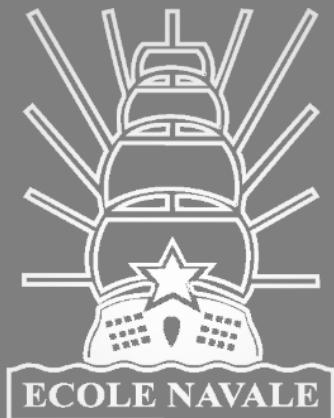


Cours



cybersécurité

cryptographie

chiffrement

AES

RSA

signature

électronique

PKI

CRL

certificat X509

SHA256

SSL https

autorité de certification

pkcs11 CSR ETSI

PADES

XMLdsig

OpenSSL

MsCapi

JCA

Code signing

Timestamp

authentification

forte

RGS

eIDAS

PKI, services de confiance & signature électronique

Anthony JULOU - Cyril THIRION

anthony.julou@ecole-navale.fr
cyril.thirion@gmail.com

Version 2.1
© 2020



Université de Bretagne Occidentale





□ PKI, services de confiance & signature électronique

Plan du cours

- Chapitre 1: La confiance numérique
- Chapitre 2: Bases cryptographiques
- Chapitre 3: Le certificat numérique, PKI et AC
- Chapitre 4: Fonctions de signature,
d'authentification, horodatage
- Chapitre 5: Formats de signature
- Chapitre 6: Les logiciels
- Chapitre 7: Programmation
- Chapitre 8: Applications exemples
- Chapitre 9: Cadre légal et juridique
- Chapitre 10: Conclusion

1) La confiance
numérique2) Bases
cryptographiques3) Le certificat
numérique4) Fonctions de
signature5) Formats de
signature

6) Les logiciels

7) Programmation

8) Applications
exemples9) Cadre légal et
juridique

10) Conclusion

 PKI, services de confiance et signature électronique

Chapitre 1 :

La confiance numérique

- Historique
- Questionnement
- La confiance numérique ?
- Tiers de confiance
- Services de confiance



Historique

Questionnement

La confiance
numérique ?

Tiers de confiance

Services de
confiance

□ Chapitre 1 : La confiance numérique

Historique

- **Besoin de sécurisation et de confiance sur Internet**
 - Sécurité des transactions et des accès
 - Confiance dans les acteurs d'internet
- **Lois et directives européennes**
 - **2000** : Loi française d'application donnant la **même valeur légale** à la signature électronique qu'à la signature papier en application de la directive Européenne (1999) instaurant les règles de la signature électronique
 - **2004** : Loi pour la Confiance dans l'Economie Numérique (LCEN) → 2 Directives Européenne (2000 et 2002) porte sur :
 - *Commerce électronique, responsabilité hébergeur, cryptologie, cybercriminalité...*

Questionnement

■ Identité numérique

- Qui suis-je sur Internet ?
 - A qui ai-je affaire ?

■ Confiance numérique

- Le site est-il de confiance ? sécurisé ?

■ Sécurité

- Un login / mot de passe suffit-il ? Mon mot de passe est-t-il sécurisé ?
 - Mes données sont-elles sécurisées ?
 - Qui a accès à mes données ?

□ Chapitre 1 : La confiance numérique

Questionnement

■ Quels sont les risques sur Internet ?

- usurpation d'identité,
- escroquerie, chantage, arnaques,
- vol de données personnelles
- prise de contrôle de l'ordinateur
- destruction/verrouillage du système/fichiers ...

■ Quels types d'attaques possibles ?

- phishing (spam, faux sites internet piégés...),
- key logger, rejeu, man in the middle,
- virus, ransomware, nouvelles menaces ...
- **Attaques de services:** Deny of Services (DoS ou Distributed Dos), exploitation de failles par intrusion (injection SQL, Cross Site Scripting XSS ...) ...

Historique

Questionnement

La confiance
numérique ?

Tiers de confiance

Services de
confiance

□ Chapitre 1 : La confiance numérique

La confiance numérique ?

- Ensemble de **bonnes pratiques, de règles, lois et de normes** pour garantir les échanges électroniques

1. Bonnes pratiques, exemple:

- L'ANSSI publie des guides à destination des usages
→ <https://www.ssi.gouv.fr/administration/bonnes-pratiques/>

2. Des lois. Exemples...

1) LCEN (2004)

Commerce électronique, responsabilité des hébergeurs,
publicité par voie électronique ...

2) LPM (Lois programmation militaire)... 1997 =>...

- 2014-2019 : sécurité des infra et données des OIV
- 2019-2025 : cybersécurité, détection des attaques

Chapitre 1 : La confiance numérique

La confiance numérique ?

3. Règles et normes, exemples:

- France : Référentiel Général de Sécurité (RGS)
- Europe: Règlements européens
 - eIDAS 2014 (*electronic IDentification Authentification and trust Services*)
 - RGPD (2018) : *Règlement pour la protection des données personnelles*
=> Normes ETSI
- Monde:
 - Normes RFC (*Request For Comment*)
 - Normes ISO (2700x...)
 - Normes du W3C pour le Web



□ Chapitre 1 : La confiance numérique

Tiers de confiance

- L'adage... « *nul ne peut se constituer de preuve à soi-même* »
- Organismes tiers (souvent privés) garantissant la confiance numérique par :
 1. le respect des règles/lois en sécurité des échanges
 2. la garantie que les règles sont respectées en apportant la **preuve** aux autorités/états.
- Qui sont-ils ?
 - Autorité de certification (AC), d'horodatage (AH) ...
 - Fournissent des **services de sécurité** (*signature électronique, archivage numérique, conservation de la preuve ...*)
 - Utilisent des **produits de sécurité homologués** (*logiciels, puces cryptographiques...*)

Services de confiance

Pratiques de gestion des preuves

Le promoteur d'application décrit les mesures organisationnelles et techniques de constitution, conservation et pérennisation des preuves électroniques qu'il traite.



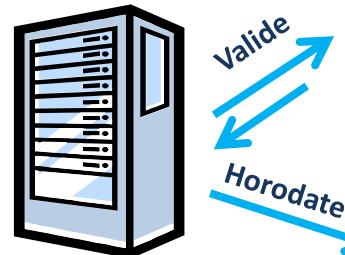
Autorité de certification

Signataire

Politique de certification

Conditions d'utilisation

- Certificat
- Services



Autorité de validation

Valide

Horodate



Autorité d'horodatage

Politique d'horodatage

Valide

Archive



Autorité d'archivage

Politique d'archivage

Politique de validation
des AC, des certificats et
des documents signés

Promoteur de
services de
signatures,
vérification de
preuve,

Politique de
signature et de
gestion de la preuve

Historique

Questionnement

La confiance
numérique ?

Tiers de confiance

Services de
confiance Chapitre 1 : La confiance numérique

Qualification d'un tiers de confiance

Exigences sur les services de confiance

Analyse de risques

Politique de certification

CGU

PSSI

Organisation interne

Ressources humaines

Gestion des biens

Contrôle d'accès

Sécurité Physique

Opérations

Réseau

Gestion des incidents

Gestion des traces

Continuité d'activité

Arrêt d'activité

- ✓ Audit réalisée par l'**ANSSI** tous les **2 ans** pour obtenir la qualification avant de fournir tout service

Chapitre 2 :

Bases

cryptographiques

- La cryptographie
- Chiffrement symétrique
- Chiffrement asymétrique
- Algorithmes de hachage



La cryptographie

Chiffrement
symétrique

Chiffrement
asymétrique

Algorithmes de
hachage

□ Chapitre 2 : Bases cryptographiques

La cryptographie

- Discipline assurant la protection des messages (*confidentialité, authenticité, intégrité*)
- Elle fournit des services de sécurité
 - Chiffrement / déchiffrement
 - Scellement / signature
- Elle implémente
 - des algorithmes de chiffrement symétrique / asymétrique
 - des fonctions de hachage...



□ Chapitre 2 : Bases cryptographiques

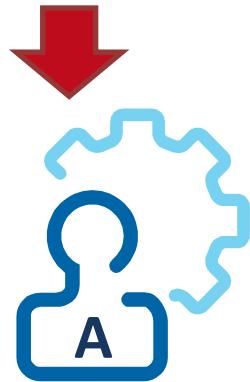
Chiffrement symétrique 1/3

But : Chiffrer/déchiffrer un message avec une **clé secrète** partagée par les 2 parties.

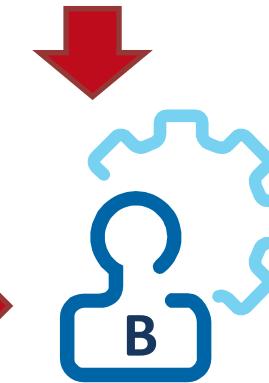
Problématique: Trouver une fonction f qui transforme le message m en c (cryptogramme) et inversement à l'aide d'une clé secrète k tel que

$$c = f(k, m) \text{ et } m = f^{-1}(k, c)$$

A chiffre
 $m =$
« bonjour » avec la
clé k



m transmis
chiffré = c =
« gX4fgt6 »



B déchiffre
 c avec la
clé k et
obtient m
= bonjour

□ Chapitre 2 : Bases cryptographiques

Chiffrement symétrique 2/3

- **Avantages:** Rapidité, adapté au chiffrement de gros volumes de données
- **Inconvénients:** Confidentialité de la clé secrète
- **Principaux algorithmes**
 - AES (*Advanced Encryption Standard* – Année 2000), DES, 3DES, Serpent, Blowfish ...
- **Algorithme recommandé par l'ANSSI:**
 - **AES CBC** (*AES Cipher Block Chaining*)
 - Clé secrète de 128 bits recommandé dès 2020

539x10⁶ millénaires pour casser une clé de 128 bits avec un ordinateur calculant 10¹⁸ de cryptogrammes par seconde

□ Chapitre 2 : Bases cryptographiques

Chiffrement symétrique 3/3

- Logiciels grand public
 - **Office 2010** => AES -256
 - **Winzip** => AES 128 ou 256
- Protocoles de communication
 - **SSL (Secure socket layer)** remplacé par **TLS (Transport layer security)** (https, ftps, ssh...)
 - **WIFI** : **WEP (RC4)**, WPA (TKIP) et WPA2-CCMP (AES)
- Logiciels de chiffrement de fichiers
 - **Zed!** (Société Prim'X) qualifié niveau standard Anssi
 - **TrueCrypt (Fin 2014)**, **AES Crypt (Open source)**
 - **Acid Cryptofiler** (Logiciel de la DGA-MI à Rennes)
 - **GnuPG (Gratuit)**: suite de chiffrement et de signature

Chapitre 2 : Bases cryptographiques

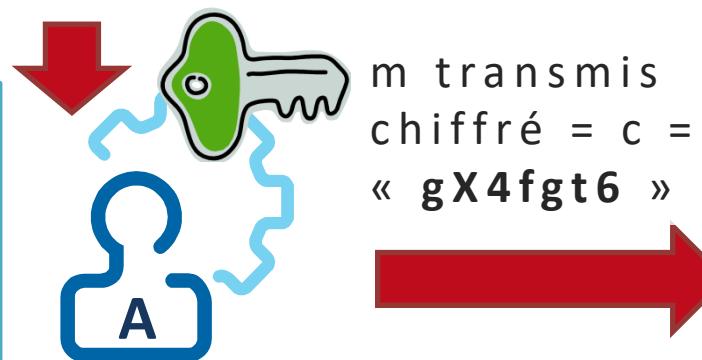
Chiffrement asymétrique 1/3

But : Chiffrement avec une **clé publique** puis déchiffrement avec la **clé privée**

Problématique: Trouver une fonction f qui transforme le message m en c (cryptogramme) avec une clé publique **k1** et déchiffre à l'aide d'une clé privée **k2** tel que:

$$c = f(k_1, m) \text{ et } m = f(k_2, c)$$

A chiffre
 $m =$
« bonjour » avec la
clé k_1



B déchiffre
c avec la
clé k_2 et
obtient m
= bonjour

Chiffrement asymétrique 2/3

Applications du chiffrement asymétrique

- Chiffrement (Confidentialité)
 - Transporter un message confidentiel codé avec la clé publique puis le décoder avec la clé privée
- Authentification
 - S'assurer de l'identité du détenteur de la clé privée en vérifiant avec sa clé publique que le défi chiffré a bien été codé par la clé privée
- Signature
 - Déchiffrer un message avec la clé publique afin de vérifier qu'il a été signé par le détenteur de la clé privée

□ Chapitre 2 : Bases cryptographiques

Chiffrement asymétrique 3/3

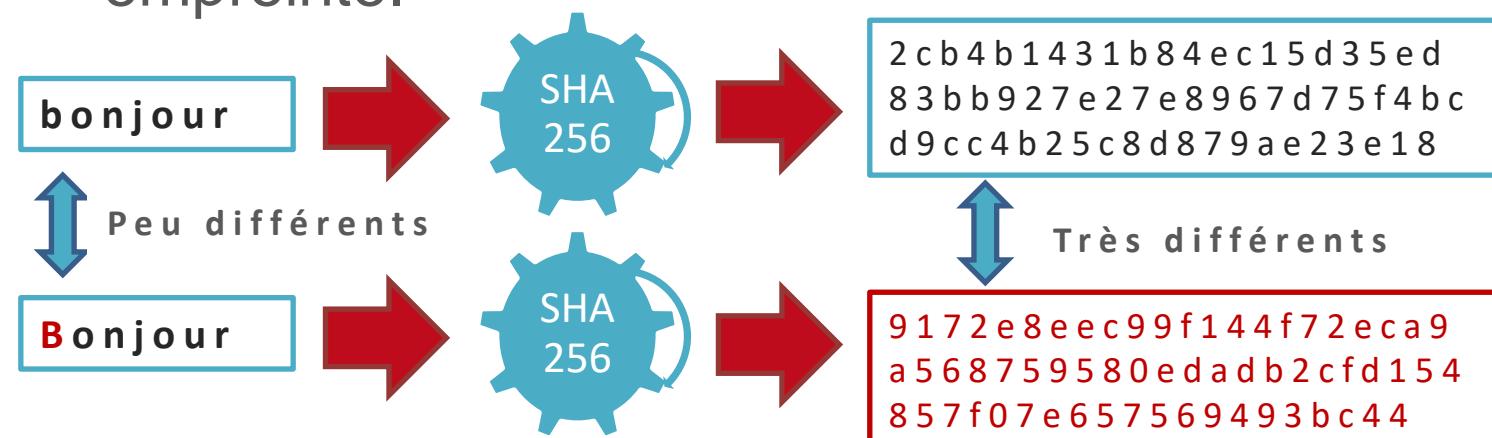
- **Avantages:** Sécurité renforcée, robustesse
- **Inconvénients:**
 - Inadapté au chiffrement de gros volumes (performance, limitation des algorithmes)
 - Mise en œuvre
- **Principaux algorithmes**
 - RSA (*Ron Rivest, Adi Shamir, Leonard Adleman*), DSA (*Digital Signature Algorithm*), Diffie-Helmann, courbes elliptiques GF...
- **Algorithme recommandé par l'ANSSI:**
 - RSA 2048 bits jusqu'en 2030 et 3072 au delà...
 - Courbes elliptiques GF 200 bits jusqu'en 2020 et 256 au delà...

□ Chapitre 2 : Bases cryptographiques

Algorithmes de hachage (1/2)

But : Obtenir une empreinte unique d'un message (condensé, scellement)

- Condense un message M de taille quelconque en une empreinte (*un condensé, un scellement*) de taille fixe (128 à 512 bits).
- Connaissant M et son empreinte, il est très difficile de construire M' ayant la même empreinte.



Chapitre 2 : Bases cryptographiques

Algorithmes de hachage (2/2)

Applications

- **Anonymisation/confidentialité**
 - Remplacer le nom d'une personne par son hash
- **Scellement**
 - Garantir qu'une donnée n'a pas été modifiée
- **Condensation**
 - Obtenir une empreinte de petite taille pour identifier un objet de grande taille
- **Principaux algorithmes**
 - SHA 2 (256, 384 ou 512 bits), SHA1 (160), MD5(128)
- **Algorithme recommandé par l'ANSSI:**
 - SHA 2 en 256 bits (*Collisions sur MD5, risques sur SHA1*)



- 1) La confiance numérique
- 2) Bases cryptographiques
- 3) Le certificat numérique
- 4) Fonctions de signature
- 5) Formats de signature
- 6) Les logiciels
- 7) Programmation
- 8) Applications exemples
- 9) Cadre légal et juridique
- 10) Conclusion

PKI, services de confiance et signature électronique

Chapitre 3 :

Le certificat numérique



- Le certificat d'identité numérique
- Format du certificat
- PKI et Autorité de certification
- Génération d'un certificat
- Conteneur de certificats
- Exemples de certificats
- Révocation d'un certificat
- Validité d'un certificat

Le certificat d'identité numérique

Le certificat est une **carte d'identité numérique** permettant de:

- authentifier une entité physique ou morale (une personne, un serveur...)
- signer numériquement
- chiffrer du contenu
- Authentifier/sécuriser une transaction

Et utilisant les mécanismes de:

- **cryptographie asymétrique** (clé privée/clé publique) et **symétrique** (clé secrète)
- scellement et hachage

□ Chapitre 3 : Le certificat numérique

Format du certificat

Standard x509 (RFC 5280), il est composé de:

- une bi-clé (*souvent RSA*) privée / publique
- données d'identité et données techniques



□ Chapitre 3 : Le certificat numérique

Format du certificat

1. Données d'identité (Attributs ASN.1)

DN (Distinguished Name) est composé de :

CN (Common Name),

SN (Surname), **T** (Title name)

O (Organisation name), **OU** (Organisation Unit name)

L (Locality), **C** (Country name),

ST (state or province name)

SN (serialNumber)

Exemple DN de personne: **CN=Bernard DUPONT**,
T=Professeur, **O=Ecole Navale**, **OU=Département Informatique**, **L=Lanvéoc**, **C=FR**

Exemple DN de serveur: **CN=www.ecole-navale.fr**, **O=Ecole Navale**, **L=Lanvéoc**, **C=FR**

Chapitre 3 : Le certificat numérique

Format du certificat

2. Données techniques

Champs	Description
Clé publique et type d'algorithme	suites de bits pour chaque clé Ex: RSA
Suite algorithmes ayant signé le certificat	Ex: sha256 avec RSA
Algorithme de hachage pour l'empreinte	Ex: sha256
Key Usage: Utilisation de la clé du certificat	Ex: Signature, Chiffrement, Authentification ...
Extended Key Usage: Usage étendu de la clé	Signature de code, authentification client ou serveur ...
DN de l'émetteur ayant émis le certificat	Ex: CN=..., OU = ..., O = ...
SKI (<i>Sujet Key Identifier</i>) AKI (<i>Authority Key Identifier</i>)	2 hash des clés publiques identifiant le certificat (<i>SKI</i>) et son émetteur (<i>AKI</i>)
Validité du certificat (Date de début et de fin)	Ex: de 1 à 3 ans
Liste de révocation et / ou Répondeur OCSP	URL de la liste + fréquence mise à jour et/ou Service OCSP
N° version X509	Ex: Version V3
n° de série du certificat	n° série une suite hexadécimale unique

□ Chapitre 3 : Le certificat numérique

Format du certificat

3. Champ « Key Usage »

Que peut-on faire avec la clé du certificat ?

