

Formation PKI d'entreprise



date de la formation :

22/01/2019



lieu de la formation : Rennes

Sommaire

partie 1 : Introduction

partie 2 : Rappels de Cryptologie

partie 3 : Certificats numériques

partie 4 : PKI / IGC

partie 5 : Bonnes pratiques IGC



© OAB

PKI

partie 1 : Introduction

partie 2 : Rappels de Cryptologie



partie 3 : Certificats numériques

partie 4 : PKI / IGC

partie 5 : Bonnes pratiques IGC



Objectifs

- Comprendre les raisons et le cheminement qui ont conduit à l'émergence des PKI
- Comprendre qu'est-ce qu'une PKI peut apporter dans une entreprise
- Comprendre les mécanismes mis en œuvre dans la mise en place et autour d'une PKI
- Comprendre les principes fonctionnels, techniques et organisationnels d'une PKI
- Comprendre pourquoi  <https://> est mieux que  ~~<https://>~~







Confiance & sécurité

- La confiance est une question de sécurité



Définitions

- Sécurité : mesures permettant d'assurer la protection des biens : données / valeurs.
 - On ne protège pas nos biens pour des besoins de sécurité mais on applique des mesures de sécurité pour protéger nos biens
- Menace : Action, événement ou entité pouvant compromettre la sécurité de ce qui est protégé
- Confiance : sentiment de sécurité ou de sureté qu'a une personne vis-à-vis quelqu'un ou de quelque chose
- Garantie : assurance ou gage de quelque chose

PKI : Base de la confiance électronique

- La sécurité est un vecteur de **confiance**.
- Si la sécurité dans un élément d'une infrastructure est compromise, toute la **confiance** envers l'infrastructure l'est.
- Si la sécurité est un vecteur de confiance la réciproque n'est pas vraie, la confiance nécessite des **garanties**

PKI : Base de la confiance électronique

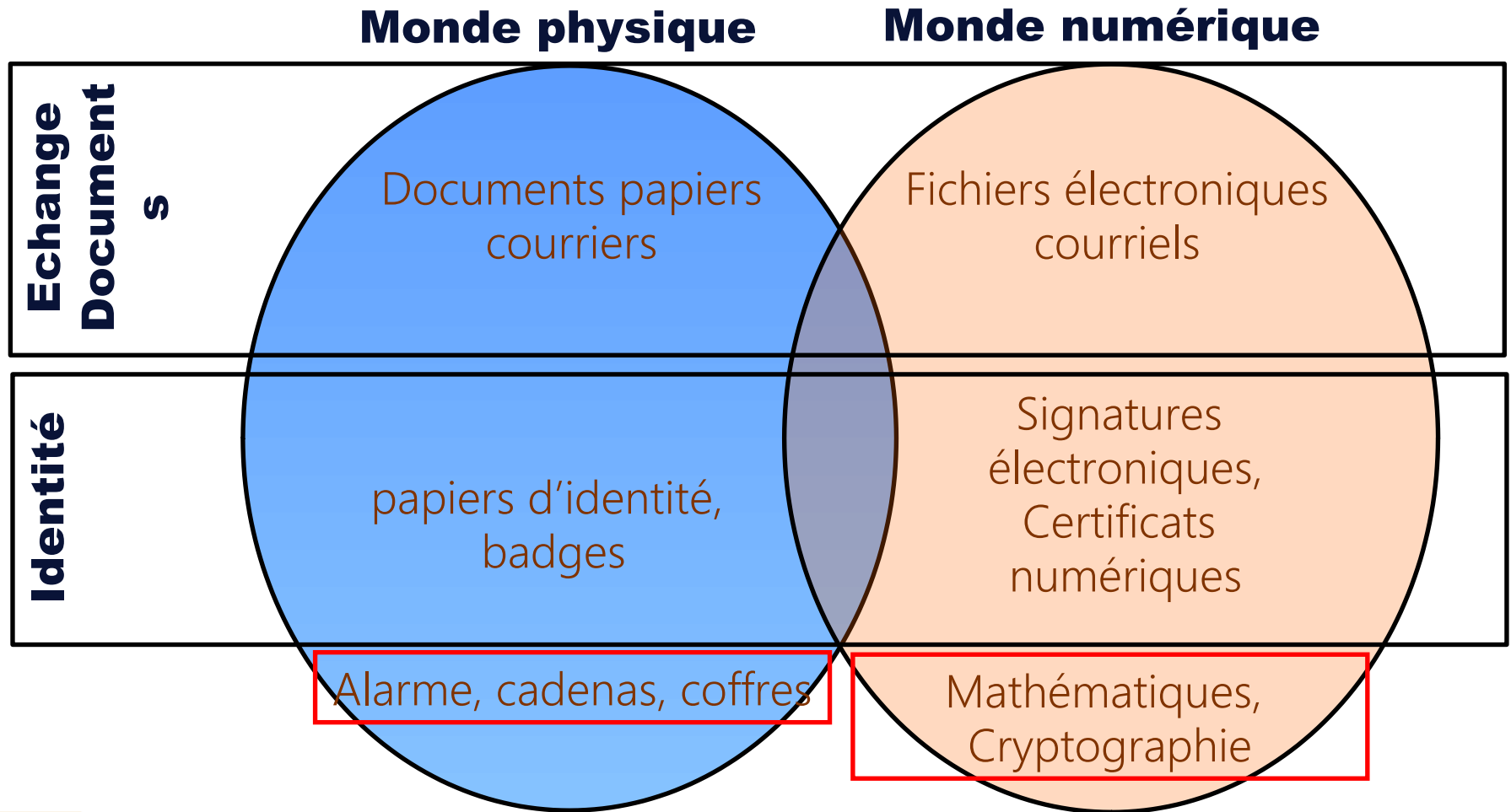
- L'objectif d'une PKI est d'établir de solides **garanties** électroniques afin d'établir la confiance
- Ces garanties doivent être d'un niveau équivalent ou supérieur à celles présentes dans le monde physique :
 - Authentification : Carte Nationale d'Identité
 - Confidentialité & Intégrité de l'information : coffre fort
 - Non répudiation : scellés ou signatures
- Une PKI permet d'instaurer un domaine de confiance entre les utilisateurs/systèmes

