Cryptographie & PKI

Mickael Rigonnaux
Twitter : @tzkuat
mickael.rigonnaux@rm-it.fr
https://rm-it.fr
https://net-security.fr

Plan

- Introduction & Définitions
- Notions & Vocabulaires
- L’histoire de la cryptographie
- Les différentes types
- SSL/TLS
- GPG
- PKI
- Quantique ?

Définition “Cryptographie”

- Cryptologie = Science
  - Cryptanalyse
  - Cryptographie

Confidentialité, authenticité & intégrité.

“Ensemble des techniques de chiffrement qui assurent l'inviolabilité de textes et, en informatique, de données.”

Pourquoi utiliser la cryptographie ?

- Monde militaire
  - Enigma, César
- Vie privée
- Liberté
- Protection des données

Prise de conscience générale depuis 2016 & l’affaire Snowden.

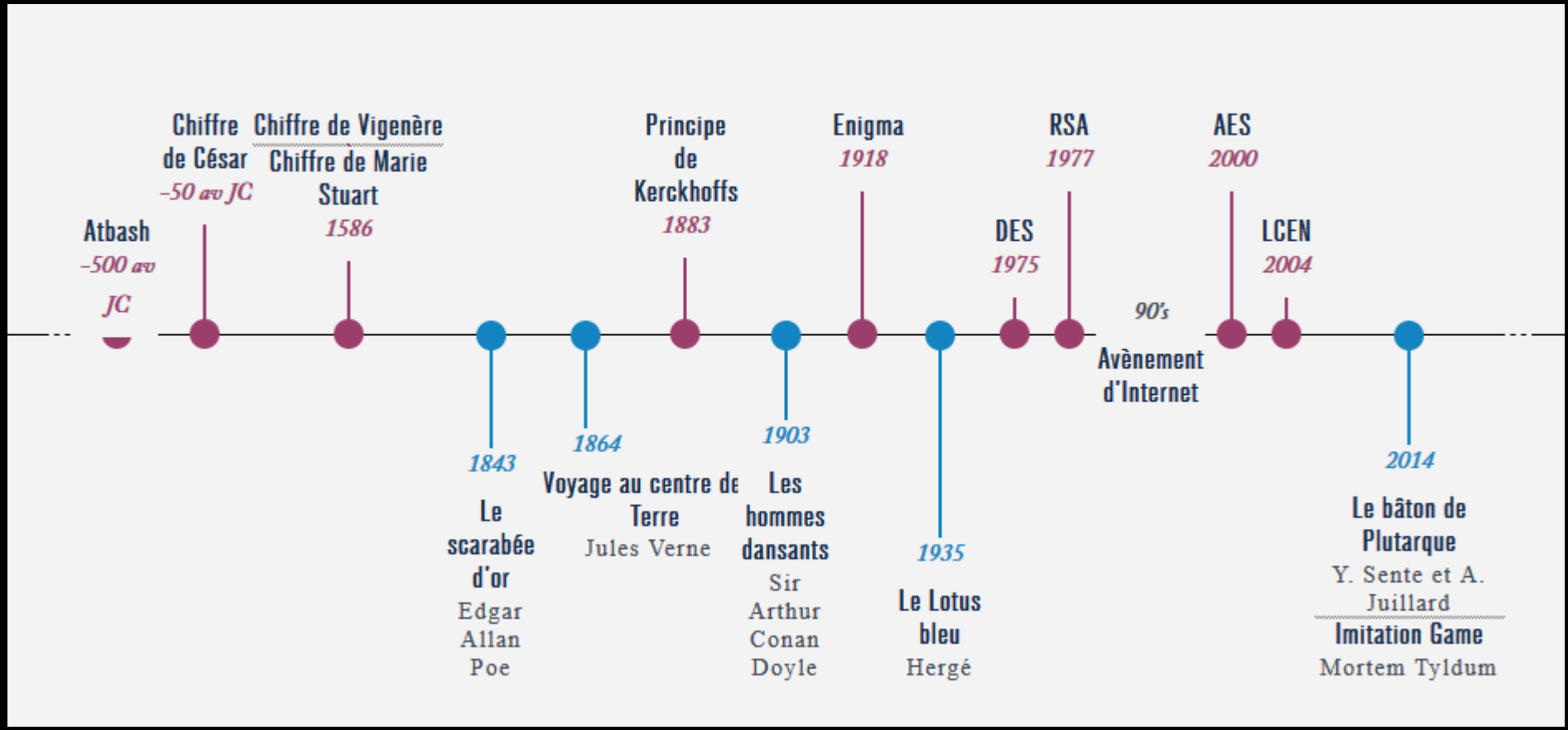
Vocabulaire

Cryptographie	**Chiffrer**	**Déchiffrer**
Discipline de la cryptologie visant à protéger des messages.	Réaliser un chiffrement, procédé de cryptographie par lequel on souhaite rendre la compréhension d'un document impossible à quiconque n'a pas la clé.	Retrouver le texte original d'un message chiffré dont on possède la clé.
Décrypter	**Message clair / chiffré**	**Crypter / cryptage**
Retrouver le texte original d'un message chiffré sans en posséder la clé.	Un message en clair est le texte original tandis que le message chiffré est le texte incompréhensible.	
Encrypter	**Chiffrage**	**Signature**
Anglicisme… donc non (et encore moins déencrypter…).	Evaluer le coût de quelque chose… donc rien à voir.	Mécanisme permettant de garantir l'intégrité d'un document et d'en identifier l'auteur.

Autres notions

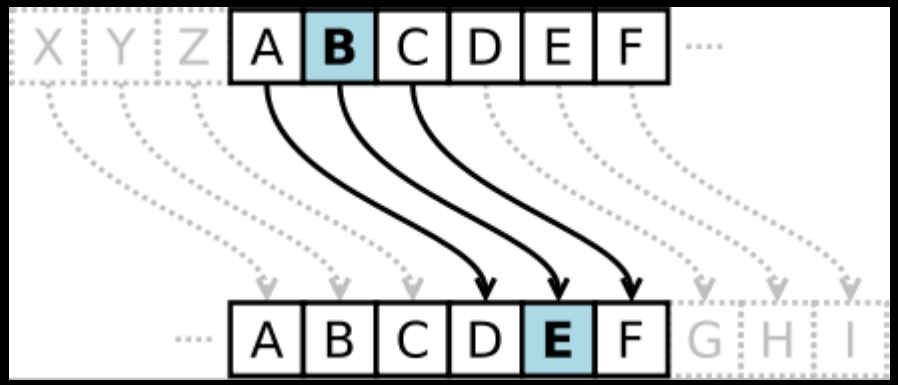
- Confidentialité
  - Cacher des informations aux personnes non-autorisées
- Intégrité
  - S’assurer que la donnée n’a pas été modifiée
- Disponibilité
  - S’assurer que la donnée soit accessible n’importe quand
- Non-répudiation
  - S’assurer qu’une action ne peut-être remise en cause
- Authentification
  - Identification des utilisateurs
- Traçabilité
  - Les élements sont tracés avec des traces conservées et exploitables

L’histoire de la cryptographie



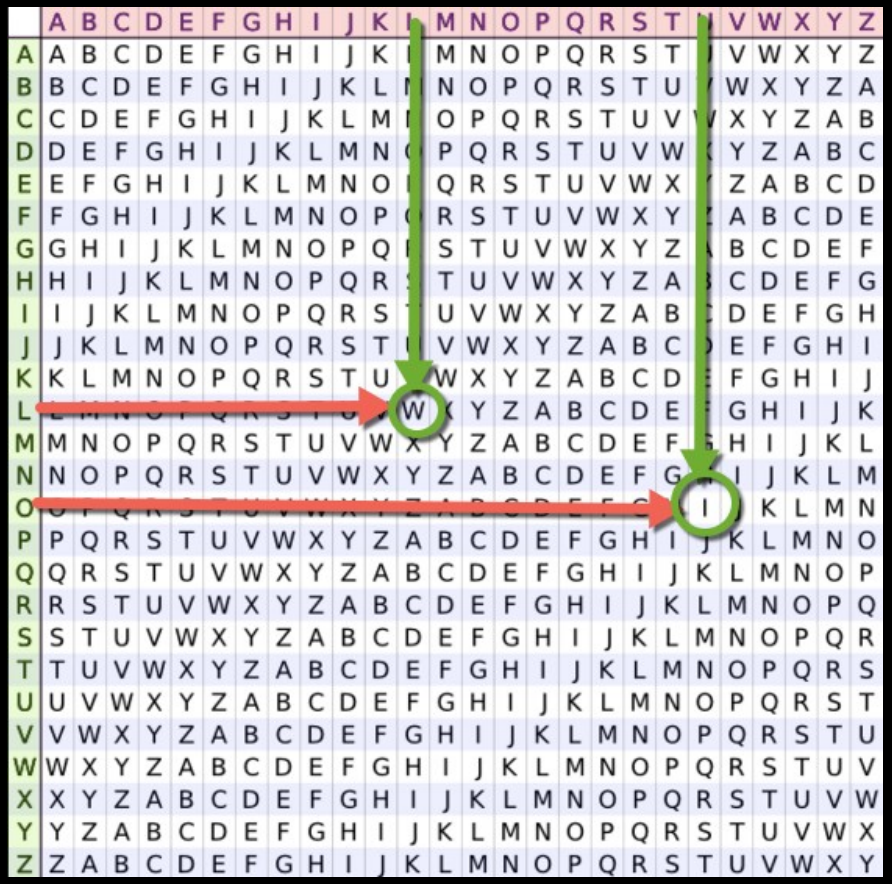
Le chiffre de César

- Utilisé par Jules César
- Utilisation militaire
- Très simple d’utilisation
- Chiffrement par substitution monoalphabétique



