

Sécurité des implémentations pour la cryptographie



Partie 1 : Architecture système

Benoît Gérard

28 novembre 2017

Exemple concret

Mise en oeuvre de la CCP (Carte Cryptographique Personnelle).

- ▶ Donnée par l'administration.
- ▶ Utilisée pour tout service nécessitant une preuve d'identité
 - ▶ démarches administratives,
 - ▶ vote,
 - ▶ contrôle d'identité,
 - ▶ déposition ...



Plan du cours

Étape 1

Définition du besoin et de l'architecture au niveau système.

Étape 2

Définition de l'interface carte/terminal : API exposée par la carte.

Étape 3

Implémentation d'une version résistante aux attaques non-crypto.

Étape 4

Implémentation d'algo. crypto. résistante aux attaques distantes.

Étape 5

Implémentation d'algo. crypto. résistante aux attaques locales.

Rappels cryptographiques

Spécification d'un système

Description du besoin

Choix des solutions cryptographiques

Spécifications

Mise en œuvre

Rappels cryptographiques

Spécification d'un système

Description du besoin

Choix des solutions cryptographiques

Spécifications

Mise en œuvre

- ▶ **Confidentialité**

Le contenu protégé est incompréhensible pour un tiers.

- ▶ **Intégrité**

Une modification par un tiers du contenu protégé est détectée.

- ▶ **Authenticité**

La provenance du contenu protégé est garantie (+ non-répudiation?).

Exemples

- ▶  : confidentialité + intégrité.
- ▶  : intégrité + authenticité.

Rappels cryptographiques

Symétrique vs asymétrique

Cryptographie symétrique



Rappels cryptographiques

Symétrique vs asymétrique

Cryptographie symétrique



Rappels cryptographiques

Symétrique vs asymétrique

Cryptographie symétrique



Cryptographie asymétrique



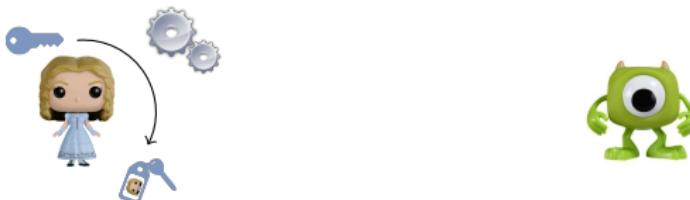
Rappels cryptographiques

Symétrique vs asymétrique

Cryptographie symétrique



Cryptographie asymétrique



Rappels cryptographiques

Symétrique vs asymétrique

Cryptographie symétrique



Cryptographie asymétrique



Rappels cryptographiques

Symétrique vs asymétrique

Cryptographie symétrique



Cryptographie asymétrique



Rappels cryptographiques

Symétrique vs asymétrique

Cryptographie symétrique



Cryptographie asymétrique



Rappels cryptographiques

Symétrique vs asymétrique

Cryptographie symétrique



Cryptographie asymétrique



CHIFFREMENT ET MAC

Objectifs

- ▶ s'assurer de la *confidentialité* d'un contenu,
- ▶ s'assurer de l'*intégrité* d'un contenu (contenu non modifié par quelqu'un ne connaissant pas la clef).



MAC = Message Authentication Code

Chiffrement + MAC = chiffrement authentifié.

Rappels cryptographiques

Chiffrement et chiffrement authentifié

CHIFFREMENT ET MAC

Objectifs

- ▶ s'assurer de la *confidentialité* d'un contenu,
- ▶ s'assurer de l'*intégrité* d'un contenu (contenu non modifié par quelqu'un ne connaissant pas la clef).



MAC = Message Authentication Code

Chiffrement + MAC = chiffrement authentifié.

CHIFFREMENT ET MAC

Objectifs

- ▶ s'assurer de la *confidentialité* d'un contenu,
- ▶ s'assurer de l'*intégrité* d'un contenu (contenu non modifié par quelqu'un ne connaissant pas la clef).



MAC = Message Authentication Code

Chiffrement + MAC = chiffrement authentifié.

Rappels cryptographiques

Chiffrement et chiffrement authentifié

CHIFFREMENT ET MAC

Objectifs

- ▶ s'assurer de la *confidentialité* d'un contenu,
- ▶ s'assurer de l'*intégrité* d'un contenu (contenu non modifié par quelqu'un ne connaissant pas la clef).



MAC = Message Authentication Code

Chiffrement + MAC = chiffrement authentifié.

Rappels cryptographiques

Chiffrement et chiffrement authentifié

CHIFFREMENT ET MAC

Objectifs

- ▶ s'assurer de la *confidentialité* d'un contenu,
- ▶ s'assurer de l'*intégrité* d'un contenu (contenu non modifié par quelqu'un ne connaissant pas la clef).



MAC = Message Authentication Code

Chiffrement + MAC = chiffrement authentifié.

CHIFFREMENT ET MAC

Objectifs

- ▶ s'assurer de la *confidentialité* d'un contenu,
- ▶ s'assurer de l'*intégrité* d'un contenu (contenu non modifié par quelqu'un ne connaissant pas la clef).



MAC = Message Authentication Code

Chiffrement + MAC = chiffrement authentifié.

SIGNATURE

Objectifs

- ▶ s'assurer de l'*intégrité* d'un contenu,
- ▶ s'assurer de l'*authenticité* (preuve de l'origine du contenu).



SIGNATURE

Objectifs

- ▶ s'assurer de l'*intégrité* d'un contenu,
- ▶ s'assurer de l'*authenticité* (preuve de l'origine du contenu).



SIGNATURE

Objectifs

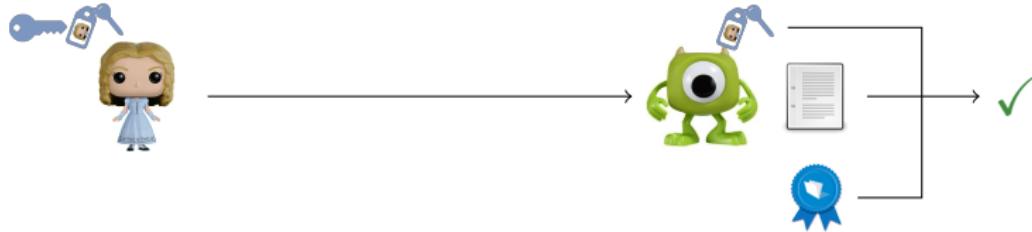
- ▶ s'assurer de l'*intégrité* d'un contenu,
- ▶ s'assurer de l'*authenticité* (preuve de l'origine du contenu).



SIGNATURE

Objectifs

- ▶ s'assurer de l'*intégrité* d'un contenu,
- ▶ s'assurer de l'*authenticité* (preuve de l'origine du contenu).



Rappels cryptographiques

Chiffrement asymétrique et échange de clefs

Utiliser la cryptographie symétrique implique une clef par correspondant ...

CHIFFREMENT ASYMÉTRIQUE

- ▶ utilise le même principe de paire de clefs que la signature,
- ▶ le secret est du côté de la personne qui déchiffre,
- ▶ les opérations sont coûteuses.

ÉCHANGE DE CLEF

- ▶ établit un secret partagé en se basant sur des opérations coûteuses,
- ▶ pour ensuite utiliser la cryptographie symétrique.