PKI : Base de la confiance électronique

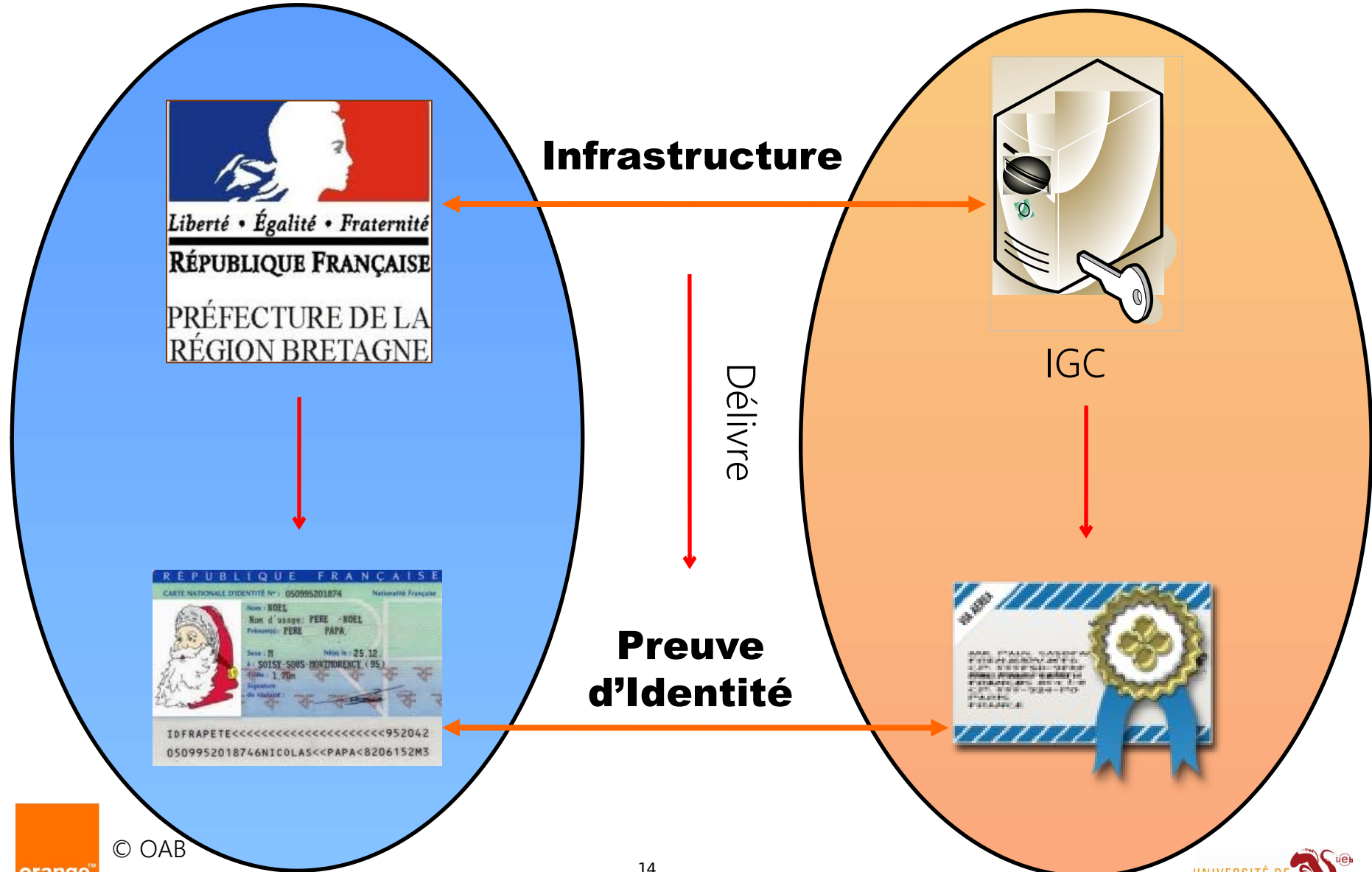
- La présence des PKI dans le monde **électronique** est requise car :
 - Les échanges électroniques se sont multipliés avec des interlocuteurs distants et inconnus
 - Les procédures électroniques et la **dématérialisation** prennent l'ascendant sur les échanges papier :
 - administration électronique (impôts, état civil)
 - simplification et accélération des démarches
 - diminution des coûts
 - De plus en plus d'**objets** sont reliés à Internet et communiquent entre eux (Internet Of Things)

- Les utilisateurs veulent avoir a minima le même niveau de sécurité dans le monde électronique que dans le monde physique

Analogie physique / numérique



Analogie physique / numérique



partie 1 : Introduction

partie 2 : Rappels de Cryptologie

partie 3 : Certificats numériques

partie 4 : PKI / IGC

partie 5 : Bonnes pratiques IGC



Qu'est-ce que la cryptologie ?

CRYPTOLOGIE

E

II

CRYPTOGRAPHIE

+

CRYPTANALYSE

Cryptographie

=

protection d'un système

Cryptanalyse

=

attaque d'un système

La cryptographie, dans quel but ?

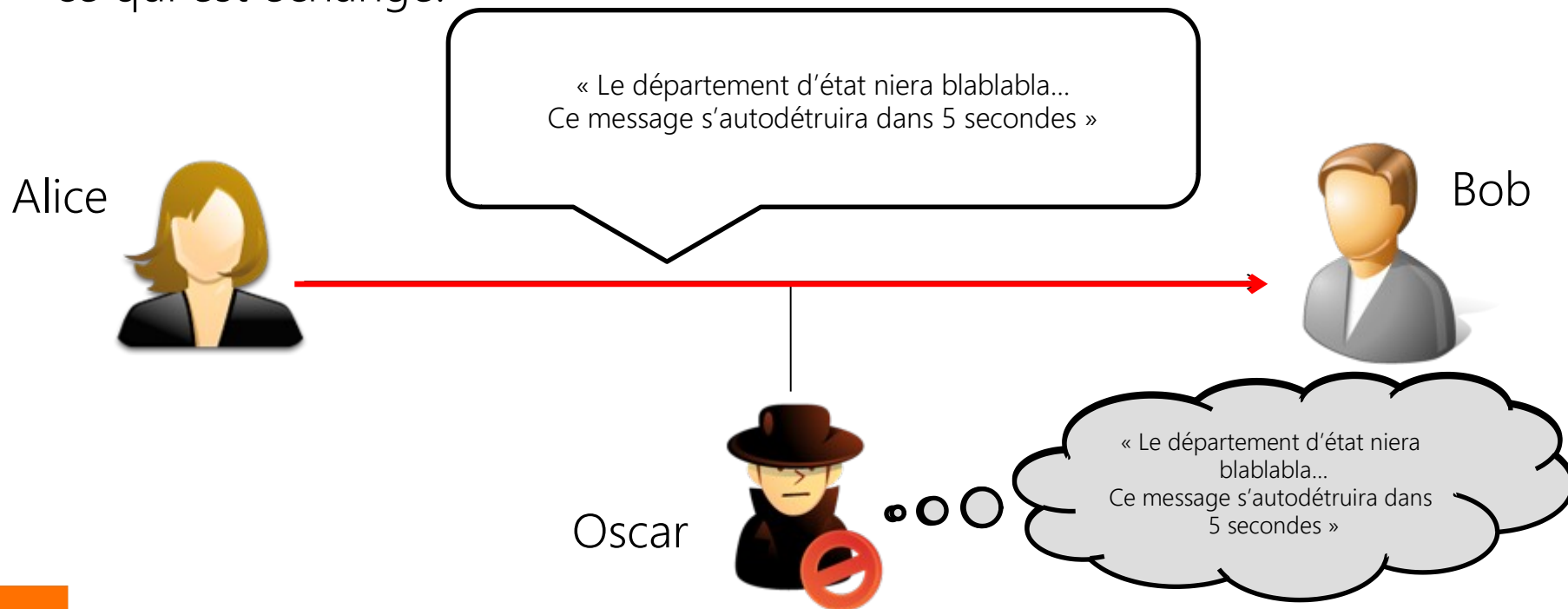
- La cryptologie permet d'assurer les fonctions de sécurité suivantes :
 - Confidentialité
 - Intégrité
 - Authentification
 - Non répudiation

- La cryptologie ne permet pas d'assurer **directement** les fonctions de sécurité suivantes :
 - Disponibilité
 - Contrôles des accès
 - Contrôles des flux

La cryptographie, dans quel but ?