Key Usage	Bit	Description
digitalSignature	0	Authentification, signature (intégrité)
contentCommitment (nonRepudiation)	1	Signature (non répudiable)
keyEncipherment	2	Chiffrement de clés privées ou secrètes
dataEncipherment	3	Chiffrement de données (peu utilisé)
keyAgreement	4	Acceptation de clés dans les protocoles
keyCertSign	5	Signature de certificats (Usage pour AC)
cRLSign	6	Signature de CRL (Usage pour AC)
encipherOnly	7	Limitation au chiffrement pendant le keyAgreement
decipherOnly	8	Limitation au déchiffrement pendant le keyAgreement

Chapitre 3 : Le certificat numérique

Format du certificat

4. Champ « Extended Key Usage »

Certificat => Application	Extended key usage	Key usage
TLS serveur authentification ⇒ Authentifier site https	id-kp-serverAuth	digitalSignature & keyEncipherment ou keyAgreement
TLS client authentification ⇒ Authentifier client	id-kp-clientAuth	digitalSignature &/ou keyAgreement
Code Signing ⇒ Signer code exécutable	id-kp-codeSigning	digitalSignature
Email protection ⇒ Signer des e-mails (1) ⇒ Chiffrer des e-mails(2)	id-kp-emailProtection	digitalSignature (1), nonrepudiation (1), keyEncipherment (2) ou keyAgreement (2)
Timestamping ⇒ Jeton d'horodatage	id-kp-timeStamping	digitalSignature &/ou nonRepudiation
OCSP Response Signing ⇒ Signer réponses OCSP	id-kp-OCSPSigning	digitalSignature &/ou nonRepudiation

Le certificat
d'identité
numérique

Format du certificat

PKI et Autorité de
certification

Génération d'un
certificat

Conteneur de
certificats

Exemples de
certificats

Révocation d'un
certificat

Validité d'un
certificat

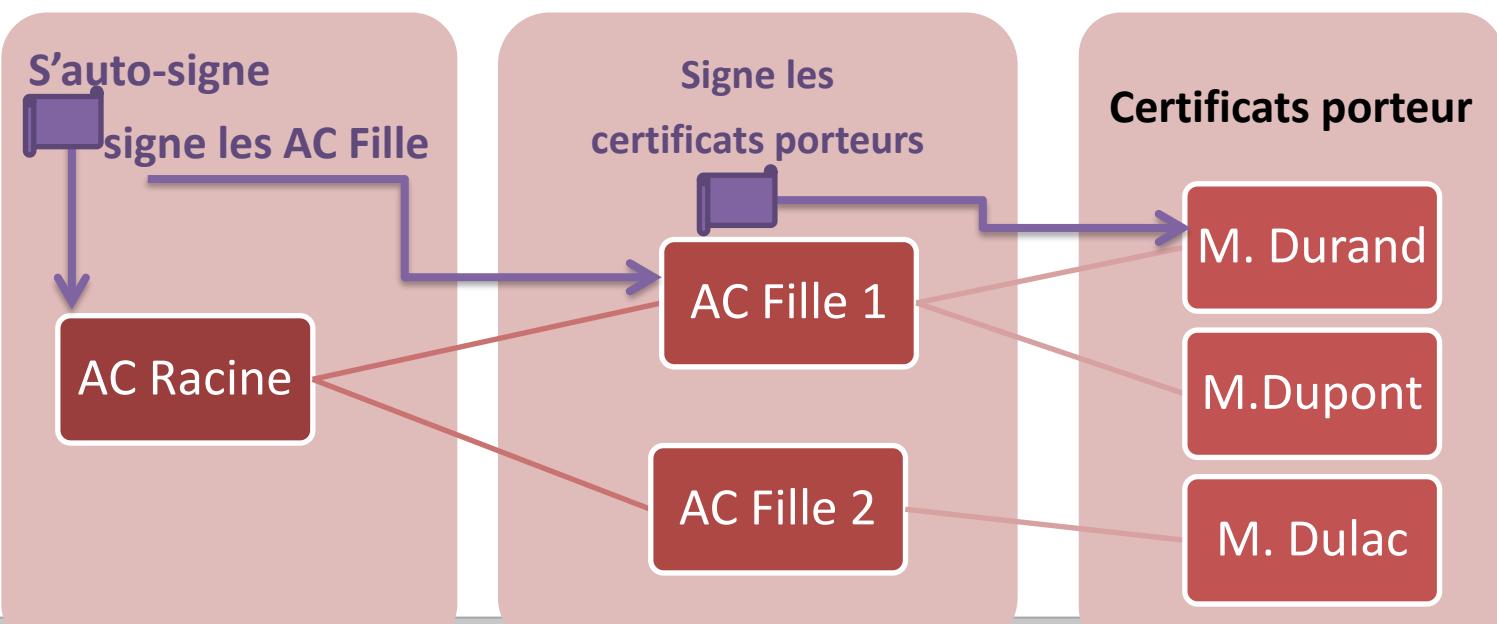
□ Chapitre 3 : Le certificat numérique

PKI et Autorité de certification

PKIX : Public Key Infrastructure for X509

AC : Autorité de Certification implémentant les services de PKIX (Emission, révocation de certificats)

Chaîne de confiance : Principe basé sur la confiance accordée à l'AC et sa chaîne de certification



Génération d'un certificat (1/3)

■ Demande administrative de X

1. X demande un certificat à une AC
2. L' autorité d'enregistrement (AE) de l'AC vérifie le dossier et l'identité :
 - du demandeur X pour un certificat d'individu
 - de l'organisation X pour un certificat/cachet serveur
3. L' AE donne l'autorisation de délivrance du certificat à l'AC
4. L' AC délivre le certificat
 - **sur carte à puce cryptographique => Individu**
 - **sous forme logiciel => Individu ou serveur**
 - **sur HSM (Hardware Security Module) => Serveur**

□ Chapitre 3 : Le certificat numérique

Génération d'un certificat (2/3)

Demande technique côté client

- Génération d'une bi-clé (clé privée/publique)** par et **sous le contrôle exclusif du demandeur**
- Création d'une CSR (*Certificate Signing Request*) au format (PKCS 10) encodée en base 64**
 - Ajout du DN (*Données personnelles*)
 - Ajout de la clé publique
 - Signature de la CSR avec la clé privée générée en 1.

Exemple de CSR PKCS 10 encodée en base64

```
-----BEGIN CERTIFICATE REQUEST-----  
MIIBNtCCAQYCAQAwXTELMAkGA1UEBhMCU0cxETAPBgNVBAotCE0yQ3J5cHRvMRIw  
PdIrrqliKNknFmHKIaCKTLRcU59ScA6ADEIWUzqmUzP5Cs6jrsRo3NKfg1bd09D1K [...]  
9rsQkRc9Urv9mRBIsredGnYECNeRaK5R1yzpOowninXC  
-----END CERTIFICATE REQUEST-----
```

Génération d'un certificat (3/3)

Traitement de la CSR côté serveur d'AC

- 3. Décodage de la CSR**
- 4. Vérification signature CSR avec la clé publique**
- 5. Vérification de la légitimité de la demande**
- 6. Génération d'un certificat x509 avec**
 - les données du DN + données complémentaires
 - la clé publique du client
 - les données techniques de l'AC
- 7. Signature du certificat par la clé privée d'AC**
- 8. Renvoi du certificat certifié au client**

□ Chapitre 3 : Le certificat numérique

Conteneur de certificats (1/2)

Certificat logiciel (*Sécurité limitée*)

- Fichier **PKCS12 .p12 ou .pfx** contient la clé privée (*chiffrée par mot de passe avec PKCS8*), clé publique, le certificat, sa chaîne d'AC

⇒ La copie du fichier engendre un risque d'usurpation d'identité

Certificats sur token type carte à puce (*Sécurité renforcée*)

- La bi-clé est générée dans la puce cryptographique
- Accès au conteneur de clés privées protégé par code pin. La clé privée ne peut être extraite de la puce.

HSM (Hardware Security Module) (*Haute sécurité*)

- Module cryptographique intégré dans un serveur
- Création, stockage, utilisation de clés cryptographiques
- Haute sécurité d'accès aux clés (**Clés d'AC**)

□ Chapitre 3 : Le certificat numérique

Conteneur de certificats (2/2)



- Lecteur carte à puce IAS ECC
(Identification Authentification Signature European Citizen Card)
- *Fournisseurs:* Gemalto, Oberthur, Morpho...

- HSM (Hardware Security Module):
 - ex: Atos Bull Proteccio



Chapitre 3 : Le certificat numérique

Exemples de certificats (1/2)

Certificat de personne

Data:

Version: 3

Serial number: 11 21 23 aa b5 e9 46 c4 58 52 77 f4 41 3f c4 5a f0 95

Signature Algorithm: sha256RSA

Issuer: CN = ChamberSign France - AC 1 étoile,
OU = 0002 433702479, O = ChamberSign France, C = FR

Validity

Not Before : Feb 25 19:33:46 2016 GMT

Not After : Feb 25 19:33:46 2019 GMT

Subject: SERIALNUMBER = 0001, CN = Anthony JULOU,
T = Chef de projet, OU = Direction technique,
OU = 0002 43370247900026, OU = CHAMBERSIGN FRANCE,
O = CHAMBERSIGN FRANCE, L = LYON, C = FR

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key (2048 bits)

```

30 82 01 0a 02 82 01 01 00 c6 78 b6 7f d2 b7 88 4d 3b 0e 09 43 8c 6c 63
77 55 fe 5d 49 1b f0 90 8f dd 96 30 6f 1b 6b 2f 8a d9 60 70 fa 9b 53 06 cb
27 9f 0e af c3 9b a8 62 a4 32 c1 5b 7a 48 57 17 d0 56 2a 19 57 0f 85 b9 09
d0 c9 19 37 66 f0 b6 57 9e f4 f1 28 d5 6d c9 13 a2 ec 49 6d 8c 7e ed 9a e1
cd c1 36 dc 8a 9a e5 f9 5a fb ea 83 07 0c db 7c a8 4c ff 7e e8 15 86 e0 47
91 96 c4 83 28 2c cb f3 e5 47 a5 35 73 f7 69 d6 8e c9 31 b3 0c 67 35 d3 fe
7f 1b 25 8b 88 c5 5e 9a de 38 d8 da 21 cd 53 3e 28 88 df 6c 5f f8 72 3d e8
6b 66 2a 39 86 2f 68 73 a7 a4 86 4b 4e b8 20 7e e6 0e 9d cd 10 6c ad e7 0e
3d a2 5d f0 fa fc 4c 00 1c f6 36 f6 a3 7d ae 1f bd 30 7f b4 1c 24 c6 b4 2a
64 22 25 ac 1e 58 da 88 10 b0 64 17 c4 97 5d ba 7f 8e ef 37 28 77 63 03 1c
6e 2e 2c 02 8e 81 74 9e 73 1e 5f 46 6c 39 1d ef 02 03 01 00 01

```

Key usages: Digital Signature, Non repudiation

Certificate Signature:

74 17 39 be df bf 7d 34 55 e6 ba 36 5c bb b3 38 90 01 e8 a2

□ Chapitre 3 : Le certificat numérique

Magasins de certificats

- Clés et certificats accessibles depuis un **keystore**
(Magasin de clés) contenant:
 - Chaine de confiance (*Certificats racines*)
 - Bi-clés personnelles et leur certificat
 - Certificats d'autres personnes (sans la clé privée)

Windows

Certmgr.msc

- **Type de stockage:** base des registres utilisateur ou locale machine
- **Utilisé par:** Internet Explorer, Outlook, Office, Chrome, ...

Macintosh

Trousseau d'accès

- **Type de stockage:** fichier /Utilisateurs/VotreCompte/Bibliothèque/Keychains
- **Utilisé par:** Safari, Chrome, Mail, ...

Mozilla

Firefox / Thunderbird

- **Type de stockage:** fichier base de données key3.db
- **Utilisé par :** « Authentification sur sites internet (FF) » et mail signé/chiffré (TB)

Java

javacpl (Java Control Panel)

- **Type de stockage:** lib/security/cacerts manipulé avec **keytool**
- **Utilisé par :** le programmeur via l'API

Chapitre 3 : Le certificat numérique

Magasins de certificats

Windows : « certmgr.msc »

certmgr - [Certificats - Utilisateur actuel\Autorités de certification racines de confiance\Certificats]

Fichier	Action	Affichage	?																																																																
Certificats - Utilisateur actuel																																																																			
<ul style="list-style-type: none"> Personnel Certificates Autorités de certification racines de confiance <ul style="list-style-type: none"> Certificates Confiance de l'entreprise Autorités de certification intermédiaires <ul style="list-style-type: none"> Liste de révocation des certificats Certificates Objet utilisateur Active Directory Éditeurs approuvés Certificats non autorisés Autorités de certification racine tierce partie Personnes autorisées Émetteurs d'authentification de client Autres personnes Local NonRemovable Certificates MSIEHistoryJournal Demandes d'inscription de certificat Racines de confiance de carte à puce 																																																																			
<table border="1"> <thead> <tr> <th>Délivré à</th> <th>Délivré par</th> <th>Date d'expir:</th> </tr> </thead> <tbody> <tr> <td> Baltimore CyberTrust Root</td> <td>Baltimore CyberTrust Root</td> <td>13/05/2025</td> </tr> <tr> <td> Bitdefender Personal CA.Net-Defender</td> <td>Bitdefender Personal CA.Net-Defender</td> <td>06/10/2028</td> </tr> <tr> <td> Certigna</td> <td>Certigna</td> <td>29/06/2027</td> </tr> <tr> <td> Certigna Root CA</td> <td>Certigna Root CA</td> <td>01/10/2033</td> </tr> <tr> <td> Certinomis - Autorité Racine</td> <td>Certinomis - Autorité Racine</td> <td>17/09/2028</td> </tr> <tr> <td> Certinomis - Root CA</td> <td>Certinomis - Root CA</td> <td>21/10/2033</td> </tr> <tr> <td> Certum CA</td> <td>Certum CA</td> <td>11/06/2027</td> </tr> <tr> <td> Certum Trusted Network CA</td> <td>Certum Trusted Network CA</td> <td>31/12/2029</td> </tr> <tr> <td> Chambers of Commerce Root - 2008</td> <td>Chambers of Commerce Root - 2...</td> <td>31/07/2038</td> </tr> <tr> <td> ChamberSign</td> <td>ChamberSign</td> <td>21/06/2031</td> </tr> <tr> <td> ChamberSign</td> <td>ChamberSign</td> <td>21/06/2031</td> </tr> <tr> <td> ChamberSign France</td> <td>ChamberSign France</td> <td>22/10/2032</td> </tr> <tr> <td> ChamberSign France</td> <td>ChamberSign France</td> <td>16/10/2032</td> </tr> <tr> <td> ChamberSign France</td> <td>ChamberSign France</td> <td>16/10/2032</td> </tr> <tr> <td> Class 2 Primary CA</td> <td>Class 2 Primary CA</td> <td>07/07/2019</td> </tr> <tr> <td> Class 3 Public Primary Certification Authority</td> <td>Class 3 Public Primary Certificatio...</td> <td>02/08/2028</td> </tr> <tr> <td> COMODO Certification Authority</td> <td>COMODO Certification Authority</td> <td>01/01/2031</td> </tr> <tr> <td> COMODO RSA Certification Authority</td> <td>COMODO RSA Certification Auth...</td> <td>19/01/2038</td> </tr> <tr> <td> Copyright (c) 1997 Microsoft Corp.</td> <td>Copyright (c) 1997 Microsoft Corp.</td> <td>31/12/1999</td> </tr> </tbody> </table>								Délivré à	Délivré par	Date d'expir:	Baltimore CyberTrust Root	Baltimore CyberTrust Root	13/05/2025	Bitdefender Personal CA.Net-Defender	Bitdefender Personal CA.Net-Defender	06/10/2028	Certigna	Certigna	29/06/2027	Certigna Root CA	Certigna Root CA	01/10/2033	Certinomis - Autorité Racine	Certinomis - Autorité Racine	17/09/2028	Certinomis - Root CA	Certinomis - Root CA	21/10/2033	Certum CA	Certum CA	11/06/2027	Certum Trusted Network CA	Certum Trusted Network CA	31/12/2029	Chambers of Commerce Root - 2008	Chambers of Commerce Root - 2...	31/07/2038	ChamberSign	ChamberSign	21/06/2031	ChamberSign	ChamberSign	21/06/2031	ChamberSign France	ChamberSign France	22/10/2032	ChamberSign France	ChamberSign France	16/10/2032	ChamberSign France	ChamberSign France	16/10/2032	Class 2 Primary CA	Class 2 Primary CA	07/07/2019	Class 3 Public Primary Certification Authority	Class 3 Public Primary Certificatio...	02/08/2028	COMODO Certification Authority	COMODO Certification Authority	01/01/2031	COMODO RSA Certification Authority	COMODO RSA Certification Auth...	19/01/2038	Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	31/12/1999
Délivré à	Délivré par	Date d'expir:																																																																	
Baltimore CyberTrust Root	Baltimore CyberTrust Root	13/05/2025																																																																	
Bitdefender Personal CA.Net-Defender	Bitdefender Personal CA.Net-Defender	06/10/2028																																																																	
Certigna	Certigna	29/06/2027																																																																	
Certigna Root CA	Certigna Root CA	01/10/2033																																																																	
Certinomis - Autorité Racine	Certinomis - Autorité Racine	17/09/2028																																																																	
Certinomis - Root CA	Certinomis - Root CA	21/10/2033																																																																	
Certum CA	Certum CA	11/06/2027																																																																	
Certum Trusted Network CA	Certum Trusted Network CA	31/12/2029																																																																	
Chambers of Commerce Root - 2008	Chambers of Commerce Root - 2...	31/07/2038																																																																	
ChamberSign	ChamberSign	21/06/2031																																																																	
ChamberSign	ChamberSign	21/06/2031																																																																	
ChamberSign France	ChamberSign France	22/10/2032																																																																	
ChamberSign France	ChamberSign France	16/10/2032																																																																	
ChamberSign France	ChamberSign France	16/10/2032																																																																	
Class 2 Primary CA	Class 2 Primary CA	07/07/2019																																																																	
Class 3 Public Primary Certification Authority	Class 3 Public Primary Certificatio...	02/08/2028																																																																	
COMODO Certification Authority	COMODO Certification Authority	01/01/2031																																																																	
COMODO RSA Certification Authority	COMODO RSA Certification Auth...	19/01/2038																																																																	
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	31/12/1999																																																																	
Le magasin Autorités de certification racines de confiance contient 80 certificats.																																																																			

Le certificat
d'identité
numérique

Format du certificat

PKI et Autorité de
certification

Génération d'un
certificat

Conteneur de
certificats

Exemples de
certificats

Révocation d'un
certificat

Validité d'un
certificat

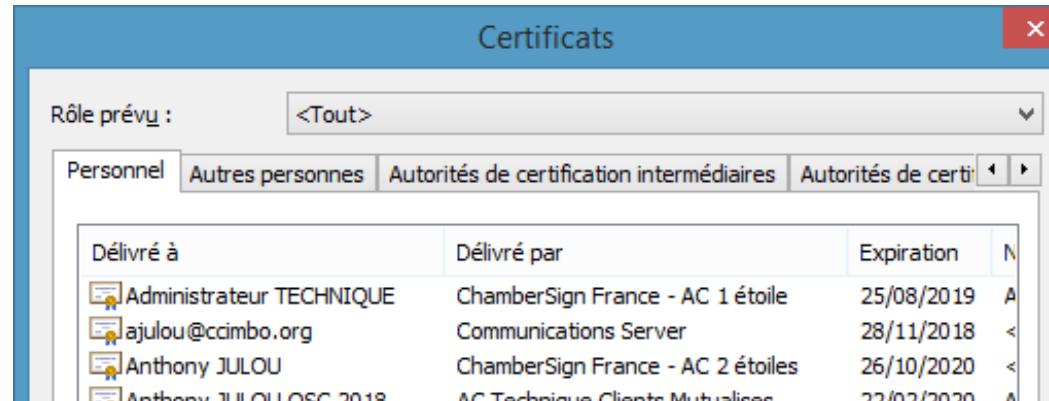
□ Chapitre 3 : Le certificat numérique

Magasins de certificats

Internet Explorer: « Outils-> Options Internet -> Contenu -> Certificats »

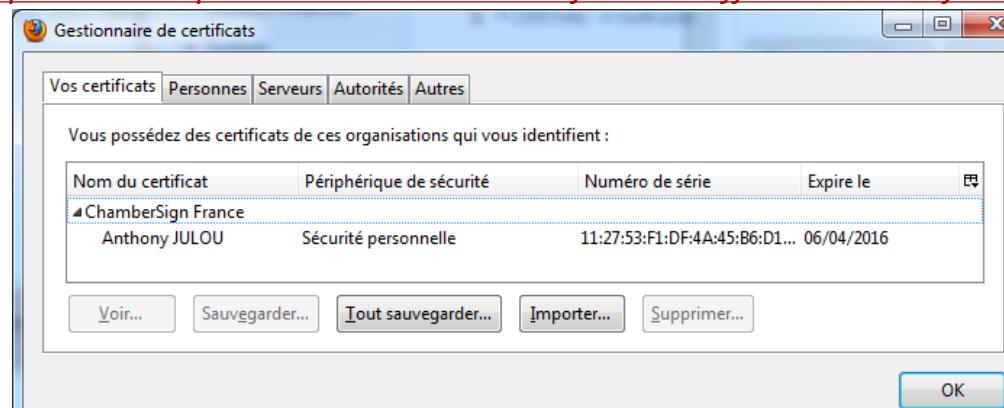
Edge : « Paramètres -> Confidentialité et services -> Confidentialité -> Gérer les certificats »

Chrome: « Paramètres -> Confidentialité et sécurité -> Gérer les certificats »



Firefox / Thunderbird :

« Outils-> Options-> Vie privée et sécurité -> Certificats -> Afficher les certificats »



Java : « Panneau de configuration -> Java -> Sécurité -> Gérer les certificats »



Chapitre 3 : Le certificat numérique

Exemples de certificats (2/2)

Certificat de personne
(Vue Windows)

Certificat

Général Détails Chemin d'accès de certification

Afficher : <Tout>

Champ	Valeur
Numéro de série	11 21 23 aa b5 e9 46 c4 58 52...
Algorithme de signature	sha256RSA
Algorithme de hachage de l...	sha256
Émetteur	ChamberSign France - AC 2 ét...
Valide à partir du	jeudi 25 février 2016 19:33:46
Valide jusqu'au	lundi 25 février 2019 19:33:46
Objet	0001, Anthony JULOU, Chef d...
Clé publique	RSA (2048 Bits)

SERIALNUMBER = 0001
CN = Anthony JULOU
T = Chef de projet
OU = Direction Technique ChamberSign France
OU = 0002 43370247900026
OU = CHAMBERSIGN FRANCE
O = CHAMBERSIGN FRANCE
L = LYON 2EME ARRONDISSEMENT
C = FR

Modifier les propriétés... Copier dans un fichier...