Rappels cryptographiques

L'homme du milieu

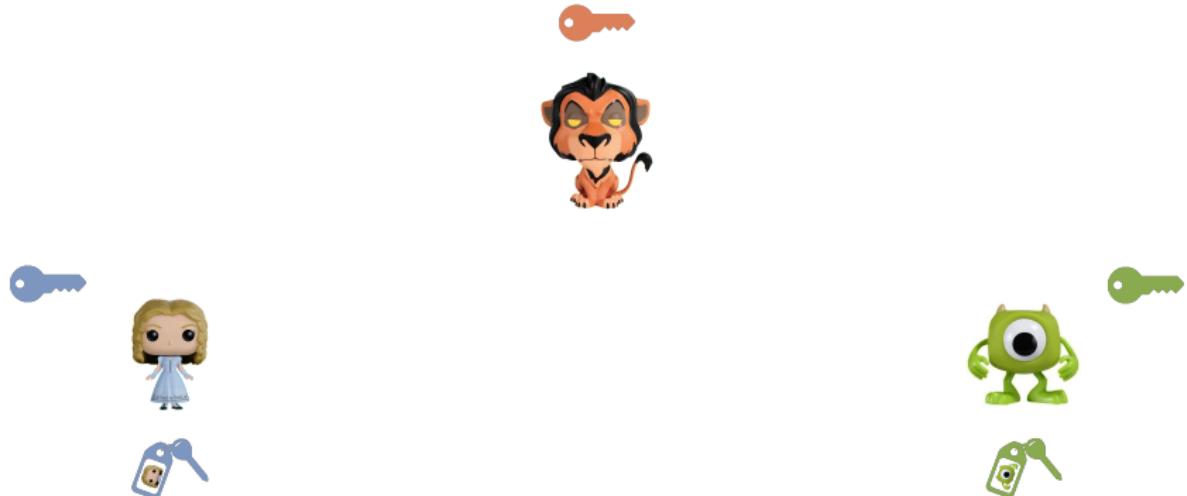
MAN IN THE MIDDLE



Rappels cryptographiques

L'homme du milieu

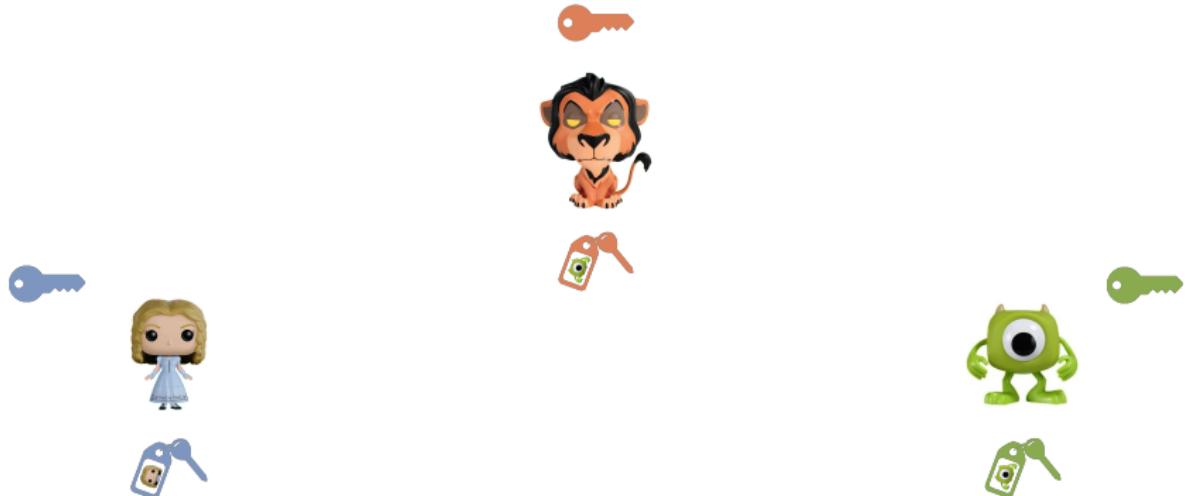
MAN IN THE MIDDLE



Rappels cryptographiques

L'homme du milieu

MAN IN THE MIDDLE



Rappels cryptographiques

L'homme du milieu

MAN IN THE MIDDLE



Rappels cryptographiques

L'homme du milieu

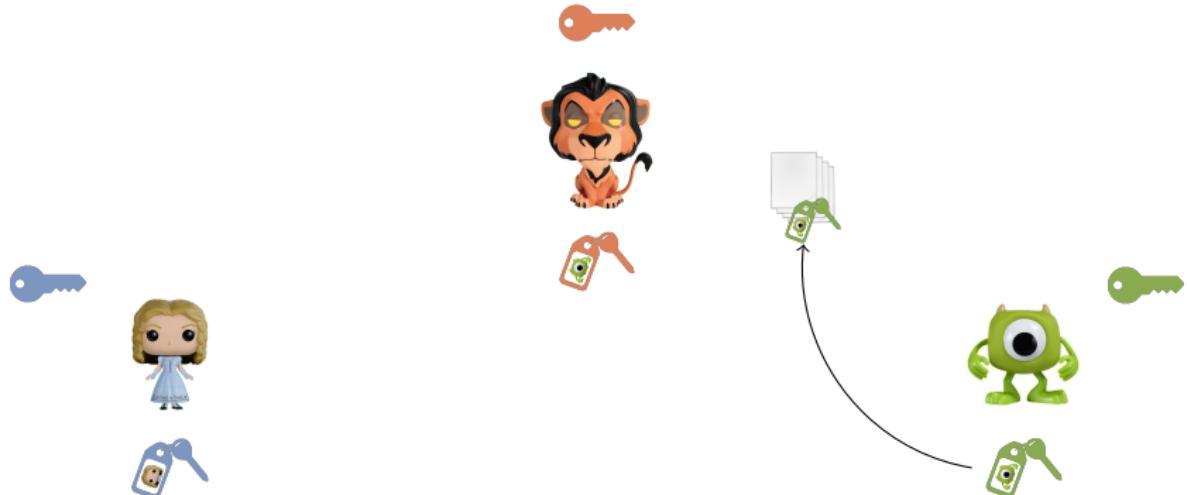
MAN IN THE MIDDLE



Rappels cryptographiques

L'homme du milieu

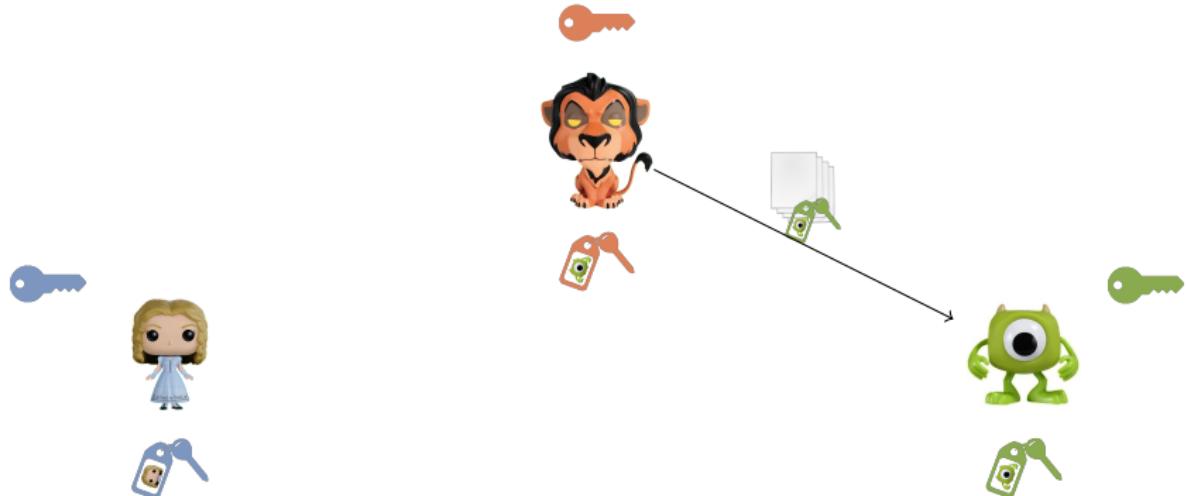
MAN IN THE MIDDLE



Rappels cryptographiques

L'homme du milieu

MAN IN THE MIDDLE



CERTIFICATS

Objectif

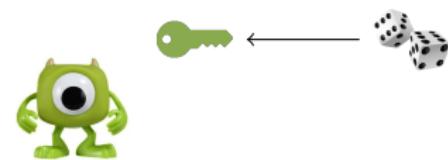
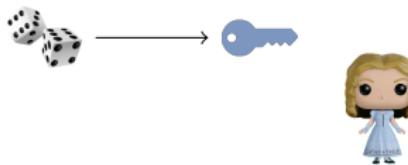
- ▶ s'assurer de l'*identité* de son correspondant.



CERTIFICATS

Objectif

- ▶ s'assurer de l'*identité* de son correspondant.



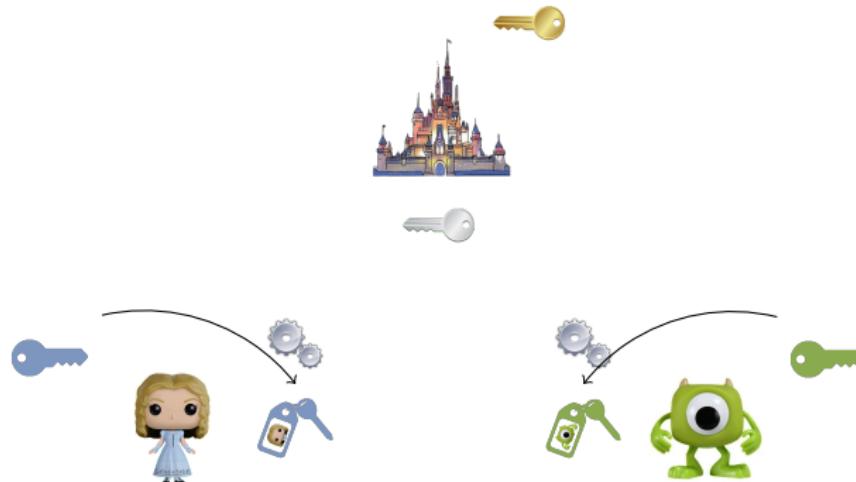
Rappels cryptographiques

Certificats

CERTIFICATS

Objectif

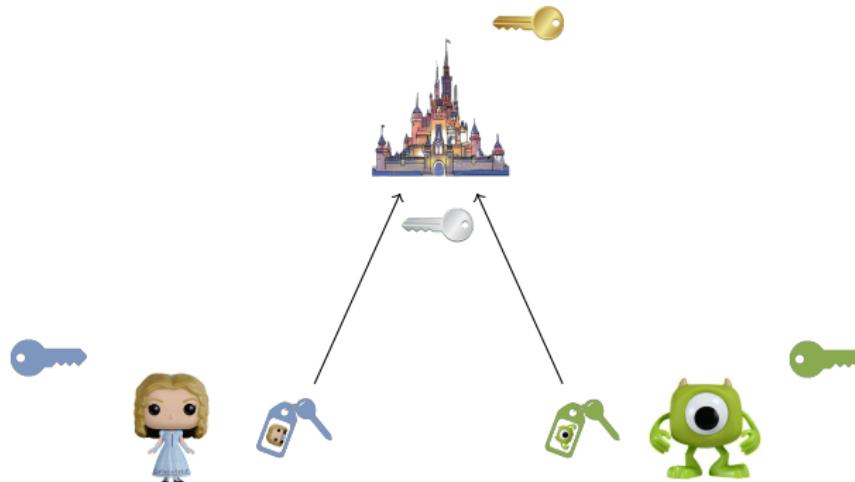
- ▶ s'assurer de l'*identité* de son correspondant.



CERTIFICATS

Objectif

- ▶ s'assurer de l'*identité* de son correspondant.



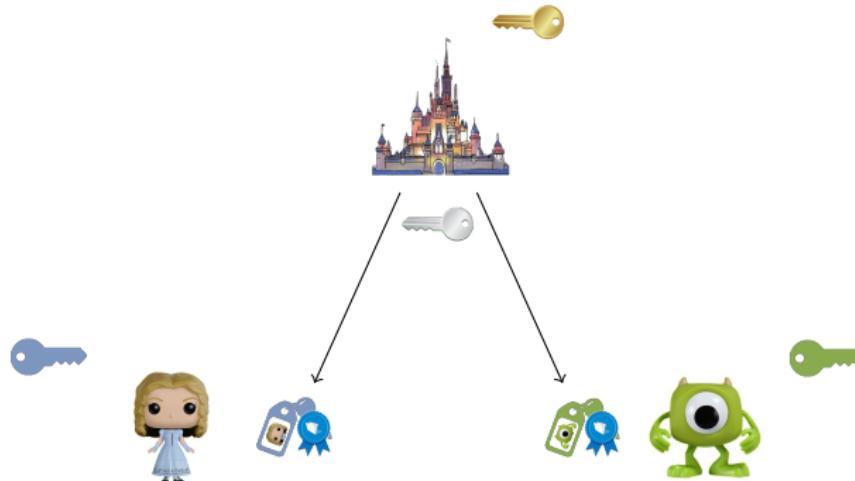
Rappels cryptographiques

Certificats

CERTIFICATS

Objectif

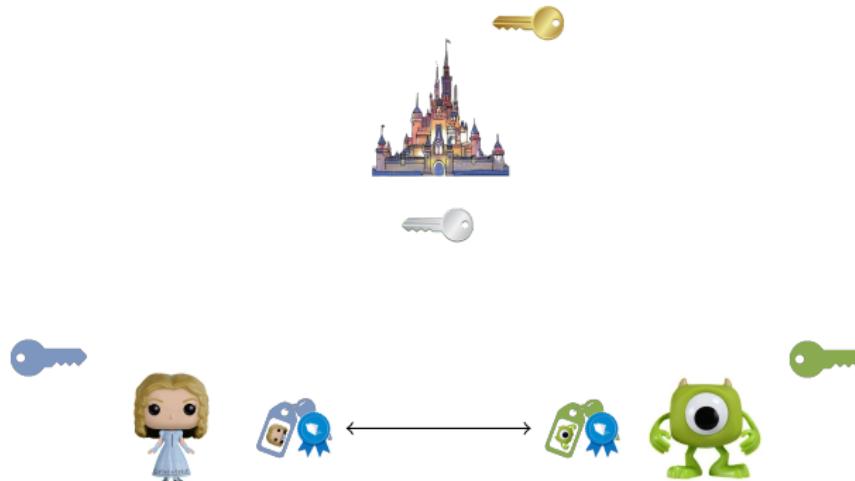
- ▶ s'assurer de l'*identité* de son correspondant.



