TLS et X509v3

Alexandre Duc

Obtenir un canal confidentiel

Question

L'on souhaite transmettre une clef symétrique via un canal de communication. Quels sont les conditions nécessaires pour que cette transmission se fasse de manière sécurisée ? Et pour une clef asymétrique ?

Obtenir un canal confidentiel

Question

Comment peut-on obtenir de la sécurité entre deux personnes qui ne se sont jamais rencontrées ?

Infrastructures à Clefs Publiques

- Les **infrastructures à clefs publiques** («Public-Key Infrastructure (PKI)») de type X.509v3 permettent d'obtenir une clef publique de manière **authentique**.
- Une PKI repose principalement sur la notion de **certificat**.
  $\rightarrow$ Utilisation d'une **tierce partie de confiance**.

Certificats X.509v3

Définition (Certificat)

Un **certificat** est un lien entre une **entité** et une **clef publique**.

- Certifié par une tierce partie de confiance, **l'autorité de certification** («certificate authority (CA)»).
- Exemples d'entités : personne, serveur (`www.banque.ch`), logiciel (un «driver» Windows 10), etc.
- Défini par le standard international X.509v3 : format d'un certificat, algorithme de validation de certificats, ...

Contenu d'un Certificat

- Version du standard X.509v3

```
Version: 3 (0x2)
```

- Numéro de série (unique à chaque certificat) :

```
Serial Number:
    0F:65:02:4B:CE:25:49:15:F3:14:72:26:33:16:11:86
```

- Émetteur (Issuer) :

```
CN = DigiCert SHA2 Extended Validation Server CA
OU = www.digicert.com
O = DigiCert Inc
C = US
```

- Période de validité (Validity) :

```
Validity
  Not Before: 11/10/23, 00:00:00 GMT
  Not After : 12/11/24, 23:59:59 GMT
```

Contenu d'un Certificat

- Sujet (Subject) :

```
CN = www.ubs.com
O = UBS AG
L = Zuerich
C = CH
```

- Clef publique :

```
Subject Public Key Info:
  Public Key Algorithm: PKCS#1 RSA Encryption
  RSA Public Key: (2048 bit)
    Modulus (2048 bit):
        D3:3D:05:B1:46:0C:88:28:78:E4:70:6B:45:C8:64:E4
        3E:A8:70:16:9E:B2:0F:45:8F:FF:46:D1:C6:50:FE:67
        [...]
        7B:90:49:BB:13:2A:10:1F:AD:DC:1A:E7:B2:5A:3C:A2
        7E:96:F2:47:73:91:ED:35:E4:60:47:D0:D7:FB:2B:3A
    Exponent: 65537 (0x10001)
```

Contenu d'un Certificat

- Extensions X.509v3

```
X509v3 extensions:
    X509v3 Subject Alternative Name:
        DNS:www1.ubs.com, DNS:www2.ubs.com, DNS:www.ubs.com
    X509v3 Basic Constraints:
        CA:FALSE
    X509v3 Key Usage:
        Digital Signature, Key Encipherment
    X509v3 CRL Distribution Points:
        URI:http://crl3.digicert.com/sha2-ev-server-g3.crl
X509v3 Extended Key Usage:
    Server Authentication, Client Authentication,
```