Confidentialité des données :

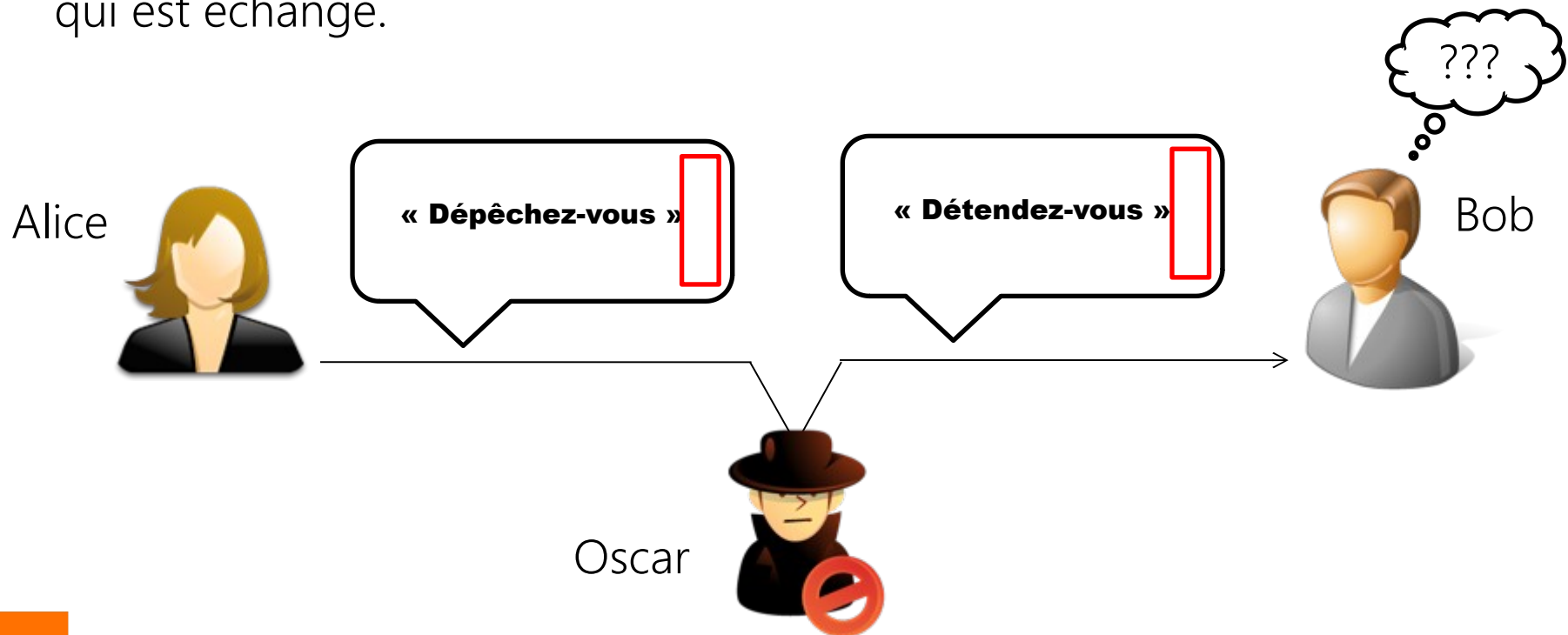
Permettre à Alice et Bob de communiquer au travers d'un canal peu sûr de telle sorte qu'un opposant, Oscar, ne puisse pas **comprendre** ce qui est échangé.



La cryptographie, dans quel but ?

Intégrité des données :

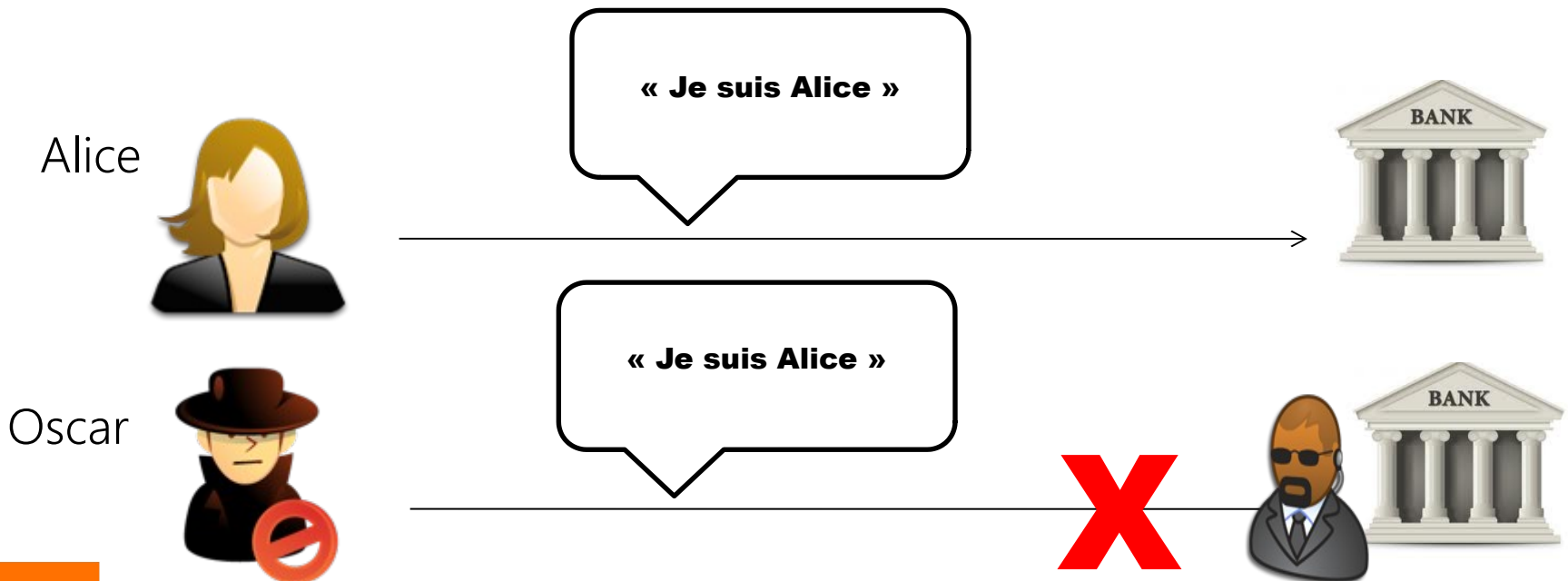
Permettre à Alice et Bob de communiquer au travers d'un canal peu sûr de telle sorte qu'un opposant, Oscar, ne puisse pas **modifier** ce qui est échangé.



La cryptographie, dans quel but ?