CERTIFICATS

Objectif

- ▶ s'assurer de l'*identité* de son correspondant.



Rappels cryptographiques

Intégrité spatiale

Chaque bloc est protégé en intégrité.

Nom | Id

toto | 1

tata | 2

bad | 3

1 | 1427

2 | 238

3 | 1

Id | Solde

Rappels cryptographiques

Intégrité spatiale

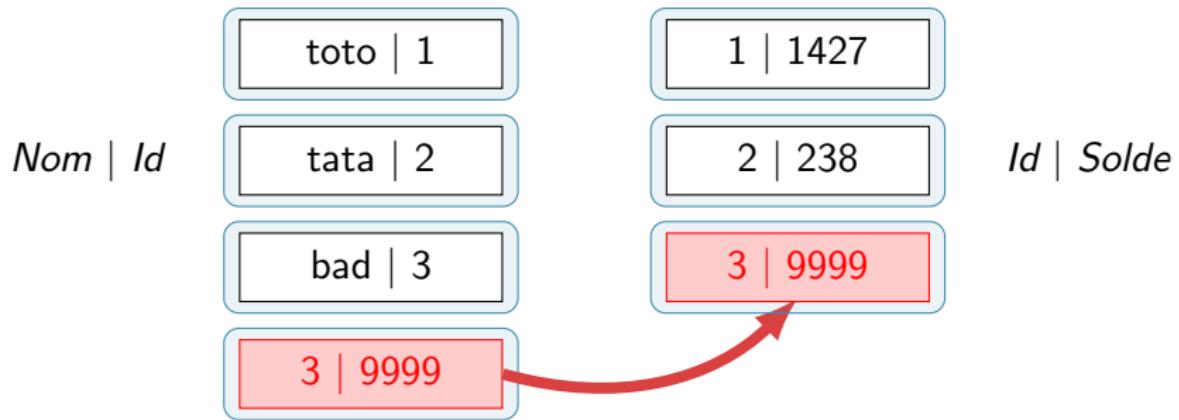
Chaque bloc est protégé en intégrité.

<i>Nom Id</i>	<i>Id Solde</i>
toto 1	1 1427
tata 2	2 238
bad 3	3 1
3 9999	

Rappels cryptographiques

Intégrité spatiale

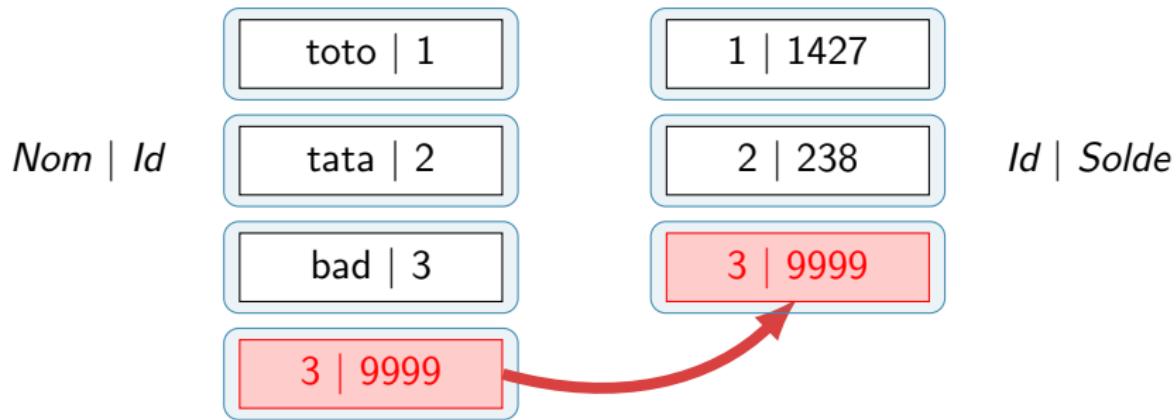
Chaque bloc est protégé en intégrité.



Rappels cryptographiques

Intégrité spatiale

Chaque bloc est protégé en intégrité.



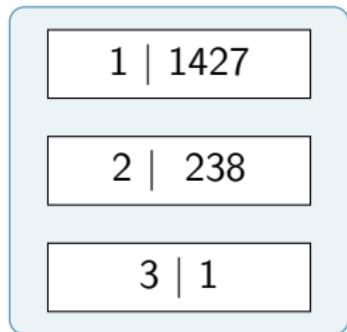
Un bloc intègre sera interprété différemment en fonction de sa place.
Pourtant il reste intègre !

Rappels cryptographiques

Intégrité temporelle

Chaque base est protégée en intégrité d'un seul tenant.

le 01/01



Rappels cryptographiques

Intégrité temporelle

Chaque base est protégée en intégrité d'un seul tenant.

le 01/01

le 02/01

1 1427
2 238
3 1

1 1136
2 48
3 8465

Rappels cryptographiques

Intégrité temporelle

Chaque base est protégée en intégrité d'un seul tenant.

le 01/01

le 02/01

le 03/01

1 1427
2 238
3 1

1 1136
2 48
3 8465

1 856
2 735
3 2

Rappels cryptographiques

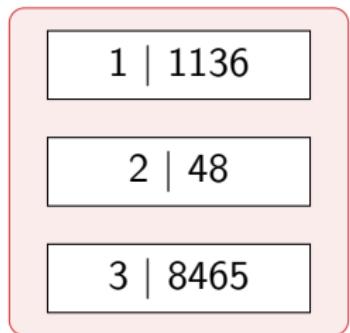
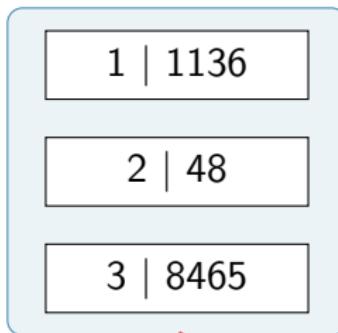
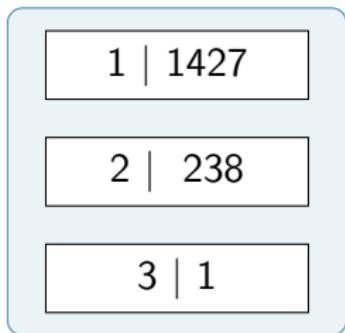
Intégrité temporelle

Chaque base est protégée en intégrité d'un seul tenant.

le 01/01

le 02/01

le 03/01



Un bloc intègre le restera dans le temps si rien n'est fait pour l'empêcher.

Rappels cryptographiques

Spécification d'un système

Description du besoin

Choix des solutions cryptographiques

Spécifications

Mise en œuvre

Description du besoin

Cahier des charges

- ▶ Utilisation administrative : toute démarche nécessitant une preuve d'identité
 - ▶ demande d'actes de naissance,
 - ▶ gestion de la situation fiscale,
 - ▶ vote,
 - ▶ contrôle d'identité,
 - ▶ déposition
 - ▶ ...
- ▶ Utilisation personnelle : faciliter l'usage de la cryptographie
 - ▶ protection de documents personnels stockés,
 - ▶ correspondance chiffrée,
 - ▶ signature de documents privés (contrats, chartes ...)
 - ▶ ...

Description du besoin

Cas d'usages

Démarche administrative physique



Description du besoin

Cas d'usages

Démarche administrative physique



Démarche administrative en ligne



Description du besoin

Cas d'usages

Démarche administrative physique



Démarche administrative en ligne



Contrôle d'identité



Description du besoin

Cas d'usages

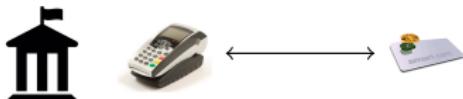
Démarche administrative physique



Démarche administrative en ligne



Contrôle d'identité



Usage privé



Description du besoin

Besoins de services

Services devant être rendus par la CCP

1. Prouver l'identité de son possesseur.
2. Créer un canal sécurisé avec un interlocuteur.
3. Sécuriser des données
 - ▶ pour envoi,
 - ▶ pour stockage.
4. Signer un documents.
5. Vérifier l'origine d'un document.

Services devant être rendus par les terminaux

1. Vérifier l'identité d'un détenteur de CCP.
2. Exposer les services de la CCP à un ordinateur.

Rappels cryptographiques

Spécification d'un système

Description du besoin

Choix des solutions cryptographiques

Spécifications

Mise en œuvre

Choix des solutions cryptographiques

Quelles solutions techniques pour quel besoin ?

- ▶ Biométrie
 - ▶ preuve/vérification d'identité.
- ▶ Échange de clef
 - ▶ sécurisation d'un canal.
- ▶ Algorithme de signature
 - ▶ signer un document,
 - ▶ vérifier l'origine d'un document,
 - ▶ sécurisation d'un canal (échange de clef authentifié).
- ▶ Algorithme de chiffrement authentifié
 - ▶ sécurisation d'un canal,
 - ▶ sécurisation de données,
 - ▶ vérifier l'origine d'un document.

Choix des solutions cryptographiques

Besoin fonctionnels vs sécuritaires

Pour le moment on n'a pas évoqué la sécurité mais juste le fonctionnel.

Bien sûr on va s'assurer que

- ▶ les algorithmes cryptographiques sont solides,
- ▶ le mécanisme de biométrie est infalsifiable.

Mais il faut aussi penser à ce que

- ▶ les données biométriques ou d'identité soient les bonnes,
- ▶ les vérifications de signatures/MAC ne soient pas "oubliées" ,
- ▶ les secrets soient **réellement** inaccessibles.

Pour s'en assurer on va

1. identifier les menaces,
2. utiliser de la cryptographie.

