PKI Concepts

Public Key Infrastructure

Votre instructeur

Thierry DECKER
mail@thierry-decker.com

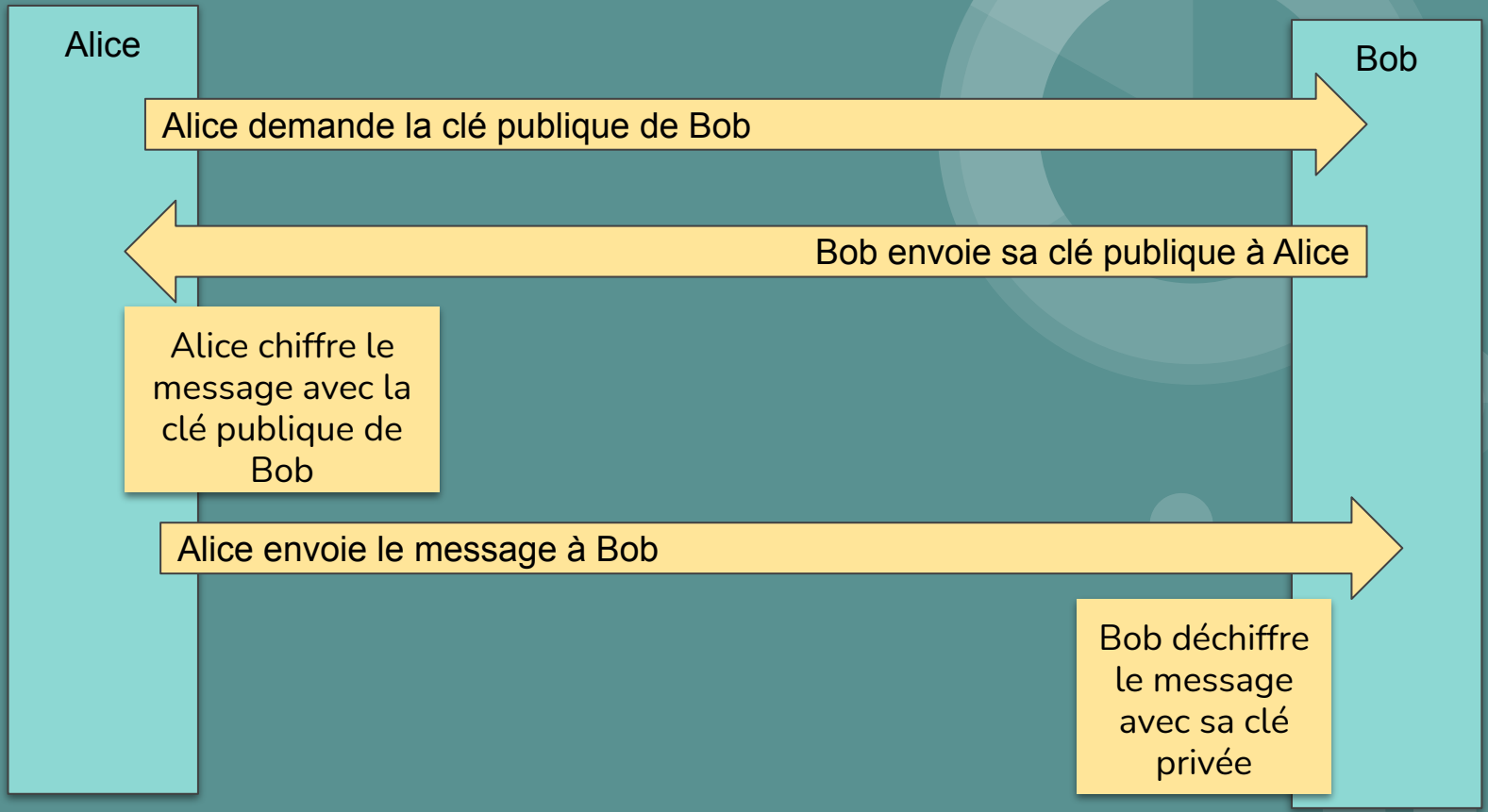
PKI Concepts Sommaire

- Survol de la PKI
- La paire clé publique et clé privée
- Certificats numériques
- Autorités de certification (CA)
- Comment la PKI fonctionne
- Autorités d'enregistrement (RA)
- Listes de révocation de certificats (CRL)
- Agent de récupération : Que faire en cas de perte de clé ?
- Séquestre des clés