En savoir plus sur les [détails du certificat](#).

OK

Certificat de serveur (SSL)
(Vue Firefox)

bdc3939.service-public.fr	Certigna Services CA	Certigna
---------------------------	----------------------	----------

Nom du sujet
Pays FR
Localité PARIS 15
Organisation DILA
Unité organisationnelle 0002 13000918600011
NTRFR-13000918600011
Nom courant bdc3939.service-public.fr
Numéro de série S9503003

Nom de l'émetteur
Pays FR
Organisation DHIMYOTIS
Unité organisationnelle 0002 48146308100036
NTRFR-48146308100036
Nom courant Certigna Services CA

Validité
Pas avant 10/07/2018 à 08:44:04 (heure normale d'Europe centrale)
Pas après 15/08/2020 à 15:43:08 (heure normale d'Europe centrale)

Noms alternatifs du sujet
Nom DNS bdc3939.service-public.fr
Nom DNS lannuaire.service-public.fr
Nom DNS lecomarquage.service-public.fr
Nom DNS www.service-public.fr

Informations sur la clé publique
Algorithme RSA
Taille de la clé 2048

Le certificat
d'identité
numérique

Format du certificat

PKI et Autorité de
certification

Génération d'un
certificat

Conteneur de
certificats

Exemples de
certificats

Révocation d'un
certificat

Validité d'un
certificat

□ Chapitre 3 : Le certificat numérique

Révocation d'un certificat

Définition : Moyen d'annuler la validité d'un certificat pour différentes raisons

Déroulement type:

1. le porteur s'authentifie sur un portail
2. sélectionne le certificat à révoquer
3. répond aux questions de révocation personnelles
4. confirme la révocation
5. L'AC met à jour la liste de révocation (CRL) avec
 1. le n° de série du certificat
 2. la raison de révocation (*si non confidentielle*)
 3. L'émetteur du certificat
 4. la date de révocation
6. L'AC signe la liste de révocation et la publie sur une URL

□ Chapitre 3 : Le certificat numérique

Révocation d'un certificat

CRL (Certificate Revocation List) contient aussi

- Le DN de l'émetteur du certificat
- La date de début et de fin de publication de la CRL
- Un numéro de série unique incrémenté
- La signature électronique réalisée par l'AC avec les algorithmes associés

Principe de confiance :

- 1) Toute application doit vérifier la non révocation du certificat dans la CRL avant de signer/authentifier
 - 2) Une signature n'est valable que si le document a été signé avec un certificat non révoqué
- cela nécessite de comparer les dates :
- Signature invalide si date révocation < date signature**

Le certificat
d'identité
numérique

Format du certificat

PKI et Autorité de
certification

Génération d'un
certificat

Conteneur de
certificats

Exemples de
certificats

Révocation d'un
certificat

Validité d'un
certificat

Chapitre 3 : Le certificat numérique

Révocation d'un certificat

Exemple d'une CRL (Fichier téléchargé, ouvert avec Firefox)

Entête et validité

Liste de révocation des certificats

Général Liste de révocation

Informations sur la liste de révocation des certificats

Champ	Valeur
Emetteur	ChamberSign France - AC 1 étoile,
Date d'effet	dimanche 2 décembre 2018 10:00
Prochaine mise à jour	jeudi 6 décembre 2018 10:00:00
Algorithme de signature	sha256RSA
Algorithme de hachage ...	sha256
Numéro de la liste de ré...	00a387
Identificateur de clé de ...	ID de la clé=ad92fb468c838f3cd0
Empreinte numérique	f7e2ebd2348a81634d2a3af45a04

Valeur :

ID de la clé=ad92fb468c838f3cd0b9da1e726d393db58dc033

Liste des révocations

Liste de révocation des certificats

Général Liste de révocation

Certificats révoqués :

Numéro de série	Date de révocation
1121d40daf585ed57c92d7f89f0536d...	vendredi 11 décembre 201...
112176c7bbe6e8b8b82d547a698ac4...	samedi 2 janvier 2016 1...
112158a3b4a5867d5ddf1070d16bc...	mercredi 6 janvier 2016 ...
1121f0519210333b3d318cff4bca8b0...	mercredi 13 janvier 201...

Entrée de révocation

Champ	Valeur
Numéro de série	112158a3b4a5867d5ddf1070d16bc...
Date de révocation	mercredi 6 janvier 2016 18:13:29

Valeur :

□ Chapitre 3 : Le certificat numérique

Révocation d'un certificat

2. SERVICE OCSP (*Online Certificate Status Protocol*) – RFC 6960

Protocole internet pour vérifier la validité en **temps réel**

Avantages par rapport aux CRL:

- a) **Statut du certificat à jour**, en temps réel
- b) **Allègement du trafic réseau** : Plus besoin de télécharger une CRL (*Taille conséquente si nombre de révocations important*)
- c) **Confidentialité**: CRL communiquent des n° série sur Internet

Consultation du service OCSP

- a) Le client récupère l'URL du service dans l'extension du certificat
- b) Envoi d'une requête OCSP avec le **n° de série et l'AC**
- c) Le serveur OCSP vérifie l'état, retourne l'état (Valide ou révoqué avec la date) dans une réponse OCSP signée par un certificat d'AC
- d) Le client vérifie la date de signature avec la date de l'état du certificat .

Chapitre 3 : Le certificat numérique

Révocation d'un certificat

Points d'informations de révocation dans le certificat

CRL

Certificat

Général Détails Chemin d'accès de certification

Afficher : <Tout>

Champ	Valeur
Stratégies de certificat	[1]Stratégie du certificat
Autre nom de l'émetteur	Nom RFC822=autorite:chan
Instructions de certificat qualifié	30 14 30 08 06 04 00 8e 4
Points de distribution de la liste de révocation des certificats	[1]Point de distribution de la liste de révocation des certificats
Accès aux informations de l'autorité	[1]Accès aux informations sur l'autorité
Identificateur de la clé du sujet	836681678bbb3be9f50a2546
Identificateur de clé de l'autorité	TD de la clé=q62dhd6q66ed58

[1]Point de distribution de la liste de révocation des certificats

Nom du point de distribution :

Nom complet :

URL=http://crl.chambersign.fr/crl/rgs/lcr-directes/crl-3.crl
 URL=ldap://ldap.chambersign.fr/CN=ChamberSign France - AC 3 ♦toiles,OU=0002 433702479,O=ChamberSign France,C=FR?certificaterevocationlist;binary?base?objectclass=pkICAO
 (ldap://ldap.chambersign.fr/CN=ChamberSign%20France%20-%20AC%203%20-%20E9toiles,OU=0002%

OK

OCSP

Certificat

Général Détails Chemin d'accès de certification

Afficher : <Tout>

Champ	Valeur
Stratégies de certificat	[1]Stratégie du certificat : Idem
Autre nom de l'émetteur	Nom RFC822=autorite:chan
Instructions de certificat qualifié	30 14 30 08 06 04 00 8e 4
Points de distribution de la liste de révocation des certificats	[1]Point de distribution de la liste de révocation des certificats
Accès aux informations de l'autorité	[1]Accès aux informations sur l'autorité
Identificateur de la clé du sujet	836681678bbb3be9f50a2546
Identificateur de clé de l'autorité	TD de la clé=q62dhd6q66ed58

[1]Accès aux informations sur l'autorité

Méthode d'accès=Protocole d'état de certificat en ligne (1.3.6.1.5.5.7.48.1)

Autre nom :

URL=http://ocsp.chambersign.fr

OK

Le certificat
d'identité
numérique

Format du certificat

PKI et Autorité de
certification

Génération d'un
certificat

Conteneur de
certificats

Exemples de
certificats

Révocation d'un
certificat

Validité d'un
certificat

□ Chapitre 3 : Le certificat numérique

Validité d'un certificat

1. Vérification de la confiance

- L'AC est-elle de confiance pour l'usage ?

2. Vérification technique des signatures

- Vérifier la signature du certificat effectuée par l'AC fille:
 - Utiliser la clé publique de l'AC Fille pour déchiffrer l'empreinte du certificat.
 - Comparer les 2 empreintes.
- Vérifier la signature de l'AC Fille par l'AC Racine

3. Vérification des dates de validité

- Dates certificat et de ses racines sont-elles toujours valides ?

4. Vérification de révocation

- Le certificat n'est **ni dans la CRL courante ni** indiqué comme révoqué **dans une réponse OCSP**
- Les certificats de chaîne de confiance ne sont pas dans les ARL (*Authority Revocation List*)

- 1) La confiance numérique
- 2) Bases cryptographiques
- 3) Le certificat numérique
- 4) Fonctions de signature
- 5) Formats de signature
- 6) Les logiciels
- 7) Programmation
- 8) Applications exemples
- 9) Cadre légal et juridique
- 10) Conclusion

PKI, services de confiance et signature électronique

Chapitre 4 : Fonctions de signature



- Principe de la signature électronique
- Principe du scellement
- Chiffrement par certificat
- Principe de l'authentification forte
- Fonctionnement https
- Authentification x509 sur https
- Horodatage

Définition

Caractéristiques

Principe signature

Principe du
scellementChiffrement par
certificatPrincipe de
l'authentification
forteFonctionnement
httpsAuthentification
x509 sur https

Horodatage

□ Chapitre 4 : Fonctions de signature

Définition de la signature électronique

- Mécanisme fiable permettant :
 - de garantir l'intégrité d'un document électronique
 - d'en authentifier l'auteur comme pour une signature manuscrite
- But:
 - Apporter confiance et sécurité dans les échanges numériques dans un cadre légal et juridique
 - Sceller un accord entre des parties en dématérialisant les actes

Caractéristiques de la signature

- **Authentique** : L'identité du signataire est retrouvée de manière certaine.
- **Infalsifiable** : La signature ne peut pas être falsifiée par quelqu'un d'autre.
- **Non réutilisable**: Elle fait partie du document signé et ne peut être copiée sur un autre document.
- **Inaltérable** : Une fois qu'il est signé, on ne peut plus le modifier
- **Non réputation (irrévocable)** : La personne qui a signé ne peut le nier.

Chapitre 4 : Fonctions de signature

Principe de la signature électronique

Rappels de la problématique:

- Authentification / non répudiation / intégrité

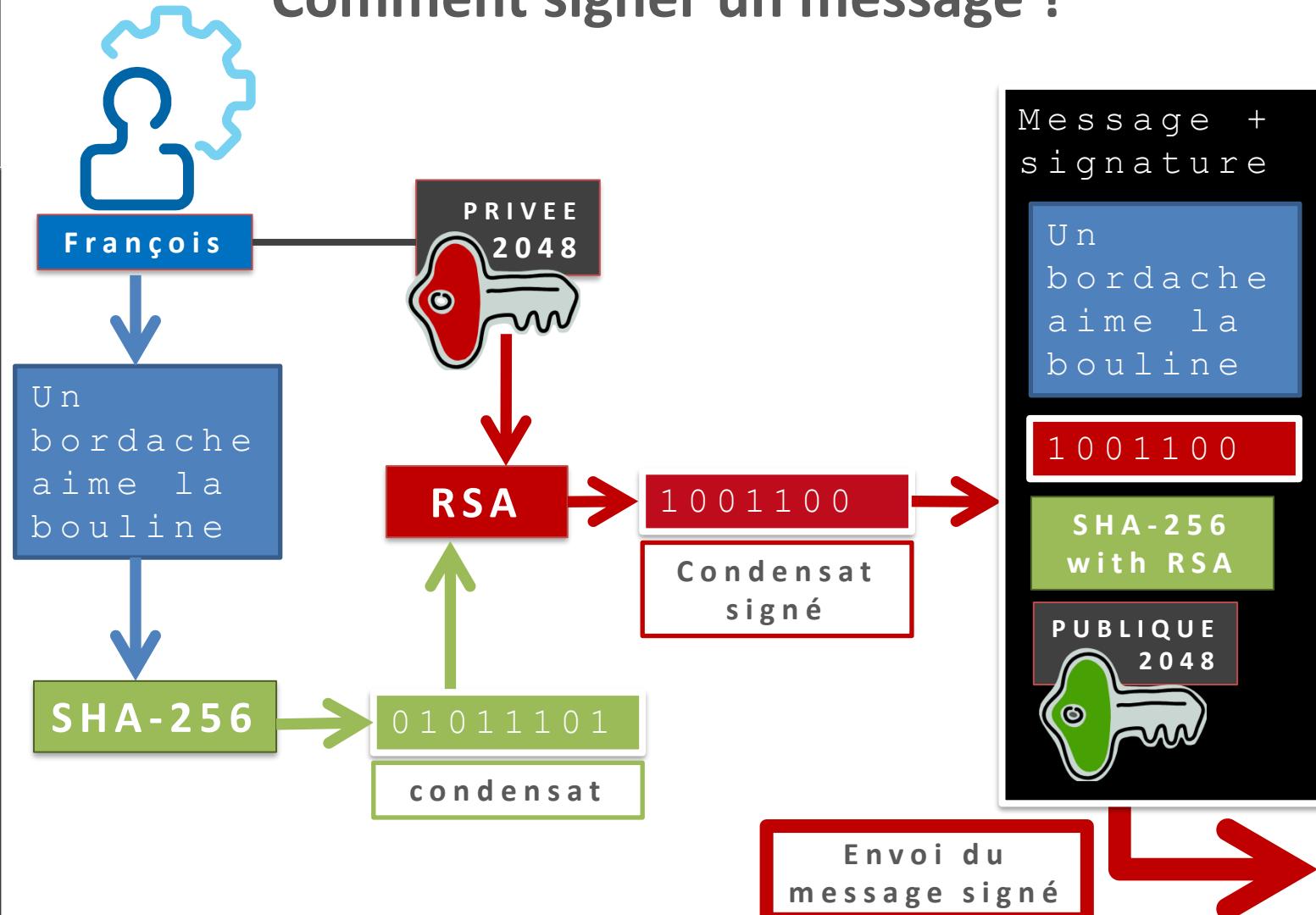
Comment faire ? En combinant les fonctions de

1. hachage
2. chiffrement/déchiffrement asymétrique

Propriété	Définition	Comment ?
Intégrité	Le message n'a pas été modifié pendant son transport	Fonction de hachage <i>Comparer le haché avant émission et après</i>
Authentification	Le message provient de la bonne personne	Cryptographie asymétrique <i>Déchiffrer un message avec une clé publique identifie l'émetteur par sa clé privée correspondante</i>
Non répudiation	Elle ne peut nier l'avoir émis	

Principe de la signature électronique

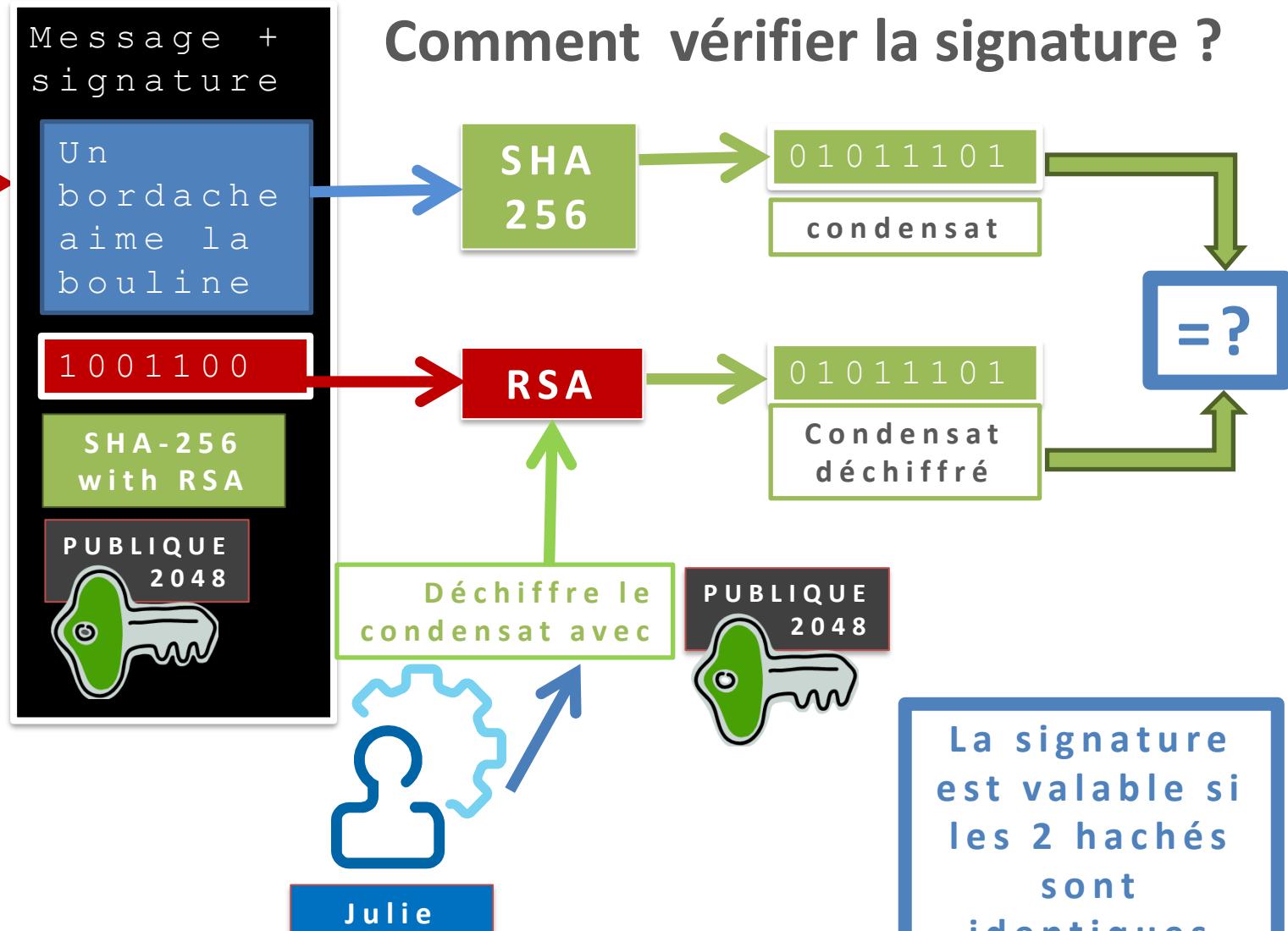
Comment signer un message ?



