IGC et HSM dans une PME

Maxence MOHR – Ingénieur IT
Responsable de la mise en œuvre d'une PKI chez KeeeX

Avant propos

- Max
- Ancien élève de **Polytech Marseille**
- Dev, sysadmin, crypto-curieux, *bidouilleur*

- Ingénieur chez **KeeeX**
- Secrétaire *et pilier de bar* de l'asso **Hack In Provence**

KeeeX

Protection, preuves et sémantique auto-portées sur tout type de fichier et applications autour du process

- Intégrité,
- Signature numérique,
- Horodatage selon la RFC3161,
- Preuve d'existence Bitcoin/Ethereum,
- Mais aussi : Tags, versionnage, titre, description...

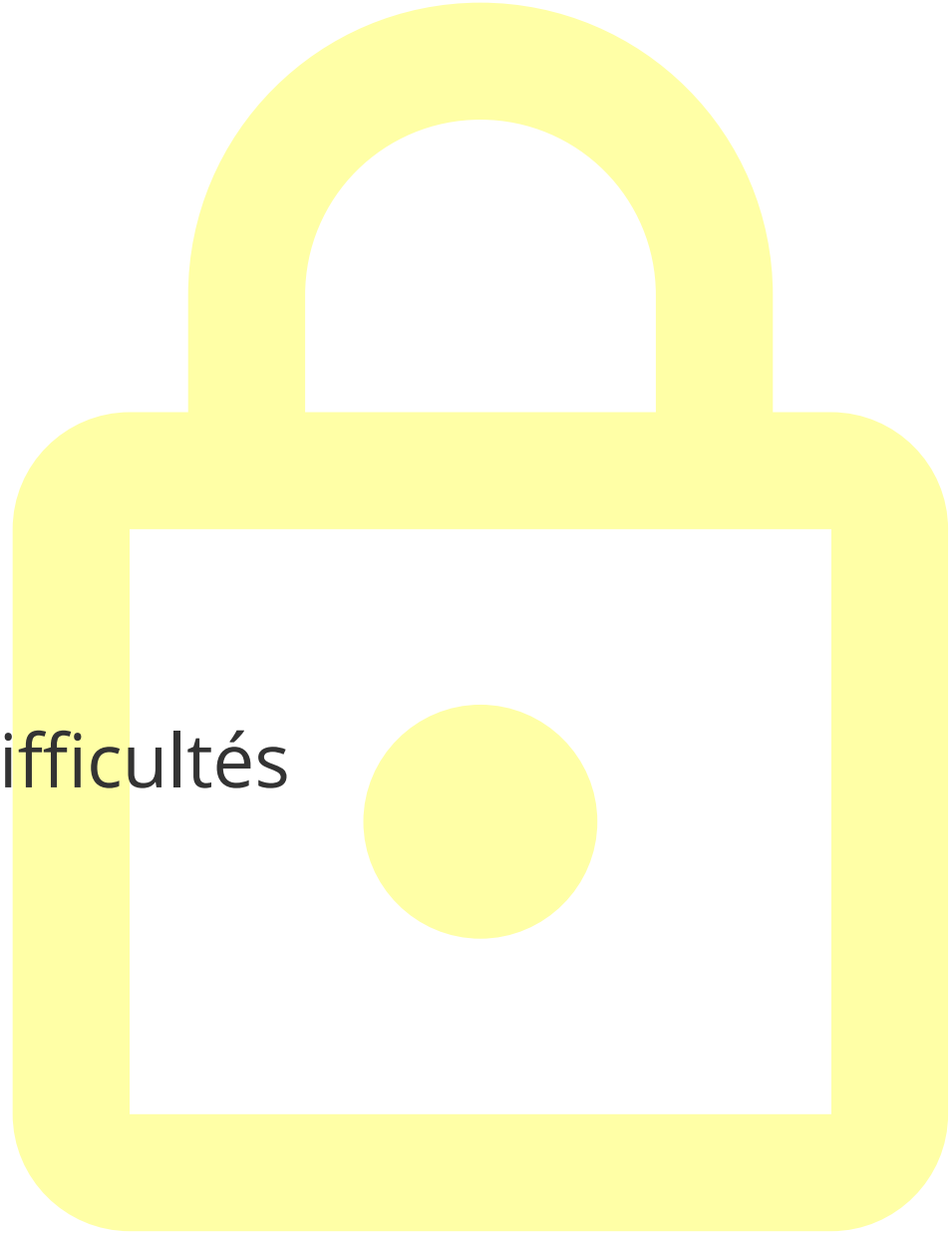
Avant propos

- *<SPOILER>*
  Une surprise à la fin, pour les curieux et les *bidouilleurs*… :)
  </SPOILER>