PKI Concepts Survol de la PKI

- Utilise un système de chiffrement à deux clés (asymétrique)
- Un framework, pas une technologie
- Infrastructure pouvant fonctionner sur de multiples systèmes
- Fournit les services d'authentification et de confidentialité
    - Authentification : Confirme la propriété des clés en utilisant des certificats numériques
    - Confidentialité : Chiffre les données transmises

PKI Concepts La paire clé publique et clé privée

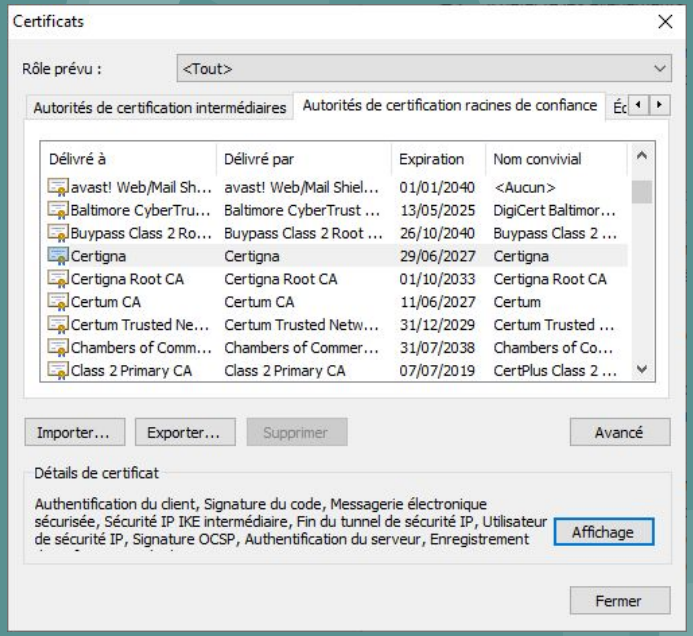


PKI Concepts La paire clé publique et clé privée

- Système de chiffrement garantissant la confidentialité
- Mais…
- Comment être sûr de l'identité de l'émetteur ?
- Quelqu'un pourrait prétendre être Alice en utilisant une autre paire de clés
- Envoyer cette autre publique et déchiffrer les messages avec cette autre clé privée
- Les certificats numériques permettent de résoudre ce problème