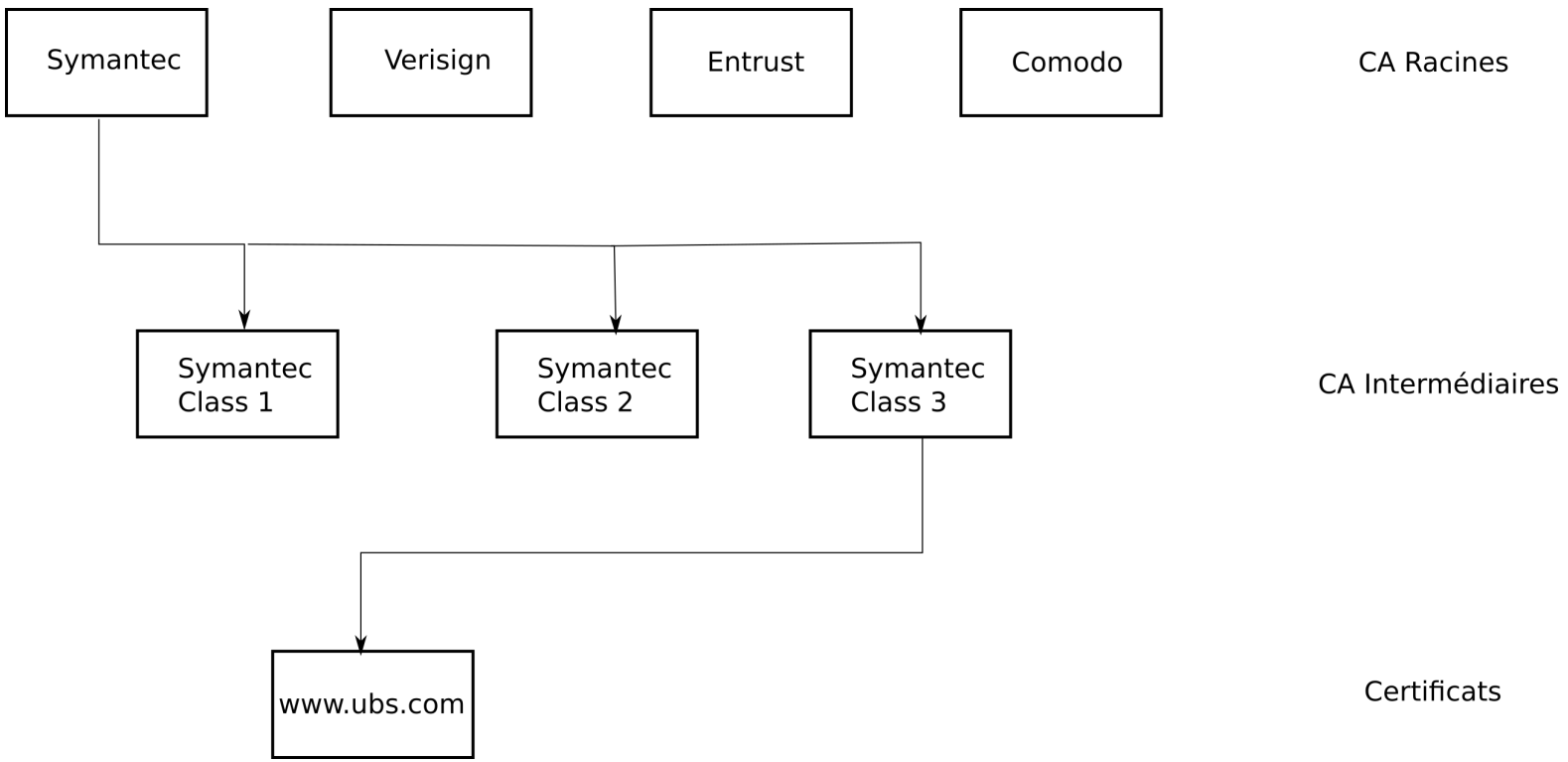
Contenu d'un Certificat

- Signature de l'autorité de certification

```
Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        01:c4:cb:86:ad:8d:f1:d7:ab:14:57:ea:9b:06:e1:d5:5b:11
        89:86:0c:57:da:a0:60:ed:2e:7b:17:fe:63:4c:5d:4b:a4:15
        [...]
        42:20:50:74:3d:44:8d:f0:d0:02:92:51:71:21:68:98:07:91
        11:31:aa:f0
```

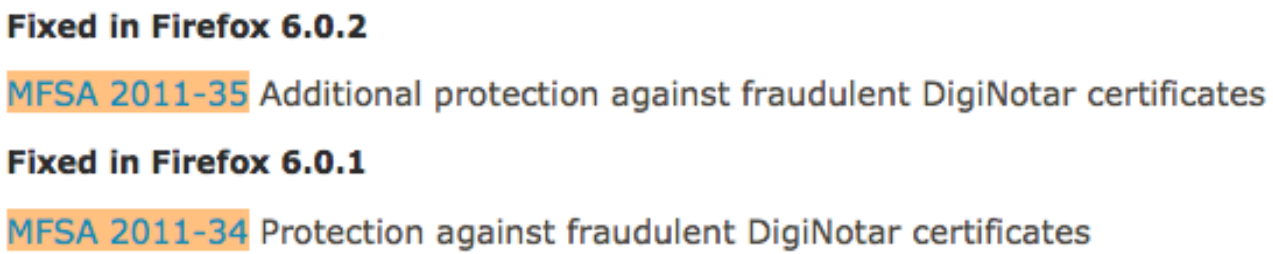
Hiérarchie de Certification

- Une PKI X.509v3 est de type **hiérarchique**. D'autres types, plus décentralisés, existent également (PGP, ...)



Hiérarchie de Certification

- Les certificats tout en haut de la hiérarchie sont appelés des **certificats racines**.
- Ils sont **auto-signés**, et possèdent souvent une longue validité (10-30 ans).
- Certificats racines souvent stockés **en dur** dans un navigateur web ou dans un OS.



