Certificats et Infrastructures à clefs publiques

Cryptographie et réalité pratique

Yann Rotella

UVSQ - Université Paris-Saclay

16 avril 2026

Plan du Cours

L'attaque de l'homme du milieu

Autorités de Confiance

Notion de Confiance

L'ATTAQUE DE L'HOMME DU MILIEU
Un premier protocole
Identifiants

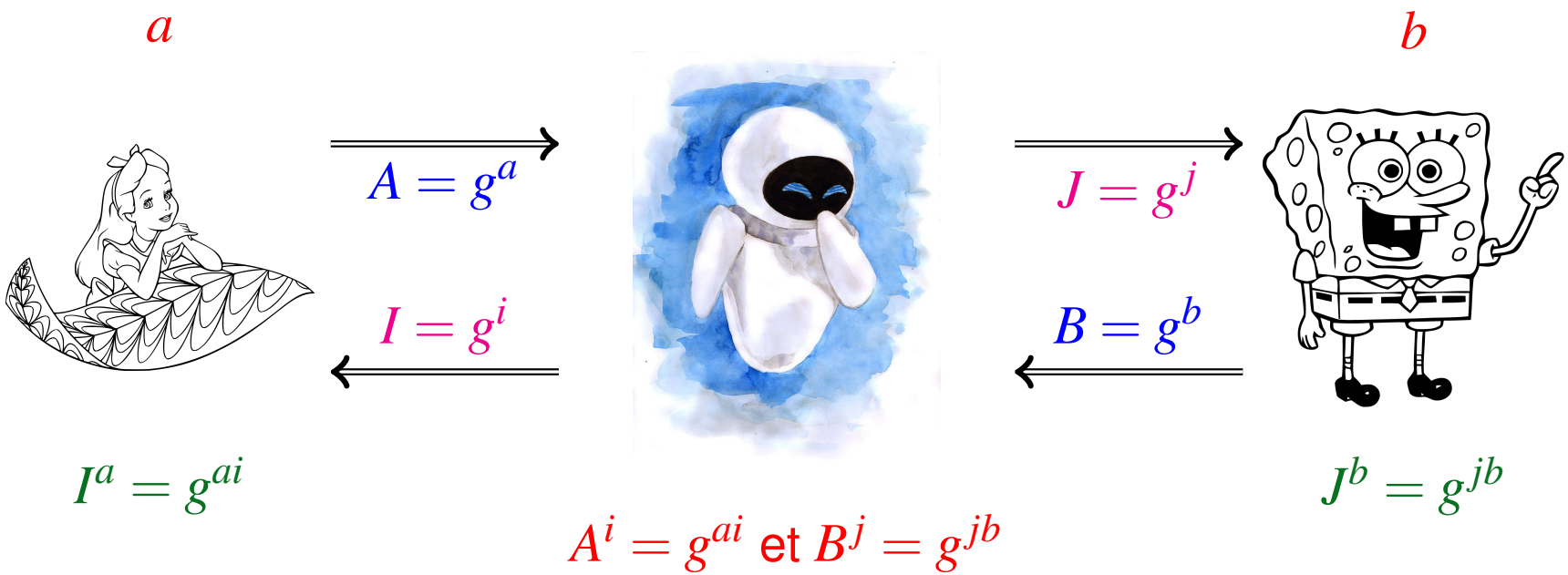
AUTORITÉS DE CONFIANCE
Le cas du Web
PKI
Certificats X.509

NOTION DE CONFIANCE

L'ATTAQUE DE L'HOMME DU MILIEU

Le cas Diffie-Hellman :

$$G = < g >$$



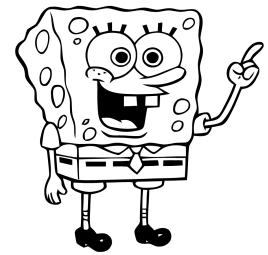
VERS UN PREMIER PROTOCOLE

Faits :

- La cryptographie asymétrique est lente (cf TP)
- La cryptographie symétrique est rapide (AES-NI instructions)
- **Idée :** Combiner les deux

VERS UN PREMIER PROTOCOLE

$$G =< g >$$



$a \leftarrow_{\$} \mathbb{Z}_{|G|}$ $\quad A = g^a \rightarrow \quad B = g^b \leftarrow$ $\quad a \leftarrow_{\$} \mathbb{Z}_{|G|}$

$B^a = g^{ab} = k_{sym}$ $\qquad$ $A^b = g^{ba} = k_{sym}$

$m \in \{0,1\}^*$

$\text{Enc}^{\texttt{AES\_GCM}}(N, k_{sym}, m) \xrightarrow{N, c, T} \text{Dec}^{\texttt{AES\_GCM}}(N, k_{sym}, c, T)$

$\rightarrow m$ `or` $\perp$

- ✍ Quelles implications si « Man-in-the-middle » ?
- ✍ À quoi sert T ?
- ✍ À quoi sert N ?