Chapitre 4 : Fonctions de signature

Principe de la signature électronique

Comment vérifier la signature ?



Chapitre 4 : Fonctions de signature

Principe de la signature électronique

Comment vérifier la signature ?

1. Vérifications cryptographiques (*schéma précédent*)
2. Chaîne de confiance (AC fiable ?)
3. Certificat valide ?
 - Champs bien formés ?
 - Non révoqué au moment de la signature ?
 - L'usage de la clé privée est-il bien « signature » ?
4. Vérification juridique
 - Signature acceptable dans ce contexte (Conforme à la politique de signature ou à la législation ?)
 - Signataire autorisé à signer ? (*ex: marchés publics*)

□ Chapitre 4 : Fonctions de signature

Principe du scellement

Utilisation du chiffrement symétrique combinant

- Les propriétés du hachage
- Le chiffrement/déchiffrement **symétrique**

Permet:

- Intégrité des données
- Authentification de l'origine des données

Ne permet pas:

- **La non-réputation** (Apportée par un certificat)

Résultat obtenu:

- Un sceau ou MAC (Message Authentication Code)

Applications: logiciels, traces légales ...

Chiffrement par certificat

Principe et rappel: Chiffrement asymétrique

1. François chiffre avec la clé publique du certificat de Julie

→ la confidentialité est garantie car

2. Julie est seule à pouvoir déchiffrer avec sa clé privée

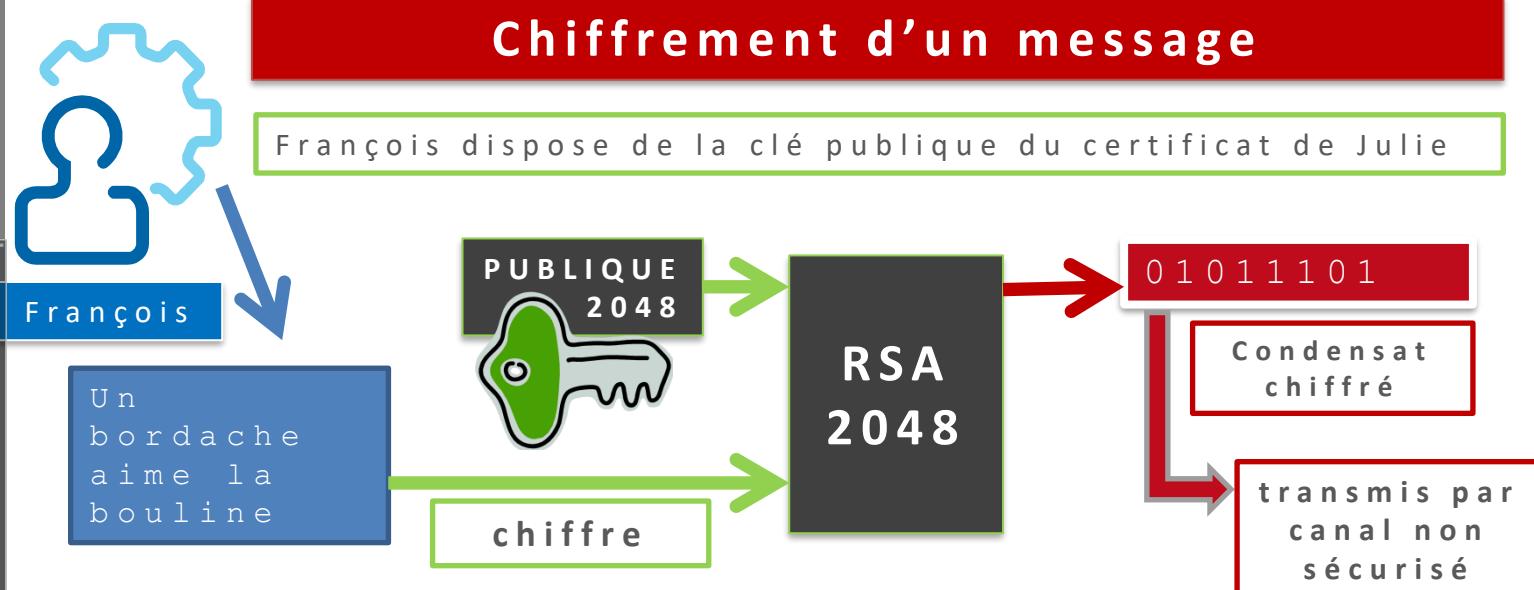
Contraintes:

- Disposer de la clé publique de son destinataire (*envoi de la clé par mail signé*)
- Ne pas perdre la clé privée → impossible de déchiffrer (*Sauvegarde, séquestre de la clé*)

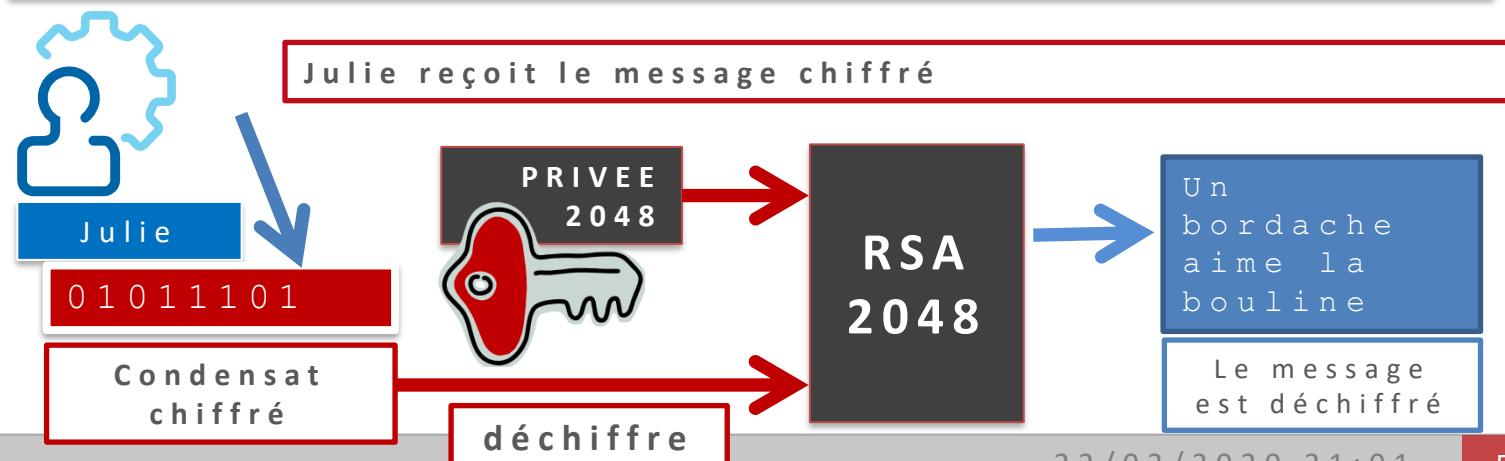
Chapitre 4 : Fonctions de signature

Chiffrement par certificat

Chiffrement d'un message



Déchiffrement du message



Principe de la
signature
électronique

Principe du
scellement

Chiffrement par
certificat

Principe de
l'authentification
forte

Fonctionnement
https

Authentification
x509 sur https

Horodatage

□ Chapitre 4 : Fonctions de signature

Chiffrement par certificat

Limitation: Le chiffrement asymétrique est trop gourmand en temps de calcul lorsque les contenus sont trop volumineux

Solution ? Combiner:

- 1. Le chiffrement asymétrique**
(authentification)
- 2. Le chiffrement symétrique** (confidentialité)

Applications:

- Applications et communications sécurisées
(VPN, https, ftps, pops, ssh ...)
- Chiffrement de fichiers & archives, mails ...

□ Chapitre 4 : Fonctions de signature

Principe de l'authentification forte

Utiliser un certificat sur un service sécurisé pour

- s'authentifier
- Établir un canal sécurisé pour l'échange chiffré (*confidentialité*)

Principe

- Signature électronique d'un défi
 - Algorithmes exemples: « **SHA256 with RSA** »
- Permet d'authentifier le détenteur du certificat
- Puis chiffrement symétrique du contenu échangé
 - Algorithme exemple: « **AES 128** »
 - Renouveler régulièrement la clé secrète

Fonctionnement https

SSL : Secure Socket Layer (remplacé par **TLS** *Transport Layer Security* en 2001) **TLS 1.3** (2018)

Protocole réseau sécurisé (Entre la couche transport et la couche application du modèle ISO)

→ **Données personnelles** (cookies, id de session, login, mots de passe, géolocalisation, formulaires postés ...)

Techniques du protocole utilisées :

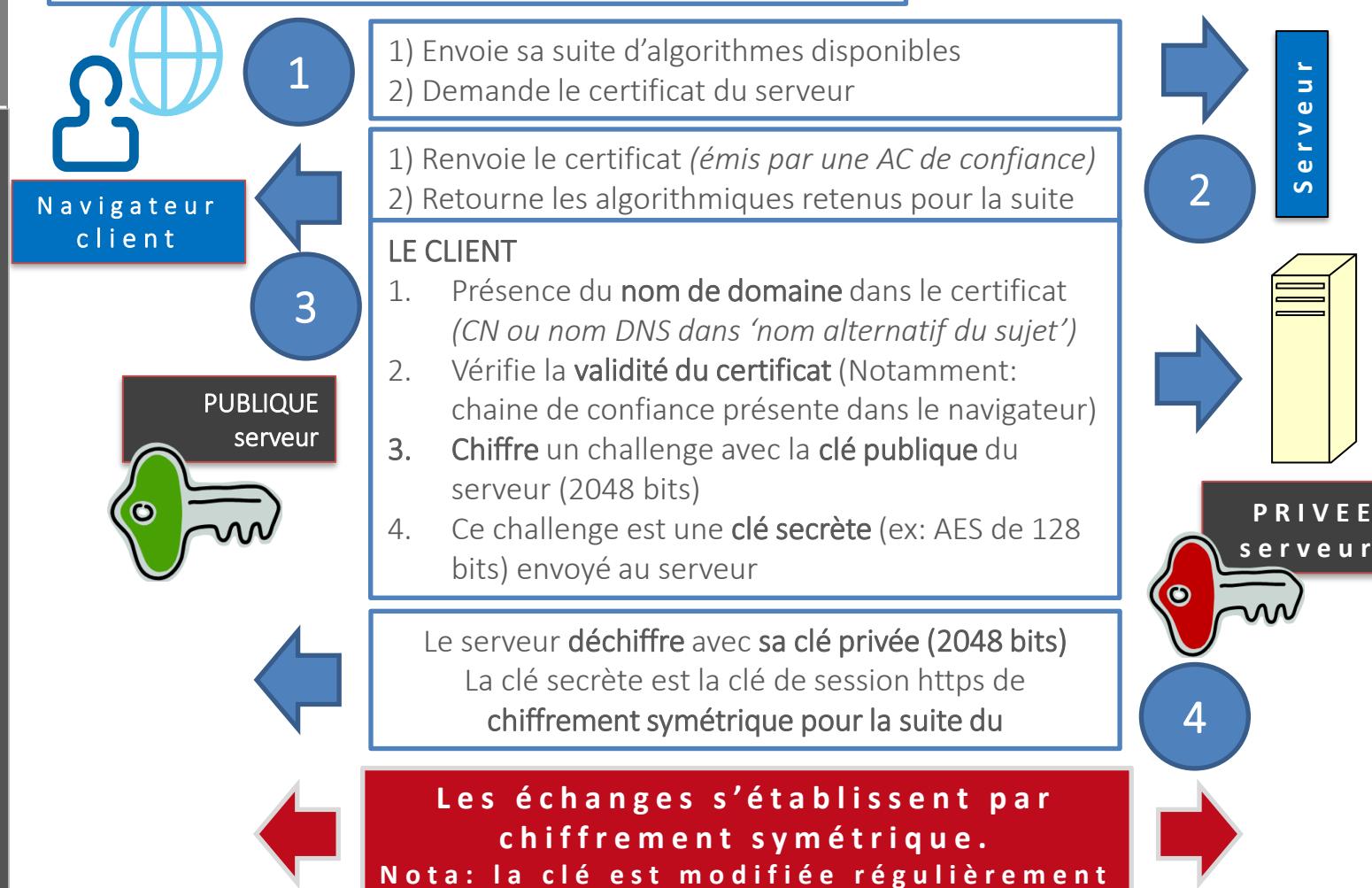
1. **Chiffrement symétrique** → Confidentialité des données échangées (*n° carte bleue...*)
2. **Algorithme de hash** → Intégrité des données
3. **Authentification**
 1. du **serveur** avec un certificat serveur type SSL
 2. du **client** avec un certificat client (authentification forte)

□ Chapitre 4 : Fonctions de signature

Fonctionnement https

Le client doit authentifier le serveur...

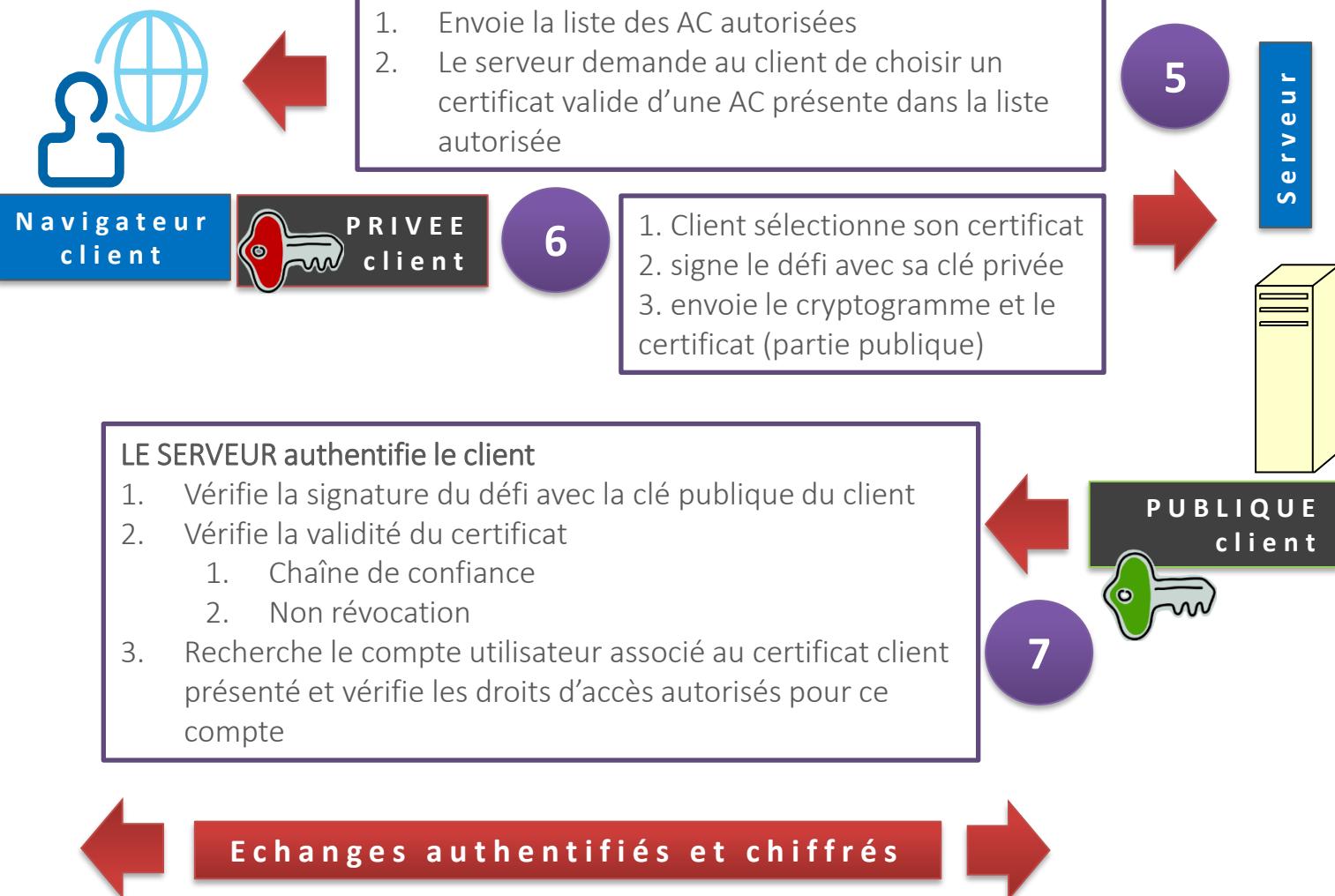
Requête DNS locale ou vers le FAI pour obtenir l'IP du serveur



Chapitre 4 : Fonctions de signature

Authentification x509 sur https

Le serveur doit à son tour authentifier le client



Principe de la
signature
électronique

Principe du
scellement

Chiffrement par
certificat

Principe de
l'authentification
forte

Fonctionnement
https

Authentification
x509 sur https

Horodatage

□ Chapitre 4 : Fonctions de signature

Horodatage

Problématique

Comment être sûr de la date de signature d'un document ? Le certificat avait-il été révoqué avant la signature ? Valeur de la signature ?

Autorité d'Horodatage (AH)

- Certifie avec un **jeton d'horodatage** l'heure exacte (NTP *Network Time Protocol*) ajoutée à la signature du document – RFC 3161

Format du jeton certifié:

1. Hash du document horodaté
2. Date et heure provenant du serveur
3. Scellement par clé privée de l'AH
4. Certificat de l'AH pour vérification

- 1) La confiance numérique
- 2) Bases cryptographiques
- 3) Le certificat numérique
- 4) Fonctions de signature
- 5) Formats de signature
- 6) Les logiciels
- 7) Programmation
- 8) Applications exemples
- 9) Cadre légal et juridique
- 10) Conclusion

Chapitre 5 :

Formats de signature

Signature valid

Digitally signed by Andis Everts
Date: 2012.02.01 08:16:34 EET



- Format d'une signature
- Vocabulaire technique
- Normalisation
- Formats normés
- Format CMS
- Format CAdES
- Format XML-Dsig
- Format XAdES
- Format PAdES

Format d'une signature

Rappel: la signature est le résultat d'un calcul cryptographique

Que contient une signature ?