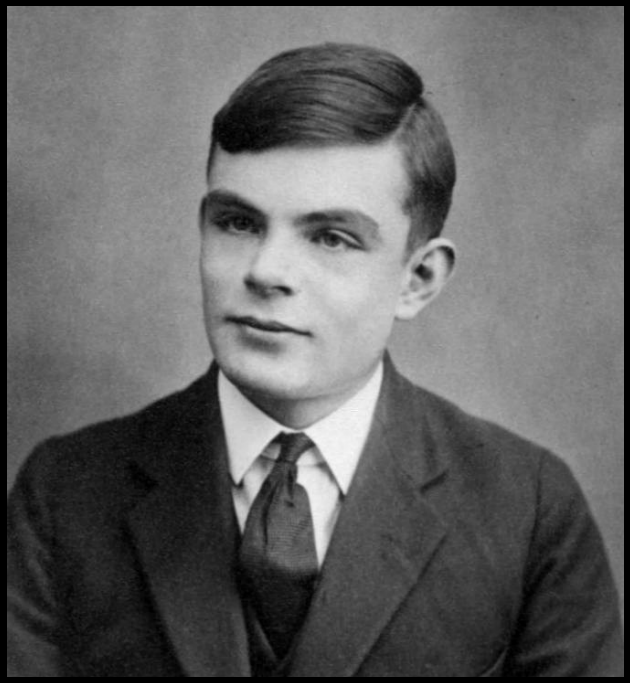
Le chiffre de Vigenère

- Inventé par Blaise de Vigenère
- Basé sur celui de César
- Très simple d'utilisation
- Chiffrement par substitution polyalphabétique



Enigma

- Machine utilisée par les allemands pendant le WW2
- Cryptanalyse par Alan Turing et son équipe
- Fondement de l’informatique



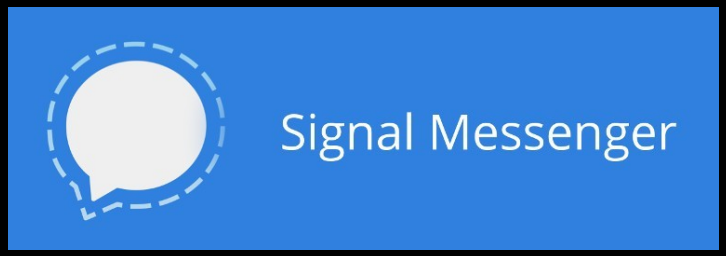
Aujourd’hui

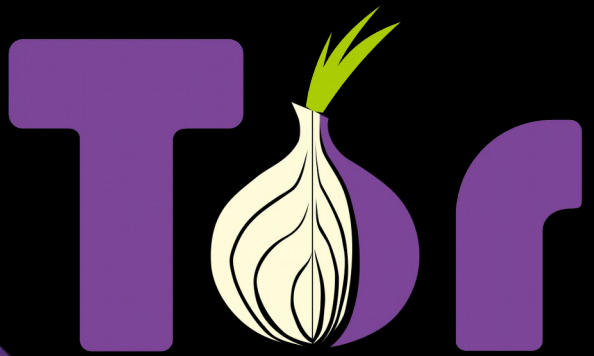
- Utilisation de la cryptographie, symétrique, asymétrique, hachage…
- SSL/TLS, GPG, AES, RSA, DES, SHA-X…
- La cryptographie est partout

Elle est le seul rempart contre l’espionnage ciblé & de masse

Aujourd'hui


ProtonMail

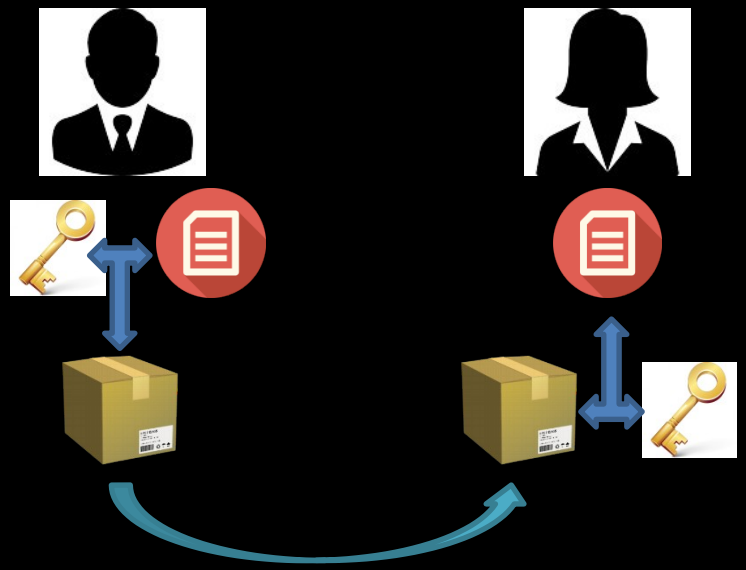

Signal Messenger


Tor


Tails
theamnesicincognitolivesystem

Chiffrement symétrique

- Secret partagé
- Comment transmettre la clé ?
- Non répudiation ?
- Rapidité ++
- Taille de clé



Chiffrement symétrique

- Chiffrement par bloc
  - Chiffrement en découpant les données en blocs de taille fixe (généralement)
- Chiffrement par flot
  - Chiffrement continu, pas de longueur de données

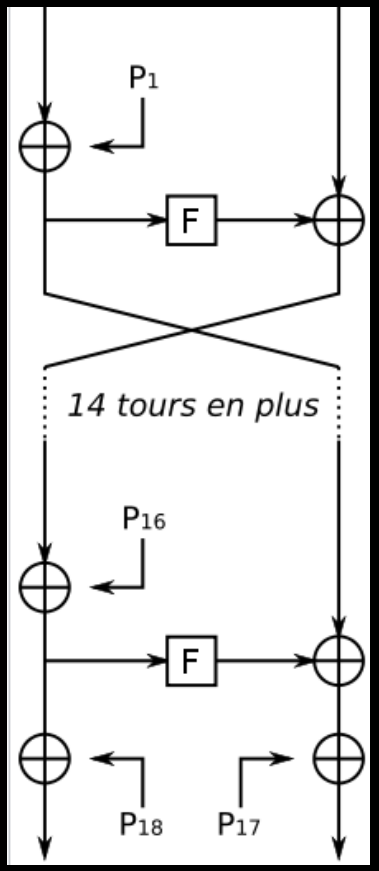
Chiffrement symétrique

- Les principaux protocoles

Obsolètes	Conseillés
DES	AES 128+
3DES	Blowfish / Twofish
RC4	CAST5
	ChaCha

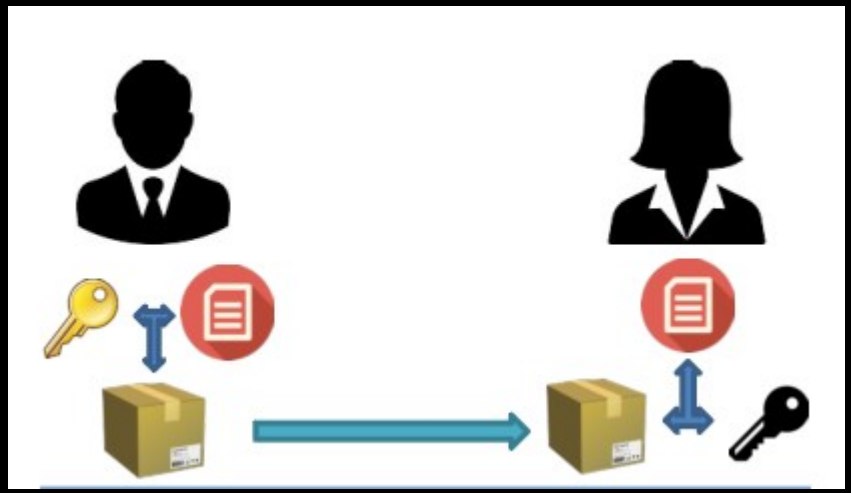
Chiffrement symétrique

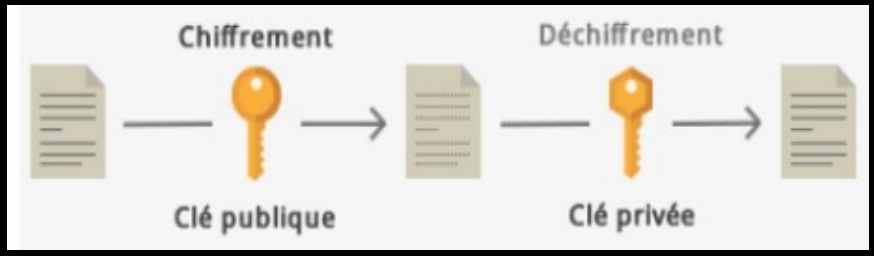
- Principalement basé sur des systèmes avec :
  - Des “xor”
  - Des matrices
  - Des tours