Choix des solutions cryptographiques

Menaces sur la preuve d'identité 1/3



Choix des solutions cryptographiques

Menaces sur la preuve d'identité 1/3



Choix des solutions cryptographiques

Menaces sur la preuve d'identité 1/3



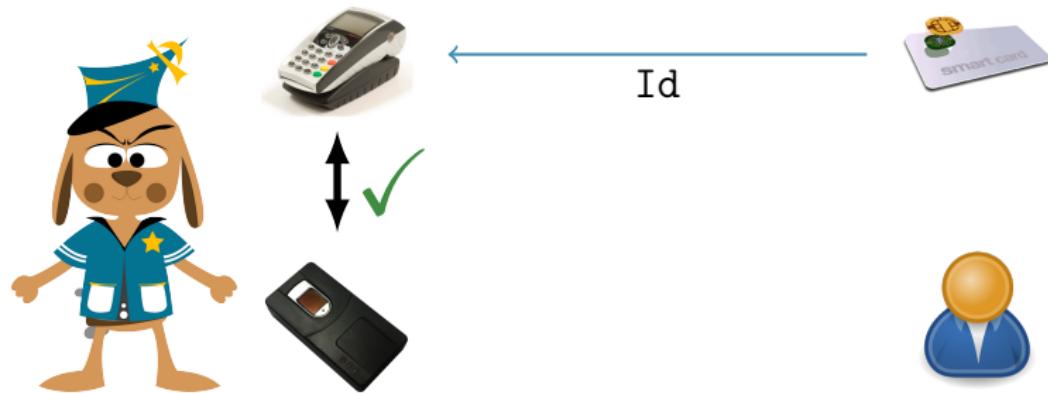
Choix des solutions cryptographiques

Menaces sur la preuve d'identité 1/3



Choix des solutions cryptographiques

Menaces sur la preuve d'identité 1/3



Choix des solutions cryptographiques

Menaces sur la preuve d'identité 2/3



Alice

1m 61

12/07/1998



Choix des solutions cryptographiques

Menaces sur la preuve d'identité 2/3



Alice

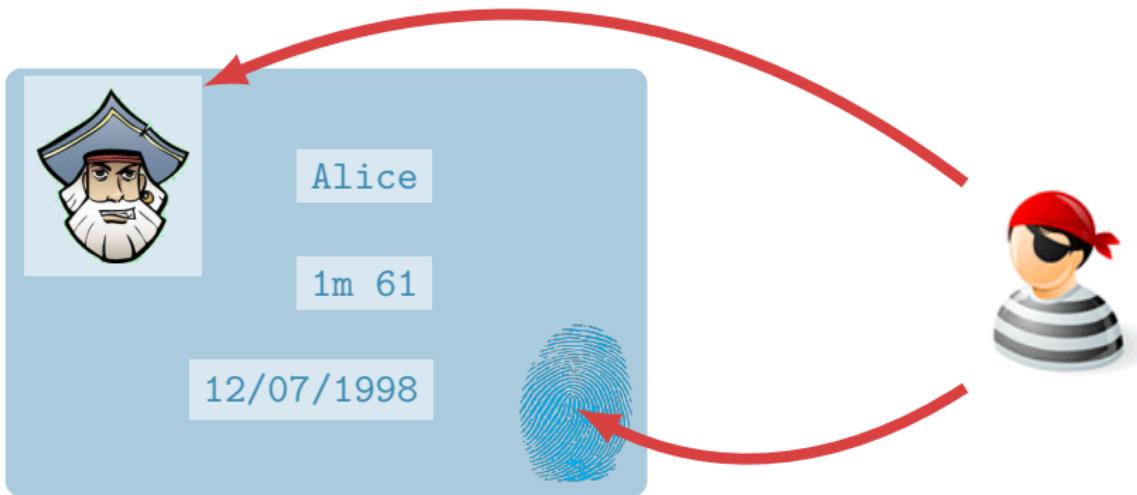
1m 61

12/07/1998



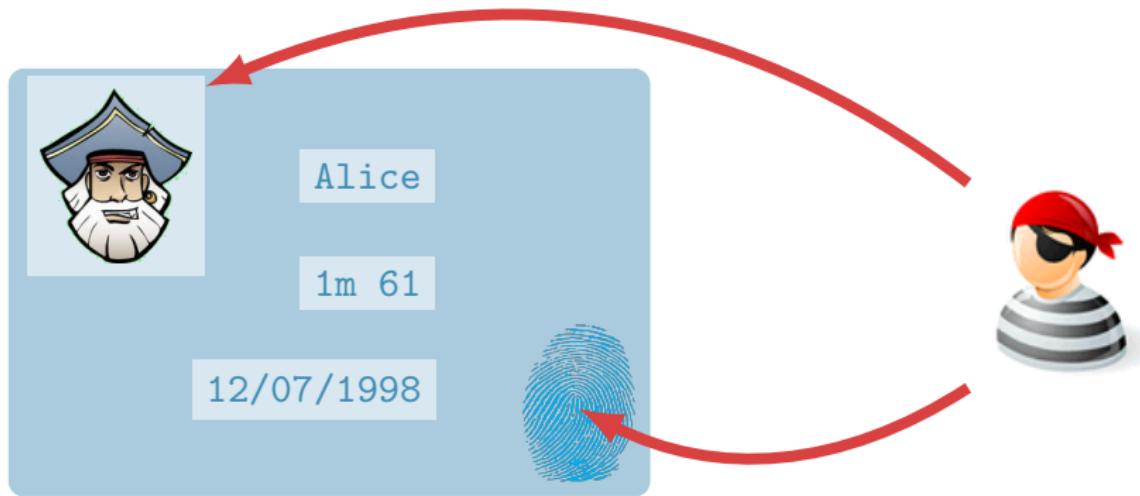
Choix des solutions cryptographiques

Menaces sur la preuve d'identité 2/3



Choix des solutions cryptographiques

Menaces sur la preuve d'identité 2/3

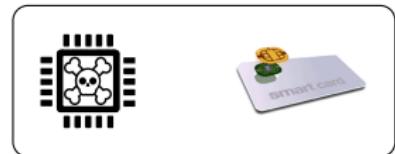


Questions

- ▶ Qui met les données biométriques et comment ?
- ▶ Un attaquant peut-il les modifier ?