- On dit chiffrer, pas crypter → chiffrer.info

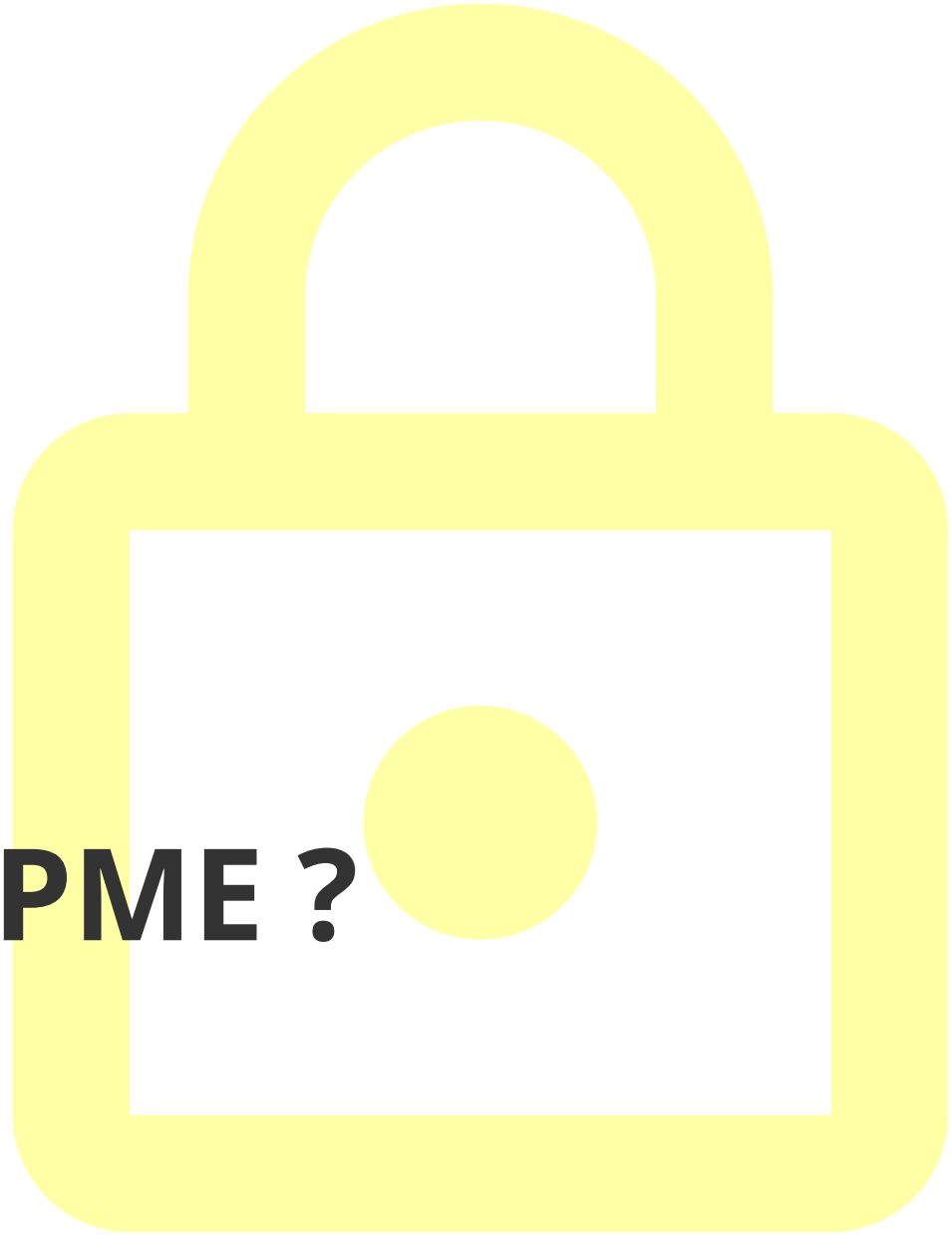
Présentation

- IGC, PKI, HSM, PME ?
- Quels besoins ?
- Comment ?
- Utilisation d’un HSM et difficultés



IGC, PKI, HSM, PME ?

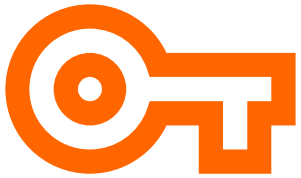
Trop d’abréviations dans ce titre.



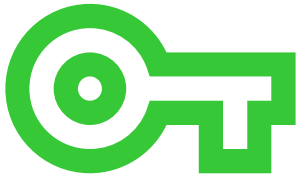
IGC, PKI, HSM, PME ?