Chiffrement asymétrique

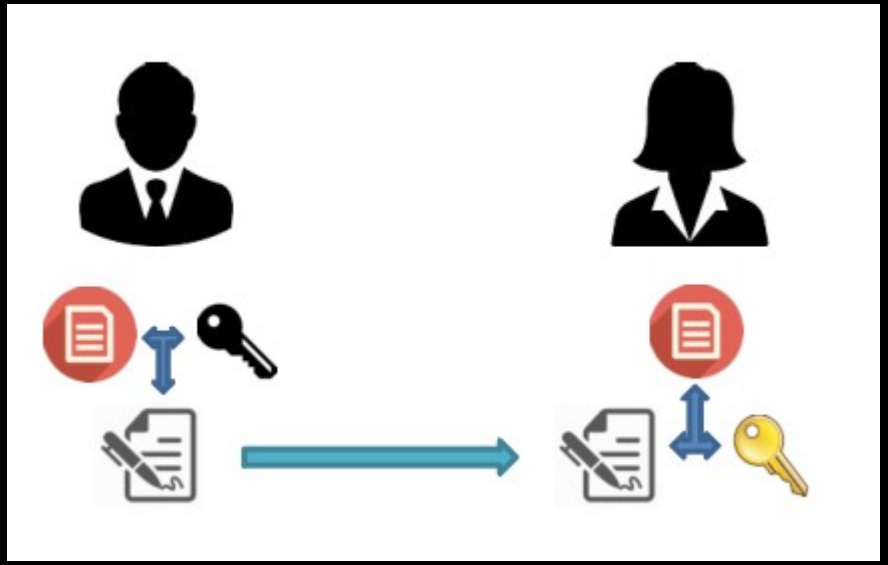
- Clé privée + publique
- Lent & Complexe
- Une paire de clé par correspondant
- Echange des clés





Chiffrement asymétrique

- Signature en utilisant la clé privée de l’expéditeur
- Permet l’authentification
- Vérification de l’intégrité



Chiffrement asymétrique

- Les 2 principaux systèmes
  - RSA & ECC
- Signature
  - RSA, DSA

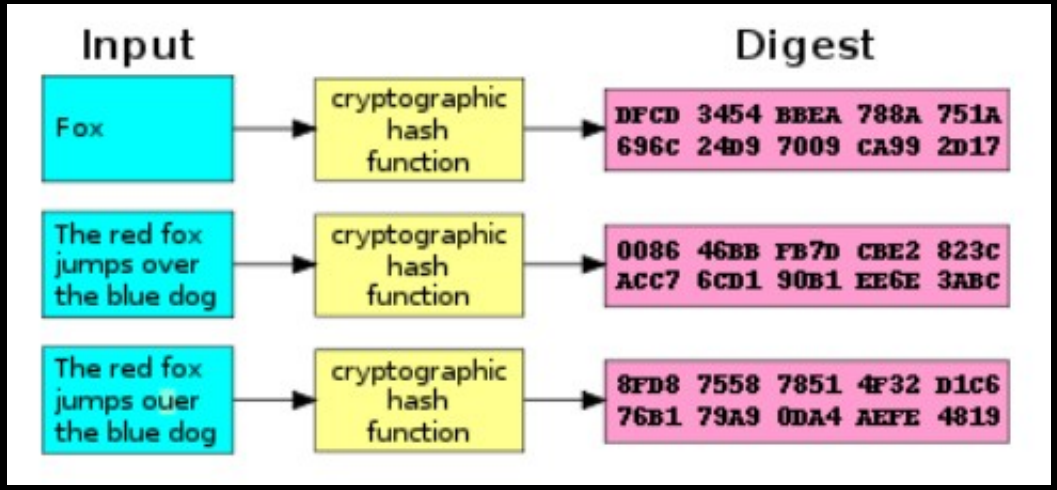
Symmetric	DH or RSA	ECC
56	512	112
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Chiffrement asymétrique

- RSA : Rivest, Shamir, Adleman
  - Problème RSA lié à la factorisation
  - n = p x q (p et q étant des grands nombres 1er)
- ECC : Elliptic Curve Cryptography
  - Problème du logarithme discret

Hachage (Hash)

- Création d’une empreinte unique à partir d’une entrée
- Propriétés :
  - Resistance aux collisions
  - Resistance sur les 2 préimages



Hachage (Hash)

- Les principaux protocoles

Obsolètes	Conseillés
SHA-0	SHA-2
SHA-1	SHA-3
MD5	BLAKE2

SSL/TLS

Secure Socket Layer / Transport Layer Security

- Défini par l'IETF
- Utilisation du chiffrement symétrique + asymétrique
- Version actuelle : TLS 1.3

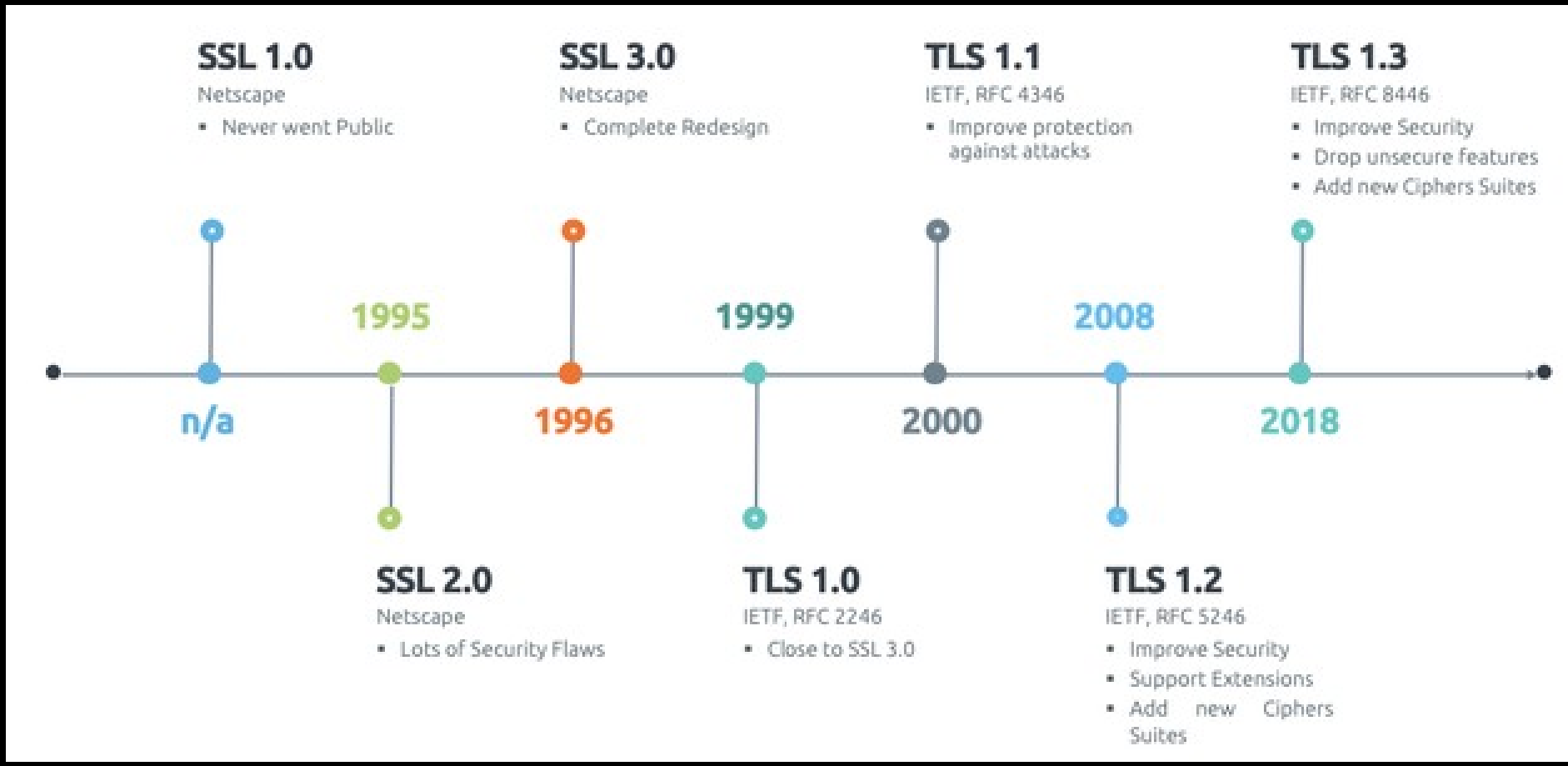
Utilisé pour HTTPS, LDAPS, FTPS…

SSL/TLS

Permet d’assurer :