Choix des solutions cryptographiques

Menaces sur la preuve d'identité 3/3



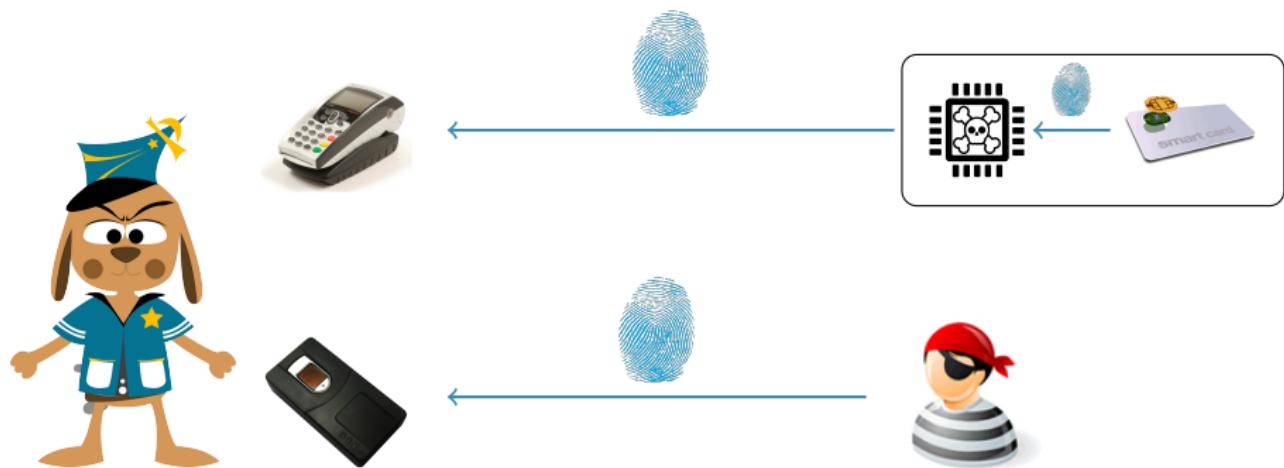
Choix des solutions cryptographiques

Menaces sur la preuve d'identité 3/3



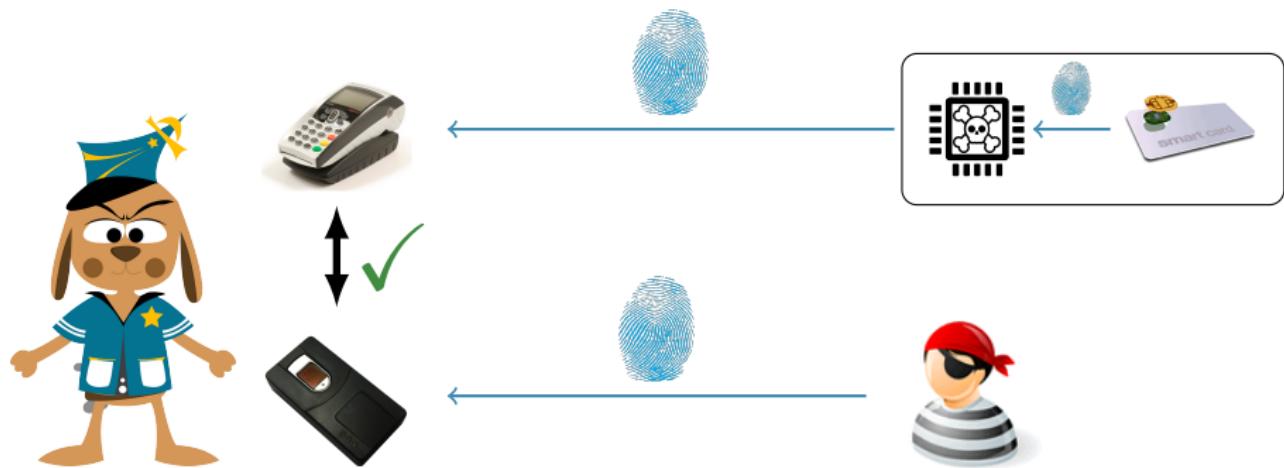
Choix des solutions cryptographiques

Menaces sur la preuve d'identité 3/3



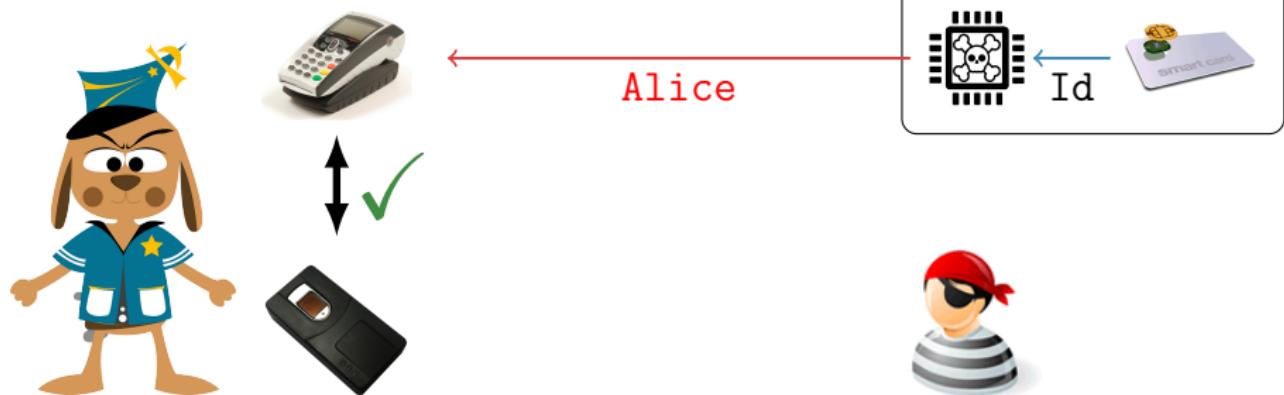
Choix des solutions cryptographiques

Menaces sur la preuve d'identité 3/3



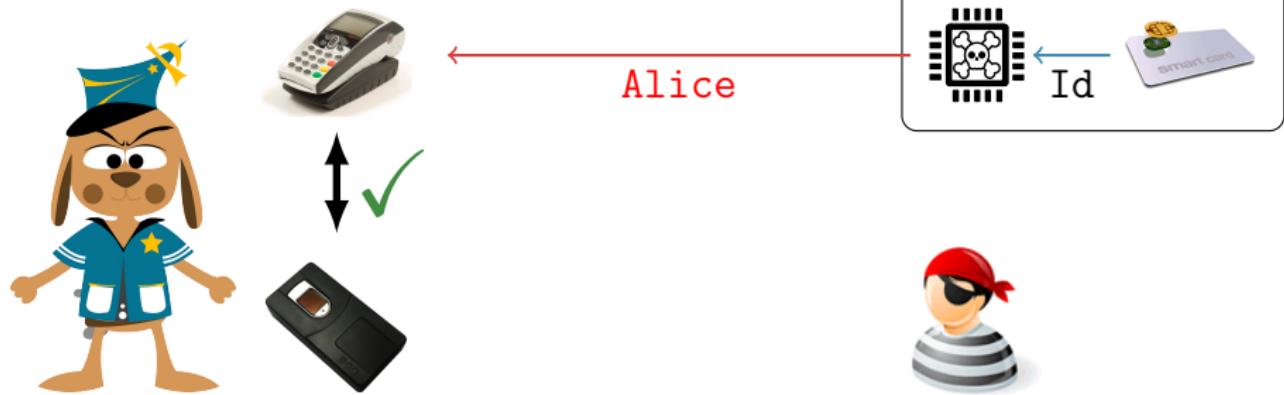
Choix des solutions cryptographiques

Menaces sur la preuve d'identité 3/3



Choix des solutions cryptographiques

Menaces sur la preuve d'identité 3/3

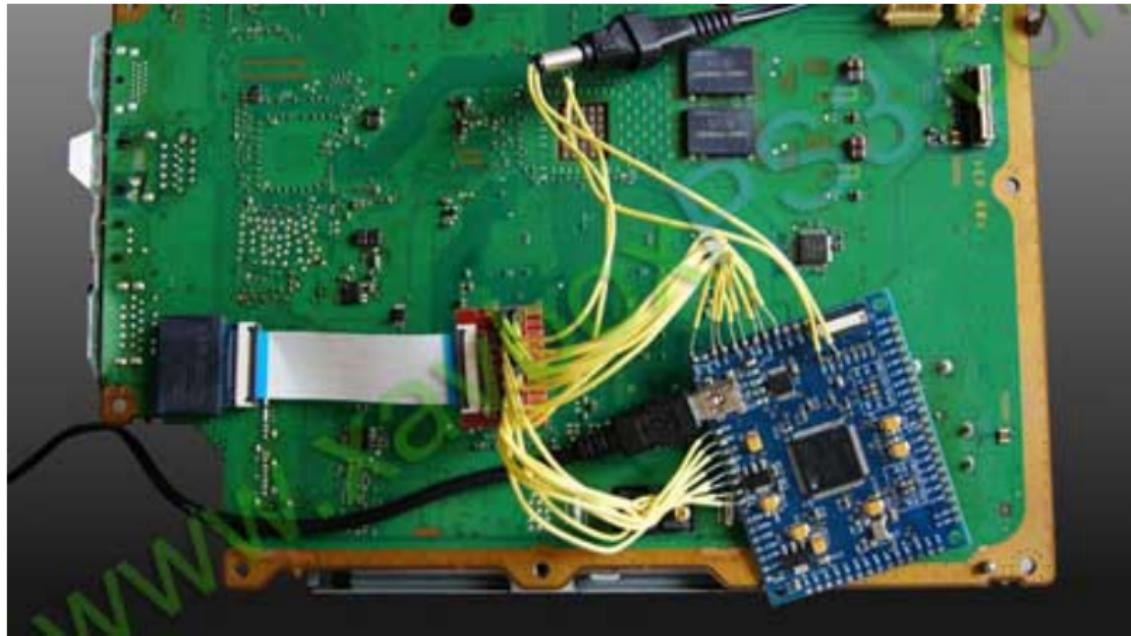


Questions

- ▶ Comment s'assure-t-on de la validité des informations reçues ?

Choix des solutions cryptographiques

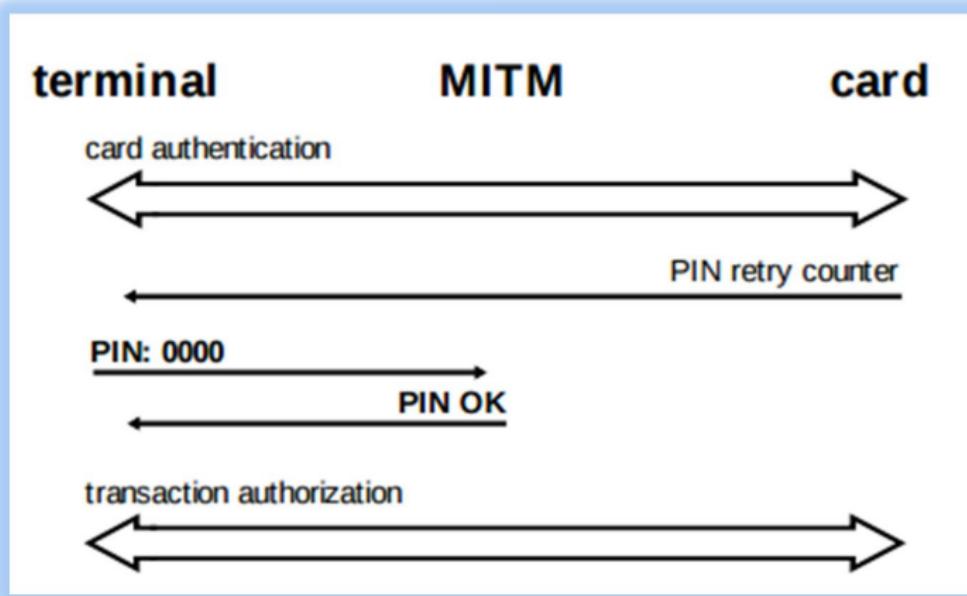
Modification du firmware en mémoire d'une PS3



Choix des solutions cryptographiques

L'exemple des cartes bancaires (1/3)

Grosse faille dans le protocole !



Choix des solutions cryptographiques

L'exemple des cartes bancaires (2/3)

Analyse de risques ...



...trop coûteux et difficile à mettre en oeuvre.

Choix des solutions cryptographiques

L'exemple des cartes bancaires (2/3)

Analyse de risques ...



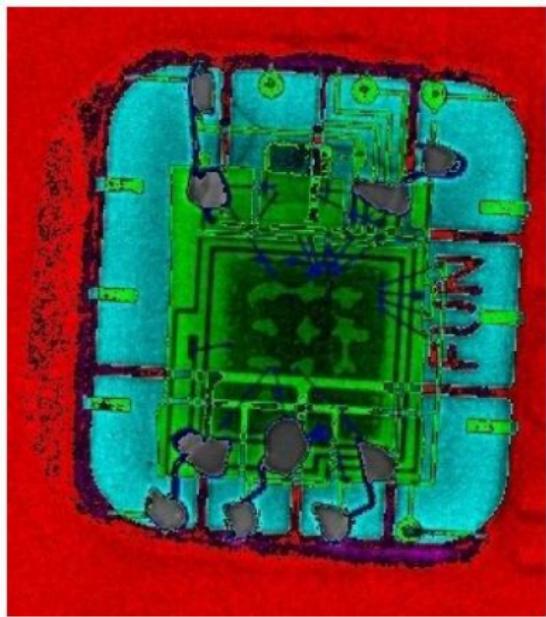
... trop coûteux et difficile à mettre en oeuvre.

run on a similar device. Miniaturization is mostly a mechanical challenge, and well within the expertise of criminal gangs: such expertise has already been demonstrated in the miniaturised transaction interceptors that have been used to sabotage point of sale terminals and skim magnetic strip data. Miniaturization is not critical though as criminals

Choix des solutions cryptographiques

L'exemple des cartes bancaires (3/3)

Quelques (deux) années plus tard au tribunal ...



Choix des solutions cryptographiques

Prise en compte de la sécurité

- ▶ Les cartes sont produites quelque part ...
 - ▶ donc ces gens connaissent le fonctionnement,
 - ▶ donc il peut exister un marché parallèle.
- ▶ L'administration sait injecter des données biométriques ...
 - ▶ donc la fonctionnalité existe sur la carte.
- ▶ L'interface avec la carte a été spécifiée ...
 - ▶ donc comme n'importe quelle entreprise, l'attaquant peut produire des éléments compatibles avec le système.
- ▶ On sait faire de la rétro-ingénierie ...
 - ▶ relecture de l'EEPROM de la machine de vote indienne par exemple.

La cryptographie peut aider ici pour sécuriser les éléments face à ces menaces.

Rappels cryptographiques

Spécification d'un système

Description du besoin

Choix des solutions cryptographiques

Spécifications

Mise en œuvre

Spécifications

Analyse de la menace

Il faut définir contre qui et pour quoi on se protège.

Types d'attaquants

- ▶ Délinquants
 - ▶ un geek, un garage et un PC de gamer.
- ▶ Mafias
 - ▶ une équipe complète et un réseau de PC zombies.
- ▶ États
 - ▶ d'un groupe de hacker à la NSA.

Cotations d'attaques

- ▶ temps de mise en oeuvre,
- ▶ connaissance requise des produits,
- ▶ compétence requise,
- ▶ ressources humaines (temps),
- ▶ ressources matérielles,
- ▶ temps d'exploitation,
- ▶ impact.

Spécifications

Cible de sécurité

Terminologie utilisée par les Critères Communs.