Authentification :

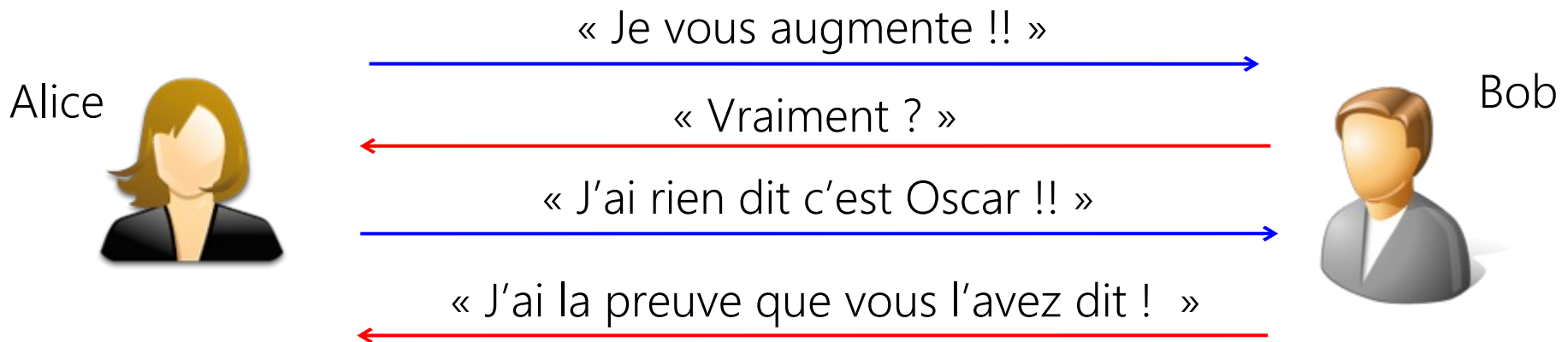
Permettre à Alice de s'authentifier auprès d'une entité au travers d'un canal peu sûr de telle sorte qu'un opposant, Oscar, ne puisse pas **se faire passer** pour elle.



La cryptographie, dans quel but ?

Non répudiation :

Permettre à Alice, lorsqu'elle communique avec Bob, de **prouver** qu'il a bien reçu ses messages et inversement à Bob de prouver qu'elle les a envoyés.



La cryptographie, les composantes

La cryptographie pour assurer les fonctions de sécurité utilise :

- Des **algorithmes** cryptographiques :
 - procédures de calcul qui permet de réaliser des opérations sur un message en utilisant une ou plusieurs clés.
- Des **clés** cryptographiques :
 - paramètre utilisé en entrée d'une opération cryptographique, ce paramètre peut se présenter sous la forme d'un mot, d'une procédure, d'une chaîne de bits...

Principe de Kerckhoff

**LA SECURITE DU PROTOCOLE REPOSE
DANS LE SECRET DES CLES ET NON PAS
CELUI DES ALGORITHMES**

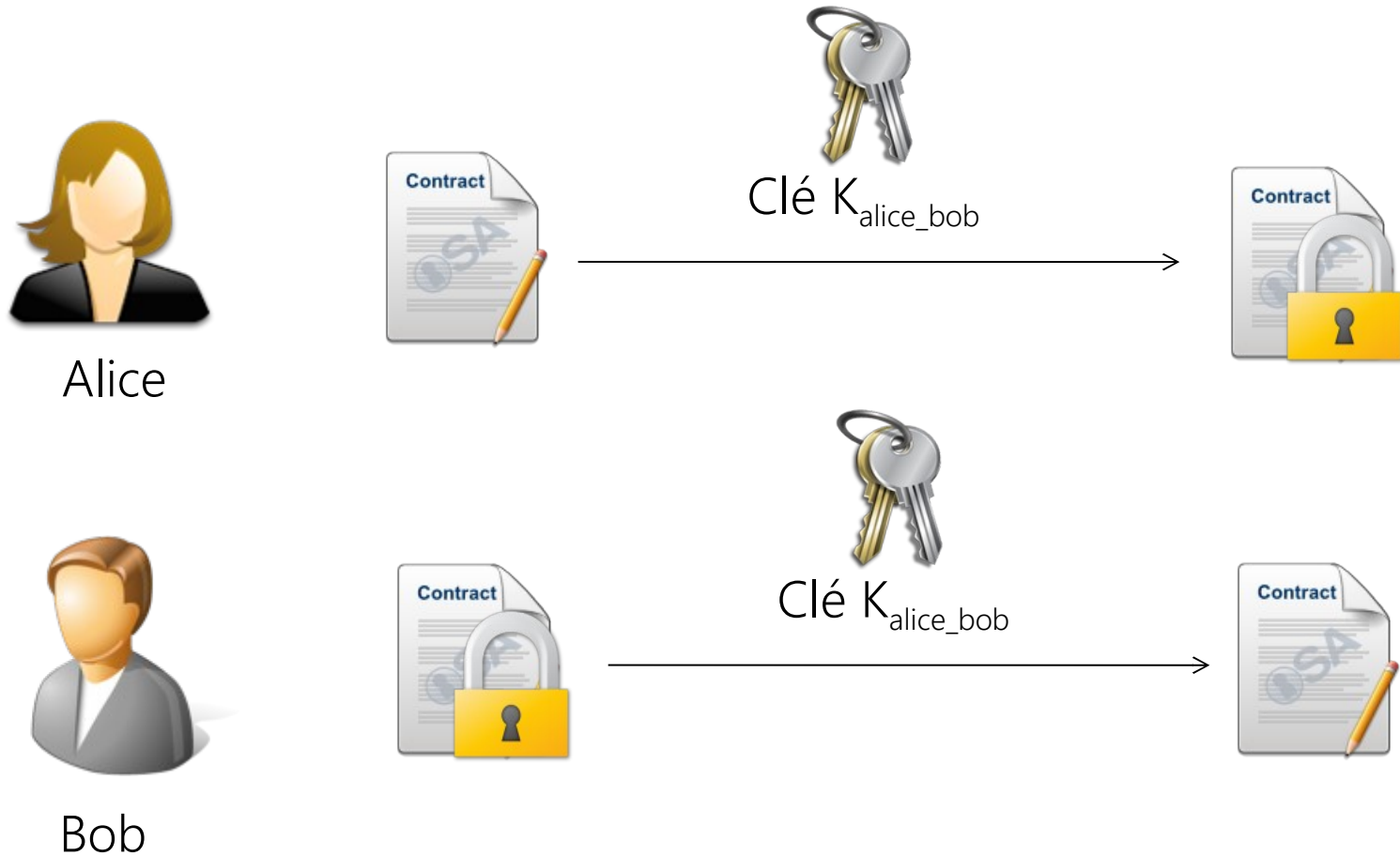
*« la sécurité d'un système de chiffrement ne doit pas reposer sur le secret de sa procédure, mais uniquement sur le secret d'un paramètre utilisé à chacune de ses mises en œuvre, paramètre appelé **clé** »*

Deux catégories de cryptographie

- Cryptographie symétrique (clé secrète)
 - une clé commune pour chiffrer / déchiffrer
 - la clé est choisie aléatoirement
 - calculs rapides
 - problématique d'échange de la clé
 - principalement utiliser pour la confidentialité
- Cryptographie asymétrique (clé publique)
 - deux clés = 1 publique + 1 privée
 - les sont choisies mathématiquement
 - calculs lents
 - pas de problématique d'échange de clé