- Confidentialité
- Intégrité
- Authentification

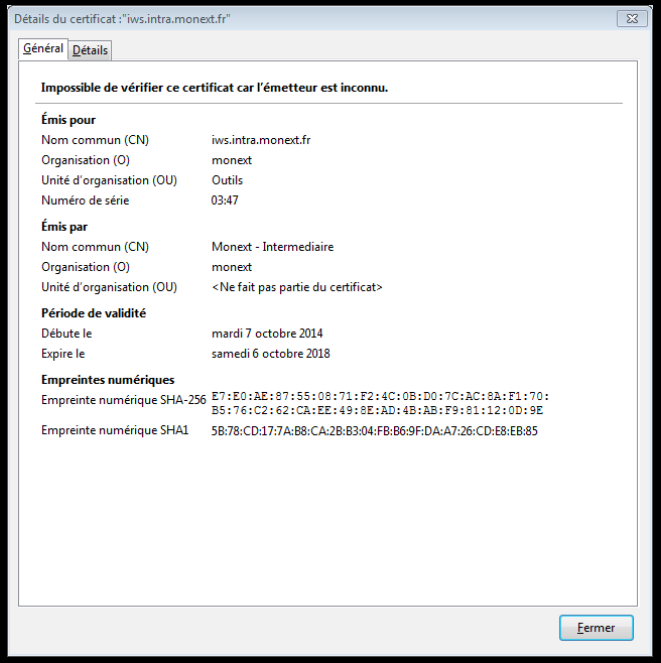
SSL/TLS : Historique



SSL/TLS : Certificat

Carte d'identité du serveur ou du client

- Lien entre physique et numérique
- Signé par un tier de confiance (CA)
- Client / Serveur / CA
- Certificat + clé
- Standard : X.509



- Création d'un certificat
  - Génération d'une clé privée
  - Génération d'une CSR
  - Signature de la CSR par une CA pour obtenir un certificat

SSL/TLS : Certificat

Structure d’un certificat X509

Version X.509
Numéro de série
Algorithme de signature du certificat
DN (distinguished name) du délivreur (autorité de certification)
Période de validité
DN de l’objet du certificat
Informations sur la clé publique
Extensions (optionnelles)
Signature des informations précédentes par l’autorité de certification

SSL/TLS : Certificat

Structure d’un certificat X509

```
-----BEGIN CERTIFICATE-----
MIIFRDCCBCygAwIBAgICAX0wDQYJKoZIhvcNAQELBQAwgZsxCzAJBgNVBAYTAkZS
MRkwFwYDVQQIExBCb3VjaGVzIGR1IHJob25lMRMwEQYDVQQHEwpBaXggZW4gUGNl
MQ8wDQYDVQQKEwZtb25leHQxKDAmBgNVBAMTH01vbmV4dCAtIEludGVybWVkaWFp
cmUgLSBzaGEyNTYxITAfBgkqhkiG9w0BCQEWEnNzbC10ZWNoQG1vbmV4dC5mcjAe
Fw0xNzAxMDIwOTMwMDVaFw0yMTAxMDEwOTMwMDVaMIGbMQswCQYDVQQGEwJGUjEZ
MBcGA1UECBMQQm91Y2hlcyBkdSByaG9uZTETMBEGA1UEBxMKQWl4IGVuIFBjZTEP
MA0GA1UEChMGbW9uZXh0MRIwEAYDVQQLEwl0aGUgU0VDT1AxFDASBgNVBAMUC21v
bl9zaXRlLmZyMSEwHwYJKoZIhvcNAQkBFhJzc2wtdGVjaEBtb25leHQuZnIwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCoDJUn0PHNYowWHYo3mhOfk0iE
dqmlgPCfC8kmPCuE2EnxIIpIEym+ZJbYEw/fUnx/OD21si1L9PTdUtvwsi9fXGO3
UY0zyEyJ6QlT/N/t4tpTrm+g53se4e6GFiFCCR9r/DQhDazgzZwFC2kmCNbnwCpw
SXVrw7REGfe0radlfrvJiBCxeL/jv09m2M2BpVC/2UZb00RrZ748uKFofEJAWTQf
lAjvi93XDUaWpWphCqbZ1/jM0b8vO2UkZjRPNhZD8IsKuRqyNWt/4juXEn+4r8QQ
9tmAym/MUpIsYcpiH8uxcj+4knVMNsYL/IjmQ2fo9xcCnSjWvT2mP3bTcsDRAgMB
AAGjggGOMIIBijAlBglghkgBhvhCAQ0EGBYWQ2VydGlmaWNhdCBTZXJ2ZXVyIFNT
TDAdBgNVHQ4EFgQU30MaKInc4N3Zvw97A/GEN/WRXfkwgbQGA1UdIwSBrDCBqYAU
xOoptl2RGy4R1h5UXClazTQQ/GWhgY2kgYowgYcxCzAJBgNVBAYTAkZSMRkwFwYD
VQQIExBCb3VjaGVzIGR1IHJob25lMRMwEQYDVQQHEwpBaXggZW4gUGNlMQ8wDQYD
VQQKEwZtb25leHQxFDASBgNVBAMTC01vbmV4dCAtIENBMSEwHwYJKoZIhvcNAQkB
FhJzc2wtdGVjaEBtb25leHQuZnKCAUAwCQYDVR0SBAIwADA9BgNVHREENjA0ghJt
b25fc2l0ZV9iYWNrdXAuZnKCEXVuX2F1dHJlX3NpdGUuY29tggttb25fc2l0ZS5m
cjAMBgNVHRMBAf8EAjAAMAsGA1UdDwQEAwIF4DARBglghkgBhvhCAQEEBAMCBkAw
EwYDVR0lBAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQELBQADggEBAKl12jyJRY+O
3xZK5UCeQszckybW5ptpNP8v0G+3W07C1qtJlrMqE1Js6pKRYSrWlEI4ZYwea9Oy
Aw8LIcislaAIzPrWI19JJp6EJLD7u8QtjuUdPeHI2nuex4Hp6LSFaJOLjzfyaulD
SwboMucpgh00B0/BLNbJ8Yorc39Y68hfXfiEmJH4p+G3yQTMALWa6IwzFiOz1AuG
tUmtNlBdbZNDHmtkBSvQiesNzas4Oa+4xrnx8Gf4qH1oEHkaIpD/q70IB2kK0mfF
y0HwA57+aSi/37Apa7k/weP7KqnvC6kHGEpdPJwErlkGo3ydWN3VSo68HAp/+tDh
QeNT0KhEFEw=
-----END CERTIFICATE-----
```

Version X.509
Numéro de série
Algorithme de signature du certificat
DN (distinguished name) du délivreur (autorité de certification)
Période de validité
DN de l’objet du certificat
Informations sur la clé publique
Extensions (optionnelles)
Signature des informations précédentes par l’autorité de certification

SSL/TLS : Certificat

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 381 (0x17d)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure
Server CA
        Validity
            Not Before: Jan  2 09:30:05 2017 GMT
            Not After : Jan  1 09:30:05 2021 GMT
        Subject: C=FR, ST=Corse, L=Ajaccio, O=Ynov, OU=SECOP, CN=mon site.fr/emailAddress=contact@rm-it.fr
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a8:0c:95:27:d0:f1:cd:62:8c:16:1d:8a:37:9a:
                    13:9f:93:48:84:76:a9:a5:80:f0:9f:0b:c9:26:3c:
                    2b:84:d8:49:f1:20:8a:48:13:29:be:64:96:d8:13:
                    0f:df:52:7c:7f:38:3d:b5:b2:2d:4b:f4:f4:dd:52:
                    db:f0:b2:2f:5f:5c:63:b7:51:8d:33:c8:4c:89:e9:
                    09:53:fc:df:ed:e2:da:53:ae:6f:a0:e7:7b:1e:e1:
                    ee:86:16:21:42:09:1f:6b:fc:34:21:0d:ac:e0:cd:
                    9c:05:0b:69:26:08:d6:e7:c0:2a:70:49:75:6b:c3:
                    b4:44:19:f7:b4:ad:a7:65:7e:bb:c9:88:10:b1:78:
                    bf:e3:bf:4f:66:d8:cd:81:a5:50:bf:d9:46:5b:d3:
                    44:6b:67:be:3c:b8:a1:68:7c:42:40:59:34:1f:94:
                    08:ef:8b:dd:d7:0d:46:96:a5:6a:61:0a:a6:d9:d7:
                    f8:cc:d1:bf:2f:3b:65:24:66:34:4f:36:16:43:f0:
                    8b:0a:b9:1a:b2:35:6b:7f:e2:3b:97:12:7f:b8:af:
                    c4:10:f6:d9:80:ca:6f:cc:52:92:2c:61:ca:62:1f:
                    cb:b1:72:3f:b8:92:75:4c:36:c6:0b:fc:88:e6:43:
                    67:e8:f7:17:02:9d:28:d6:bd:3d:a6:3f:76:d3:72:
                    c0:d1
                Exponent: 65537 (0x10001)
```

- Version X.509
- Numéro de série
- Algorithme de signature du certificat
- DN (distinguished name) du délivreur (autorité de certification)
- Période de validité
- DN de l'objet du certificat
- Informations sur la clé publique
- Extensions (optionnelles)
- Signature des informations précédentes par l'autorité de certification

SSL/TLS : Certificat