1. Identifier les biens à protéger (on utilise le terme *assets*)
 - ▶ clefs secrètes,
 - ▶ données personnelles,
 - ▶ propriété intellectuelle.
2. Délimitation du périmètre de protection
 - ▶ un processeur,
 - ▶ une carte,
 - ▶ une infrastructure et ses acteurs.
3. Définition d'objectifs de sécurité
 - ▶ tel clef ne doit pas être retrouvée durant la durée de vie d'un équipement,
 - ▶ tel contenu ne doit pas pouvoir sortir sur les interfaces externes même en cas de panne,
 - ▶ l'équipement doit permettre de lister les secrets possédés par un utilisateur authentifié.

Déterminer

1. les propriétés de sécurité devant être garanties,
 - ▶ confidentialité,
 - ▶ tracabilité,
 - ▶ protection de la vie privée ...
2. les menaces à prendre en compte,
 - ▶ toutes les attaques nécessitant moins de x ans ;
3. les éléments potentiellement corrompus,
 - ▶ i.e. éléments qui ne résistent pas aux menaces identifiées ;
4. les mécanismes pour étendre la confiance aux éléments corruptibles.
 - ▶ signature des données personnelles contenues dans la carte,
 - ▶ sécurisation des canaux potentiellement accessibles ...

Déterminer

1. les propriétés de sécurité devant être garanties,
 - ▶ confidentialité,
 - ▶ tracabilité,
 - ▶ protection de la vie privée ...
2. les menaces à prendre en compte,
 - ▶ toutes les attaques nécessitant moins de x ans ;
3. les éléments potentiellement corrompus,
 - ▶ i.e. éléments qui ne résistent pas aux menaces identifiées ;
4. les mécanismes pour étendre la confiance aux éléments corruptibles.
 - ▶ signature des données personnelles contenues dans la carte,
 - ▶ sécurisation des canaux potentiellement accessibles ...

Cela implique d'avoir **une racine de confiance**.

Spécifications

Besoin de confiance

Au “début du monde”, il y a une confiance *organisationnelle*.

- ▶ Autorité de certification racine (certificats web, windows)
 - ▶ S'assure de l'identité des utilisateurs.
 - ▶ Signe leur(s) certificat(s) (clef publique + identité).
 - ▶ Signe le code à exécuter.
- **Confiance dans la protection de la clef privée.**
- ▶ Toile de confiance (PGP)
 - ▶ Les utilisateurs s'assurent de l'identité des interlocuteurs.
 - ▶ Ajout de sa signature aux clefs des personnes rencontrées.
- **Confiance dans la communauté (pas de collusion).**

Spécifications

Identification du possesseur

Risques

Modification de la carte pour usurper l'identité.

Solution

Données biométrique + signature cryptographique des données.

- ▶ Lier l'utilisateur à la carte (déploiement)
 - ▶ organisationnel : confiance en le personnel.
 - ▶ technique : signature des données sur la carte + schéma à seuil.
- ▶ Vérifier l'identité d'un porteur de carte (utilisation)
 - ▶ organisationnel : confiance dans l'autorité signataire.
 - ▶ technique : vérification de la signature des données.

Mise en place d'un système de délégation de signature (arborescence de clefs ou signature de groupe/anneau).

Spécifications

Canal sécurisé

Risques

- ▶ Espionnage
- ▶ Attaque man-in-the-middle

Solution

Canal sécurisé : échange de clef après identification réciproque.

En option

- ▶ PFS (*perfect forward secrecy*)
- ▶ Confirmation des clefs négociées

PFS

Si une clef corrompue à un instant t , alors la sécurité des éléments protégés à un instant $t' < t$ est garantie.

Spécifications

Sécurisation des données

Risques

- ▶ Lecture de données secrètes
- ▶ Modification de données sensibles
- ▶ Réutilisation de données sensibles

Solution

- ▶ Chiffrement
- ▶ Intégrité spatiale
- ▶ Anti-rejeu (intégrité temporelle)

Intégrité spatiale

On utilise en général un arbre de Merkle pour les grands volumes de données.

Spécifications

Valider et vérifier la validité de documents

Risques

- ▶ Usurpation d'identité
- ▶ Répudiation

Solution

- ▶ Algorithme de signature
- ▶ Un couple clef/certificat par carte
- ▶ Clef publique racine de confiance

Cela implique de générer une clef privée par carte.