- **PME :** on commence facile ;-)
- **HSM : Module de Sécurité Matériel**
  Module autonome sécurisé de **génération**, **calcul**, **stockage** et **protection** de clés cryptographiques.
  Formats multiples : carte PCI, clé USB, carte à puce. Protocole de com avec appli : **PKCS#11**
- **PKI/IGC : Infrastructure de Gestion de Clés**

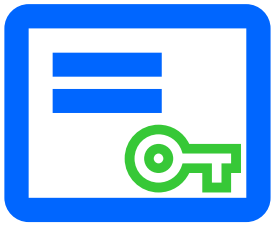
IGC : Infra de Gestion de Clés



Clé privée

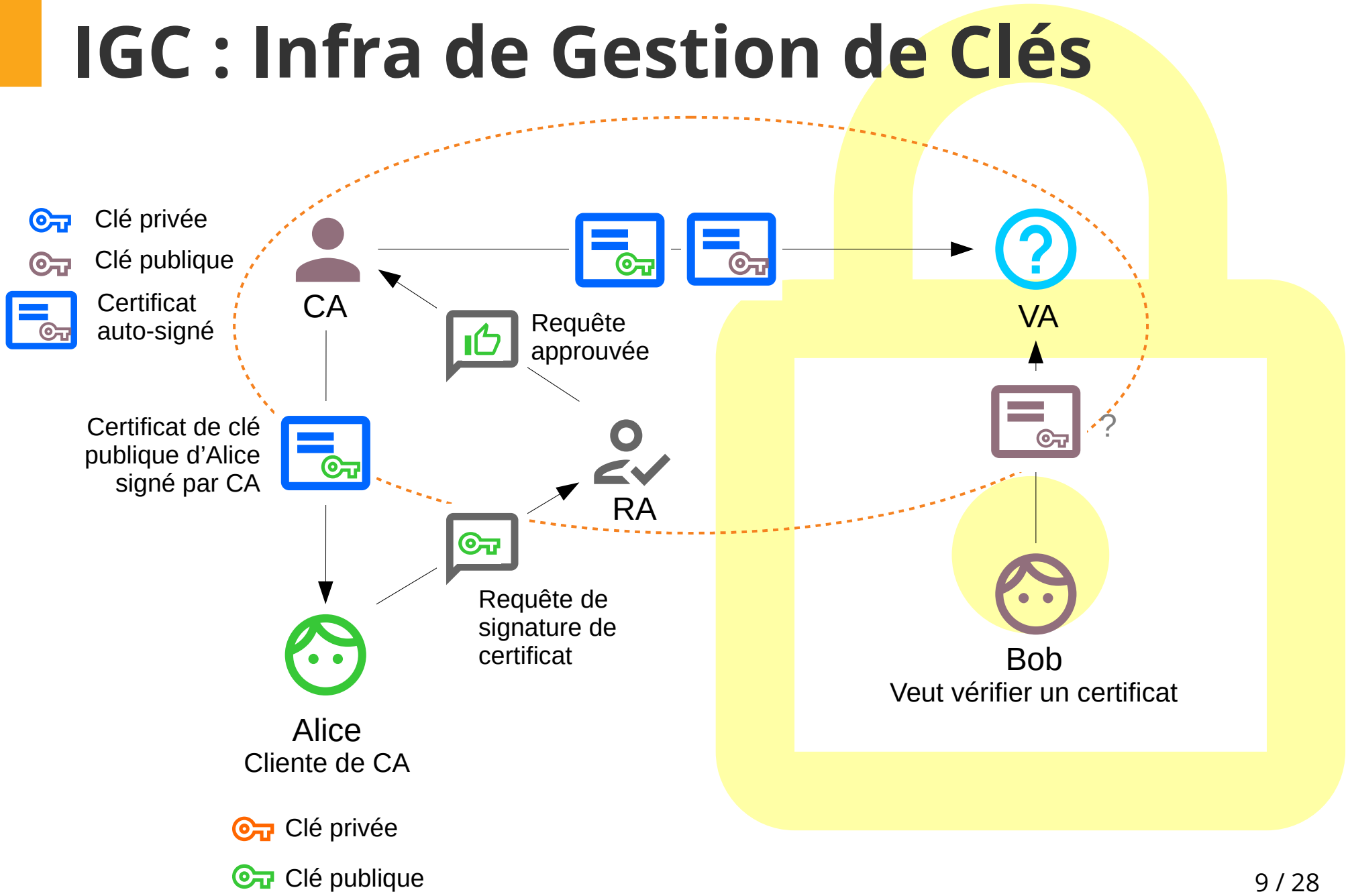


Clé publique

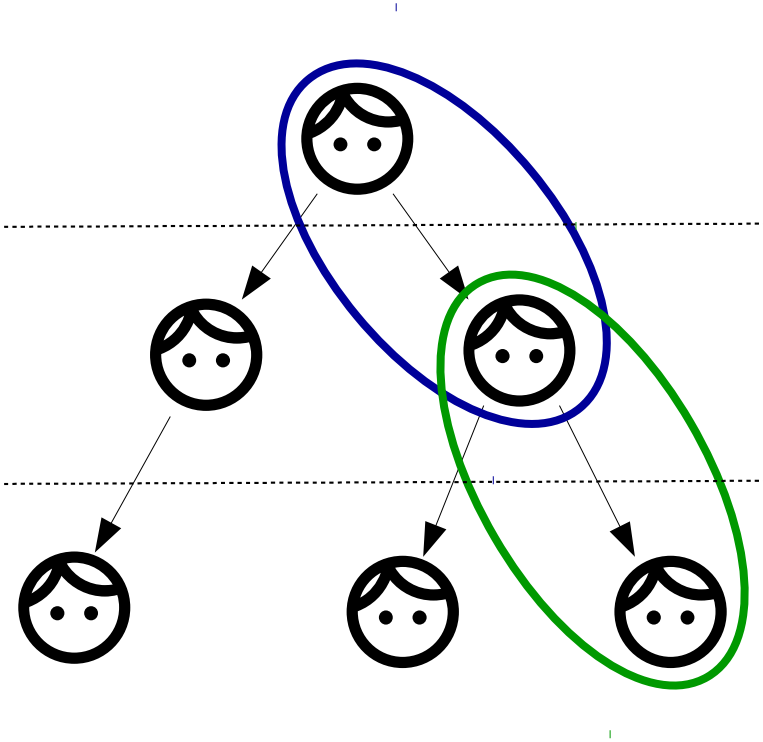


Certificat de clé publique

IGC : Infra de Gestion de Clés



IGC : Infra de Gestion de Clés



CA (Autorité de certification)

Sub CA (Sous-autorité de certification)

End Entity (Entité finale)

IGC et HSM dans une PME

Quels besoins ?

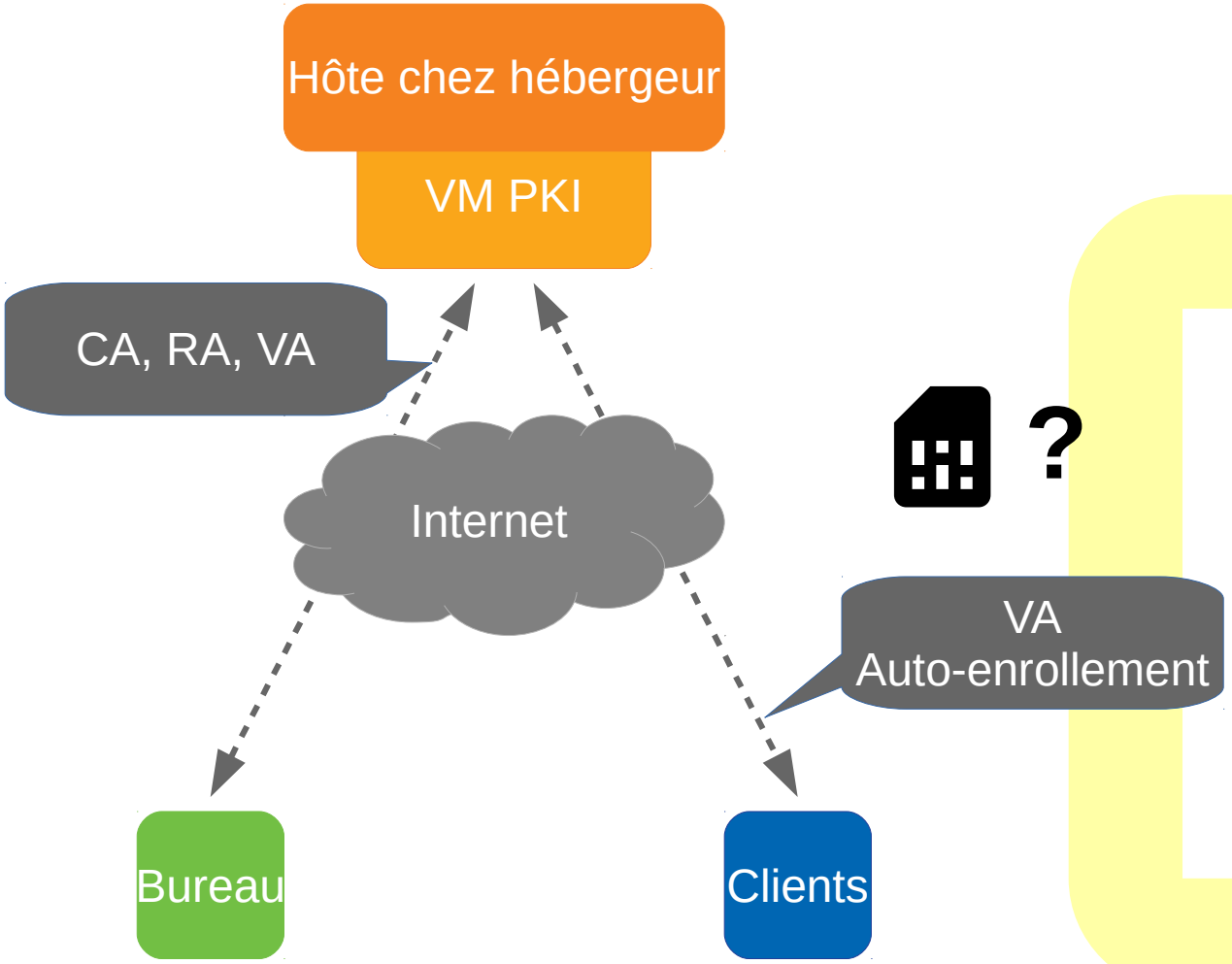
Quels besoins ?