```
 X509v3 extensions:
            Netscape Comment:
                Certificat Serveur SSL
            X509v3 Subject Key Identifier:
                DF:43:1A:28:89:DC:E0:DD:D9:BF:0F:7B:03:F1:84:37:F5:91:5D:F9
            X509v3 Authority Key Identifier:

keyid:C4:EA:29:B6:5D:91:1B:2E:11:D6:1E:54:5C:29:5A:CD:34:10:FC:65
                DirName:C=GB/ST=Greater Manchester/L=Salford/O=Sectigo
Limited/CN=Sectigo RSA Domain Validation Secure Server CA
                serial:40

            X509v3 Issuer Alternative Name:
                <EMPTY>

            X509v3 Subject Alternative Name:
                DNS:mon_site_backup.fr, DNS:un_autre_site.com, DNS:mon_site.fr
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            Netscape Cert Type:
                SSL Server
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
```

- Version X.509
- Numéro de série
- Algorithme de signature du certificat
- DN (distinguished name) du délivreur (autorité de certification)
- Période de validité
- DN de l’objet du certificat
- Informations sur la clé publique
- **Extensions (optionnelles)**
- Signature des informations précédentes par l’autorité de certification

SSL/TLS : Certificat

```
Signature Algorithm: sha256WithRSAEncryption
       a9:75:da:3c:89:45:8f:8e:df:16:4a:e5:40:9e:42:cc:dc:93:
       26:d6:e6:9b:69:34:ff:2f:d0:6f:b7:5b:4e:c2:d6:ab:49:96:
       b3:2a:13:52:6c:ea:92:91:61:2a:d6:94:42:38:65:8c:1e:6b:
       d3:b2:03:0f:0b:21:c8:ac:95:a0:08:cc:fa:d6:23:5f:49:26:
       9e:84:24:b0:fb:bb:c4:2d:8e:e5:1d:3d:e1:c8:da:7b:9e:c7:
       81:e9:e8:b4:85:68:93:8b:8f:37:f2:6a:e9:43:4b:06:e8:32:
       e7:29:82:1d:34:07:4f:c1:2c:d6:c9:f1:8a:2b:73:7f:58:eb:
       c8:5f:5d:f8:84:98:91:f8:a7:e1:b7:c9:04:cc:00:b5:9a:e8:
       8c:33:16:23:b3:d4:0b:86:b5:49:ad:36:50:5d:6d:93:43:1e:
       6b:64:05:2b:d0:89:eb:0d:cd:ab:38:39:af:b8:c6:b9:f1:f0:
       67:f8:a8:7d:68:10:79:1a:22:90:ff:ab:bd:08:07:69:0a:d2:
       67:c5:cb:41:f0:03:9e:fe:69:28:bf:df:b0:29:6b:b9:3f:c1:
       e3:fb:2a:a9:ef:0b:a9:07:18:4a:5d:3c:9c:04:ae:59:06:a3:
       7c:9d:58:dd:d5:4a:8e:bc:1c:0a:7f:fa:d0:e1:41:e3:53:d0:
       a8:44:14:4c
```

- Version X.509
- Numéro de série
- Algorithme de signature du certificat
- DN (distinguished name) du délivreur (autorité de certification)
- Période de validité
- DN de l’objet du certificat
- Informations sur la clé publique
- Extensions (optionnelles)
- Signature des informations précédentes par l’autorité de certification

SSL/TLS : Certificat

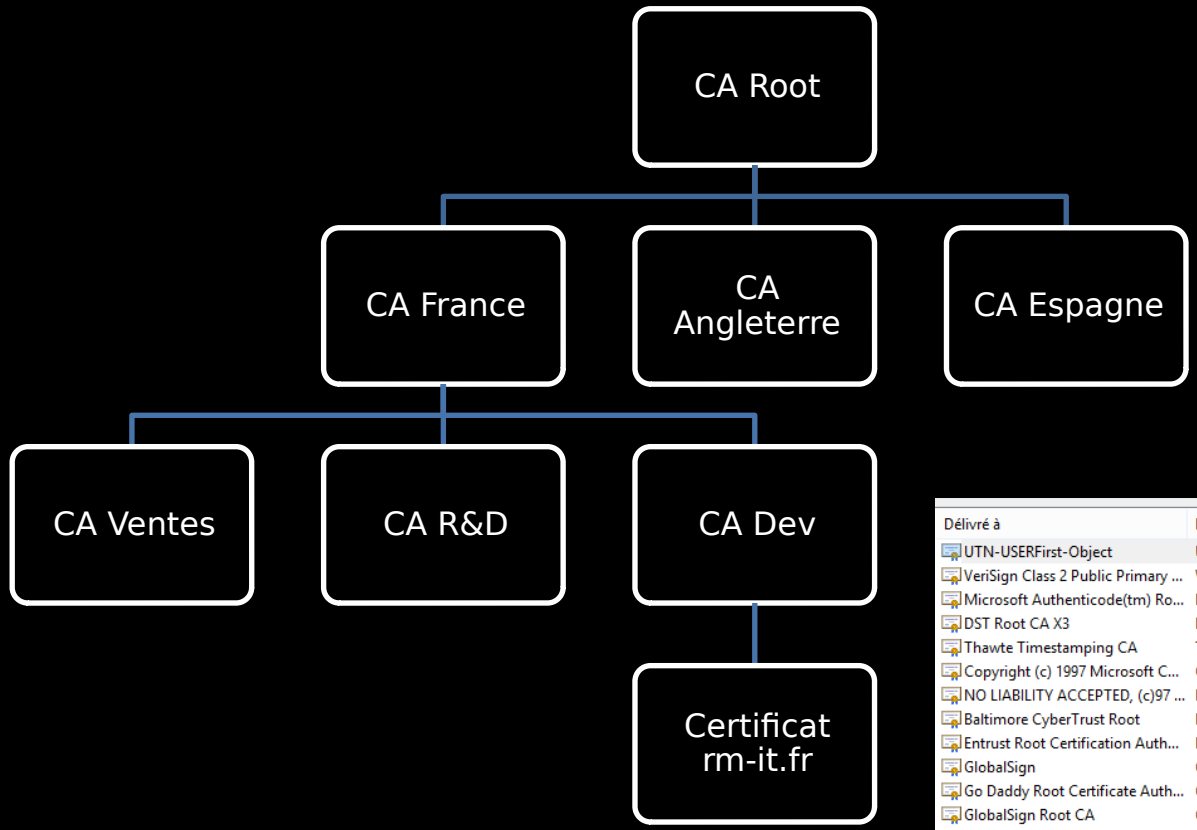
```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAnmzO1+9AR0ctYD+QwlQLpYifIc02IWdevHpxglUFwof14R0i
Xl5q7WNjV6OKefKJmGfgFeB4wHwCwVbIq44WlI+ZYl6xBU5NyW4V1WMprN2INykH
ahAOiet//hgbGQNWes63H1tFK9YDSz0sL7rmrwo6IerpmjY4nZOZAtMr8uuswvVB
4o7sZvaXAHmVujswuCI35KDtYtZ23Q8Z1ULfxAqLWYH2C58E2OH9dv5hS+Q+dTG2
SWxML9/8Has6MgSyoJv23VGK5afgv1DgNEUi5v59MDVGt43OeBSAFqQfg9lJCAzW
mk1itt8p5y5ibhrM8dL/tVoi76aNkcGpPGOIXwIDAQABAoIBAQCbh3CNVwlAsKTg
b6ca0E3axcSL952jr4q2+HIFJJkSAE4oIWUDRigtQzxc5mXlEHF6mMfKUmPZfCVs
T1mT6ltKn6tSgmnBLr14+cUfh0l7tsSqenIX8wmC5xrxhhLcPIWi7NukQgMnZOQ4
8iY1+YPM5fpqH+gUCBUOxb8aodvsj1zN36u1zEb9bzWf5v5woCk9nQIvaXx9h2lM
Kw9iR/nzUc0llg+bOdi622ZjQM4BGSQ/k8SZ97QG7QEmQH3U4Iazeo694WWwBJU9
IjLtb8pXUl72EnTwXDhbTBzmgeNfqJg0UNn7A7GIajywzUFIPeMeXxQoXZDtBiPS
1ZBJnHQRAoGBAMstNCARzpkV2Pc9f+uAjPeqxQ3vW8P/n3pqZE0Ef5cFFq2sDcD3