Rappels cryptographiques

Spécification d'un système

Description du besoin

Choix des solutions cryptographiques

Spécifications

Mise en œuvre

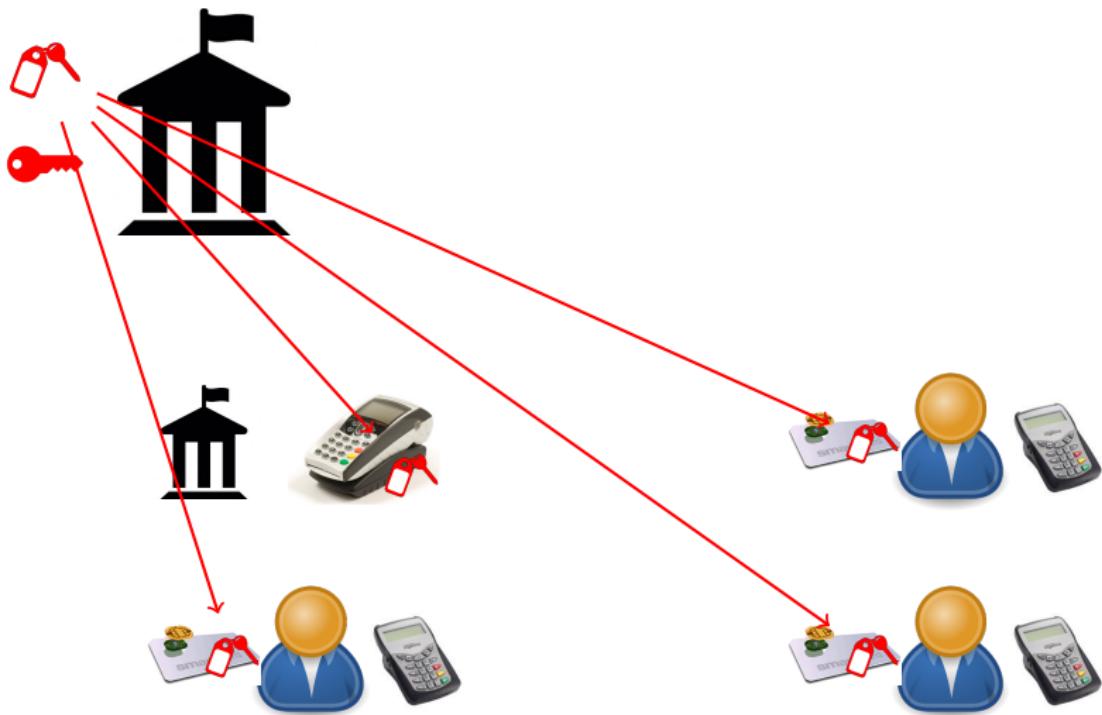
Mise en œuvre

Vue générale des secrets



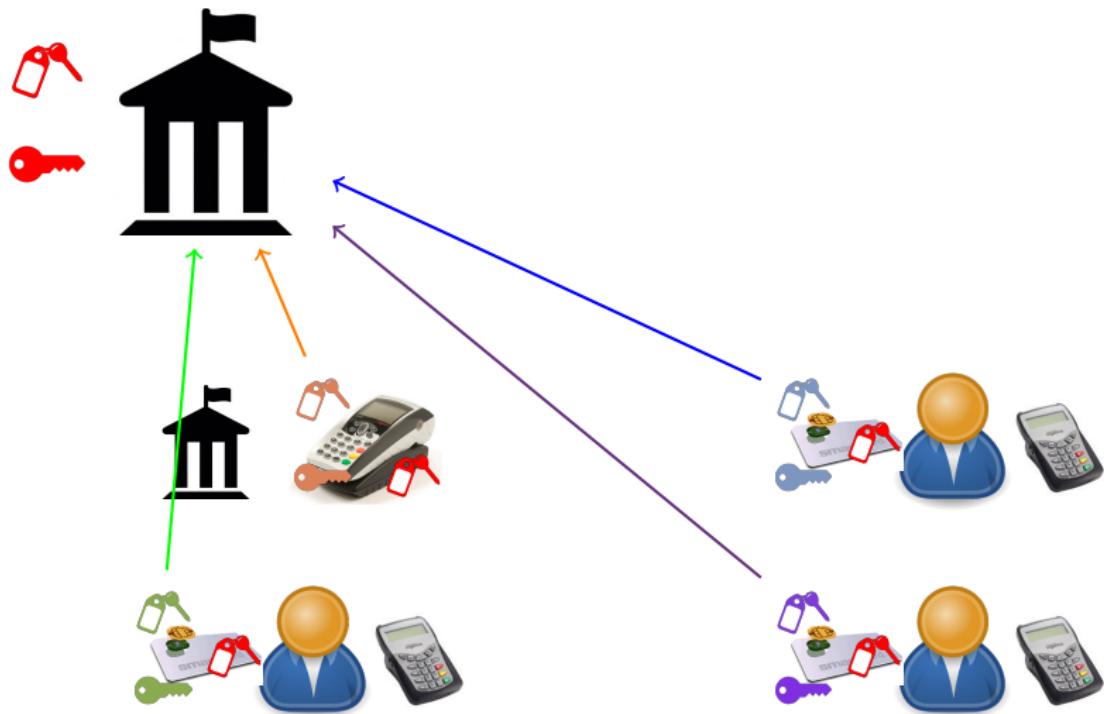
Mise en œuvre

Vue générale des secrets



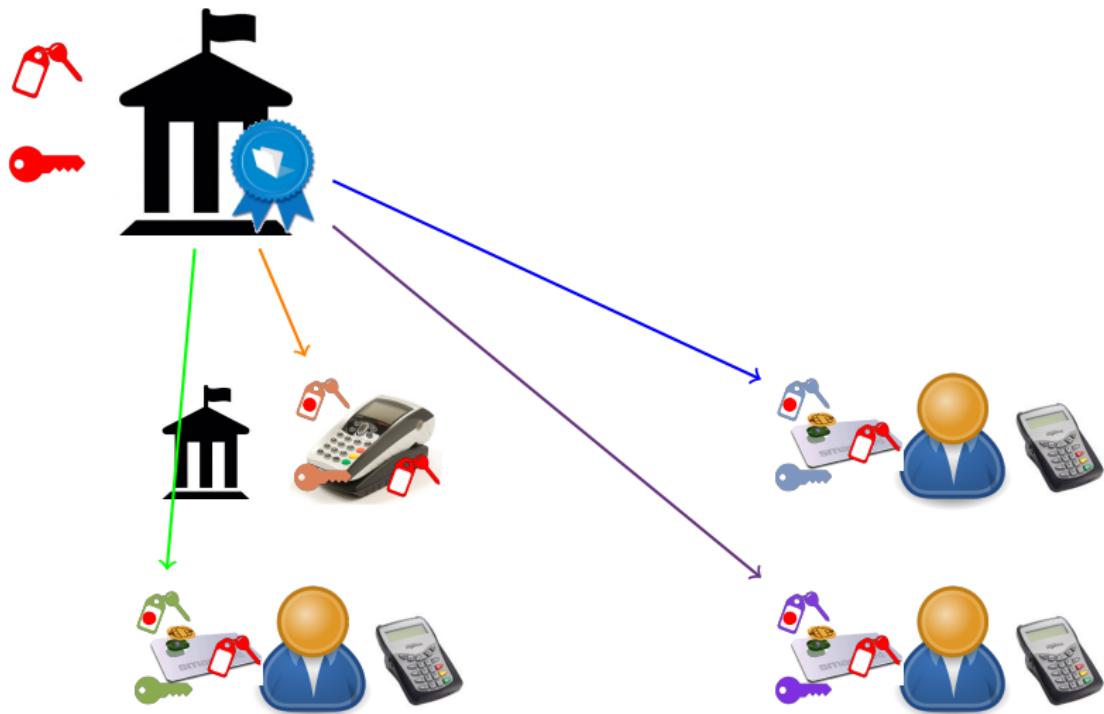
Mise en œuvre

Vue générale des secrets



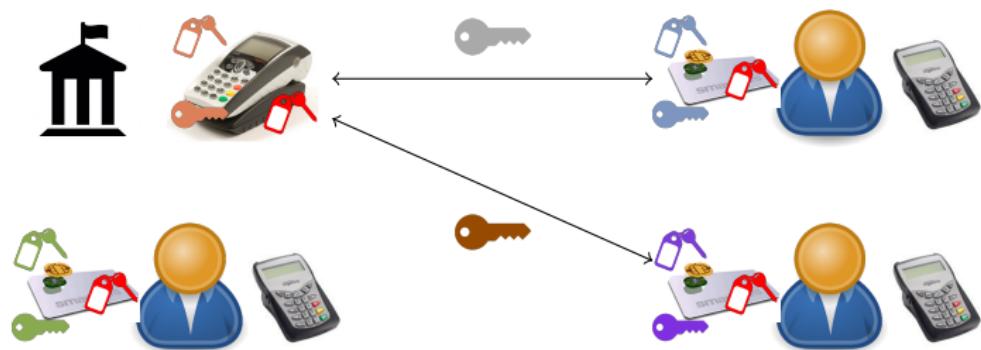
Mise en œuvre

Vue générale des secrets



Mise en œuvre

Vue générale des secrets



Mise en œuvre

Délégation de signature



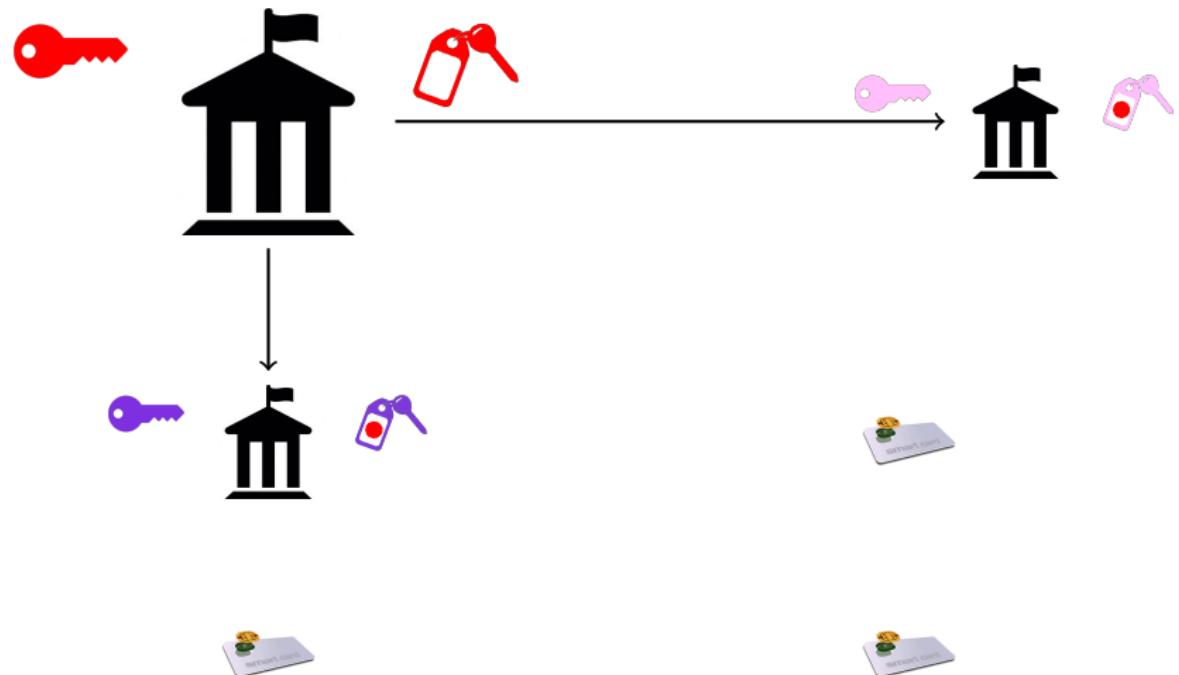
Mise en œuvre

Délégation de signature



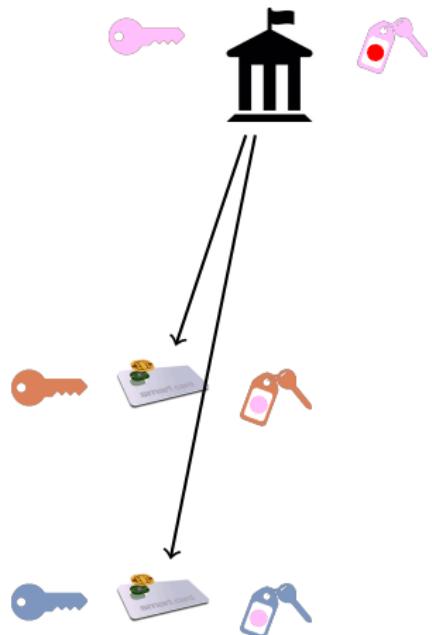
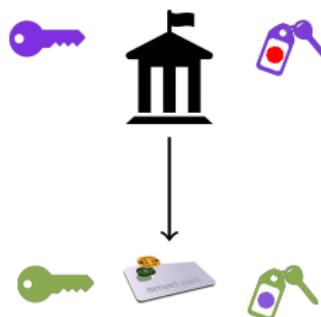
Mise en œuvre