- **Signature individuelle ou '*cachet serveur*' de fichiers** via notre technologie et nos applis
- **HTTPS/TLS** serveur et authentification client sur serveurs de préprod/tests/production
- **Authentification sur OpenVPN** (clients, partenaires, employés)
- **Horodatage RFC3161**
- **Centralisation de logs** via RSyslogD over TLS

Quels besoins ?

- **Root CAs et chaînes disponibles publiquement** pour clients/testeurs
- **Gestion d'entités finales simple (RA simple)** Bonus si possibilité d'auto-enrollement
- **Auto-génération des informations de révocation** (CRL et OCSP)
- **Stockage** de clés cryptographiques **sécurisé**
- Environnement **auto-hébergé**
- **Journal d'audit**

Quels besoins ?



IGC et HSM dans une PME

Comment ?

Comment ?

- **OpenSSL :** Brique cryptographique complète
- Maintenu par The OpenSSL Project
- **FOSS**
- **Support de HSM (au module PKCS#11 près)**
- **Auto-hébergeable, mais interfaces et programme à développer**
- Support de Sous-CA, CRL, OCSP, **à condition de développer dessus**

Non praticable à court ou moyen terme

Comment ?

EJBCA PKI by PrimeKey

- **EJBCA :** Entreprise JavaBeans Certificate Authority
- Développé par PrimeKey, entreprise suédoise
- **Auto-hébergeable**
- **FOSS** pour la version Community
- Interface **publique**, Administration **CA**, Administration **RA**
- **Support de HSM, au module PKCS#11 près**
- **Support de Sous-CA, CRL, OCSP, audit**

IGC et HSM dans une PME

Comment ?

EJBCA
PKI by PrimeKey

Enroll
- Create Browser Certificate
- Create Certificate from CSR
- Create Keystore
- Create CV certificate

Register
- Request Registration

Retrieve
- Fetch CA Certificates
- Fetch CA CRLs
- List User's Certificates
- Fetch User's Latest Certificate

Inspect
- Inspect certificate/CSR
- Check Certificate Status

Miscellaneous
- Administration

Welcome to the public EJBCA pages

Enroll

- Create Browser Certificate - Install a certificate in your web browser. This certificate may be export
- Create Certificate from CSR - Send a PKCS#10 certificate request generated by your server, and r
- Create Keystore - Create a server generated keystore in PEM, PKCS#12 or JKS format and save t
- Create CV Certificate - Used for EU EAC ePassport PKI. Send a CVC certificate request generated certificates, CV certificates are completely different.

Retrieve

- Fetch CA Certificates - Browse and download CA certificates.
- Fetch CA CRLs - Download Certificate Revocation Lists.
- Fetch User's Latest Certificate - Download the last issued certificate for a user for whom you know

Inspect

- Inspect certificate/CSR - Inspect a dump of a CSR or a certificate. This gives an output of a CVC o

Miscellaneous

- List User's Certificates - List certificates for a user for whom you know the certificate Distinguished
- Check Certificate Status - Check revocation status for a certificate where you know the Issuer Dist
- Administration - Go to the EJBCA Admin-GUI. Requires client certificate authentication

