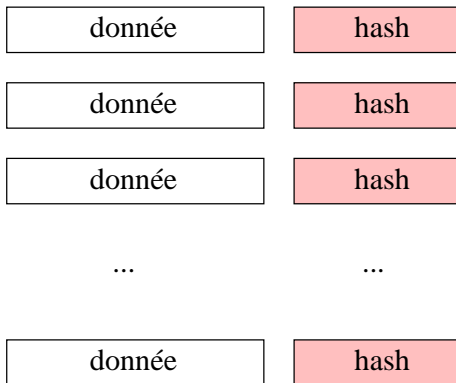
donnée

donnée

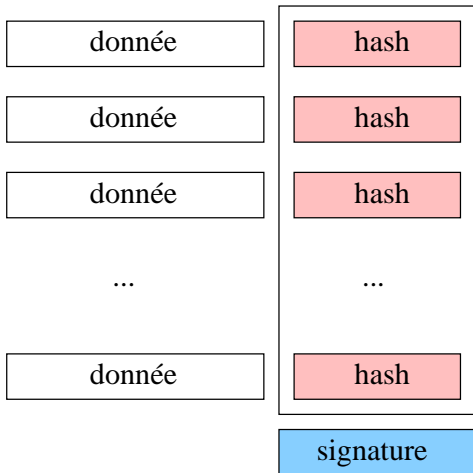
...

donnée

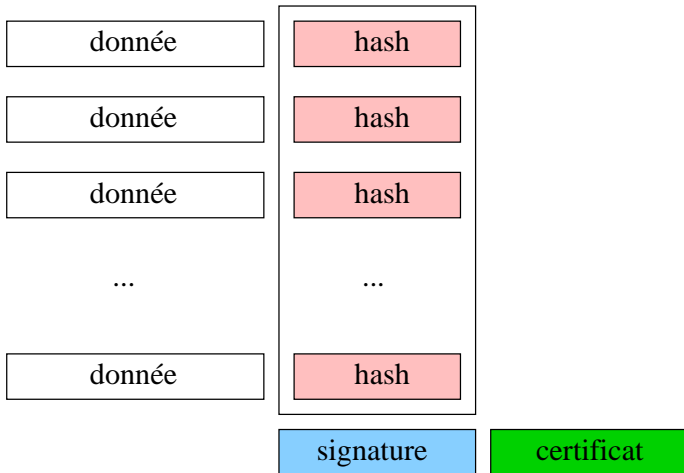
Authentication passive



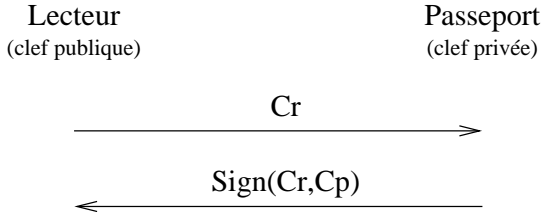
Authentication passive



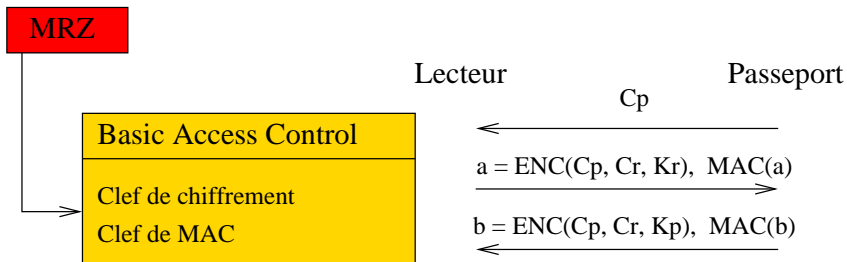
Authentification passive



Authentication active



Basic Access Control and Secure Messaging



Basic Access Control and Secure Messaging