Délégation de signature



Mise en œuvre

Délégation de signature



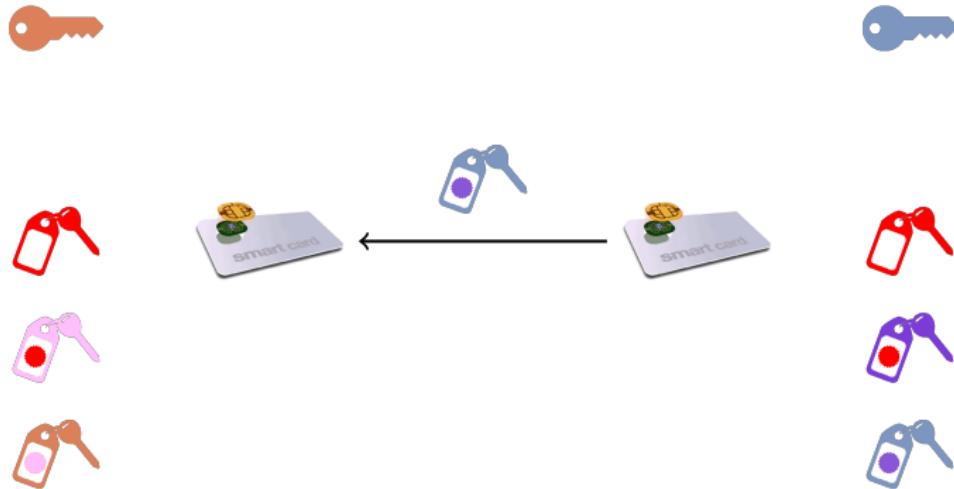
Mise en œuvre

Vérification d'une chaîne de certificats



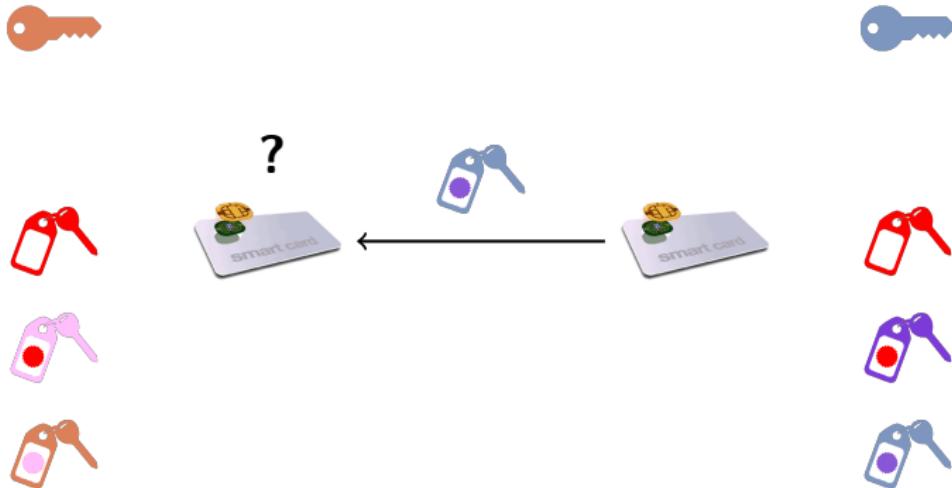
Mise en œuvre

Vérification d'une chaîne de certificats



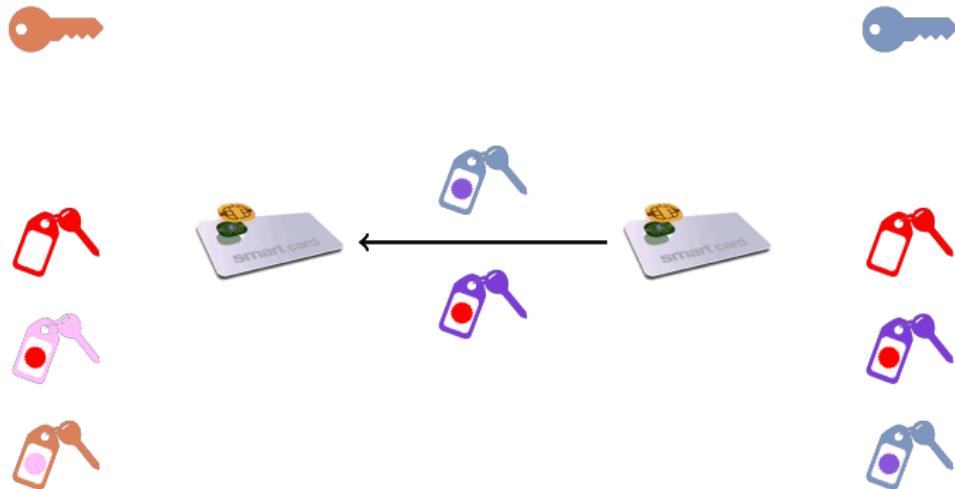
Mise en œuvre

Vérification d'une chaîne de certificats



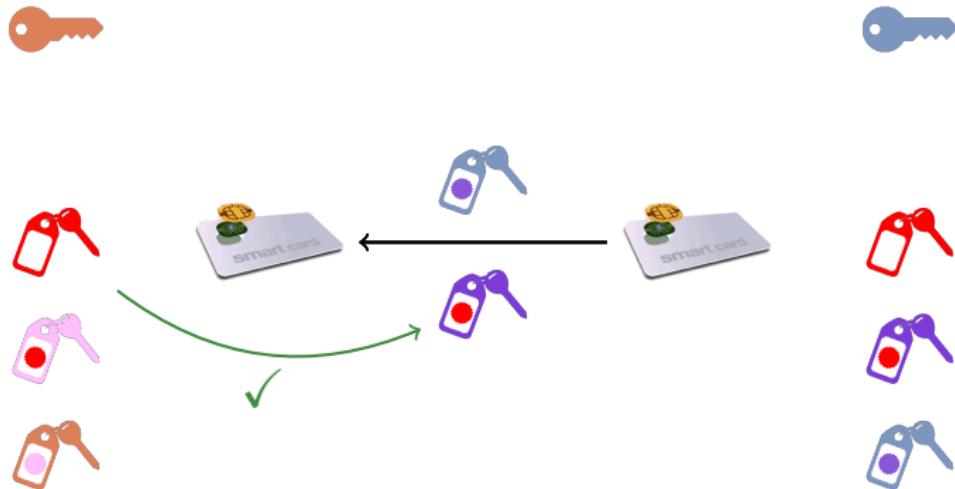
Mise en œuvre

Vérification d'une chaîne de certificats



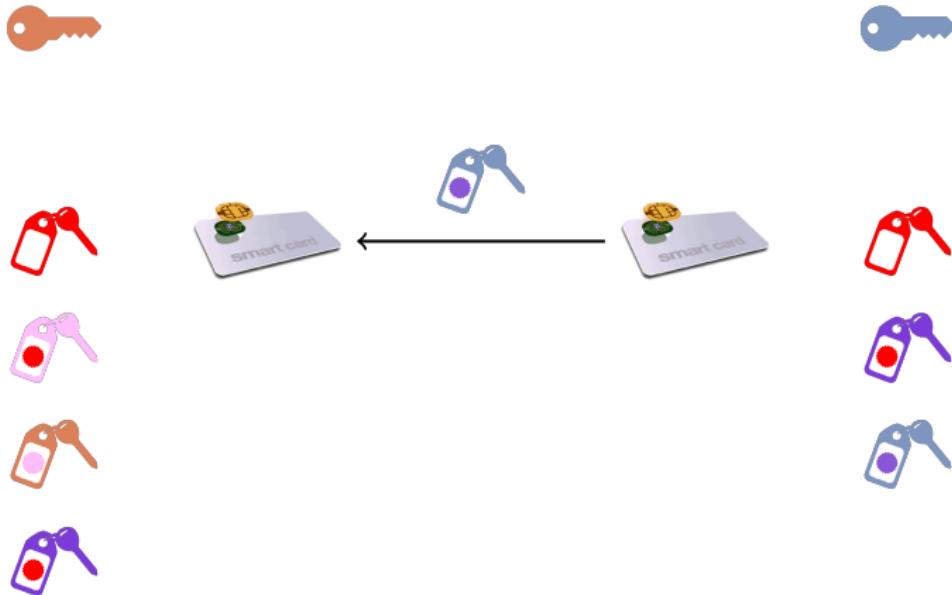
Mise en œuvre

Vérification d'une chaîne de certificats



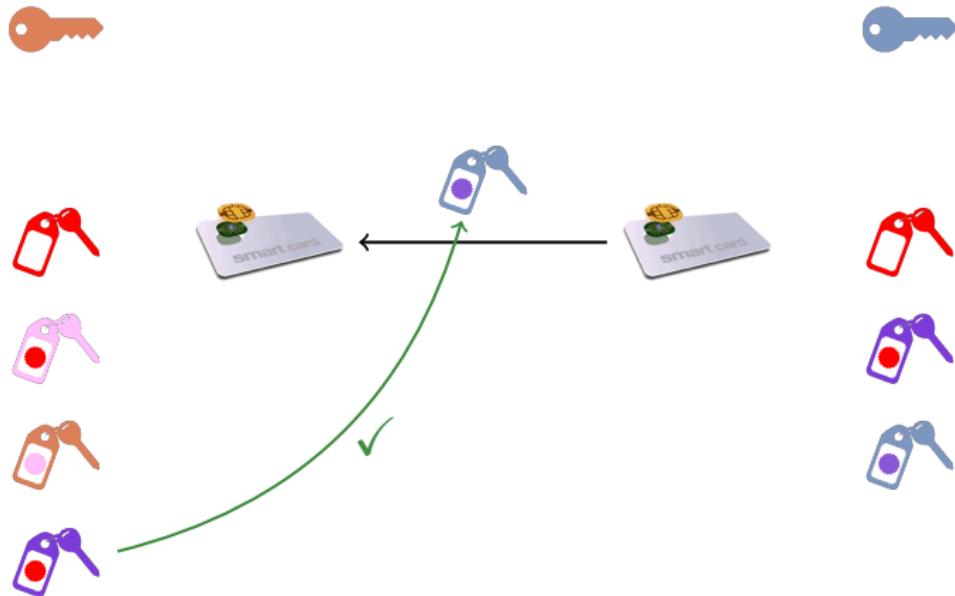
Mise en œuvre

Vérification d'une chaîne de certificats



Mise en œuvre

Vérification d'une chaîne de certificats

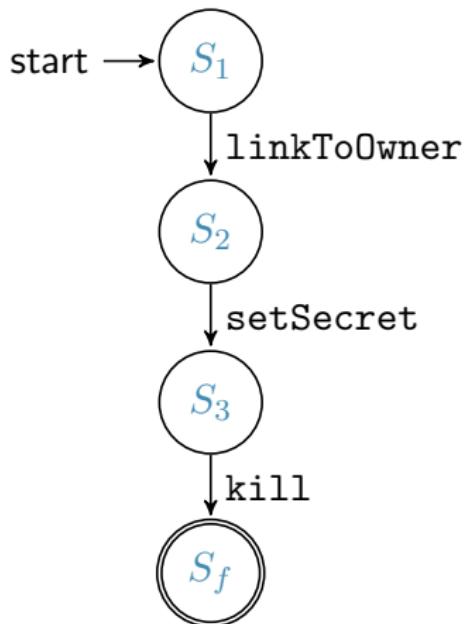


Mise en œuvre

Vérification d'une chaîne de certificats



Les éléments du système devront respecter :



S_1 Sortie Usine/Personnalisation

S_2 Initialisation

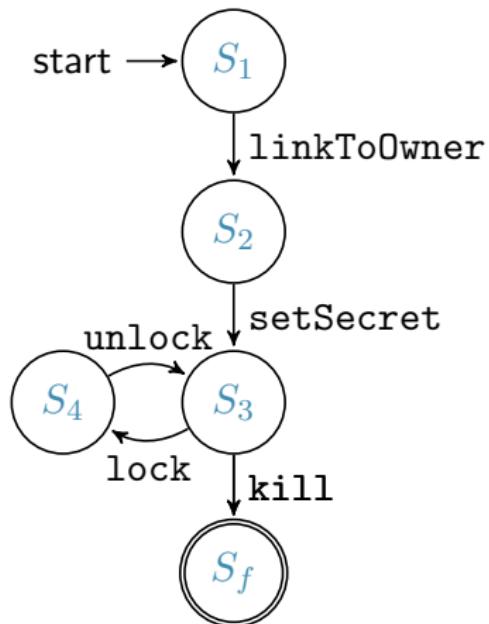
S_3 Utilisation

S_f Destruction

Mise en place de :

- ▶ procédures,
- ▶ moyens (humains, infra.).

Les éléments du système devront respecter :



- S_1 Sortie Usine/Personnalisation
- S_2 Initialisation
- S_3 Utilisation (déverouillé)
- S_4 Utilisation (verouillé)
- S_f Destruction

Mise en place de :

- ▶ procédures,
- ▶ moyens (humains, infra.).

- ▶ Carte avec mot de passe,
 - ▶ en cas de perte (tant pis, schéma à seuil . . .) ?
- ▶ Révocation d'éléments / cryptopériode / mise à jour logicielle
 - ▶ connexion avec l'autorité possible ?
 - ▶ accès à une horloge sécurisée ?
 - ▶ notion d'administrateur ?
- ▶ Clef secrète de la carte
 - ▶ générée par l'administration (big brother),
 - ▶ générée en interne (manipulation à prévoir à la remise).

Message

- ▶ Mettre en oeuvre de la cryptographie est souvent compliqué.
- ▶ Difficile de penser à tout
(surtout si on n'a pas toutes les informations).

Bonne pratiques

- ▶ Ne pas négliger un type d'attaquant pertinent.
~~C'est trop difficile à faire.~~
- ▶ Prendre en compte les contraintes le plus tôt dans la conception.

Pour cela il faut **communiquer** avec les personnes impliquées ...

Message

- ▶ Mettre en oeuvre de la cryptographie est souvent compliqué.
- ▶ Difficile de penser à tout
(surtout si on n'a pas toutes les informations).

Bonne pratiques

- ▶ Ne pas négliger un type d'attaquant pertinent.
~~C'est trop difficile à faire.~~
- ▶ Prendre en compte les contraintes le plus tôt dans la conception.

Pour cela il faut **communiquer** avec les personnes impliquées . . .
 . . .mais aussi être pédagogue et convaincant.