IGC et HSM dans une PME

Utilisation d’un HSM et difficultés

Utilisation d’un HSM et difficultés

Thales USB nShield Edge HSM - Developer Edition (No FIPS validation) $2,243.00

SafeNet Network HSM - 1700, FIPS 140-2 L2, PW-Auth & Key Export $17,400.00

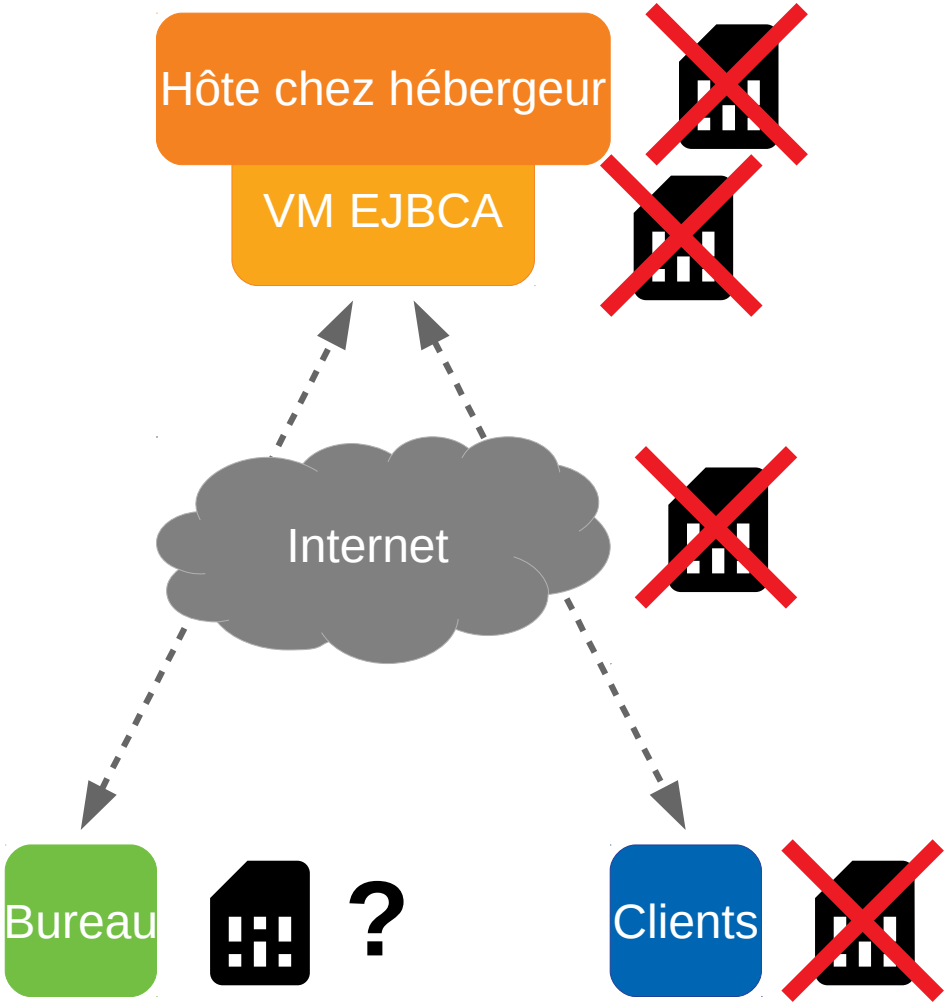
*Attention : prix trouvés sur un **site ‘louche’**, mais seuls prix publiquement disponibles...*

Conclusion raisonnable :
Prix > 1 000 €

Utilisation d'un HSM et difficultés

- Prix : **60€ TTC + Port**, **fabriqué à Berlin**
- Connectique USB
- 31 clés **ECC GF(p) 256 bits**
- 20 clés **RSA 2048 bits**
- Basé sur **SmartCard-HSM**, standard FOSS connu
- PIN, SOPIN
- Schéma n parmi m, exports et imports chiffrés