IDENTIFIANTS NUMÉRIQUES OU PHYSIQUES

- ✍ Donner des identifiants *a priori* uniques d'utilisateurs.
- ▶ On note maintenant $\texttt{ID}_A$ toute suite d'identifiants d'Alice.
- ✍ $\texttt{ID}_A$ ou $\texttt{ID}_A$?
- ✍ Expliquer pourquoi transmettre un couple $(sk_A, \texttt{ID}_A)$ ne fonctionne pas ?

L'attaque de l'homme du milieu
Un premier protocole
Identifiants

Autorités de Confiance
Le cas du Web
PKI
Certificats X.509

Notion de Confiance

Les tiers de confiance

- Il faut authentifier les clefs publiques !
- **Idée :** On suppose l'existence d'une **Autorité de Confiance** qui possède un couple de clefs (pk_{AC}, sk_{AC})
- Alice veut communiquer avec des gens de manière sécurisé et fait confiance à l'Autorité
- Alice demande un **Certificat** à l'autorité. L'autorité va alors
  1. Vérifier $\texttt{ID}_A$
  2. Vérifier qu'Alice a un couple de clefs (pk_A, sk_A)
  3. Produire enfin un certificat de la forme

$$\texttt{ID}_A || pk_A || (\texttt{Sign}(sk_{AC}, \texttt{ID}_A || pk_A))$$

- Tout le monde qui a pk_{AC} peut **vérifier** que l'Autorité de Confiance a signé la paire $(\texttt{ID}_A, pk_A)$.

AUTORITÉ DE CERTIFICATION - LE CAS DU WEB

pk_A, sk_A

Je veux un Certificat !

Ok, c'est quoi ta clef publique ?

Tu as les droits sur le serveur IP 192.xxx ?

Quel ϵ

Peux-t

C

en déposé

192.xxx,

ppelé

a signature

Autorité de Certification avec plus de pouvoir

- Dans certains cas, on peut vouloir que l'autorité génère les clefs d'accès.
- Cas d'application : carte d'accès à un bâtiment



Je veux un accès !

pk_A User $\mathtt{ID}_A$ OK

Peux-tu signer m ?

Oui c'est bien toi

Cool j'ai un accès !

Carte d'identité OK

$\mathtt{Sign}(sk_A, m)$

σ

$\mathtt{KeyGen} \rightarrow (sk_A, pk_A)$

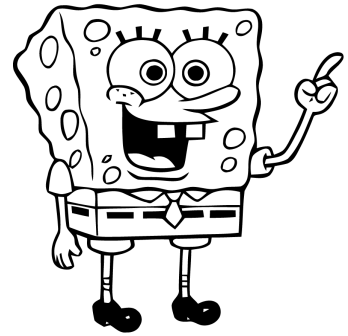
Voilà, je mets pk_A dans le système

Garde bien sk_A secrète sinon tu vas devoir revenir !

$\mathtt{Verif}(pk_A, m, \sigma) = \mathtt{Oui}$

✍ On pourrait utiliser des MAC, pourquoi c'est une mauvaise idée ?

Diffie-Hellman avec Certificats



$sk_A = a, pk_A = g^a$

$sk_B = b, pk_B = g^b$

$\mathrm{ID}_A || pk_A || \sigma_{AC}$ $\xrightarrow{\mathrm{Cert}_A}$

$\xrightarrow{\mathrm{Cert}_J}$

$\xleftarrow{\mathrm{Cert}_I}$

$\xleftarrow{\mathrm{Cert}_B}$ $\mathrm{ID}_B || pk_B || \sigma_{AC}$

$\mathtt{Verif}(\mathrm{Cert}_B, pk_{AC})$

- Expliquer pourquoi Alice et Bob détectent une attaque de type « Man-in-the-middle » ?

Mais qu'a t'on résolu ?

- On doit **vraiment** faire confiance à l'autorité !
- Il peut y avoir des problèmes à l'établissement du certificat de type man-in-the-middle, mais on essaye de le détecter par d'autres moyens (plusieurs canaux de communication, liaison physique, etc)
- Une fois que les certificats ont été établis, on peut établir des sessions différentes sans avoir à se rencontrer physiquement
- Authentification du canal une seule fois
- On a réalisé un *Transfert de Confiance*
- Réalisable individuellement, pour chaque utilisateur, pour ensuite que chacun fasse confiance à chacun.

PKI ET PROPRIÉTÉS

DÉFINITION (INFRASTRUCTURE À CLÉ PUBLIQUE)