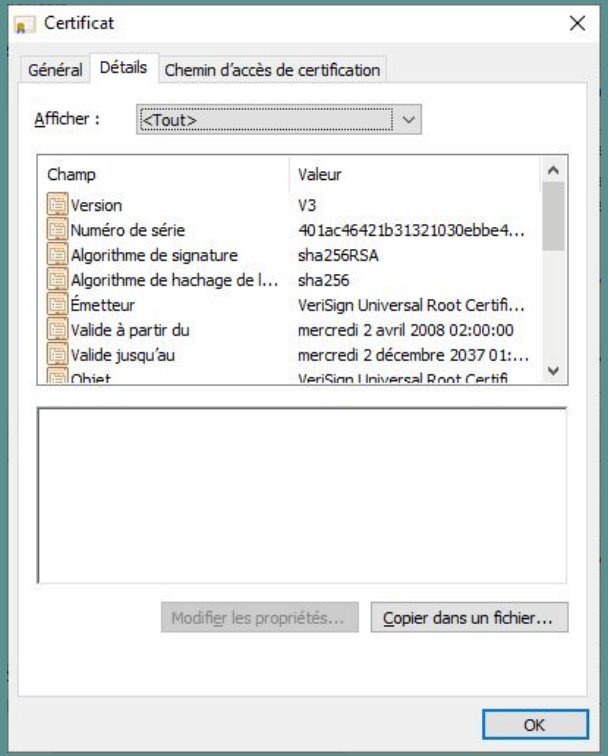
PKI Concepts Certificats numériques

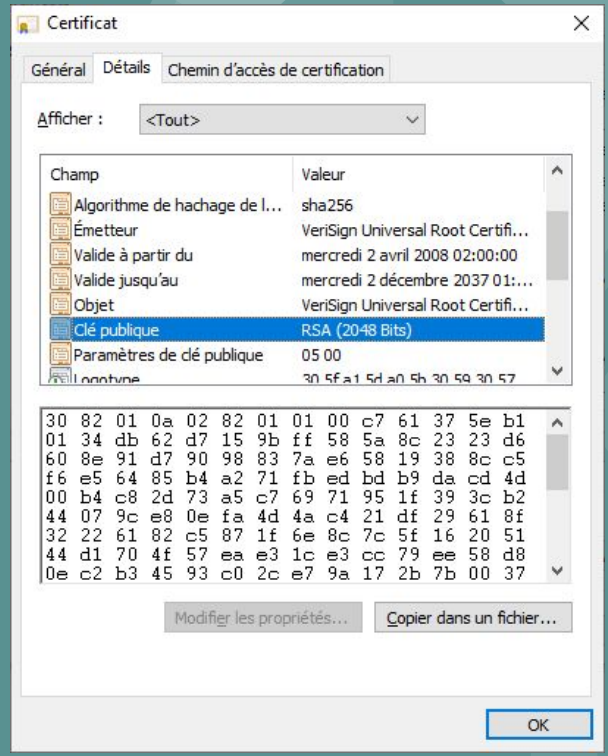
- Aident à résoudre le problème de l'authentification
- Associent une clé publique à un individu ou une organisation
- Sont publiés par une autorité de certification (CA)