- Les certificats racines sont utilisés pour signer des **certificats intermédiaires** (plus d'un niveau possible), qui eux sont utilisés pour signer des certificats individuels.

Certificats Intermédiaires

Question

Pourquoi avons-nous besoin de certificats intermédiaires ?

Infrastructure à Clefs Publiques (PKI)

Définition (PKI)

Une **infrastructure à clefs publiques** («Public-Key Infrastructure (PKI)») est un ensemble d'éléments matériels, logiciels, de protocoles et de services permettant de gérer des clefs publiques à grande échelle.

Question

Qui doit générer les clefs ? L'autorité de certification ou son propriétaire ?

Eléments Vitaux à Vérifier dans un Certificat

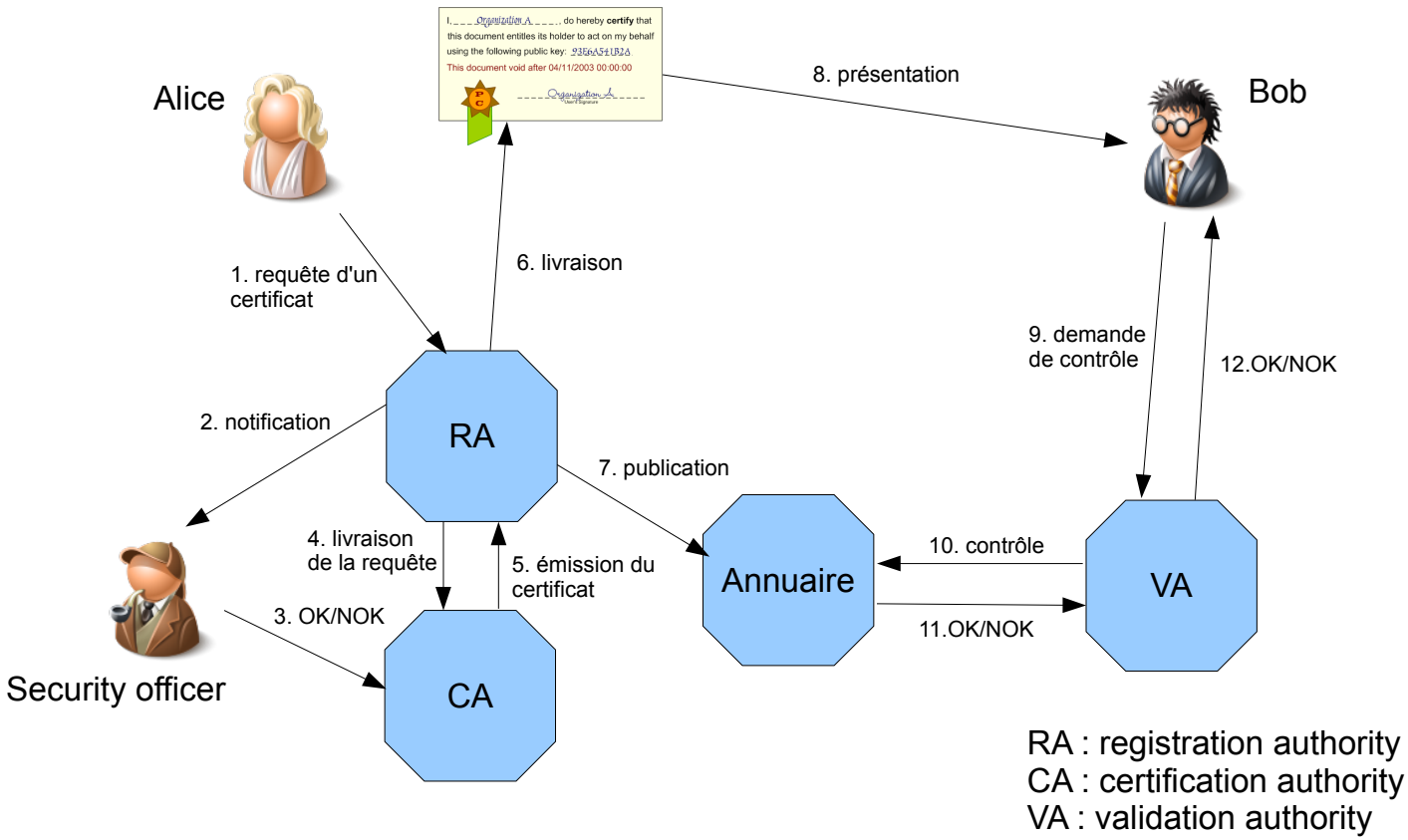
- Date de validité
- Sujet correct
- Signature valide
- Chaîne de signatures valides
- CA = True pour les CAs.
- Révocation
- ...