1. Suite chiffrée (condensat) représentant le haché crypté par la clé privée (*sha256withRSA*)
2. Certificat du signataire (*X509*)
3. Chaîne de confiance du certificat (AC)
4. Jeton d'horodatage certifiant l'horaire de signature
5. Preuve de non révocation du certificat du signataire au moment de la signature (CRL)

Format d'une
signature

Vocabulaire
technique

Normalisation

Formats normés

Format CMS

Format CAdES

Format XML-Dsig

Format XAdES

Format PAdES

□ Chapitre 5 : Formats de signature

Vocabulaire technique

X509 V3 : Norme pour le format de certificat numérique

ASN 1: standard pour définir une structure de données

Normes PKCS (*Public Key Cryptographic Standard*): formats, algorithmes et protocoles définis par la société RSA Security

PKCS1 : recommandations pour l'implémentation de systèmes crypto utilisant RSA

PKCS7 : syntaxe de messages cryptographiques (certificat, signature)

PKCS8 : syntaxe pour des données mémorisant des clés privées

PKCS10 : syntaxe pour une requête de certification (CSR)

PKCS11 : API (*Application Programming Interface*) pour réaliser des fonctions cryptographiques sur des supports crypto

PKCS12 : fichier comprenant le **certificat X509 + clé privée + clé publique** (*extension de fichier: *.pfx ou *.p12*)

□ Chapitre 5 : Formats de signature

Vocabulaire technique

Fichier .CER, .DER, .CRT: contient un certificat (sans la clé privée) au format DER ou PEM

Encodages

1. DER (*Distinguished Encoding Rules*)

Encodage binaire de l'ITUT (*International Telecommunication Union*) pour les structures de données ASN.1

2. PEM (*Privacy Enhanced Mail*)

Encodage des structures ASN.1 au format base 64

Base 64: codage utilisant 64 caractères (A-Z a-z 0-9 et 3 autres: +/=)

Exemple de clé privée au format PEM

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC, EEC5FF75AC6E6743
azdowx+bhgR8ff5EPH8DFQK+zVta4YOa3FpBJsU2ykGzSOihPaY2dNQFJPnJgDh
2CNVuz0M6qc1lPlsshUwTYeMyD0kqrWnah9dXMTNI4O+n2KQ4WIqEpS+gCFjmIlR
hgAFTwnnI/IITY0w1WGPh3A8YcySTMI3I9hs6qxkYfrJsxoxtgNo109wgg81C6N
cVnAZIe0v+G6RUFMVir2n7D9PzEM/gFCCOWtnBXcklzclAUJ1tjhQ8Yjd3G1uVgB
Tqf0bcWWPTWjw0vmO6jbPbxcn6f8xIm9YfqhY/9H65qNVABcbvJd7A==
-----END RSA PRIVATE KEY-----
```

□ Chapitre 5 : Formats de signature

Normalisation

IETF (*Internet Engineering Task Force*)

- PKIX (*Public-Key Infrastructure X.509*) est le groupe technique chargé des normes cryptographiques
- Rédige des normes techniques: les RFC (*Request For Comments*) RFC 5280, 2527, 3370, 3161, 3270, 6960 ...

W3C (*World Wide Web Consortium*)

- Normalise les technologies du web
Exemple: HTML, XHTML, XML, XML-DSig, CSS, PNG, SVG, SOAP...

ETSI (*European Telecommunications Standards Institute*)

- Produit des normes de télécommunications
Exemples grand public: DECT, GSM, UMTS (3G)

Formats de signature normés

- **CMS (Cryptographic Message Syntax)**
 - RFC 5652 de PKIX définissant un « *Format d'enveloppe cryptographique CMS* » pour signer des fichiers
- **XML-Dsig (XML Syntax for Digital Signature)**
 - Norme année 2000 par le W3C
 - Signer des documents au format XML
- **Normes actuelles ETSI (Directive européenne)**
 - **CAdES (CMS Advanced Electronic Signatures)**
 - Améliorations de CMS
 - **XAdES (XML Advanced Electronic Signatures)**
 - Améliorations de XML-Dsig
 - **PAdES (PDF Advanced Electronic Signatures)**
 - Améliorations d'Adobe PDF et ISO 32000-1

□ Chapitre 5 : Formats de signature

Format CMS

Issu du standard PKCS#7 et S/MIME

(Secure/Multipurpose Internet Mail Extensions) :

1. syntaxe générale des messages signés ou chiffrés encodés en PEM ou DER
2. Récursivité (ex: *Chiffrement de données signées*)
3. Format des enveloppes (*fichiers*)
 - .p7s : contient des données signées
 - .p7m: contient des données chiffrées

Format d'un message signé

```
SignedData ::= SEQUENCE {  
    version INTEGER,  
    digestAlgorithms DigestAlgorithmIdentifiers,  
    contentInfo ContentInfo,  
    certificates [0] IMPLICIT Certificates OPTIONAL,  
    crls [1] IMPLICIT CertificateRevocationLists OPTIONAL,  
    signerInfos SignerInfos [...]}
```

□ Chapitre 5 : Formats de signature

Format CAdES (1/2)

CAdES : CMS Advanced Electronic Signature

1. Permet la signature :

- « **détachée** » : le document et la signature sont 2 fichiers séparés
- « **enveloppée** » : le tout dans un seul fichier

2. Signature multiple permise

3. Conservation longue durée selon *directive européenne 1999/93/EC*

→ **Signature non visible graphiquement**

□ Chapitre 5 : Formats de signature

Format CAdES (2/2)

Différentes versions/options du format:

CAdES-T : (*Timestamp*) Extension à CAdES pour se protéger de la répudiation => horodatage

CAdES-C : (*Complete*) Extension à CAdES-T pour ajouter les **références** aux certificats et LCR

CAdES-X : (*Extended*) Inclut un horodatage pour valider le format CADES-C (compromission AC)

CAdES-X-L : (*Extended Long Term*): Intégration des certificats et LCR au moment de la signature

CAdES-A : inclut une estampille d'horodatage en vue de l'Archivage sur de nombreuses années

Format XML-Dsig (1/3)

Rappels sur XML:

- **XML (*Extensible Markup Language*)**
- Langage de balisage extensible « < » « /> »
- Définir son propre langage avec sa grammaire
- *Utilisation: webservices, xhtml, rss, EDI...*

XML-Dsig : Digital Signature for XML

1. Souplesse du XML pour signer certaines parties d'un document
2. Forme canonique

Référence de la spécification W3C (2013)

<http://www.w3.org/TR/xmldsig-core/>

Format XML-Dsig (2/3)

Comment procéder ?

1. Déterminer quelle(s) ressource(s) à signer
<Reference>
2. Calculer le haché de chaque ressource
<DigestMethod> et <DigestValue>
3. Incorporer toutes les ressources dans un élément de signature <SignedInfos> avec son type d'algorithme
4. Signer le nœud <SignedInfos> ajouter la valeur dans <SignatureValue>
5. Ajouter le certificat qui a signé dans <KeyInfo>

Format d'une
signatureVocabulaire
technique

Normalisation

Formats normés

Format CMS

Format CAdES

Format XML-Dsig

Format XAdES

Format PAdES

□ Chapitre 5 : Formats de signature

Format XML-Dsig (3/3)

```
<?xml version="1.0" encoding="UTF-8"?>

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo Id="foobar">
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1" />
    <Reference URI="http://www.abccompany.com/news/2000/03_27_00.htm">
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
    </Reference>
    <Reference URI="http://www.w3.org/TR/2000/WD-xmldsig-core-20000228/signature-example.xml">
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <DigestValue>UrXLDLBIta6skoV5/A8Q38GEw44=</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>MC0E~LE=</SignatureValue>
  <KeyInfo>
    <X509Data>
      <X509SubjectName>CN=Ed Simon, O=XMLSec Inc., ST=OTTAWA, C=CA</X509SubjectName>
      <x509Certificate>MIID5jCCA0+gA...1VN</x509Certificate>
    </X509Data>
  </KeyInfo>
```

□ Chapitre 5 : Formats de signature

Format XAdES

XAdES : XML Advanced Electronic Signature est une extension de XML-Dsig avec en plus:

- moyen d'identifier les politiques de la signature
 - date de la signature
- <Unsigned Properties> informations non signées :
- Le format des objets signés
 - Le type d'engagement des signataires
 - Le rôle du signataire et lieu où le rôle est valable
 - cachets d'horodatage
 - chaîne de certificats et liste de révocation ou réponse OCSP.

1. **Signature multiple « enveloppée » ou « détachée » longue durée**

→ Signature non visible graphiquement

Formats: XAdES-T, XAdES-C, XAdES-X-L and XAdES-A

Format PAdES

PAdES (PDF Advanced Electronic Signatures)

Repose sur le format CAdES

Sur un PDF, on distingue 2 modes de signature:

1. “**Certification**” : cachet émis par le **créateur** du PDF (*ex: cachet serveur*)
2. “**Signature(s)**”: Approbation du contenu du document par un (des) signataire (s)

→ **Signature visible (ou non) spécifiée par l’ETSI**

102 718-1 avec :

- nom du signataire (CN), Organisation (O), image validant la signature

PAdES-XML : Possibilité d’intégrer du XAdES dans le PDF

- 1) La confiance numérique
- 2) Bases cryptographiques
- 3) Le certificat numérique
- 4) Fonctions de signature
- 5) Formats de signature
- 6) Les logiciels**
- 7) Programmation
- 8) Applications exemples
- 9) Cadre légal et juridique
- 10) Conclusion

□ PKI, services de confiance et signature électronique

Chapitre 6 : **Les logiciels**



- Logiciels utilisateurs
- Exemple signature PDF avec Adobe Reader
- Signature de code

Logiciels utilisateurs

A. Signature de documents

1. Format PDF (*Portable Document Format*)

■ **Document certifié** (*Signature de certification*)

- Certifier être l'auteur du document

Caractéristiques:

- Première signature du document
- 1 seule signature non visible sur le document

■ **Document signé** (*Signature d'approbation*)

- Signer pour approuver le contenu du document

Caractéristiques:

- 1 ou plusieurs signataires
- Signature(s) visible(s) ou non visible(s)

Chapitre 6 : Les logiciels

Logiciels utilisateurs

Logiciels PDF



- **Acrobat Reader**
 - Lecture d'un PDF signé
 - Signature visible (depuis version 11.0.9)
 - Format: **CAdES et PAdES norme (PDF/A-2) à partir de la version 10**
- **Acrobat Standard ou Acrobat Pro**
 - Création de documents signés ou à faire signer par un Adobe Reader et par plusieurs signataires
 - Service de signature en ligne (echoSign => parapheur)
- **JSignPdf**
 - Ajout signatures visibles
 - **Conçu en Java (librairie iText)**
- **Perfect PDF Reader et XolidoSign (CAdES), DigiSigner, Portable Signer**

Logiciels utilisateurs

2. Bureautique

▪ Microsoft Office

- Signature visible et non visible dans Word, Excel
 - Non visible dans PowerPoint
 - Format: XmlDsig depuis Office 2007
 - Format: XAdES depuis Office 2010



■ LibreOffice

- Signature visible
 - Writer (*traitement de texte*), Calc (*tableur*), Impress (*présentation*), Draw (*dessin*) et Math (*formules mathématiques*)
 - Format: XAdES, PAdES



□ Chapitre 6 : Les logiciels

Logiciels utilisateurs

B. Signature de mails

- **Format S/MIME (Secure / Multipurpose Internet Mail Extensions)**
- Signature détachée, ajoutée en PJ au format P7S
- **Attention:** l'e-mail dans le certificat doit être la même que celle configurée dans le client mail
- **Microsoft Outlook**

Récupère les certificats du magasin Windows

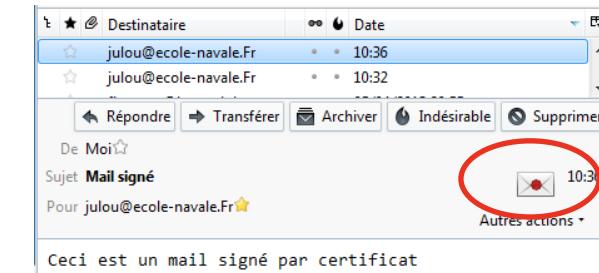
Icône « cocarde » apparaît sur l'enveloppe →



- **Thunderbird**

Magasin propre de certificats

Icône avec une enveloppe cachetée →



➔ Possibilité de chiffrer des mails

Chapitre 6 : Les logiciels

Signature PDF avec « Adobe Reader DC »

1. Ouvrir le document PDF
 2. Cliquer sur le menu « Outils » → puis sur l'icône « Certificats »
 3. Cliquer sur « Signer numériquement »
 - Placer, dessiner le rectangle de signature
 - Cliquer sur le bouton « Signer »
 5. Choisir le certificat, entrer le code pin
 - Option : *Modifier l'apparence de la signature*
 6. Choisir le nom du fichier et l'endroit pour stocker le nouveau fichier PDF signé
-
- Possibilité d'ajouter un jeton d'horodatage dans les options

□ Chapitre 6 : Les logiciels

Signature PDF avec «Adobe Reader DC»

TP 1 - VA SIM - Adobe Acrobat Reader DC

Fichier Edition Affichage Fenêtre Aide

Accueil Outils TITRE TP 1 - VA SIM x

1 / 6 147% 100% 125% 150% 175% 200% 250%

Certificats Signer numériquement Tampon temporel Valider toutes les signatures

CYBERSECURITE : PKI, services de confiance & signature électronique

TP : Signature électronique avec JAVA (3 heures)

Anthony JULOU Signature numérique de Anthony JULOU Date : 2018.11.27 10:08:26 +01'00'

Le but de ce TP est d'implémenter une signature électronique dans un document PDF en utilisant l'API JCA (Java Cryptography Architecture).
Exercice 1 : Stocker un mot de passe dans un fichier.
Exercice 2 : Générer et valider une signature électronique à l'aide d'un algorithme de hachage.
Exercice 3 : Utiliser une API spécifique pour ajouter une signature électronique à un document PDF.

Préquis :

Etat de validation de la signature

La signature est VALABLE (signée par Anthony JULOU <anthony.julou@chambersign.fr>).
 - Les documents n'ont pas été modifiés depuis l'apposition de la signature.
 - Le document est signé par l'utilisateur actuel.

Propriétés de la signature... Fermer

Signature de code

- **But: Signer du code exécutable pour garantir**
 - **l'authenticité** de la compagnie ou de l'auteur
 - **l'intégrité du code** (*Non modifié ... non contaminé*) avant de l'exécuter !
- **Contrôle avant exécution**

Exemples:

- **Windows**
 - peut avertir qu'un « .exe » n'est pas signé et qu'il est risqué de l'exécuter
 - Bloque le fonctionnement d'un périphérique si son driver n'est pas signé numériquement
- **Mac**
 - Empêche l'exécution d'une application non signée

□ Chapitre 6 : Les logiciels

Signature de code

■ Comment signer ?

1. Obtenir un **certificat « développeur »** (*Extended Key Usage: Code signing*) avec une AC de confiance spécialisée
2. Utiliser **l'outil de signature** adéquat en fonction du code/exécutable à signer

Microsoft **Signtool.exe**

- **Type de fichiers:** .exe, .dll, .cab, msi, xpi...
- **Pré-requis:** Télécharger le SDK windows

Java **Jarsigner**

- **Type de fichiers:** librairies .jar...
- **Pré-requis:** Télécharger le JDK Java (pas le JRE)

Autres

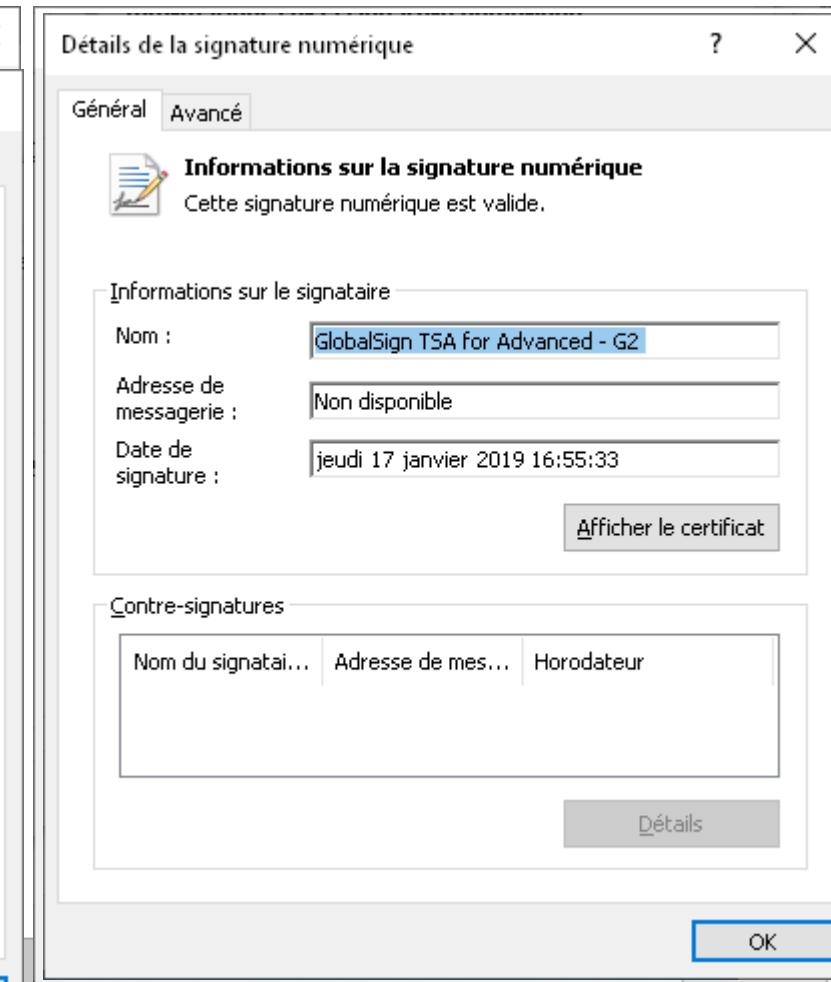
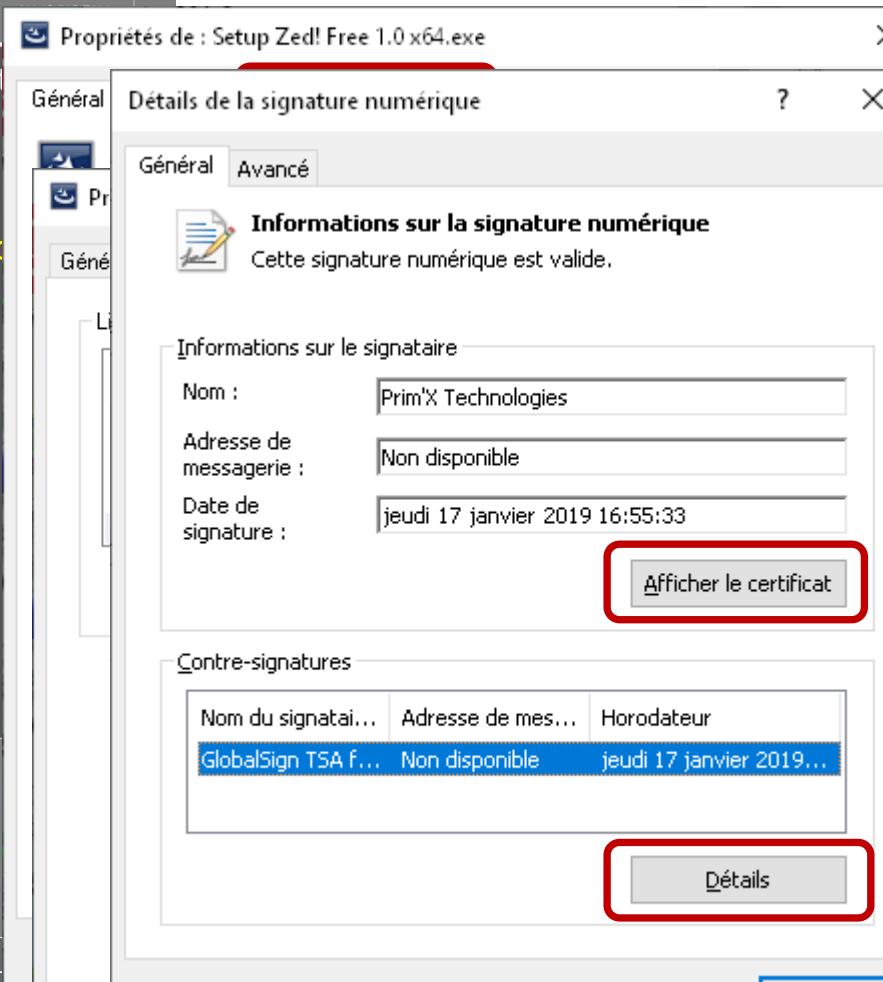
- Mac => codesign
- Adobe (*AIR: Moteur Flash et ActionScript*) => adt (*Flex SDK*)

Chapitre 6 : Les logiciels

Signature de code

Téléchargement d'un .exe dans Windows

Enregistrer le fichier, puis Afficher téléchargements, puis bouton droit sur Propriétés du fichier pour voir la signature



Chapitre 6 : Les logiciels

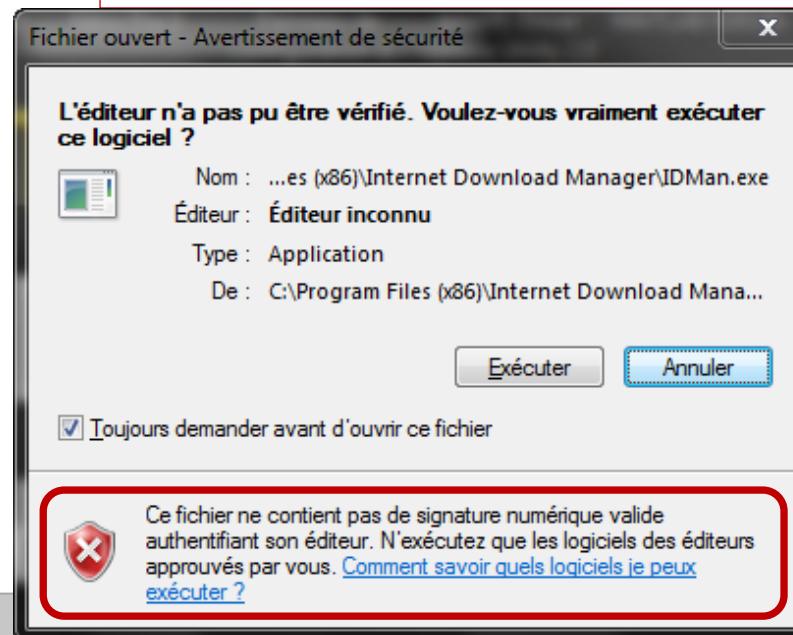
Signature de code

Exécutable Windows avec certificat logiciel