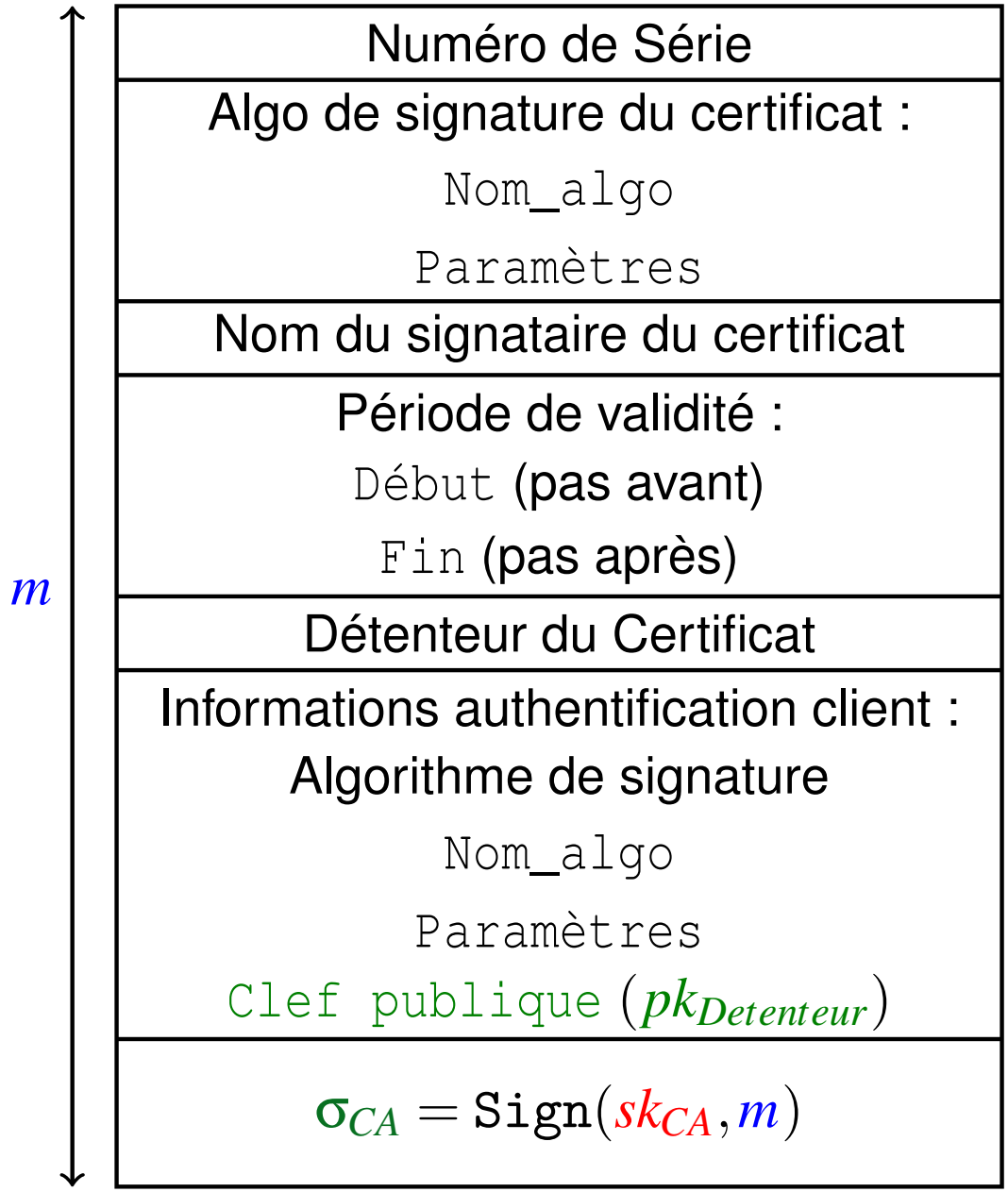
Ensemble de composants matériels, logiciels et de procédures déstinés à la gestion des clefs publiques d'un système informatique.

PROPRIÉTÉ

- *Confidentialité : chaque message destiné à un utilisateur spécifique ne sera lisible que par celui-ci.*
- *Authentification : identité des utilisateurs garantie*
- *intégrité : non-modification des messages (ou détection si c'est le cas)*
- *non-répudiation : Comme on a lié la clef publique à l'identification des individus, les utilisateurs ne peuvent renier leurs actions*

Contradiction entre Anonymat et les propriétés ci-dessus

CERTIFICATS X.509



L'attaque de l'homme du milieu
Un premier protocole
Identifiants

Autorités de Confiance
Le cas du Web
PKI
Certificats X.509

Notion de Confiance

Chaînes de confiances

- Il y a plusieurs autorités de certification
- On peut vouloir **déléguer** la confiance
- **Idée :** que l'autorité AC_1 signe et valide la clef publique de AC_2 (et réciproquement)
- Chaque utilisateur validé par AC_1 peut alors faire confiance aux utilisateurs validés par AC_2 (et réciproquement)
- ✍ Montrer comment faire

Révocation et rupture de confiance

- **Discussion :** qu'est-ce qu'une autorité de confiance pourrait vouloir faire ? Donner plusieurs contextes possibles
- En pratique, les navigateurs Web (Mozilla, Chrome, Safari) font un travail permanent de détection de problèmes
- En Europe : le règlement eIDAS : exigences de sécurité, interopérabilité et cadre juridique
- Nouveau règlement en 2024 : obligation des états membres de délivrer des portefeuilles d'identité numérique
- Stocker des données d'identification, justificatifs et attributs

Problématique : Comment concilier cela un respect d'anonymat et/ou de protection de la vie privée ? Face à qui ? Pourquoi ?