La cryptographie symétrique

Une clé commune à Alice et Bob pour chiffrer et déchiffrer



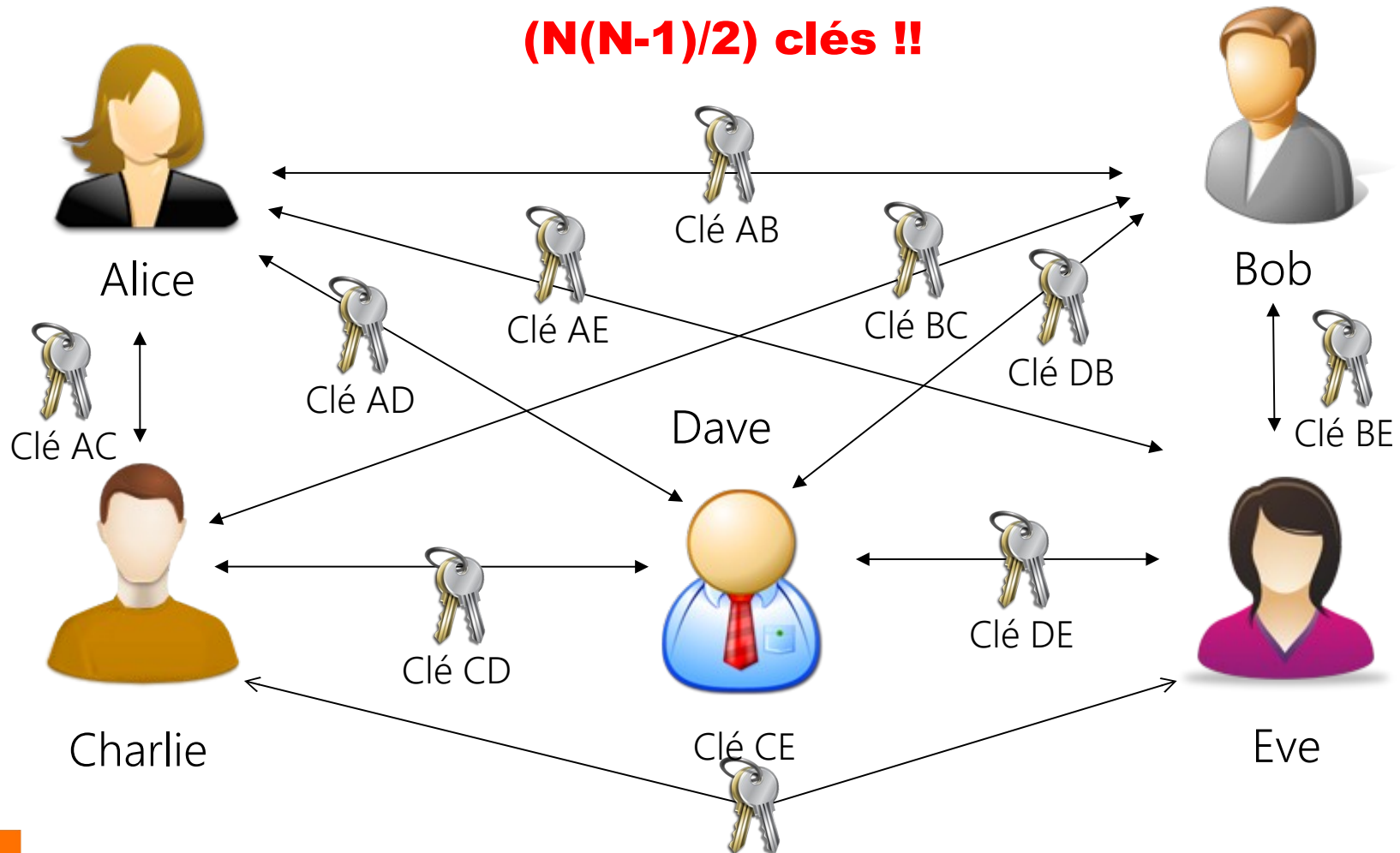
La cryptographie symétrique

- Chiffrement « idéal » (masque jetable)
 - Chiffrement de Vernam : clé de même longueur que le message à chiffrer
- Chiffrement par flot (stream cipher)
 - RC4 : utilisé dans SSL/TLS ou WEP
 - A5/1 : utilisé dans les communications GSM
 - ChaCha : principalement software
- Chiffrement par blocs (blocks cipher)
 - DES : blocs de 64 bits, clés de 56 bits
 - 3DES : blocs de 64 bits, 2 à 3 clés de 56 bits
 - AES (Rijndael) : blocs de 128 bits, clés de 128 à 256 bits

La cryptographie symétrique

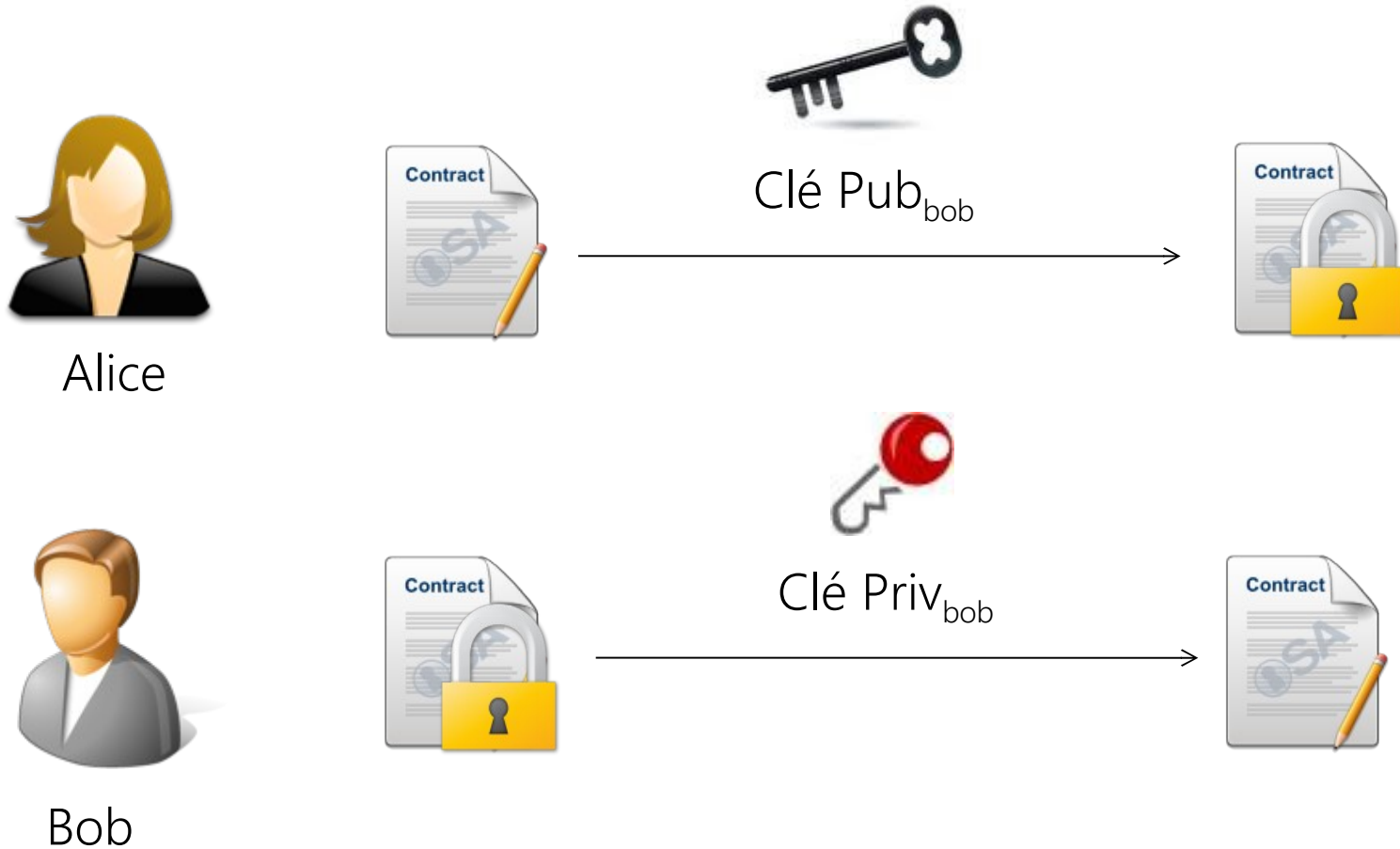
Problématique d'échange de la clé

$(N(N-1)/2)$ clés !!