```
➤ Signtool.exe sign /t http://timestamp.digicert.com  
/f "c:\path\mycert.pfx" /p pfxpassword  
"c:\path\file.exe"
```

Exemple d'exécution avec défaut de signature

Blocage d'un exe non signé



Chapitre 7 :

Programmation

- Introduction
- Librairie Openssl
- Problématique de la programmation
- Type de certificat
- Environnement d'exécution
- Librairie MS Capi
- Standard PKCS11
- Signature en Java
- Failles et vulnérabilités



Introduction

- Domaine spécialisé nécessitant des connaissances en cryptographie
- Librairies cryptographiques multiples, riches et diversifiées (Java, MS Capi, OpenSSL...)

Points délicats à étudier:

- Environnements d'exécution
- Interopérabilité des systèmes d'exploitation et logiciels de signature
- Évolution des algorithmes et api

Introduction

Librairie Openssl

Problématique de la
programmation

Type de certificat

Environnement
d'exécution

Librairie MS Capi

Standard PKCS11

Signature en Java

Failles vulnérabilités

□ Chapitre 7 : Programmation

Librairie Openssl

Bibliothèque de fonctions cryptographiques
écrites en langage C et permettant

1. création de clés RSA, DSA
2. mise en œuvre de PKIX
3. création de certificats X509
4. calcul d'empreintes (SHA, ...)
5. fonctions d'encodage (Base64...)
6. chiffrement et déchiffrement (AES...)
7. réalisation de tests de clients et serveurs
SSL/TLS
8. signature électronique p7 et S/MIME

Introduction

Librairie Openssl

Problématique de la
programmation

Type de certificat

Environnement
d'exécution

Librairie MS Capi

Standard PKCS11

Signature en Java

Failles vulnérabilités

□ Chapitre 7 : Programmation

Librairie Openssl

Utilisation par des logiciels de sécurisation

- Systèmes d'exploitation (*Linux*)
 - Samba (partage de fichiers...)
 - Sendmail (*Mailer*)
- Apache-SSL (*Serveur https*)
- Wu-FTP (*Daemon ftps*)
- OpenCA (*Pki*)

<https://www.openssl.org>

Introduction

Librairie Openssl

Problématique de la
programmation

Type de certificat

Environnement
d'exécution

Librairie MS Capi

Standard PKCS11

Signature en Java

Failles vulnérabilités

□ Chapitre 7 : Programmation

Librairie Openssl

Interpréteur de commandes

Ex 1: Génération d'une bi-clé RSA 2048 bits

```
# 2048-bit private key, saved to file mykey.pem  
➤ openssl genrsa -out mykey.pem 2048
```

```
# 2048-bit public key of private key  
➤ openssl rsa -in mykey.pem -pubout
```

Ex 2: Génération d'une demande de certificat

```
# Generate Certificate Signed Request (CSR)  
➤ openssl req -new -key mykey.pem \  
-subj '/C=FR/L=Lanveoc/CN=www.ecole-navale.fr' \  
-out myCsr.pem
```

□ Chapitre 7 : Programmation

Librairie Openssl

Ex 3: Vérification / affichage

```
# Verify certificate (config file must be set)
```

➤ **openssl verify cert.pem**

```
cert.pem: OK
```

```
# Display certificate
```

➤ **openssl x509 -text cert.pem** (sortie visible sur
la diapositive n°30)

Ex 4: Haché et signature

```
# Generate sha256 digest
```

➤ **openssl dgst -sha256 myFile.txt**

```
21db5897ba36301b546152040e51ffbb01fbee253abac37f9b0733da89931ecf
```

```
# signed digest will be found in myFile.txt.sha2
```

➤ **openssl dgst -sha256 -sign mykey.pem**

➤ **-out myFile.txt.sha2 myFile.txt**

Introduction

Librairie Openssl

Problématique de la
programmation

Type de certificat

Environnement
d'exécution

Librairie MS Capi

Standard PKCS11

Signature en Java

Failles vulnérabilités

 Chapitre 7 : Programmation

Librairie Openssl

Ex 5: Vérification de la signature

```
# to verify myFile.txt using myText.txt.sha2 and pubkey.pem
openssl dgst -sha256 -verify pubkey.pem \
-signature myFile.txt.sha2 myFile.txt
```

Verified Ok

Ex 6: Chiffrement / déchiffrement asymétrique

```
# Encrypt file content with public key
```

- echo "Bouline ce soir" > **encrypt.txt**
- cat **encrypt.txt**

Bouline ce soir

- **openssl autil -encrypt -inkey public_key.pem \ -pubin -in encrypt.txt -out encrypt.dat**

```
# Decrypt using private key
```

- **openssl rsautl -decrypt -inkey private_key.pem \ -in encrypt.dat -out encrypt.txt**
- cat **encrypt.txt**

Bouline ce soir

Introduction

Librairie OpenSSL

Problématique de la
programmation

Type de certificat

Environnement
d'exécution

Librairie MS Capi

Standard PKCS11

Signature en Java

Failles vulnérabilités

□ Chapitre 7 : Programmation

Problématique de la programmation

Quels sont les objets à utiliser et les cibles d'exécution ?

1. Magasins de certificats

2. Type de certificat

- Certificat logiciel
- Certificat sur support physique

3. Environnement d'exécution

- Système d'exploitation
- Navigateur internet

Type de certificat

Certificat logiciel

- Stocké entièrement dans un fichier **keystore**
- Transport et sauvegarde par fichier **pkcs12** (*.p12 ou .pfx Microsoft*) protégé par un mot de passe haché

Accès: Lecture et utilisation du fichier p12 par API (Application Programming Interface) sans passer par le keystore du système ou du navigateur

Avantage: Facilité de chargement et manipulation de la clé privée

Inconvénient: Authenticité non garantie, usurpation d'identité par copie

Type de certificat

Certificat sur puce cryptographique ou HSM

- Clés privées protégées par code PIN
- Un middleware (*intergiciel*) à installer pour reconnaître la puce.

ACCES: Interface spécifique pour signer/chiffrer

Avantage: Sécurité et fiabilité de l'authenticité grâce à la protection de la clé privée (pin)

Inconvénient:

- Obligation d'installer un middleware propre au système; déploiement multi-plate OS plus compliqué (*pkcs11*)

Introduction

Librairie OpenSSL

Problématique de la
programmation

Type de certificat

Environnement
d'exécution

Librairie MS Capi

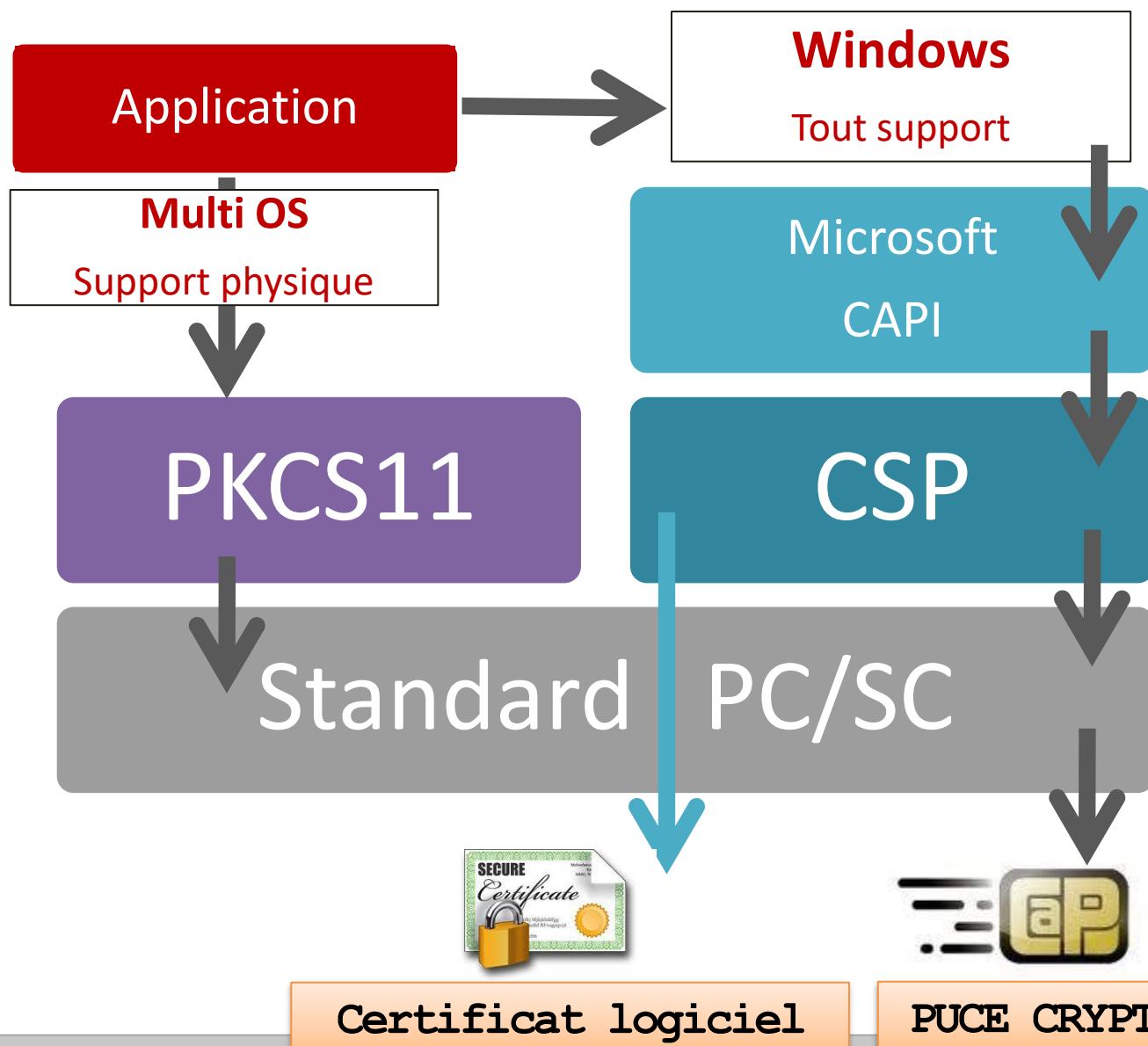
Standard PKCS11

Signature en Java

Failles vulnérabilités

Chapitre 7 : Programmation

Environnement d'exécution



□ Chapitre 7 : Programmation

Librairie Microsoft CryptoAPI

MS-CAPI (*Cryptographic Application Programming Interface*)

- Ensemble de fonctions cryptographiques sous Windows (Langage C)
- Appelle les fonctions implémentées par le CSP

➤ **SignerSign:** Signs the specified file
➤ **CryptVerifySignature:** Verifies a digital signature, given a handle to the hash object
....

CSP: (*Cryptographic Service Providers*)

- Implémentation cryptographique pour un dispositif cryptographique d'une marque donnée
- Fourni par le constructeur sous la forme d'une DLL

□ Chapitre 7 : Programmation

Standard PKCS11

Librairie standard d'appels de fonctions cryptographiques sur des tokens

- Ecrite en langage C
- Le constructeur du token fournit la librairie compilée pour différents OS (.dll, .so, .dylib, ...)
- Le développeur utilise un Wrapper encapsulant les appels depuis un autre langage (*ex: en Java, Python, Ruby ou .NET*)

Exemples de quelques fonctions pkcs11

- **C_Sign()** : fonction de signature
- **C_OpenSession()** : ouvre une session carte (PIN)
- **C_GenerateKeyPair()** : génère un bi-clé
- **C_Verify()** : vérifie une signature
- **C_Digest()** : fonction de hachage
- **C_Encrypt()** : fonction de chiffrement

Introduction

Librairie OpenSSL

Problématique de la
programmation

Type de certificat

Environnement
d'exécution

Librairie MS Capi

Standard PKCS11

Signature en Java

Failles vulnérabilités

□ Chapitre 7 : Programmation

Signature en Java

JAVA : Langage Orienté Objet (1995)

- Simplicité, robustesse, riche, portable...
- Disponible sur multiples OS et navigateurs

Richesse de l'API de sécurité et de cryptographie:

- **JCA (Java™ Cryptography Architecture)**
 - **JCE (Java Cryptography Environment)**
 - **JSSE (Java Secure Socket Extension)**
 - **JAAS (Java Authentication Authorization Service)**
- **PKCS 11 Oracle implementation**
- **XMLDSig (XML Digital Signature)**

□ Chapitre 7 : Programmation

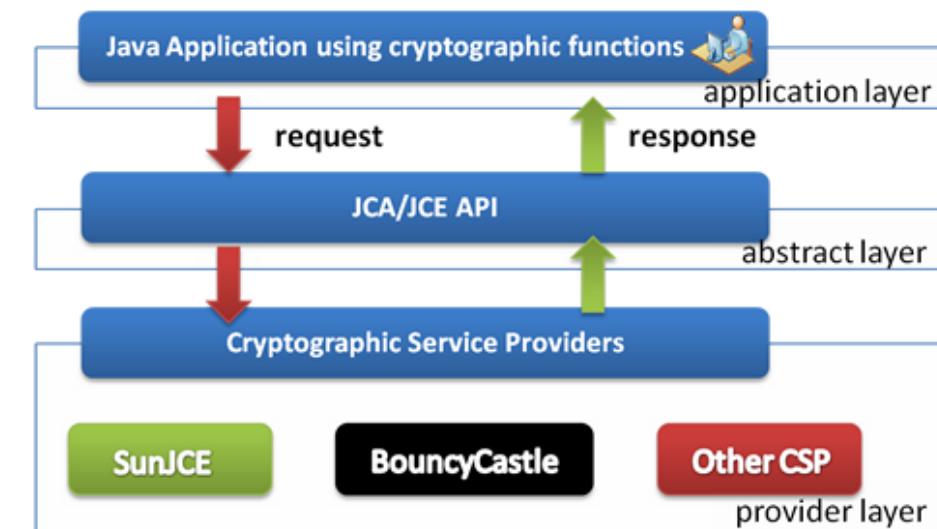
Signature en Java

JCE (*Java™ Cryptography Extension*)

Extension de JCA fournissant des classes de

- Cryptage / signature
- Génération de clés
- Contrôle d'intégrité

Principe des
fournisseurs
de sécurité



Packages *javax.crypto*, *java.security*

Signature en Java

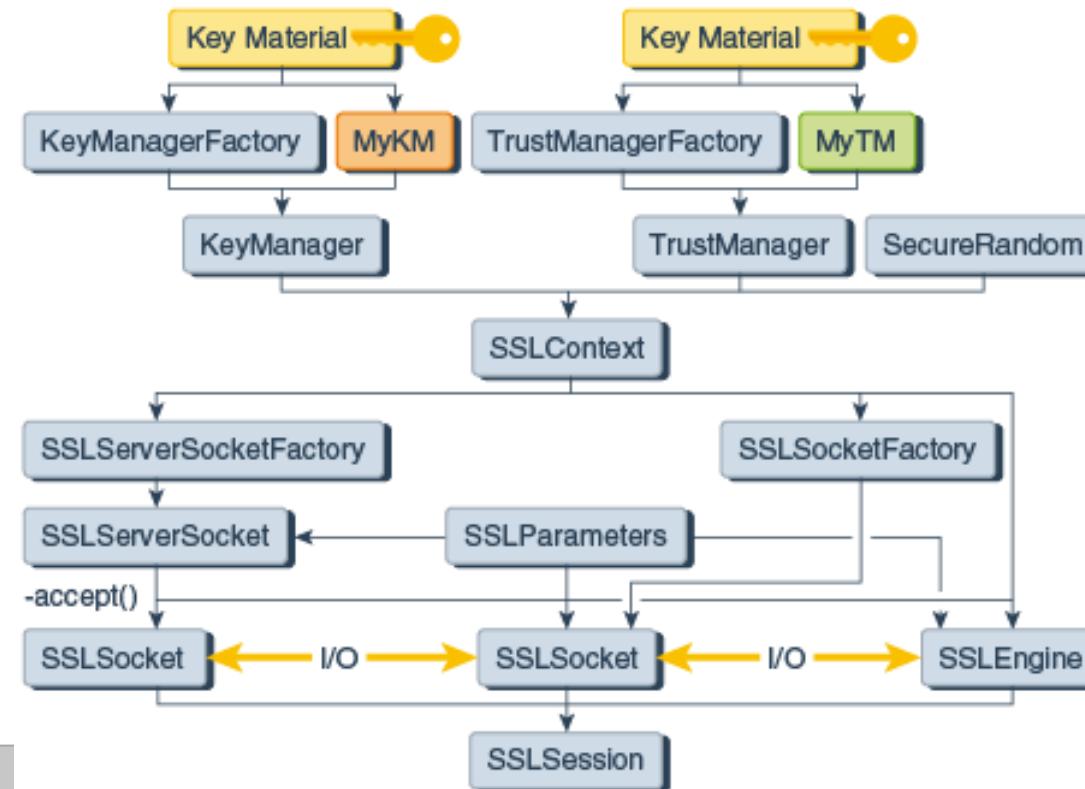
Exemples de classes JCA

- **MessageDigest**: the message digest (hash) of specified data.
- **Signature**: initialized with keys, these are used to sign data and verify digital signatures.
- **Cipher**: initialized with keys, these used for encrypting/decrypting data.
- **KeyFactory**: used to convert existing opaque cryptographic keys of type Key into key specifications (transparent representations of the underlying key material), and vice versa.
- **KeyStore**: used to create and manage a keystore.
- **CertificateFactory**: used to create public key certificates and Certificate Revocation Lists (CRLs) ...

Signature en Java

API de sécurisation des communications réseau

- TLS (SSL Secure Socket Layer) .
 - Authentication https



Introduction

Librairie Openssl

Problématique de la
programmation

Type de certificat

Environnement
d'exécution

Librairie MS Capi

Standard PKCS11

Signature en Java

Failles vulnérabilités

□ Chapitre 7 : Programmation

Signature en Java

PKCS11: Sun PKCS#11 Provider

- Ajouter la DLL en tant que nouveau fournisseur de sécurité (*Provider*) dans le fichier de configuration