Non-vérification du Sujet

Question

Un site marchand utilise un logiciel permettant de créer un tunnel sécurisé entre son site et la banque. Ce tunnel est utilisé pour valider les transactions. Malheureusement, ce logiciel a un bug. Les signatures et dates sont correctement vérifiées. Par contre, le sujet ne l'est pas. Que peut faire une attaquant ?

Processus dans une PKI X.509



Autorité de Certification (CA)

- Emet et renouvèle les certificats.
- Emet et renouvèle les **listes de révocations (CRL)**.
- La liste de révocation contient les numéros de série des certificats révoqués ; cette liste est signée par la CA.
- La sécurité de la CA est primordiale, car une grande partie de la confiance mise dans la PKI repose sur elle.
- N'importe qui peut se dire CA.
- En pratique, une CA est publique si certifiée par les certificats racines contenus dans les navigateurs et systèmes d'exploitation les plus courants.

Autorité de Certification (CA)

Home > Security

News

DigiNotar dies from certificate hack caper

'Unlikely many are going to shed tears' over Dutch company's demise, says security researcher

By Gregg Keizer
September 21, 2011 04:09 PM ET

Like 16

Computerworld - The Dutch company that was hacked earlier this summer by certificate thieves has gone bust and shut down, its U.S.-based owner said Tuesday.

DigiNotar filed for bankruptcy in a Netherland court on Monday, and its assets will be liquidated by a court-appointed trustee, said Vasco Data Security International, the Chicago company that purchased DigiNotar last January for $13.1 million.

"Effective as of the beginning of business today, the Trustee has taken over the management of DigiNotar's business activities," Vasco said in a statement on Tuesday.

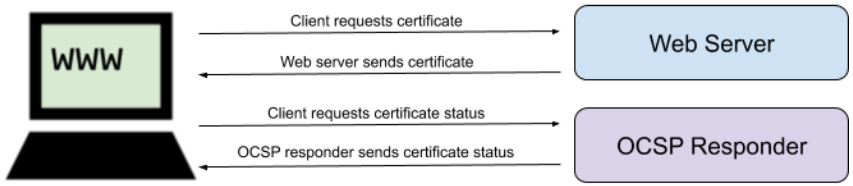
In late August, DigiNotar admitted that hackers had illegally generated numerous SSL (secure socket layer) certificates, including one for *google.com* that was later found to have been used to spy on some 300,000 Iranians through their Gmail accounts.

Source `http://www.computerworld.com/s/article/9220175/DigiNotar_dies_from_certificate_hack_caper`

Autorité d'Enregistrement (RA)

- Gère les demandes de certificats.
  - Stocke et contrôle les données d'identification
  - Communique avec l'entité
  - Vérifie le respect de la politique de certification (liée dans le certificat)
  - Publie les certificats et les CRLs.
- Par exemple, une banque, une administration, ou un guichet de poste peut offrir des services (partiels) de RA.

OCSP



- Utiliser des **CRL**s pour revoquer demande au client de récupérer la liste complète des certificats révoqués.
- Online Certificate Status Protocol (OCSP) : demande le statut d'un certificat au serveur OCSP.
- Problème : vulnérable à des **replay attacks** si pas de nonces (la plupart du temps).
- **Vie privée** : les clients informent un serveur externe des sites visités.
- **Charge** sur les serveurs OCSP : ils doivent répondre à chaque requête.

OCSP Stapling

- Résout les problèmes précédents : le **serveur** agit comme un proxy et stoque des réponses OCSP avec un **time-stamp**.
- Si aucune réponse du serveur, fallback sur un OCSP normal.
- Doit être **activé** sur le serveur
  (p. ex. sur Apache : `sssl stapling on;`
  `ssl_stapling_verify on;`)
- Petit **délai** lorsque un certificat est révoqué (la dernière réponse doit expirer).

Règles de Certifications

- Une CA doit déclarer les pratiques qu'elle utilise dans un document appelé **«Certification Practice Statement»**.
- Plus l'effort fait par la RA pour vérifier l'identité de l'entité est grand, plus le certificat sera cher, et plus la sécurité sera bonne.
- **«Extended Validation (EV)»** : la norme la plus stricte actuellement.

Certificats de Type EV

- Établissement de l'identité légale ainsi que de la présence opérationelle et physique de l'entité ;
- Vérification que l'entité possède bien les droits sur le nom de domaine désiré ;
- Confirmation légale de l'identité et des droits établie par un notaire.