lCJl5eRpib++QZqSAqQ9gx86kWIhKqr+4nCRgp8Et6M5EnfgDQGLVfosLQ5kQxMJ
GucDGLLCQtf7n3x5N4gYxYPj6Vx6wPSbOw6KdABLqylZOaEE5LAhXpnJAoGBAMed
FOr+9WSpgbi8pG9d2b6vbbFyXWfYPD84TIZ0bjKrbtg7m651TTGKFwCbgJ5YvSmN
dDMZunqezx/bMSrlxi71ysEpmX8yqQ12IdqMEXhiJh+BwumOCCutc1womMUc3de6
Jcd7UikkWJMn8UMp6IcdmNlibVJQtN4YTI66cqTnAoGAWBkMrg8qlwR7JJF9Ix+F
gGqCsU0lbDIt84WoYiDeNhyVvc6J1C9GAzhN26HLgeG8ToqbLJ4jeeoKWhNpjeWh
SBBAJDWGbvbzRBlZal8Bc82t57yfvORIzvxvvCsxkrdfazigVJnxIwQzDs+HVUjt
7ZspO2uUFwTCUUhu5NRDUckCgYEAkXu+JCvghBY60n7Cxdw7+At5wkudIjNqbZVF
yPUQ3+MsbXK8W6FouoNvkmTDkCUS8TcEir3kuLwIL6qcoixHjjBcLv53vkoZBhOk
RtmxXfEC4hG8EmcPM24+VtvLxFXupe0o3cPWtN+lotMIty/TJq7+mOlwzf6+Y+SH
37qqFd8CgYBsFi8+coCMLFzUkwK1A5zy5YEs1WjPnXQKeBLQD6LF9am9goqUPuoT
V2CKDG0f7Cl2GBtB3dBvK1qA1i+DWGwDIGIe9KlOBmC5MSYmiP9ppx8Hd8oROq1Q
G+Va+ykzd5Nr8Pu0T/ltvzF1rl3DX/ymxHtU//r20PnwMOdspMZUfA==
-----END RSA PRIVATE KEY-----
```

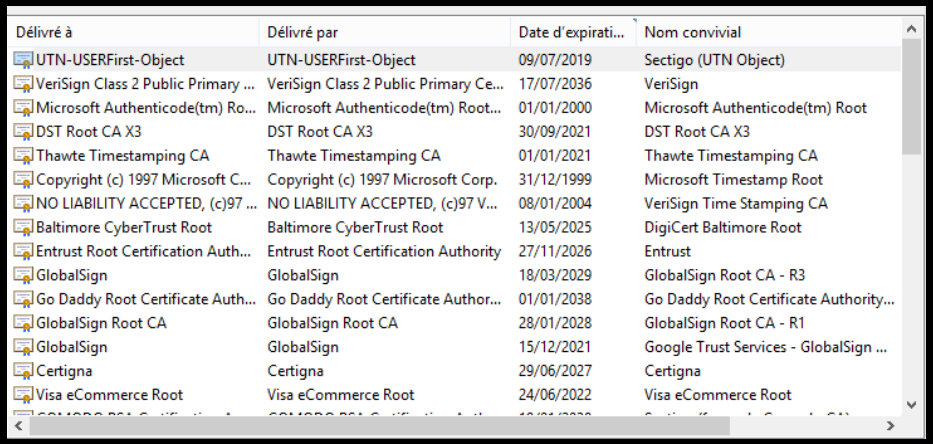
```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQCebM7X70BHRy1g
P5DCVAuliJ8hzTYhZ168enGCVQXCh/XhHSJeXmrtY2NXo4p58omYZ+AV4HjAfALB
VsirjhaUj5liXrEFTk3JbhXVYyms3Yg3KQdqEA6J63/+GBsZA1Z6zrcfW0Ur1gNL
PSwvuuavCjoh6umaNjidk5kC0yvy66zC9UHijuxm9pcAeZW6OzC4IjfkoO1i1nbd
DxnVQt/ECotZgfYLnwTY4f12/mFL5D51MbZJbEwv3/wdqzoyBLKgm/bdUYrlp+C/
UOA0RSLm/n0wNUa3jc54FIAWpB+D2UkIDNaaTWK23ynnLmJuGszx0v+1WiLvpo2R
wak8Y4hfAgMBAAECggEBAJuHcI1XCUCwpOBvpxrQTdrFxIv3na0virb4cgUkmRIA
TighZQNGKC1DPFzmZeUQcXqYx8pSY9l8JWxPWZPqW0qfq1KCacEuvXj5xR+HSXu2
xKp6chfzCYLnGvGGEtw8haLs26RCAydk5DjyJjX5g8zl+mof6BQIFQ7Fvxqh2+yP
XM3fq7XMRv1vNZ/m/nCgKT2dAi9pfH2HaUwrD2JH+fNRzSWWD5s52LrbZmNAzgEZ
JD+TxJn3tAbtASZAfdTghrN6jr3hZbAElT0iMu1vyldSXvYSdPBcOFtMHOaB41+o
mDRQ2fsDsYhqPLDNQUg94x5fFChdkO0GI9LVkEmcdBECgYEAyy00IBHOmRXY9z1/
64CM96rFDe9bw/+fempkTQR/lwUWrawNwPeUImXl5GmJv75BmpICpD2DHzqRYiEq
qv7icJGCnwS3ozkSd+ANAYtV+iwtDmRDEwka5wMYssJC1/uffHk3iBjFg+PpXHrA
9Js7Dop0AEurKVk5oQTksCFemckCgYEAx50U6v71ZKmBuLykb13Zvq9tsXJdZ9g8
PzhMhnRuMqtu2DubrnVNMYoXAJuAnli9KY10Mxm6ep7PH9sxKuXGLvXKwSmZfzKp
DXYh2owReGImH4HC6Y4IK61zXCiYxRzd17olx3tSKSRYkyfxQynohx2Y2WJtUlC0
3hhMjrpypOcCgYBYGQyuDyqXBHskkX0jH4WAaoKxTSVsMi3zhahiIN42HJW9zonU
L0YDOE3bocuB4bxOipssniN56gpaE2mN5aFIEEAkNYZu9vNEGVlqXwFzza3nvJ+8
5EjO/G+8KzGSt19rOKBUmfEjBDMOz4dVSO3tmyk7a5QXBMJRSG7k1ENRyQKBgQCR
e74kK+CEFjrSfsLF3Dv4C3nCS50iM2ptlUXI9RDf4yxtcrxboWi6g2+SZMOQJRLx
NwSKveS4vAgvqpyiLEeOMFwu/ne+ShkGE6RG2bFd8QLiEbwSZw8zbj5W28vEVe6l
7Sjdw9a036Wi0wi3L9Mmrv6Y6XDN/r5j5IffuqoV3wKBgGwWLz5ygIwsXNSTArUD
nPLlgSzVaM+ddAp4EtAPosX1qb2CipQ+6hNXYIoMbR/sKXYYG0Hd0G8rWoDWL4NY
bAMgYh70qU4GYLkxJiaI/2mnHwd3yhE6rVAb5Vr7KTN3k2vw+7RP+W2/MXWuXcNf
/KbEe1T/+vbQ+fAw52ykxlR8
-----END PRIVATE KEY-----
```

SSL/TLS : Certificat/Clé/CSR

- RSA
  - `openssl x509 -noout -modulus -in www.example.com.crt | openssl sha256`
  - `openssl req -noout -modulus -in www.example.com.csr | openssl sha256`
  - `openssl rsa -noout -modulus -in www.example.com.key | openssl sha256`
- ECC
  - `openssl x509 -in example.crt -pubkey -noout`
  - `openssl req -in example.csr -pubkey -noout`
  - `openssl ec -in example.key -pubout`

SSL/TLS : Autorités (CA)





Délivré à	Délivré par	Date d'expirati...	Nom convivial
UTN-USERFirst-Object	UTN-USERFirst-Object	09/07/2019	Sectigo (UTN Object)
VeriSign Class 2 Public Primary ...	VeriSign Class 2 Public Primary Ce...	17/07/2036	VeriSign