```
String s1 = "D:/pkcs11.cfg";
SunPKCS11 sunpkcs11 = new SunPKCS11(s1);
Security.addProvider(sunpkcs11);

KeyStore keystore = KeyStore.getInstance("pkcs11");
keystore.load(null, ac);
String alias = null;
while (aliases.hasMoreElements()) {
    alias = aliases.nextElement().toString();
}
if (alias != null) {
    PrivateKey privKey = (PrivateKey) ks.getKey(alias, null);
    byte[] data = input.getBytes();
    java.security.Provider p = ks.getProvider();
    Signature sig = Signature.getInstance(SIG_ALGORITHM, p);
    sig.initSign(privKey);
    sig.update(data);
    byte[] signature = sig.sign();
}
```

Autres fournisseurs cryptographiques en Java:

Bouncy Castle (Australie), IAIK (Autriche)

Introduction

Librairie Openssl

Problématique de la
programmation

Type de certificat

Environnement
d'exécution

Librairie MS Capi

Standard PKCS11

Signature en Java

Failles vulnérabilités

□ Chapitre 7 : Programmation

Signature en Java

XMLDSig (*XML Digital Signature API*)

But: Générer et valider la signature XML

Packages: *javax.xml.crypto.dsig*

Exemple de code (*extrait*)

```
DocumentBuilderFactory dbf =  
    DocumentBuilderFactory.newInstance();  
dbf.setNamespaceAware(true);  
Document doc =  
    dbf.newDocumentBuilder().  
    parse(new FileInputStream("myfile"));  
  
DOMSignContext dsc = new DOMSignContext  
(kp.getPrivate(), doc.getDocumentElement());  
  
XMLSignature signature = fac.newXMLSignature(si, ki);  
signature.sign(dsc);
```

Autres fournisseurs: Santuario (Apache)

Introduction**Librairie Openssl****Problématique de la programmation****Type de certificat****Environnement d'exécution****Librairie MS Capi****Standard PKCS11****Signature en Java****Failles vulnérabilités**

□ Chapitre 7 : Programmation

Signature en Java

Signature de PDF: Librairie iText

- Génération de PDF à la volée
- Ajout de signatures électroniques