La cryptographie asymétrique

Une clé pour chiffrer et une pour déchiffrer



La cryptographie asymétrique

- RSA (Rivest Shamir Adelman)
 - Basé sur l'exponentiation modulaire et le problème de la factorisation
 - Algorithme de chiffrement et signature breveté par le MIT
 - Très répandu dans les échanges électroniques
 - Grande taille de clé (clé de 3072 bits pour une sécurité de 128 bits)

- DSA (Digital Signature Algorithm)
 - Basé sur le problème du logarithme discret dans un groupe fini
 - Algorithme de signature standard du NIST

- ECC (Elliptic Curve Cryptography)
 - Basé sur les courbes elliptiques
 - Algorithmes de chiffrement et signature (ECDSA, ECDH, ...)
 - Taille de clé réduite (clé de 256 bits pour une sécurité de 128 bits)

La cryptographie asymétrique : les avantages

- Pas de problématique d'échange ou de multiplication de clés
- Permet d'assurer la **confidentialité** mais aussi l'**authentification**
- Permet de mettre en place des mécanismes tels que la signature numérique qui assure la fonction de **non répudiation**

La cryptographie asymétrique : les défauts

- Cryptographie très **lente** (pour la même sécurité ~1000 fois plus lente)
- Il est aisé de fabriquer un couple clé privée / clé publique donc :
 - comment être sûr qu'une clé publique reçue **provient bien** de l'expéditeur annoncé ?
- Où et comment conserver les clés qui doivent rester **secrètes** ?
- Comment être sûr qu'une **clé** n'a pas été **volée** ?

Les fonction de condensation

- Appelées aussi fonctions de hashage, de calcul d'empreinte, de somme de contrôle (checksum)
- Calcule une **empreinte** unique d'une donnée fournie en entrée :
 - « donnée » : d41d8cd98f00b204e9800998ecf8427e
 - « Donnée » : 3b7a7b4bb91ce3a25adab34a9d2533a4
- Ces fonctions permettent d'assurer l'**intégrité** des données
 - 2 données ne doivent pas avoir la même empreinte
 - fonctions à sens unique (impossibilité de retrouver la donnée à partir du hash)
 - la longueur du hash est définie par l'algorithme

Les fonction de condensation

- MD5 (Message Digest #5)
 - conçu par Ronald Rivest en 1991
 - crée une empreinte de 16 octets de la donnée d'entrée
 - considéré comme « non sûr » depuis 2004
- SHA-1 (Secure Hash Algorithm #1)
 - conçu par la NSA et standardisé par le NIST en 1995
 - crée une empreinte de 20 octets de la donnée d'entrée
 - déconseillé pour une utilisation après 2015
- SHA-2 (Secure Hash Algorithm #2)
 - conçu par la NSA et standardisé par le NIST en 2002
 - crée une empreinte de 32 à 64 octets de la donnée d'entrée
- SHA-3 (Secure Hash Algorithm #3)
 - Issu d'une compétition organisée par le NIST (oct. 2012) standardisé 2015
 - Alternative à SHA-2

Quel algorithme choisir ?

▪ Approuvé par l'ANSSI (France)

- Agence Nationale de la Sécurité des Systèmes d'Information
- http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf

▪ Approuvé par le NIST (Etats-Unis)

- National Institut of Standards and Technology
- <http://csrc.nist.gov/groups/STM/cavp/index.html#01>

▪ Approuvé par l'ENISA (UE)

- European union Network and Information Security Agency
- <https://www.enisa.europa.eu/>

Tailles de clés acceptées par l'ANSSI

Algorithmes symétriques

Taille minimale des clés utilisées jusqu'en 2020	100 bits
Taille minimale des clés utilisées au-delà de 2020	128 bits

Algorithmes asymétriques

Taille minimale du module RSA pour une utilisation ne devant pas dépasser 2020	2048 bits
Taille minimale du module RSA pour une utilisation au-delà de 2020	3072 bits

partie 1 : Introduction

partie 2 : Rappels de Cryptologie

partie 3 : Certificats numériques

partie 4 : PKI / IGC

partie 5 : Bonnes pratiques IGC

Clés + Autorité = Certificats

- Rappel : comment être sûr qu'une clé publique reçue **provient bien** de l'expéditeur annoncé ?
- Pour certifier qu'une clé publique **provient** bien de son expéditeur, les certificats numériques sont utilisés.
- L'information certifiée est de ce fait transportée dans un certificat électronique délivré et **signé** par une autorité.

Clés + Autorité = Certificats



Photo &
facture EDF



Autorité



Clés + Autorité = Certificats



Clé Publique



Autorité



Certificat

Qu'est-ce qu'un certificat électronique ?

- C'est une **carte d'identité** informatique.
- C'est un document **public**, voué à être distribué à tout le monde.
- Il possède d'une période de **validité** et des **usages** précis
- Il est **signé** par un tiers de **confiance** (l'**Autorité**)
- Seul le **titulaire** d'un certificat possède la clé privée associée.

Que contient un certificat électronique ?

- Une clé **publique**
- Un numéro de Série, unique dans une AC
 - aléatoire ou incrémenté
- Des informations d'identification
 - nom, localisation, adresse email, etc.
- Des informations de durée de validité
- Des informations sur son émetteur
- Une **signature**
- Des informations sur son **usage**



Quel est le format des certificats ?

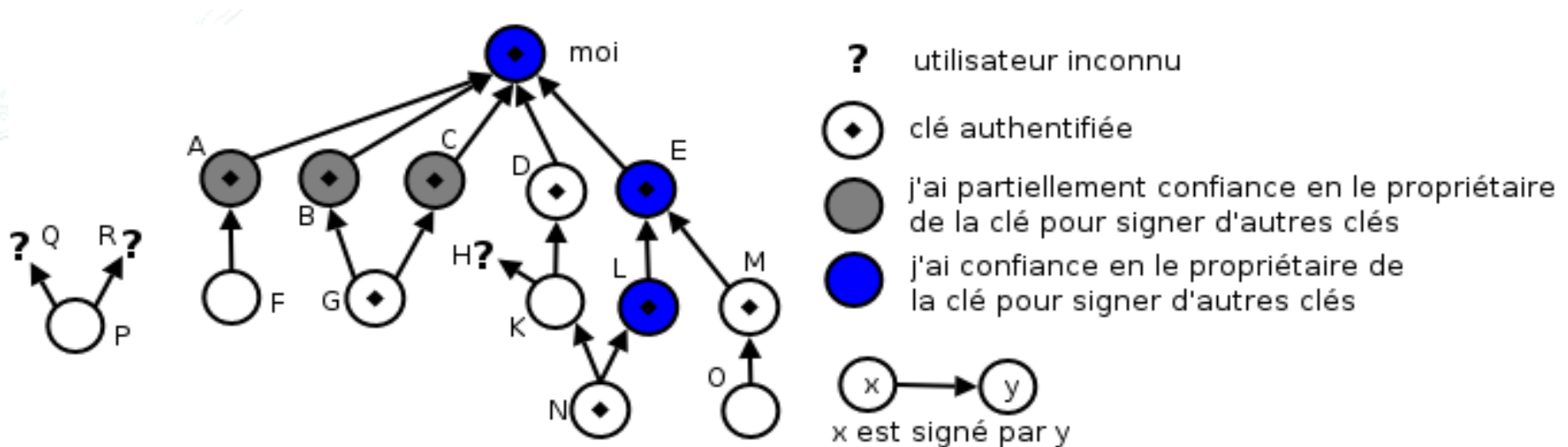
- Certificat X509
 - défini dans les RFC 3280 & 5280.
 - basé sur une IGC (hiérarchie d'Autorités de Certification).
 - certificat signé par une seule autorité de certification.