Règles de Certifications

Exemple des règles appliquées par Verisign Inc. (état en janvier 2012)

3.2.3 Authentication of Individual Identity

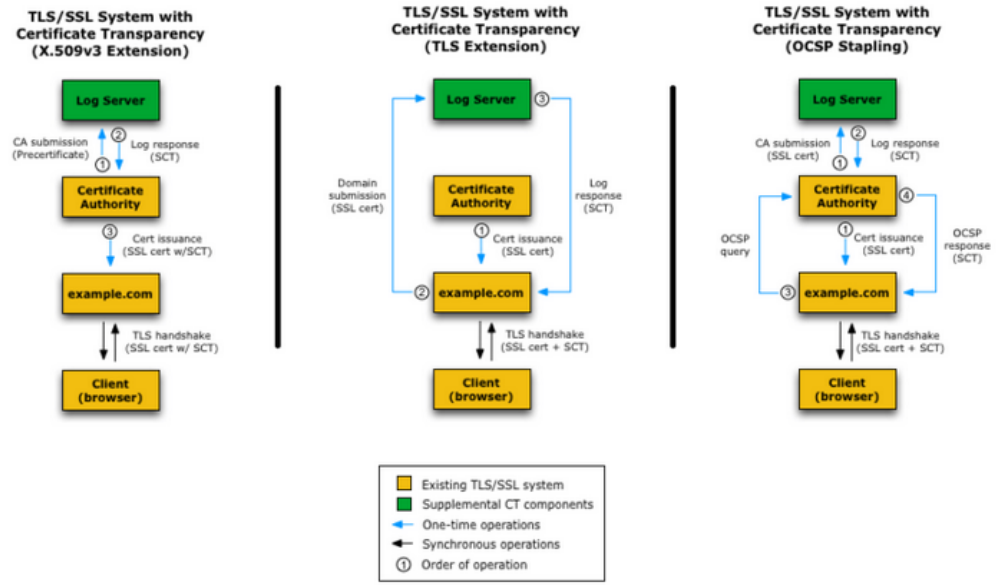
Authentication of individual identity differs according to the Class of Certificate. The minimum authentication standard for each class of VTN certificate is explained in Table 7 below.

Certificate Class	Authentication of Identity
Class 1	No identity authentication. There is a limited confirmation of the Subscriber's e-mail address by requiring the Subscriber to be able to answer an e-mail to that address.
Class 2	Authenticate identity by matching the identity provided by the Subscriber to: ▪ information residing in the database of a Symantec-approved identity proofing service, such as a major credit bureau or other reliable source of information providing, or ▪ information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals
Class 3	The authentication of Class 3 individual Certificates is based on the personal (physical) presence of the Certificate Applicant before an agent of the CA or RA, or before a notary public or other official with comparable authority within the Certificate Applicant's jurisdiction. The agent, notary or other official shall check the identity of the Certificate Applicant against a well-recognized form of government-issued photographic identification, such as a passport or driver's license and one other identification credential. The authentication of Class 3 Administrator certificates is based on authentication of the organization and a confirmation from the organization of the identity and authorization of the person to act as Administrator. Symantec may also have occasion to approve Certificate Applications for their own Administrators. Administrators are "Trusted Persons" within an organization. In this case, authentication of their Certificate Applications shall be based on confirmation of their identity in connection with their employment or retention as an independent contractor and background checking procedures.[8]
Shared Service Provider Certificates for Non Federal entities	The identity of the Certificate Subscriber is verified substantially in compliance with the requirements of the X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) and the VeriSign® Non-Federal Shared Service Provider (SSP) Certification Practice Statement.

Table 7. Authentication of individual identity

Source http://www.verisign.com/repository/CPSv3.8.4_final.pdf

Certificate Transparency



- Comment détecter si un CA est corrompu et émet des faux certificats ?
- **Certificate transparency** (obligatoire depuis 2018) : les CAs doivent logger tous leurs certificats.
- Preuves que le certificat est loggé : signed certificate timestamp (SCT) envoyées avec le certificat

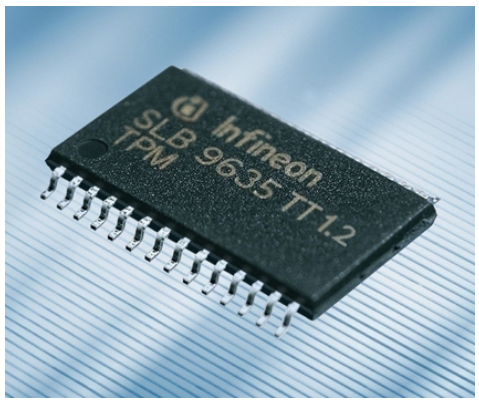
Image : https://cheapsslsecurity.com/blog/what-is-certificate-transparency-ct-how-does-it-work/

PKI en Pratique

- Utilisation des certificats X.509v3 :
  - SSL/TLS : authentification du serveur, et, en option, du client
  - IPSec, smartcard logon, ... : authentification de l'entité ;
  - S/MIME : signature de courrier électronique ;
  - Windows OS, Apple iOS, Android : signature de code.
- Points critiques d'une PKI :
  - Stockage des clefs privées
  - PRNG utilisé pour générer les clefs (cf. le fiasco Debian, voir http://en.wikinews.org/wiki/Predictable_random_number_generator_discovered_in_the_Debian_version_of_OpenSSL).