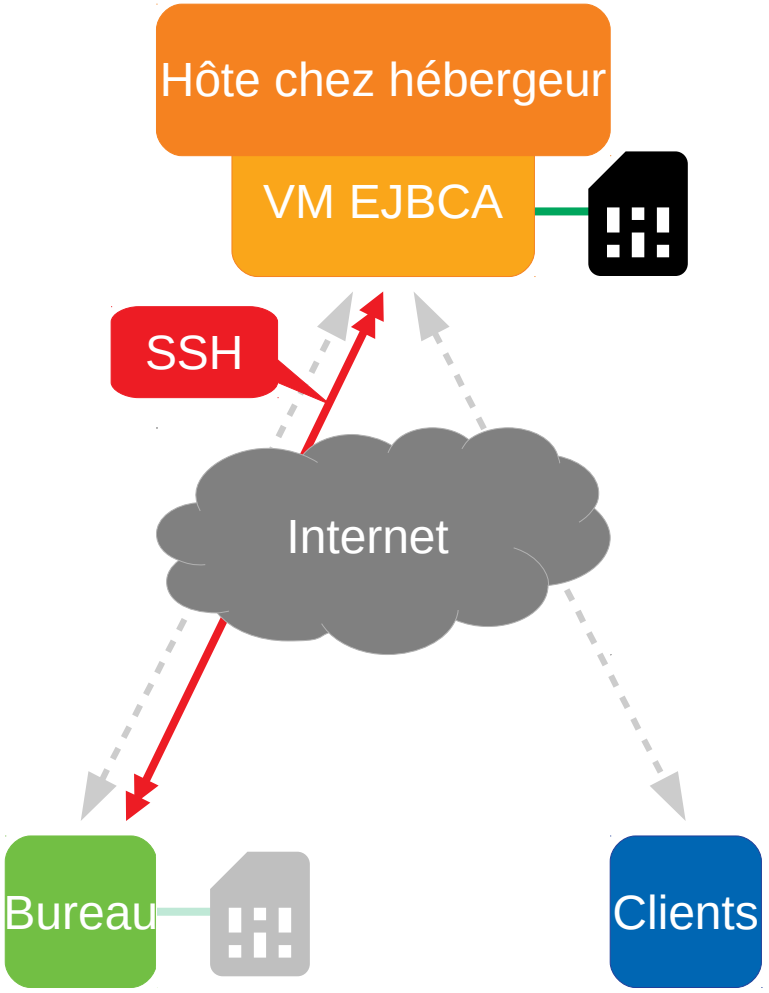
Utilisation d'un HSM et difficultés



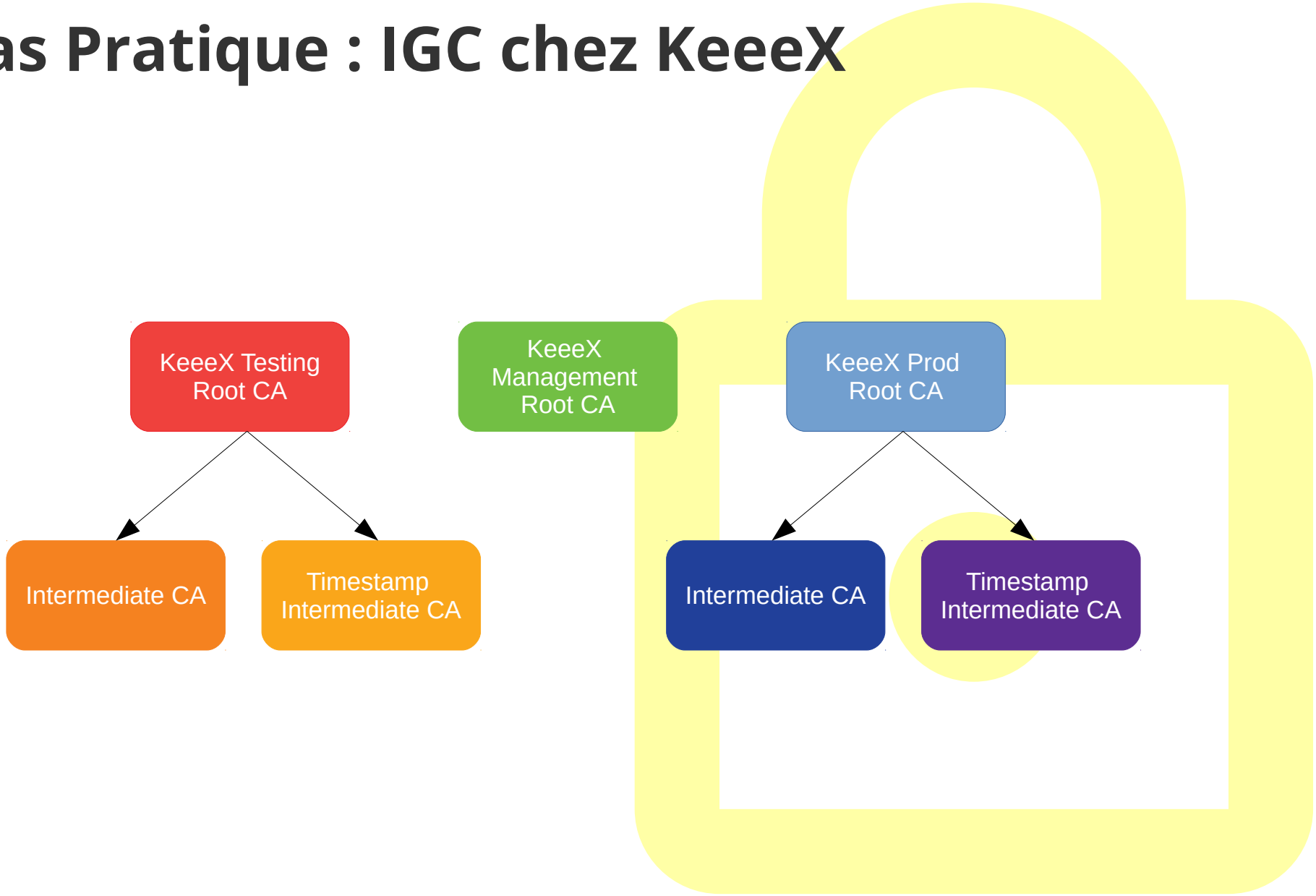
Utilisation d'un HSM et difficultés

- p11-kit
  Librairie standard de PKCS#11…
- … mais bien plus : **partage de HSM** d'un système à l'autre !
  → *Forwarding* de socket UNIX
- **Sécurisé à travers d'une connexion SSH**
- Reste à compiler l'outil et ses dépendances…