- Certificat PGP
 - défini dans la RFC 4880.
 - basé sur des réseaux de confiance.
 - certificat signé par plusieurs personnes.

- Certificat CVC
 - Défini dans les normes 7816 & EAC (Extended Access Control).
 - Basé sur une IGC CSCA (hiérarchie d'Autorités de Certification).
 - certificat signé par une seule autorité de certification.

Le format des certificats - OpenPGP

- Principe de l'anneau de confiance (« Web Of Trust »)
 - Utilisation adaptée aux communautés...
- La confiance dans une paire de clé PGP est associée à :
 - Un niveau de confiance en l'identité du propriétaire
 - Un niveau de confiance en la capacité du propriétaire à signer correctement les clés des autres.



Le format des certificats – X509

Version
Certificate serial number
Signature Algorithm identifier
Issuer X.500 name
Subject X.500 name
Validity period
public key information
<i>Authority key identifier</i>
<i>Subject key identifier</i>
<i>Extensions</i>
CA Signature

- **Version du format de certificat (1, 2 ou 3)**
- **N° de série UNIQUE du certificat**
- **Identification des algorithmes utilisés pour signer le certificat**
- **Noms X.500 de l'AC et du détenteur**
- **Période de validité du certificat (date de début, date de fin)**
- **Identification des algorithmes utilisés pour générer la clé privée & publique de l'utilisateur**
- **Extensions du certificat (options). Valable à partir de la version 3**
- **Signature du certificat par l'Autorité de Certification**

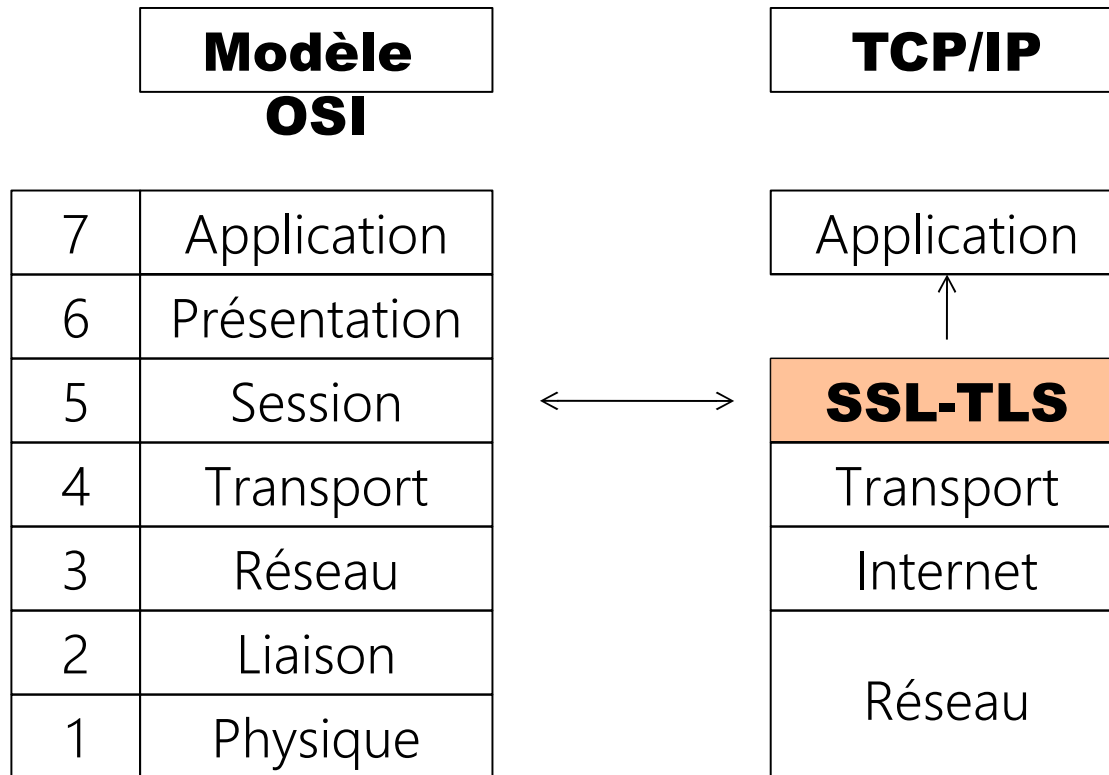
Applications des certificats X509

- SSL/TLS
 - Secure Sockets Layer/Transport Layer Security
 - Sécurisation des échanges sur internet
- IPSec (VPN)
 - Internet Protocol Security
 - Sécurisation des communications sur réseau IP
- S/MIME
 - Secure / Multipurpose Internet Mail Extensions
 - Norme de cryptographie et de signature numérique de mail encapsulés en format MIME