PKI en Pratique

- Stockage sécurisé des clefs :
  - **«Hardware Security Module»** : ordinateur blindé physiquement



  - Cartes à puces («smartcard»)

SSL/TLS

- La famille de protocoles cryptographiques **SSL** («Secure Socket Layer») et **TLS** («Transport Layer Security») offre les fonctionalités suivantes :
  - Authentification (unidirectionnelle ou mutuelle) avec infrastructure X509v3.
  - Confidentialité et intégrité des communications ;
  - Négociation des algorithmes cryptographiques utilisés ;
  - Gestion des clefs de session ;
  - Compression des communications, etc.

Historique de SSL/TLS

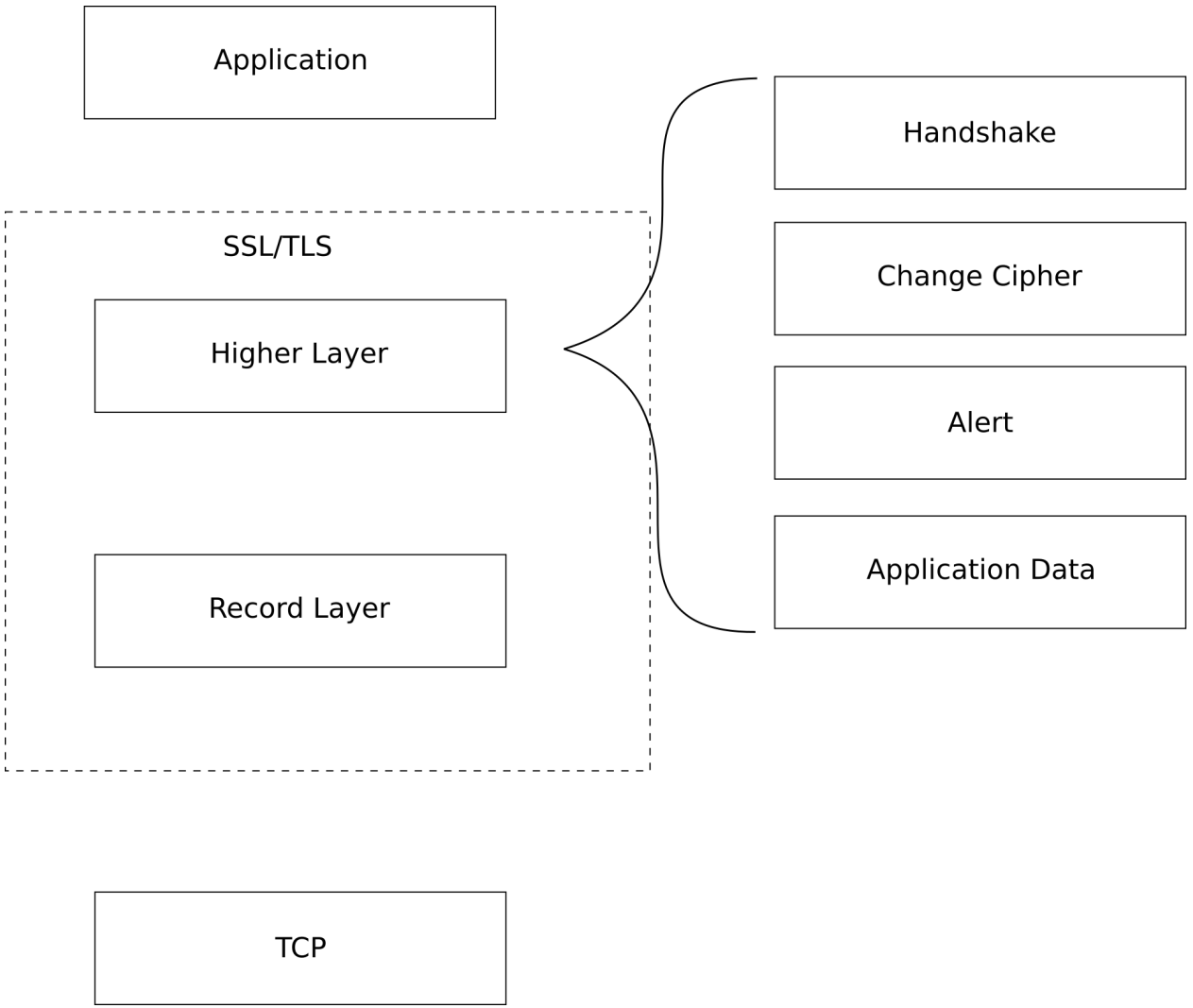
SSL v1.0	Netscape	1993 (?)	Jamais publié
SSL v2.0	Netscape	1995	Contient de nombreuses failles de sécurité
SSL v3.0	Netscape	1996	Voir également la RFC 6101 (publié comme document historique par l'IETF)
TLS v1.0	IETF	1999	RFC 2246.
TLS v1.1	IETF	2006	RFC 4346. Protection contre un certain nombres de problèmes sécuritaires en relation avec le mode CBC.
TLS v1.2	IETF	2008	RFC 5246 and RFC 6176. Support de SHA-256 dans la PRF. Version la plus rencontrée.
TLS v1.3	IETF	2018	RFC 8446. Nouveau design propre. Version la plus sûre.