Utilisation d'un HSM et difficultés



Cas Pratique : IGC chez KeeeX



IGC et HSM dans une PME

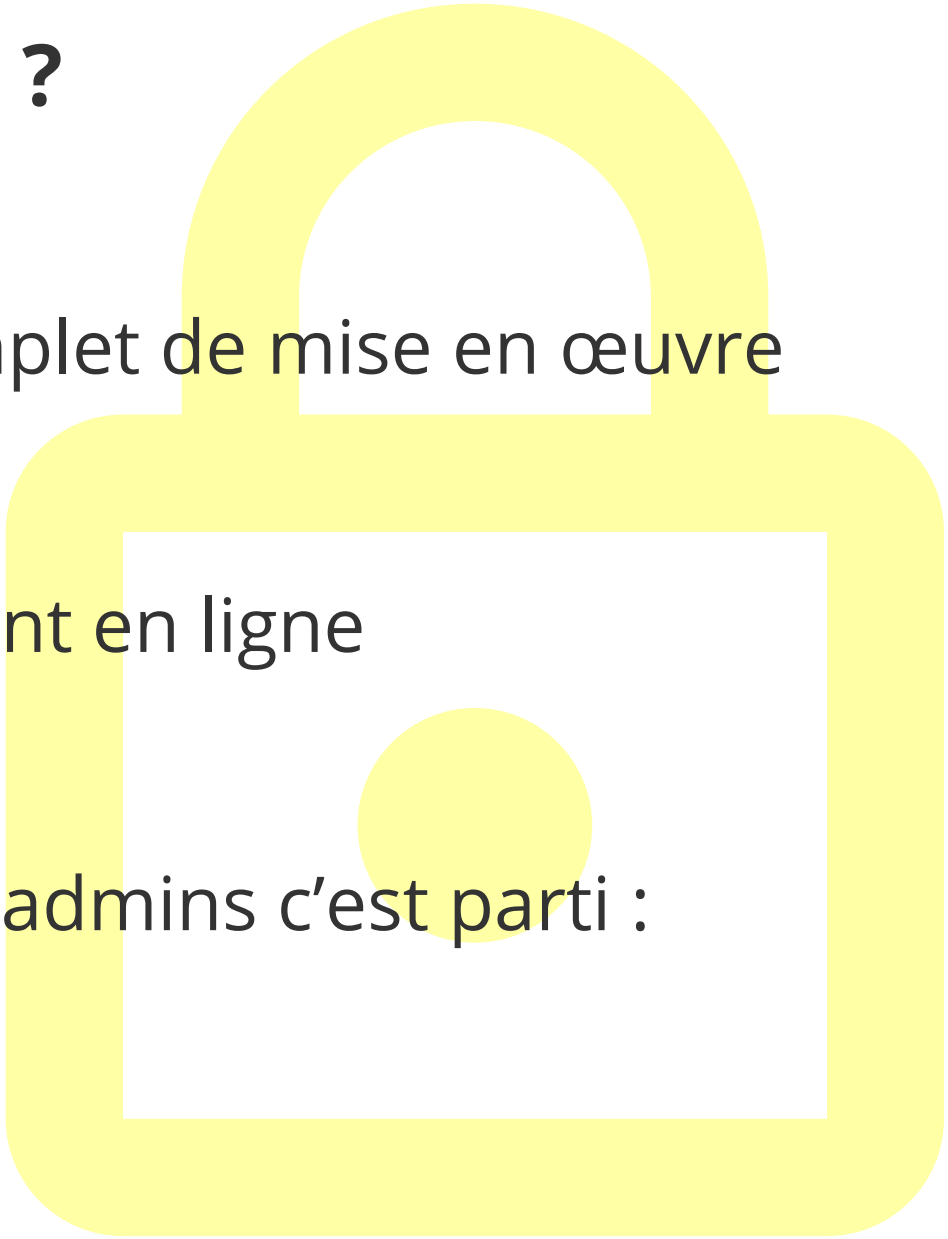
Remerciements et conclusion

Hé, et la surprise alors ?

“ Je vois bien qu’il reste quelque chose, c’est pas la dernière diapo.”

– Cap’tain Obvious

Hé, et la surprise alors ?



- Tutoriel ligne à ligne complet de mise en œuvre
- Disponible dès maintenant en ligne
- Curieux, bidouilleurs, sysadmins c'est parti :

  → **fladnag.net**

  (Gandalf à l'envers #nerd)