cethun
in innovation we trust

PKI Concepts Certificats numériques



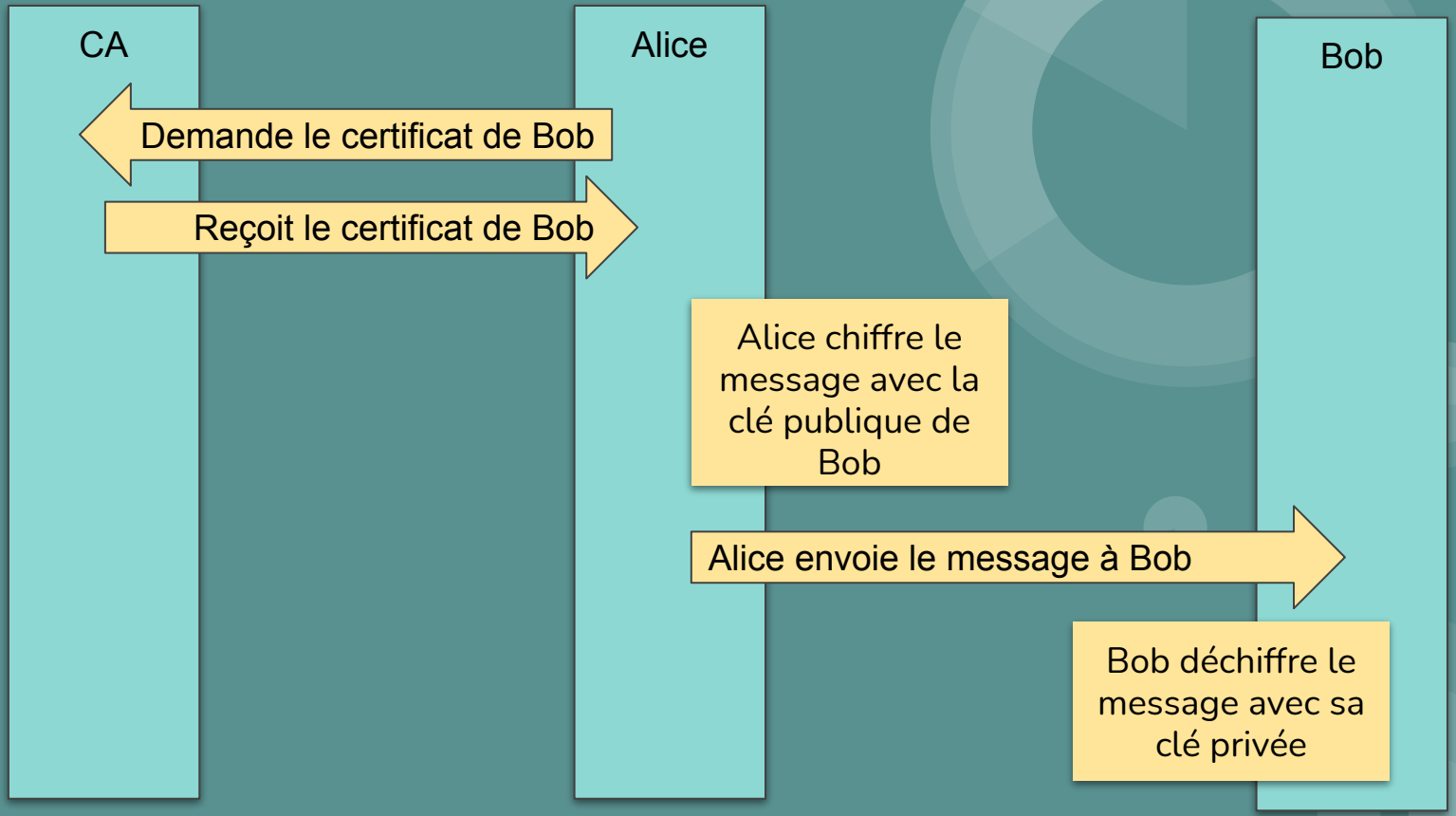


cethun
in innovation we trust

PKI Concepts Autorité de certification (CA)

- Serveur responsable de :
  - la publication des clés,
  - la révocation et
  - la distribution de certificats numériques ou de la mise à disposition de ces certificats
- Souvent une organisation tierce, digne de confiance
  - DigiCert
  - VeriSign
  - GlobalSign
  - etc.
  - Les organisations peuvent avoir une autorité de certification en interne
- Stockent les clés publiques dans un répertoire accessible à quiconque souhaite vérifier le certificat numérique

PKI Concepts La paire clé publique et clé privée



PKI Concepts Autorité d'enregistrement (RA)

- Entité avec laquelle vous interagissez
- Agit comme un "Secrétaire" ou un "Assistant administratif"
- Soulage la charge de travail de l'autorité de certification (CA)
- Vous fournissez à la RA vos informations (et paiement...)
- Vérifie votre identité avant de confirmer à la CA qu'elle peut délivrer un certificat numérique
- Ne signe pas le certificat numérique
- Une clé publique peut être fournie si elle existe déjà (plus sûr)

PKI Concepts Listes de certificats révoqués (CRL)

- Les certificats doivent êtres gérés..., valides et à jour
- La CA maintient ces listes de révocation
- La CRL est publiée régulièrement
- Pourquoi un certificat serait-il dans cette liste :
  - Expiration
  - Révocation (permanente)
    - Clé privée compromise
    - Raisons RH
    - L'organisation change de nom, d'adresse, de nom de domaine
    - Toute raison intervenant avant l'expiration du certificat
  - Suspension (Certification Hold)
- A la demande du propriétaire ou administrateur du certificat

PKI Concepts Agent de récupération (Recovery Agent)

- Que se passe-t-il si une clé est perdue ?
- L'agent de récupération est une personne physique
- A accès au serveur de récupération
- Généralement interne à l'organisation
- Extrêmement sécurisé
- La récupération peut faire intervenir plus d'un agent (Ils doivent être tous présent lors de la récupération)
- Information pour la récupération (KRI)
  - Preuve que la demande récupération provient d'un agent autorisé
  - Nom du propriétaire, date de création
  - CA serveur publicateur

PKI Concepts Séquestre de clé (Key Escrow)

- Comme les agents de récupération, les organismes de séquestre possèdent une ou plusieures copies des clés privées (Key Escrow Agency, Key Archival system)
- Les clés peuvent êtres stockées en plusieures parties dans des bases de données distinctes
- Les clés ne sont accessibles aux agents de récupération
- Utilisables par les forces de l'ordre, avec un garant (généralement la justice en France)

PKI Concepts - Q&A

Merci de votre attention !