Ce cours

TLS 1.2

Dans ce cours, nous nous focalisons sur TLS 1.2 qui est la version la plus rencontrée.

Fonctionnement de SSL/TLS



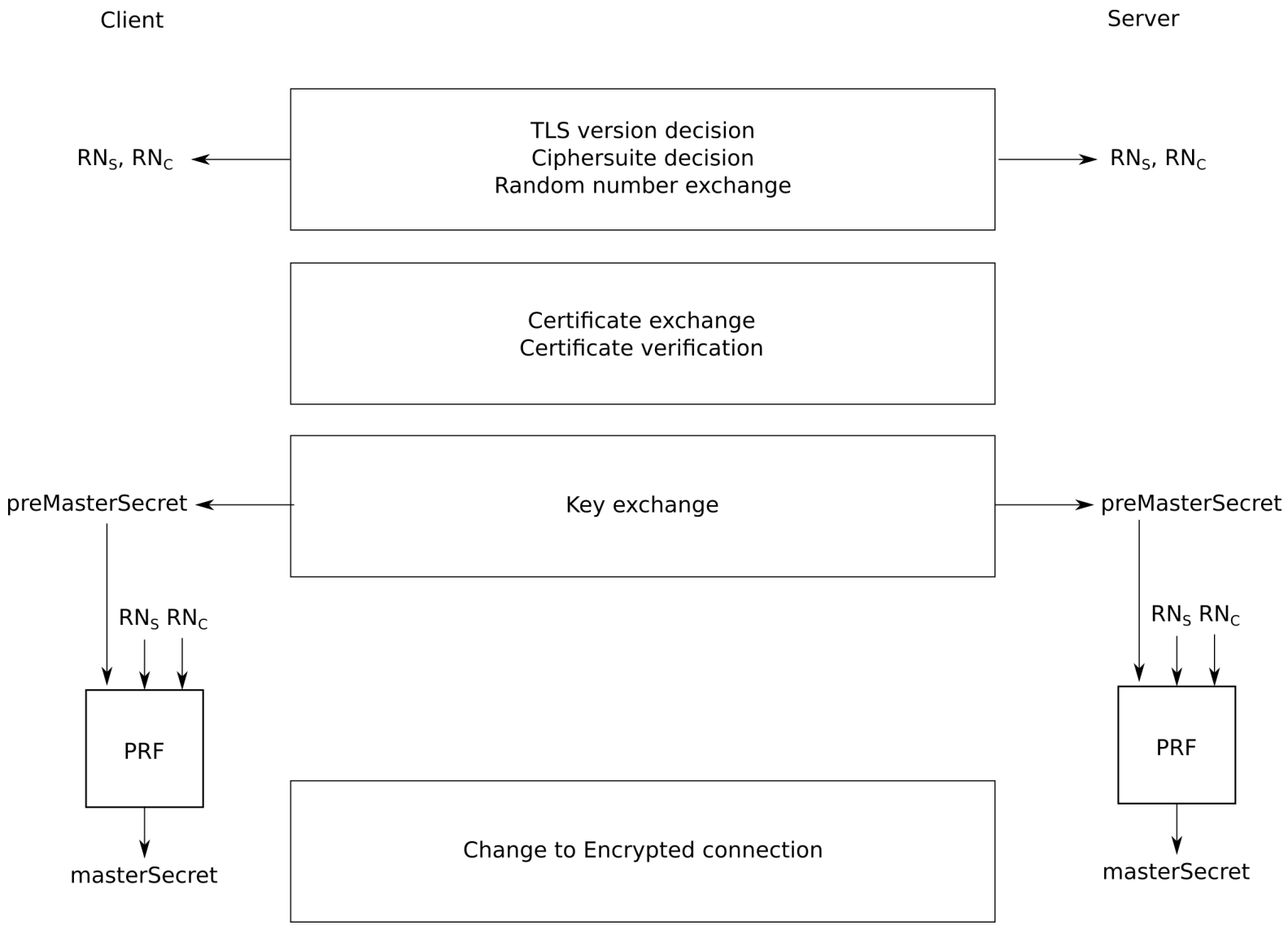
SSL/TLS Record Layer (jusqu'à TLS 1.2)