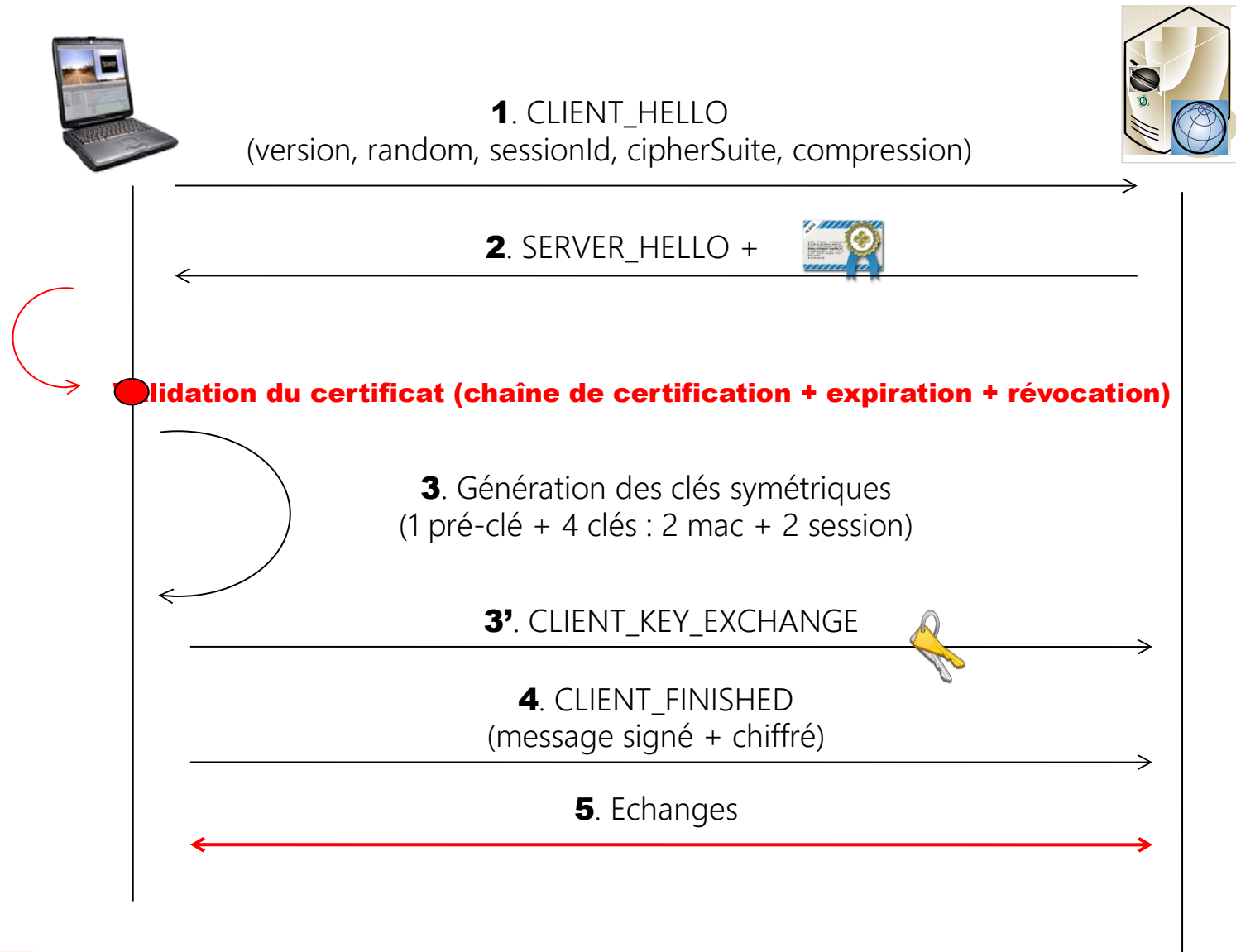
Applications des certificats X509 : SSL

- SSL (Secure Socket Layer) et TLS (Transport Secured Layer) sont deux protocoles permettant de sécuriser les échanges de la couche application (HTTP, LDAP, etc.)
 - SSLv1 & SSLv2 (obsolètes)
 - SSLv3 (déconseillé)
 - TLS 1.0
 - TLS 1.1 & TLS 1.2 (recommandés mais...)
- Ils permettent :
 - L'authentification du serveur notamment mais aussi du client
 - La confidentialité des échanges
 - L'identification et l'intégrité des échanges

Applications des certificats X509 : SSL



Applications des certificats X509 : SSL



Un certificat par usage...

- Certificat d'authentification
 - Pour assurer la fonction d'**authentification**
- Certificat de Signature
 - Pour assurer les fonctions d'**intégrité** et de **non-répudiation**
- Certificat de chiffrement
 - Pour assurer la fonction de **confidentialité**

Un certificat par usage...

- Certificat d'authentification
 - authentication TLS cliente, authentication TLS serveur, authentication IP Sec, SmartCard Logon
- Certificat de Signature
 - signature de courriels, de documents, de code, de jetons d'horodatage, de certificats, de LCR
- Certificat de chiffrement
 - chiffrement de courriels, de documents ou fichiers (EFS)

Les extensions X509

Extensions d'informations sur les clés

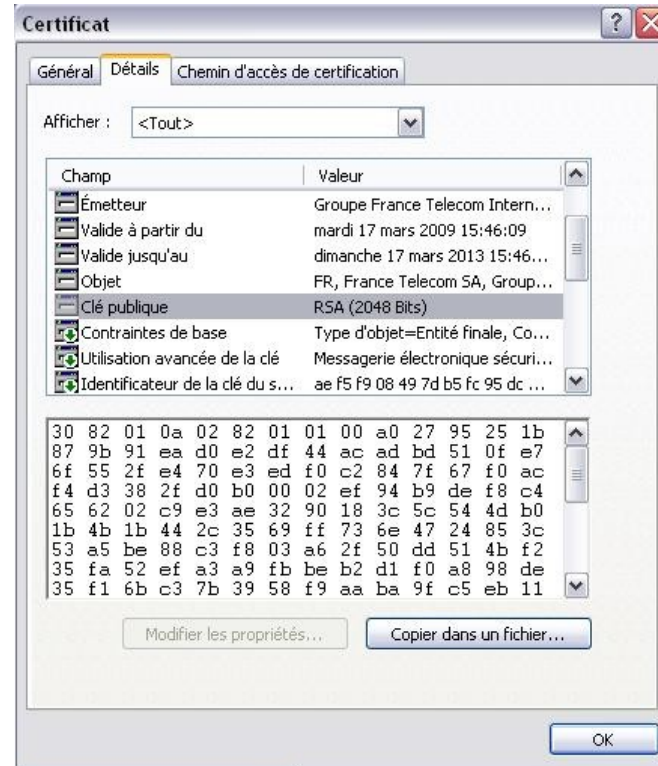
Authority Key Identifier	Identifiant de la paire de clé de l'AC utilisée pour signer le certificat.	Lorsque l'AC utilise plusieurs clés depuis sa mise en œuvre, cette extension permet de connaître la clé publique à utiliser pour vérifier la signature du certificat.
Subject Key Identifier	Identifiant de la clé publique contenue dans le certificat.	
Key usage	Utilisation qui doit être faite de la clé.	Non-répudiation, Signature de certificats, Signature de LCR, signature numérique, Chiffrement de données, Chiffrement de clés, Agreement de clés
Extended Key Usage	Spécialisation du certificat	Authentification cliente, SmartCard Logon, Signature de code...
Certificate Policies	Politique de certification qui a présidé à l'émission du certificat.	OID de la PC de l'AC émettrice

Les extensions X509

Extensions sur les attributs des utilisateurs et des AC

Subject Alternative Name	Autre nom du propriétaire	Informations sur le propriétaire du certificat. Les valeurs autorisées sont : <ul style="list-style-type: none">■ Adresse mail (RFC 822)■ Nom de domaine■ Adresse IP■ Adresse mail X400■ Nom EDI■ URL■ Nom défini par une OID (UPN par exemple)
Issuer Alternative Name	Autre nom de l'Autorité	Permet de donner un nom spécifique à une AC
CRL Distribution Point	Emplacement des LCR.	Point de distribution des LCR (HTTP, LDAP)
Basic Constraints	Contraintes de base	Précise si le certificat appartient à une AC ou à un utilisateur final et la distance de certification pour les certificats d'AC.

Exemple de certificat X509



Où stocker les clés privées ?

Support	Avantages	Inconvénients
Disque dur	Coût réduit Simple à mettre en œuvre	La sécurité dépend du poste de travail. Possibilité de duplication
Carte à puce	Calculs faits par la puce cryptographique. Clé privée non exportable. Saisie du PIN sur lecteur de carte avec clavier intégré (PINPad).	Coût : cartes + lecteur + distribution
Token sur port USB	Calculs faits par le token. Clé privée non exportable. Moins coûteux qu'une carte à puce car pas besoin de s'équiper de lecteurs.	Port USB nécessaire Pas de clavier dédié.
HSM (Hardware Security Module)	Équipement dédié. Protégé physiquement. Génération et stockage de données sensibles (ex : clé d'AC) Calculs faits dans le HSM. Clé privée non exportable. Accélération des calculs cryptographiques	Coût très élevé. Dispositif fixe.



Questions



© OAB

Merci