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	01/01/2000	Microsoft Authenticode(tm) Root
DST Root CA X3	DST Root CA X3	30/09/2021	DST Root CA X3
Thawte Timestamping CA	Thawte Timestamping CA	01/01/2021	Thawte Timestamping CA
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	31/12/1999	Microsoft Timestamp Root
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	08/01/2004	VeriSign Time Stamping CA
Baltimore CyberTrust Root	Baltimore CyberTrust Root	13/05/2025	DigiCert Baltimore Root
Entrust Root Certification Auth...	Entrust Root Certification Authority	27/11/2026	Entrust
GlobalSign	GlobalSign	18/03/2029	GlobalSign Root CA - R3
Go Daddy Root Certificate Auth...	Go Daddy Root Certificate Author...	01/01/2038	Go Daddy Root Certificate Authority...
GlobalSign Root CA	GlobalSign Root CA	28/01/2028	GlobalSign Root CA - R1
GlobalSign	GlobalSign	15/12/2021	Google Trust Services - GlobalSign ...
Certigna	Certigna	29/06/2027	Certigna
Visa eCommerce Root	Visa eCommerce Root	24/06/2022	Visa eCommerce Root

SSL/TLS : Autorités (CA)

CA ? Bundle ?

- Regroupe l'ensemble de la chaîne de certification

CA Intermédiaire

CA Root

Péremption & révocation

2 fins possible pour un certificat

- Dépassement de la date de validité
  - Le certificat devient non valide
  - Message d’erreur ou accès coupé
- Révocation du certificat par la CA
  - Vérification des CLR (Certificate Revocation List)
  - Causes
    - Leak de la clé privée
    - Certificat frauduleux

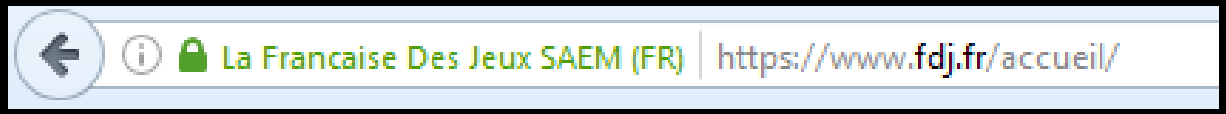
Les niveaux de validation

3 niveaux de certification

- Domain Validation
- Organisation Validation
- Extended Validation

- Un certificat DV vérifie juste la possession du domaine
- Un certificat EV/OV vérifie que l'entreprise/organisme existe

- Résultat pour l'OV



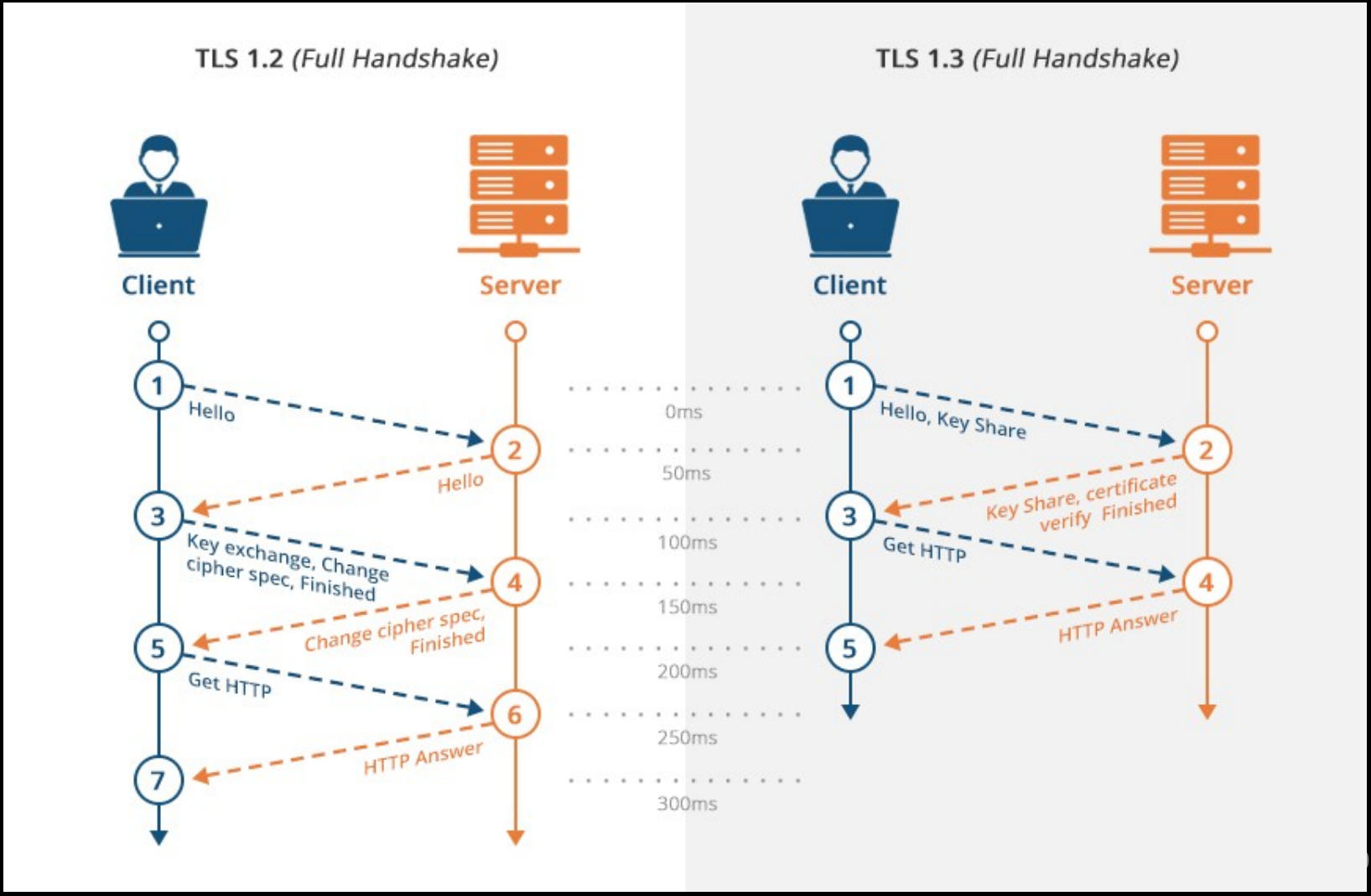
Les formats

Formats	Utilisations	Extensions	Particularités
X64	Apache, OpenVPN, etc.	.crt .key .pem	Fichiers séparés
Binaire	Java	.cer .der .key	Fichiers séparés
P7B	Windows / JAVA	.p7b .p7c	Only Cert/CA
PFX/P12	Windows / WS/ Java	.p12 .pfx	1 seul fichier
JKS	Java / WS	.jks / cacerts	Keystore +Trustore

PKCS

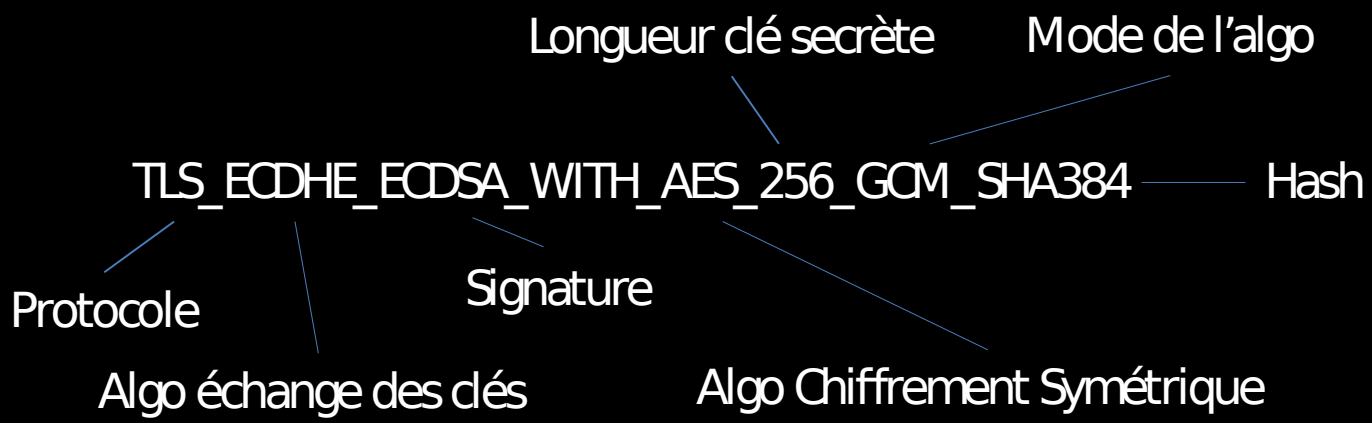
PKCS#*	Version	Nom	Commentaires
PKCS#1	2.1	Cryptographie RSA	RFC 3447
PKCS#7	1.5	Standard de syntaxe de message cryptographique	RFC 2315 Signature CA. Transmission cert.
PKCS#8	1.2	Standard de syntaxe d'information de clé privée	Cf. RFC 5958[6]
PKCS#10	1.7	Standard de requête de certificat	RFC 2986. CSR.
PKCS#11	2.20	Interface de périphérique cryptographique (cryptoki)	
PKCS#12	1.0	Standard de syntaxe d'information personnelle	Certificat +clé + passphrase

Exemple d’une session



Cipher Suites

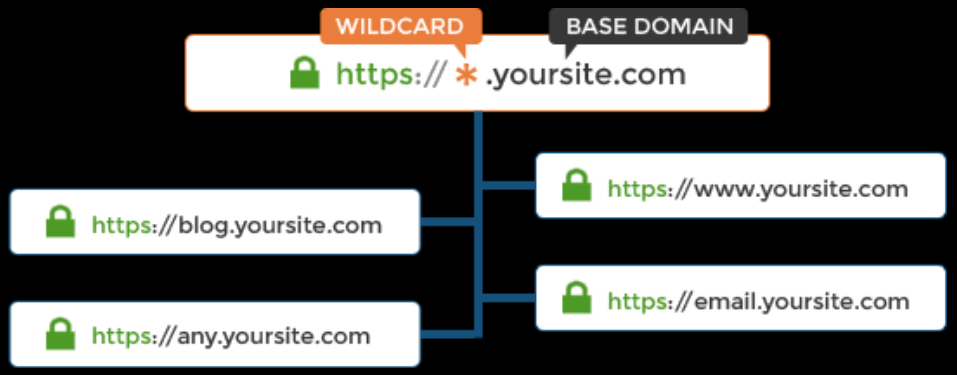
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA



Autres cas & fonctionnalités

- HSTS (HTTP Strict Transport Security)
  - Données en cache
  - Requête 301

- Certificat Wildcard (*.ynov.com)
  - Valable pour plusieurs domaines
  - Une seule clé privée



Autres cas & fonctionnalités

- Certificate Transparency
  - Base de données pour toutes les générations

- Certificate Pinning
  - Réduction de la confiance
  - Mobile principalement

Ressources

- Manipuler des certificats : OpenSSL
- Cheat-Sheet : https://rm-it.fr/openssl-cheatsheet/
- Tester sa configuration : https://net-security.fr/security/testez-votre-configuration-ssl/