- Cette couche du protocole SSL/TLS est responsable de :
  - Traitement des données échangées (fragmentation) ;
  - Compression des données (facultatif) ;
  - Chiffrement et déchiffrement symétrique des données ;
  - Authentification symétrique et contrôle de l'intégrité des données.
  - Communiquer avec la couche TCP.

SSL/TLS Higher Layer

- **Handshake protocol** permet de choisir les algorithmes cryptographiques et d'échanger des clefs.
- **Change Cipher Spec Protocol** permet de signaler une transition de mode (chiffré / clair), par exemple à la fin du «handshake».
- **Alert Protocol** permet de signaler à l'application des erreurs ou des avertissements concernant la session en cours.
- **Application Data protocol** permet de passer les données de l'application de manière transparente au «record layer».

Protocole de Handshake SSL/TLS (jusqu'à TLS 1.2)



«Ciphersuites» SSL/TLS (jusqu'à TLS 1.2)

- Une «ciphersuite» est une combinaison nommée d'une méthode d'authentification, d'un algorithme de chiffrement ainsi que d'un MAC.
- **Structure** : `Prot_EchCléEtAuth_WITH_ChiffrSym_FonctHach`
- **Protocole** : `SSL`, `TLS`
- **Échange de clef** : `NULL`, `RSA`, `DH_anon`, `DHE`, `ECDHE`, `ECDH_anon`
- **Authentification** : `NULL`, `RSA`, `RSA_EXPORT`, `KRB5`, `PSK`, `DSS`, `ECDSA`, ...
- **Chiffrement symétrique** : `NULL`, `RC4_40`, `RC4_128`, `RC2_CBC_40`, `IDEA_CBC`, `DES40_CBC`, `DES_CBC`, `3DES_EDE_CBC`, `AES_128_CBC`, `AES_256_CBC`, `AES_128_GCM`, `AES_256_GCM`, ...
- **Hachage** : `SHA`, `MD5`, `SHA256`, `SHA512`,...

«Ciphersuites» SSL/TLS

- Exemples :

  ```
  TLS_NULL_WITH_NULL_NULL
  TLS_RSA_EXPORT_WITH_RC4_40_MD5
  TLS_RSA_WITH_RC4_128_SHA
  TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
  TLS_RSA_WITH_AES_256_CBC_SHA
  ...
  ```

- Une liste exhaustive des «ciphersuites» définies est disponible sous http://www.iana.org/assignments/tls-parameters/tls-parameters.xml
- Néanmoins, toutes les implémentations du protocole SSL/TLS ne supportent pas forcément toutes ces «ciphersuites» !

TLS 1.3

- Suppression de la cryptographie cassée.
- Handshake plus rapide.
- Sécurité du handshake plus rapide.
- Attention au 0-RTT.

Recommandation

Utilisez TLS 1.3 dès que possible !

Solutions

Obtenir un canal confidentiel

Solution

Pour une clef symétrique, il faut un canal authentique, intègre et confidentiel. Pour une clef asymétrique, il faut un canal authentique et intègre.

Obtenir un canal confidentiel

Solution

Il nous faut un mécanisme d'authentification. Par exemple, un autre canal de communication (courrier, téléphone) afin d'authentifier une clef asymétrique. Une autre solution est d'utiliser un intermédiaire de confiance.

Non-vérification du Sujet

Solution

Un attaquant peut simplement créer un certificat valide à son nom et faire une attaque man-in-the-middle. Le logiciel va demander le certificat et l'attaquant va fournir le sien. Même si ce certificat ne correspond pas au certificat de la banque, il est valide et sera accepté par le site marchand. L'attaquant pourra donc récupérer les informations du client.

Certificats Intermédiaires

Solution

Ils sont plus faciles à révoquer que les certificats racines et sont utilisés plus souvent que les certificats racines.

Infrastructure à Clefs Publiques (PKI)

Solution

Toujours le propriétaire.