```
KeyStore ks = KeyStore.getInstance("pkcs12", "BC");
ks.load(new FileInputStream(path), keystore_password.toCharArray());
String alias = (String)ksAliases().nextElement();
PrivateKey pk = (PrivateKey) ks.getKey(alias, key_password.toCharArray());
Certificate[] chain = ks.getCertificateChain(alias);
// reader and stamper
PdfReader reader = new PdfReader(src);
FileOutputStream os = new FileOutputStream(dest);
PdfStamper stamper = PdfStamper.createSignature(reader, os, '\0');
// appearance
PdfSignatureAppearance appearance = stamper.getSignatureAppearance();
appearance.setImage(Image.getInstance(RESOURCE));
appearance.setReason("I've written this.");
appearance.setLocation("Foobar");
appearance.setVisibleSignature(new Rectangle(72, 732, 144, 780), 1, "first");
// digital signature
ExternalSignature es = new PrivateKeySignature(pk, "SHA-256", "BC");
ExternalDigest digest = new BouncyCastleDigest();
MakeSignature.signDetached(appearance, digest, es, chain, null, null, null, 0,
CryptoStandard.CMS);
```

Format PADES : iText => IAIK**Autre librairie : Apache PDFBox Open source**

Signature en Java

Application de signature

Intérêt:

- Permettre à un logiciel d'accéder en local - sous le contrôle du signataire - à la clé privée pour signer

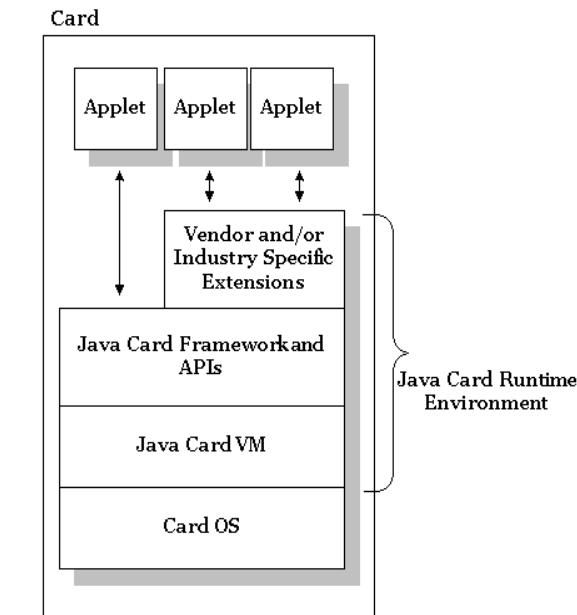
Comment ?

- Utiliser
 - une interface d'accès aux **keystores** ou
 - **pkcs11** pour accéder au token
- Faire signer dans un fichier, un document PDF ou un flux XML échangé avec le serveur

Signature en Java

JavaCard: OS pour gérer une carte à puce

- Java Card Runtime Environment (*JCRE*)
- Applets embarquées permettant de gérer la cryptographie:
 1. Génération clés
 2. Ajout de certificats
 3. Signatures
 4. Chiffrement



Ex: MultiApp ID IAS ECC de Gemalto

Introduction

Librairie Openssl

Problématique de la
programmation

Type de certificat

Environnement
d'exécution

Librairie MS Capi

Standard PKCS11

Signature en Java

Failles vulnérabilités

□ Chapitre 7 : Programmation

Failles et vulnérabilités (1/2)

Exemple d'attaque d'une autorité de certification Diginotar (2011)

- Attaque « *Man In The Middle* » (*Réseau fragile, pas d'antivirus, pas de logiciel de détection d'intrusions...*)
- Délivrance de faux certificats serveurs google.com pour espionner des comptes Gmail Iraniens
- Les utilisateurs pensaient être sur le serveur https gmail officiel ... ont été écoutés sur un faux serveur...

Espionnage de comptes facebook (*Man in the middle*)

- Utilisation d'un faux certificat de chiffrement
- Le pirate intercepte le flux, le décode, l'enregistre en clair et l'exploite à l'insu de l'utilisateur
- Les utilisateurs avaient pourtant une alerte du navigateur web, mais ...

□ Chapitre 7 : Programmation

Failles et vulnérabilités (2/2)

Recommandations pour la sécurité

1. Utiliser des mots de passe de qualité et les changer régulièrement (*non stockés en clair, non mémorisés*)
2. Mettre à jour son système d'exploitation et logiciels (Notamment l'antivirus et le pare-feu), attention aux spyware et key logger
3. Ne pas utiliser de compte admin pour naviguer sur internet
4. Contrôler la diffusion d'informations personnelles et la confiance aux sites (cadenas ssl et réputation)
5. Ne pas ouvrir les pièces jointes et réfléchir avant de cliquer sur un lien, ne pas exécuter de fichiers téléchargés

→ Guides de recommandations sur le site de l'ANSSI

- 1) La confiance numérique
- 2) Bases cryptographiques
- 3) Le certificat numérique
- 4) Fonctions de signature
- 5) Formats de signature
- 6) Les logiciels
- 7) Programmation
- 8) Applications exemples
- 9) Cadre légal et juridique
- 10) Conclusion

Chapitre 8 :

Applications

exemples



- Schéma général
- Le SIV (Système d'immatriculation des véhicules)
- Les marchés publics
- Hélios de la DGFiP: comptabilité publique
- Chorus Pro dématérialisation des factures
- Autres usages professionnels
- Signature à la volée

Domaine d'application

■ Dématérialisation

- de procédures administratives
- factures, bons de commandes, contrats, bulletins de salaire...
- coffre fort électronique
- archivage à valeur probante
- contractualisation en ligne, vote électronique

■ Sécurisation et authentification

- Sites sécurisés avec **authentification forte** (par certificat)
 - Accès à sa banque, jeux en ligne...
 - accès à des télé services (dossiers administratifs...)

CHIFFRES

En 2018:37.000 pro
11,5 M de
cartes grises Chapitre 8 : Applications exemples

SIV : Système d'immatriculation des véhicules

- Service en ligne accessible par les professionnels géré par l'**ANTS** (*Agence nationale des titres sécurisés*)
 - Immatriculation des véhicules neufs et d'occasions
 - Emission des certificats
 - d'immatriculation de véhicule
 - de cession ou destruction
- Utilisateurs
 - Garagistes, mandataires, police ...
- Type d'accès
 - **Authentification forte par certificat RGS 2***
(Clé USB cryptographique ou carte à puce)



□ Chapitre 8 : Applications exemples

SIV : Système d'immatriculation des véhicules

Enregistrer son certificat à la demande d'habilitation

1) Exporter la clé publique du certificat

- Génération du fichier «.cer» avec les assistants des conteneurs de confiance

2) Charger la clé publique du certificat dans le SIV

- Cette partie consiste à associer le compte au certificat dans l'annuaire de comptes du SIV

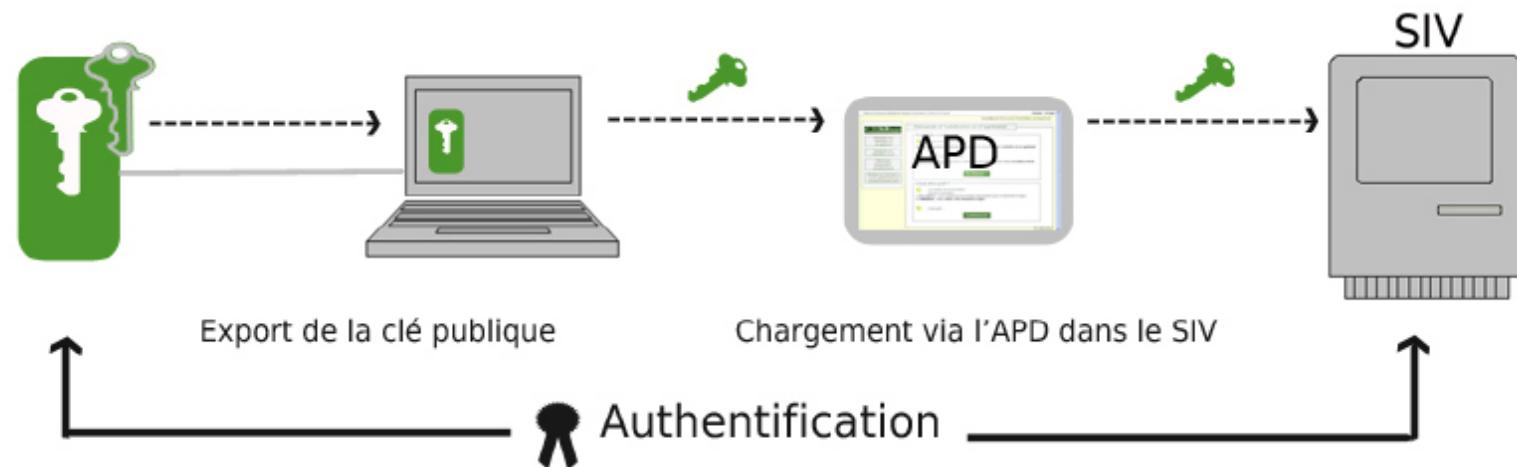


Schéma général

Les marchés publics

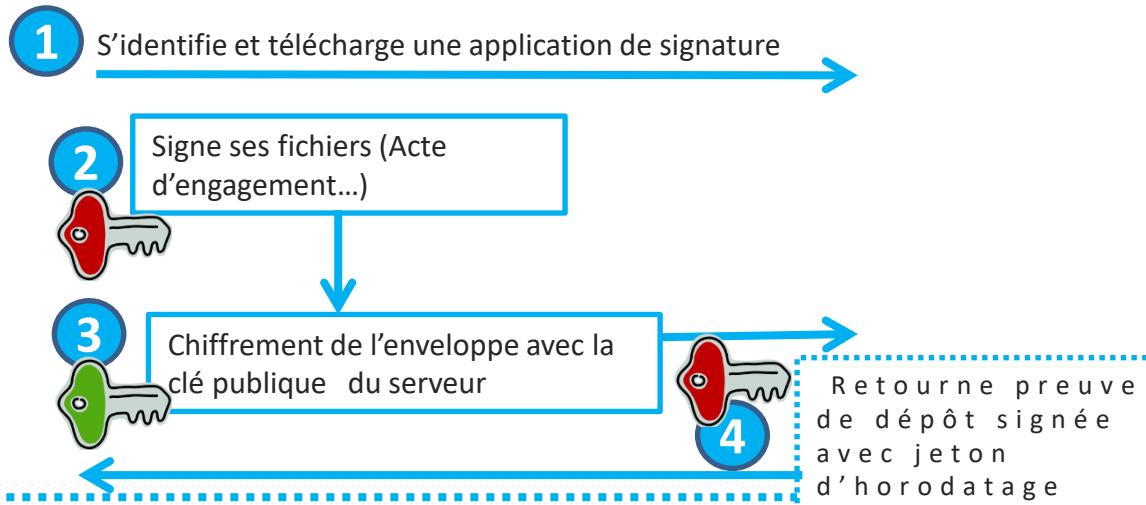
Echanges bancaires
électroniquesAutres usages
professionnels

Signature à la volée

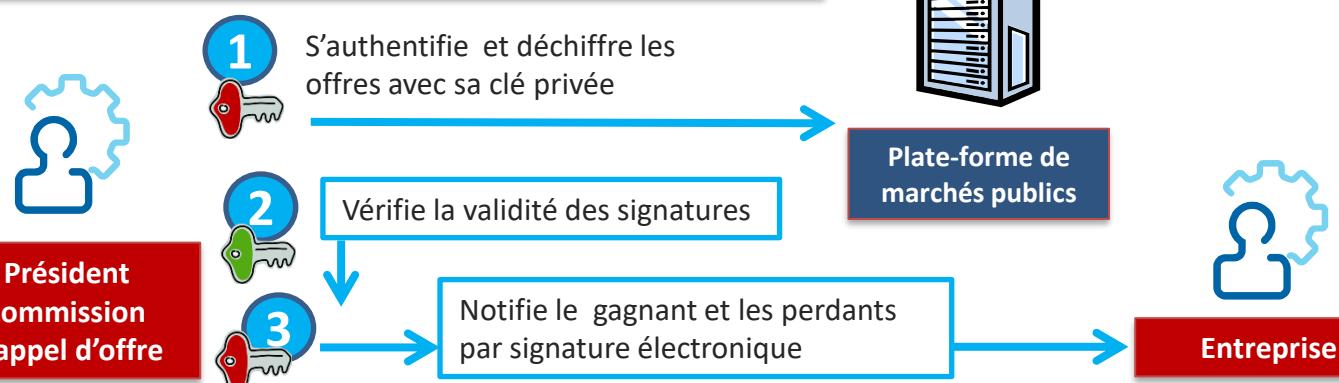
Chapitre 8 : Applications exemples

Les marchés publics

Dépôt d'une offre par une entreprise



Ouverture des plis côté acheteur public



Les marchés publics

Arrêté du 12 avril 2018 *relatif à la signature électronique dans la commande publique*

- Obligation de signer avec un certificat eIDAS (Règlement Européen EU N°910/2014)
- Obligation d'utilisation d'un des 3 formats de signature: **XAdES, PAdES ou CAdES**
- La signature peut être multiple (parapheur)
- Vérification de la signature par l'acheteur
- ✓ **Signature obligatoire à la fin du marché** entre l'entité publique et l'entreprise retenue.

□ Chapitre 8 : Applications exemples

HELIOS : dématérialisation de la comptabilité publique

- **Application de la DGFiP (*direction générale des Finances publiques*)**
- **But :** Dématérialisation de la gestion budgétaire et comptable des collectivités locales



CHIFFRES

107.000 utilisateurs
6,9 M de flux envoyés

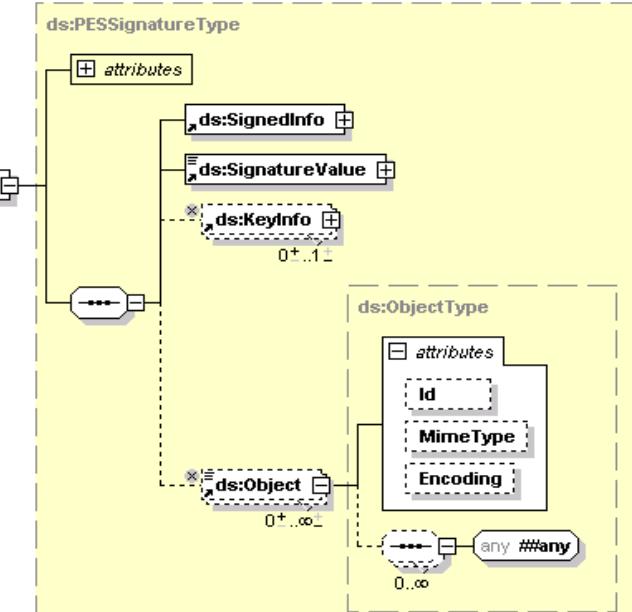
□ Chapitre 8 : Applications exemples

HELIOS : dématérialisation de la comptabilité publique

=> « Signature électronique avancée » des flux

- Remplace la signature manuscrite des ordonnateurs (Maire, DGS, Directeur Hospitalier ...)
- Rend exécutoire les titres de recette et atteste du « service fait » les dépenses de l'entité publique émettrice (Commune, Conseil Départemental, Hôpital ...)

- Protocole d'Echange Standard (PES v2)
- Besoin d'un **certificat eIDAS** (ou RGS) pour une **signature avancée** au format **XADES enveloppé**
- **Politique de signature :**
https://portail.dgfp.finances.gouv.fr/documents/PS_Helios_DGFiP.pdf

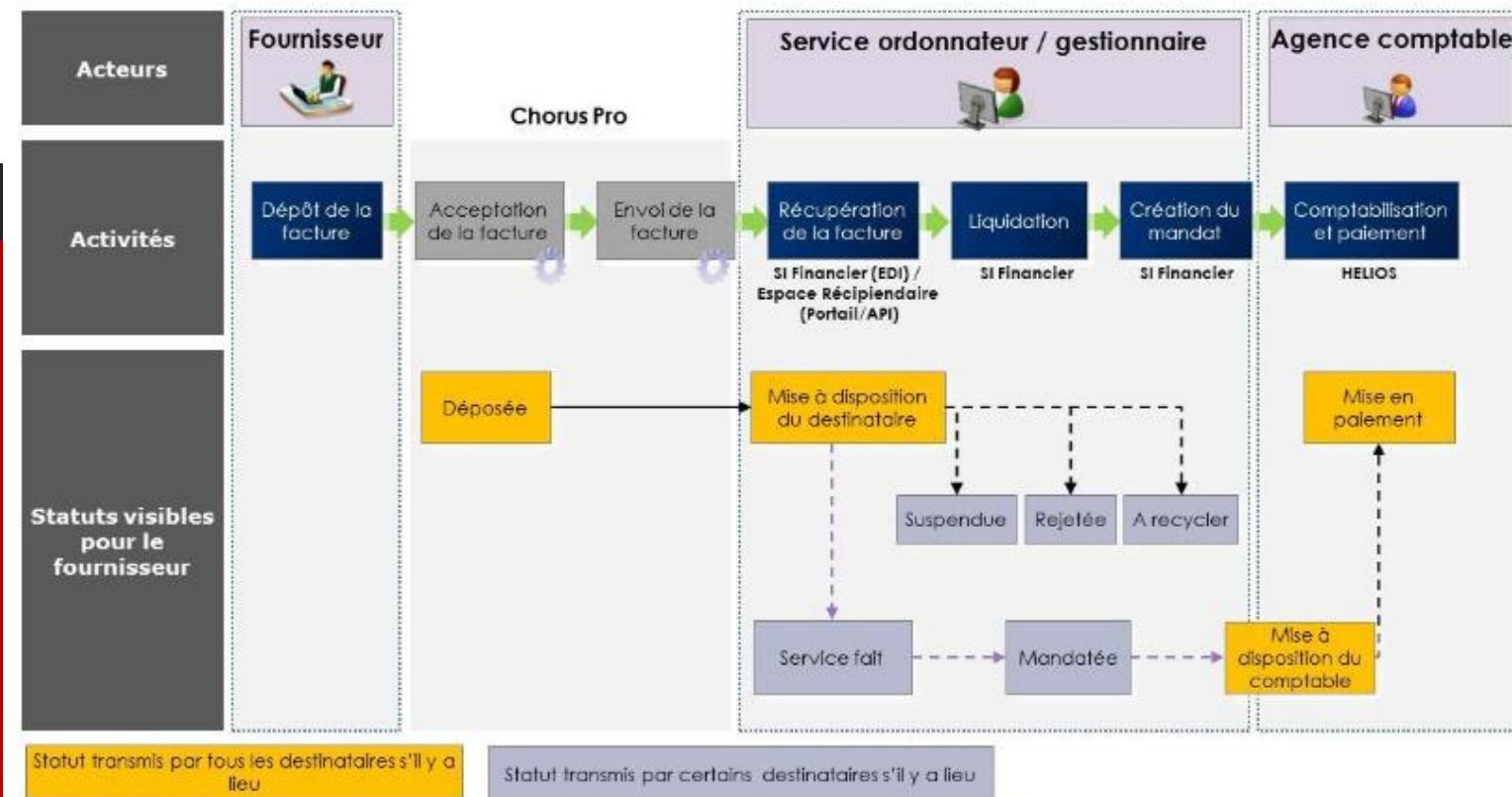


□ Chapitre 8 : Applications exemples

Chorus PRO dématérialisation des factures

Système de gestion des factures à destination des organismes publics (Géré par l'AIFE)

=> Obligation pour les entreprises (*fournisseurs*) de transmettre leurs factures en mode dématérialisé



CHIFFRES

En 2018

139.000

collectivités

350.000

entreprises

25 M de

factures

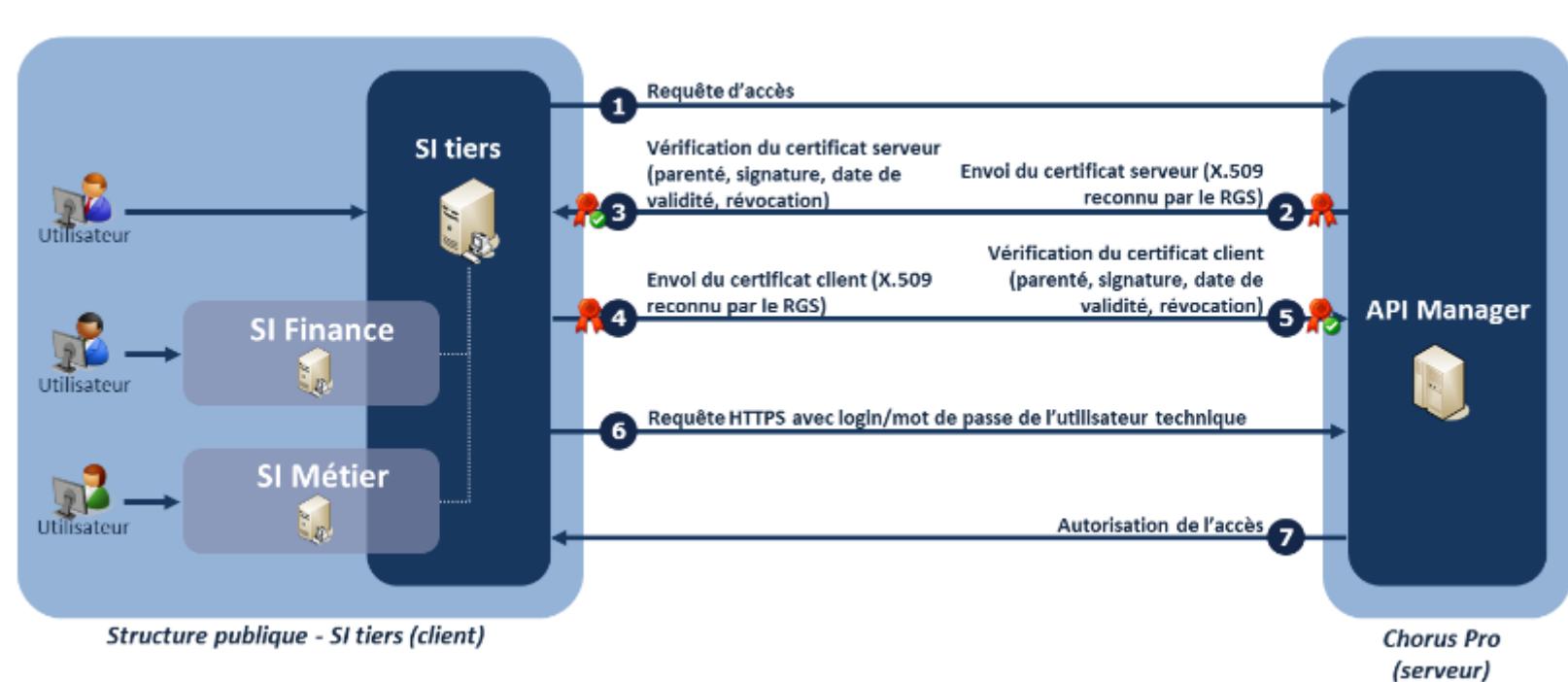
dématérialisées

□ Chapitre 8 : Applications exemples

Chorus PRO dématérialisation des factures

Authentification du téléservice sécurisé (https)

- Mode API : Web Services / JSON
- Authentification SSL de la machine de la collectivité ou du fournisseur sur le serveur Chorus Pro
- Utilisation d'un **certificat cachet d'authentification RGS 1***



Autres usages professionnels

- Dématérialisation: remplacer les processus « papiers » par des processus électroniques

DEMATERIALISATION ADMINISTRATIVE

Appel D'offre et Réponses aux marchés publics

Sylae
Déclarations contrats aidées

ANTAI

Ebics-ts

Insee, Infogreffé

SIV Cartes grises

Dématérialisation comptabilité publique :
Helios.
Chorus Pro

Dématérialisation contrôle de légalité: Actes

Tracfin (Lutte fraude financière), Egide, Pro Douane

DEMATERIALISATION ORGANISATIONNELLE

Signature de documents:

- Facturation
- Bulletin de salaire
- Courriels
- Circuit documentaire et parapheur

Archivage électronique

DEMATERIALISATION METIER

Notaires, avocats, banques (Transactions) ...

Schéma général

Les marchés publics

Echanges bancaires
électroniquesAutres usages
professionnels

Signature à la volée

□ Chapitre 8 : Applications exemples

Signature à la volée

Signature de contrats (*ouverture de comptes bancaires, prêts... téléphonies*) sans devoir acquérir un certificat

Fonctionnement:

1. Le client est authentifié sur le site internet avec différents facteurs d'authentification (login, mdp, OTP...)
2. Le client visualise le document et est informé qu'une signature électronique va être apposée pour validation de son consentement
3. La clé privée est générée sur le serveur/cloud (ou en local avec une application de signature)
4. La signature est opérée avec la clé privée sur le document (PDF)
5. La clé privée est supprimée
6. Le contrat PDF signé est retourné au client

- 1) La confiance numérique
- 2) Rappels cryptographiques
- 3) Le certificat numérique
- 4) Fonctions de signature
- 5) Formats de signature
- 6) Les logiciels
- 7) Programmation
- 8) Applications exemples
- 9) Cadre légal et juridique
- 10) Conclusion

Chapitre 9 :

Cadre légal et juridique



- Législation
- Cadre juridique



□ Chapitre 8 : Cadre légal et juridique

Législation

Directive Européenne 1999/93/CE => Loi du 13 Mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique

Favoriser la signature électronique dans les états membres et contribuer à sa reconnaissance juridique

Décret n°2001-272 du 30 mars 2001

- Notion de signature électronique sécurisée
 - Définition de dispositifs sécurisés
 - Signature présumée fiable avec certificat qualifié

□ Chapitre 8 : Cadre légal et juridique

Législation

Reconnaissance des autorités de certification

Loi n° 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique*

L'article 33 précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés

Naissance du RGS (*Référentiel Général de Sécurité*)

Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques ...

[...] Le RGS fixe les règles que doivent respecter les fonctions des systèmes d'information [...]

□ Chapitre 8 : Cadre légal et juridique

Législation française

Décret n°2010-112 dit « RGS »

- Mise en place d'une procédure de qualification des AC, des supports cryptographiques ...

Caractéristiques d'un certificat RGS V2

Certificats de personne, de serveur, cachet, chiffrement et horodatage

Tailles des clés à **2048 bits**

Algorithme
SHA 2 car
SHA 1 interdit

Limitation à **10 ans** de vie pour une AC

Niveaux de sécurité de **1* à 3***

S'applique aux services de l'administration depuis le **19 mai 2013**

Chapitre 8 : Cadre légal et juridique

Règlement européen eIDAS

Règlement (UE) n ° 910/2014 du Parlement Européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE

- sécuriser les interactions entre les entreprises, les citoyens et les administrations.
- améliorer l'efficacité des services en ligne public et privé, du commerce électronique et des relations commerciales dans l'UE
- améliorer la confiance dans les transactions électroniques sur le marché interne
- Entrée en vigueur en juillet 2016

Règlement européen eIDAS : TSL

Signature électronique eIDAS

	Signature de niveau 1 - sans enregistrement -	Signature de niveau 2 - ETSI 102 042 -	Signature de niveau 3 - ETSI 101 456 -	Signature de niveau 4 - ETSI 101 456 + SSCD -
Législation	Intégrité  Horodatage qualifié	Intégrité  Horodatage qualifié	Intégrité  Horodatage qualifié	Intégrité  Horodatage qualifié
Cadre	Identité  Pas de certificat ou certificat à la volée	Identité  Certificat européen simple	Identité  Certificat européen qualifié	Identité  Certificat européen qualifié
	Traçabilité  Preuves électroniques	Traçabilité  Preuves électroniques  Vérification CNI  Carte à puce virtuelle	Traçabilité  Preuves électroniques  Vérification CNI  Carte à puce virtuelle  Face à face	Traçabilité  Preuves électroniques  Vérification CNI  Carte à puce  Face à face
	Valeur juridique 	Valeur juridique 	Valeur juridique 	Valeur juridique 

Chapitre 8 : Cadre légal et juridique

Règlement européen eIDAS : TSL

Liste des services qualifiés par l'Europe



Trusted List Browser

Tool to browse the national Trusted Lists and the European List of Trusted Lists (LOTL).

[Menu ▾](#)

[European Commission](#) > [CEF Digital](#) > [eSignature](#) > [Trusted List Browser](#)

Search a trust service by



Type of service

Search by type of trust service (e.g. time-stamping, certificate for e-signature) and country



Name of trust service

Search based on the name of a trust service



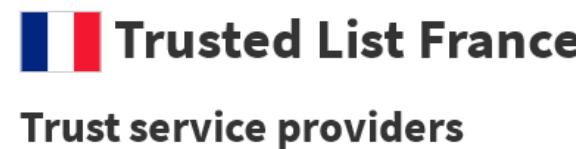
Signed file

Find the trust service that issued the signing certificate(s) contained in a file

 Austria Issue date 2019-10-11	 Belgium Issue date 2019-09-05	 Bulgaria Issue date 2019-11-15
 Croatia Issue date 2019-10-02	 Cyprus Issue date 2019-07-17	 Czech Republic Issue date 2019-11-22
 Denmark Issue date 2019-08-05	 Estonia Issue date 2019-09-05	 Finland Issue date 2019-08-12
 France Issue date 2019-11-14	 Germany Issue date 2019-11-21	 Greece Issue date 2019-10-10

□ Chapitre 8 : Cadre légal et juridique

Règlement européen eIDAS : TSL



Currently active trust service providers

AR24 QeRDSCDC ARKHINEO QVal for QESig QPres for QESig QVal for QESeal QPres for QESealCaisse des dépôts et consignations QCert for ESigCertinomis QCert for ESig QCert for ESeal QWACClick and Trust QCert for ESigCryptolog International QCert for ESig QCert for ESeal QTimestampDhimyotis QCert for ESig QCert for ESeal QWAC QTimestampEquisign QeRDSLe Groupe La Poste QTimestamp QeRDSMinistère de la Justice QCert for ESig

QCert for ESig : Qualified Certificate for Electronic Signature

QCert for ESeal : Qualified Certificate for Electronic Seal

QTimestamp : Qualified electronic Time stamp

QWAC (officiel) ou QCWA : Qualified Certificate for Website Authentication

QeRDS : qualified electronic registered delivery service

Agence Nationale des Titres Sécurisés QCert for ESigCLEARBUS QeRDSCertEurope QCert for ESig QCert for ESeal QWACChamberSign France QCert for ESig QCert for ESealConseil Supérieur du Notariat QCert for ESig QTimestampDARVA QTimestamp QeRDSDocuSign France QCert for ESig QCert for ESeal QTimestampImprimerie Nationale QCert for ESigMinistère de l'Intérieur QCert for ESig QTimestampTESSI DOCUMENTS SERVICES QeRDS

□ Chapitre 8 : Cadre légal et juridique

Législation

Application du règlement européen eIDAS

Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique

Article 1: *La fiabilité d'un procédé de signature électronique est présumée, jusqu'à preuve du contraire, lorsque ce procédé met en œuvre une **signature électronique qualifiée**. Est une signature électronique qualifiée une **signature électronique avancée**, conforme à l'article 26 du règlement susvisé et créée à l'aide d'un **dispositif de création de signature électronique qualifié** répondant aux exigences de l'article 29 dudit règlement, qui repose sur un **certificat qualifié de signature électronique** répondant aux exigences de l'article 28 de ce règlement.*

Chapitre 8 : Cadre légal et juridique

Cadre juridique

Modification du code civil

Code civil – Article 1366

L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité

Code civil – Article 1367

« Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat

- 1) La confiance numérique
- 2) Bases cryptographiques
- 3) Le certificat numérique
- 4) Fonctions de signature
- 5) Formats de signature
- 6) Les logiciels
- 7) Programmation
- 8) Applications exemples
- 9) Cadre légal et juridique
- 10) Conclusion

□ PKI, services de confiance et signature électronique

Chapitre 10 : Conclusion



- Les points forts
- Les points faibles
- Perspectives
- Références et normes
- Remerciements

[Les points forts](#)[Les points faibles](#)[Perspectives](#)[Références et
normes](#)[Remerciements](#)

Chapitre 10 : Conclusion

Les points forts

- Procédé technique fiable
 - Non imitable
 - Non répudiable
 - Non modifiable
- Dématérialisation des processus
 - Souplesse d'utilisation
 - Sécurisation
 - Gain de temps
 - Gain financier

Les points faibles

- Relative complexité de mise en œuvre
 - Obtention d'un certificat numérique
 - Mise en place des outils cryptographiques
 - Recherche/utilisation de logiciels de signature
- Défaut de connaissance du procédé et de son statut juridique
 - Procédé peu utilisé par les particuliers
- Utilisation forcée par l'obligation de l'état
- Evolution rapide de la technologie rendant les algorithmes cryptographiques obsolètes...

□ Chapitre 10 : Conclusion

Perspectives

- Développement de la dématérialisation dans les entreprises et collectivités
 - Echanges de flux, archivage électronique, coffre fort, chaîne de décision...
- Développement de la signature dans le Cloud et sur smartphone/tablette
- Interopérabilité des signatures de l'UE avec le règlement européen applicable en 2016

Grand public: Mobilité due au Web 3.0

- Signature à la volée, cloud, vote électronique
- Dossier médical, signature de contrats en ligne, d'actes administratifs

Références et normes

Sites institutionnels

- **ANSSI:** <https://www.ssi.gouv.fr/>
- **Commission européenne :**
<https://ec.europa.eu>

Normalisation

- **W3C:** <https://validator.w3.org/>
- **IETF RFC:** <https://tools.ietf.org/>

Les points forts

Les points faibles

Perspectives

Références et
normes

Remerciements

□ Chapitre 10 : Conclusion

Références et normes

- **IETF (Internet Engineering Task Force)**
 - <https://www.ietf.org/>
 - RFC 5280** : Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
 - RFC 3647** : Certificate Policy and Certification Practices Framework
 - RFC 6960** : Online Certificate Status Protocol - OCSP
 - RFC 5652** : Cryptographic Message Syntax
 - RFC 3739** : Internet X.509 Public Key Infrastructure Qualified Certificates Profile
 - RFC 3161** : Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
 - RFC 3647** : Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
 - RFC 4055** : Algorithms and Identifiers for RSA Cryptography in PKI
 - RFC 5905** : Simple Network Time Protocol (SNTP)

Les points forts

Les points faibles

Perspectives

Références et
normes

Remerciements

□ Chapitre 10 : Conclusion

Références et normes

■ ETSI (European Telecommunications Standards Institute)

- <https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx>

EN 319 401 General Policy Requirements for Trust Service Providers

x19 411 Policy and security requirements for Trust Service Providers issuing certificates

EN 319 411-1 : General requirements

EN 319 411-2 : Requirements for trust service providers issuing EU qualified certificates

TR 119 411-4 : Checklist supporting audit of TSP against

EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps

TS 119 441 Policy requirements for TSP providing signature validation services

EN 319 412 Certificate Profiles

EN 319 412-1 : Overview and common data structures

TS 119 412-1 (interim TS version to support PSD2 features and TS 119 495)

EN 319 412-2 : Certificate profile for certificates issued to natural persons

EN 319 412-3 : Certificate profile for certificates issued to legal persons

EN 319 412-4 : Certificate profile for web site certificates issued to organisations

EN 319 412-5 : QCStatements

EN 319 422 : Time-stamping protocol and electronic time-stamp profiles

Remerciements

- **Marie-Christine LE MEUR CRENN**, conseillère signature électronique à ChamberSign,
- **Line GILET**, responsable Qualité Sécurité chez Giesecke+Devrient Mobile Security,
- **Pierre-Yves NICOLAS**, DSI à la Chambre de Commerce et d'Industrie de Bretagne Ouest;
- à
- **David BROSSET** et **Eric SAUX**, maîtres de conférence au département informatique de l'Ecole Navale pour leurs précieux conseils et leur soutien à la création de ce support de cours.