```
root@DESKTOP-58N49LO:~/testssl.sh# ./testssl.sh 192.168.145.129

###########################################################
    testssl.sh       3.0rc1 from https://testssl.sh/dev/
    (f230363 2018-09-10 20:09:39 -- )

      This program is free software. Distribution and
             modification under GPLv2 permitted.
      USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!

       Please file bugs @ https://testssl.sh/bugs/

###########################################################

 Using "OpenSSL 1.0.2g  1 Mar 2016" [~124 ciphers]
 on DESKTOP-58N49LO:/usr/bin/openssl
 (built: "reproducible build, date unspecified", platform: "debian-amd64")


 Start 2018-09-11 14:09:34        -->> 192.168.145.129:443 (192.168.145.129) <<--

 rDNS (192.168.145.129): --
 Service detected:       HTTP
```

GPG ?

- Gnu Privacy Guard
  - Implémentation libre (GnuPG) d'OpenPGP
  - Chiffrement asymétrique

Confidentialité
Intégrité
Authentification

GPG ?

- Comment ça marche ?
  - Principalement en ligne de commande
  - Utilise des algorithmes symétrique, asymétrique, de hash & de compression
  - Utilisé dans divers outils (Mail, Stockage, Chiffrement des PDT)

SSL/TLS : Certificat

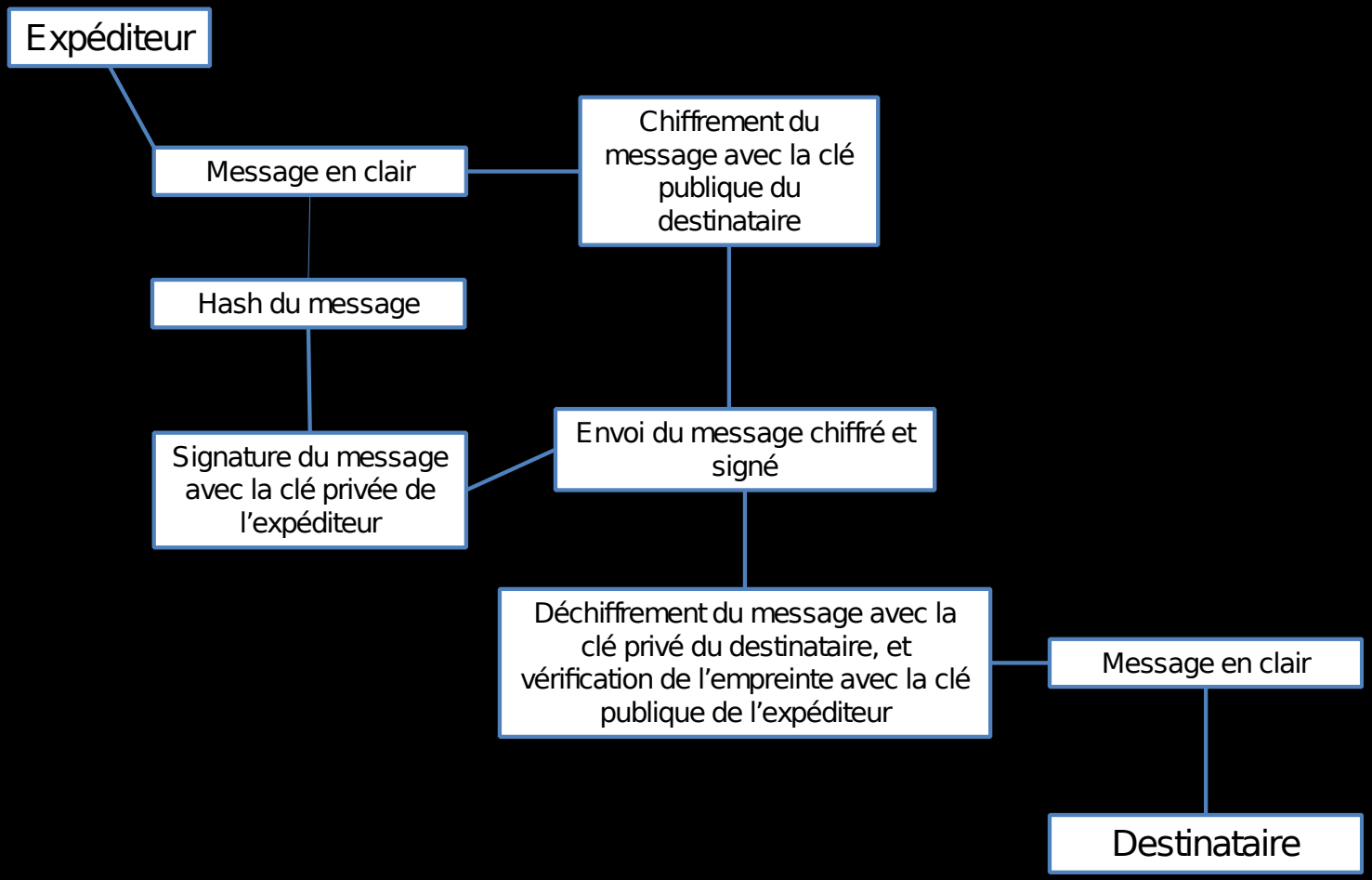
```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: Keybase OpenPGP v1.0.0
Comment: https://keybase.io/crypto

xm8EXihfGhMFK4EEACIDAwSUu5o6NBGB9/P9aUoOfE9qr35ffvDhw+PSWgcTRuN/
ZMZE2eAVBSOvW7vhAOVm5VLTM2mqTHw0GYfAE8nZstsK2hbsa5QJ6lw2TtdS9U08
JHJ8EJrl261a5X4WRrh+IsbNE3Rlc3QgPHRlc3RAdGVzdC5mcj7CjwQTEwoAFwUC
XihfGgIbLwMLCQcDFQoIAh4BAheAAAoJEEO9XsBb6qd2DQABfifNRe382v+SxMjB
57xQ7ibW1/+7k+PocyMYn0mEDZxkji3h13FdbGs3tC2zbRCQzAF/VTI02b6mttFH
zcLmqTHXcJk0Cg+t25MSpJj5LE5zUMMd7PodjWiCJs1sU1GT5e3azlIEXihfGhMI
KoZIzj0DAQcCAwSVpjHP8NUdlNkgenr3n0ZSAt/bl60PwELhk+xXBJWaB7zcbxMS
cUPwC9YiH86B1cGaWB4JJ2SblCGfsoS2AVl5wsAnBBgTCgAPBQJeKF8aBQkPCZwA
AhsuAGoJEEO9XsBb6qd2XyAEGRMKAAYFAl4oXxoACgkQyh7tM7dq9S61kQEApg3A
gSEWJ9MIXyylZ6G9l9AoU5KD8AnlBiYwmHIq2X4A+weBxSWyaJbZfGz34EBnIvw5
4NNVknpY991Tglvn/rzYhHIBgIpPU0F+HajAKxjyrrlvncoDh5BSRoxkCiyvSlUY
GzAzBMAFb787M4dEFmo5kvPw2gGAwTo2Hxd7BocrOfgkHdMr73Ol4OS4tlqKHibx
Rvq69xsb+uoQyMfTTy7jnNTz57C5zlIEXihfGhMIKoZIzj0DAQcCAwRfmmdynkLX
kmXvIj5N3CapmU9DodtDk22LzMhfzh30YvMLDfrWBjdj1JPskzEsiTELkxi6f3CS
bhWzW/xP91kEwsAnBBgTCgAPBQJeKF8aBQkPCZwAAhsuAGoJEEO9XsBb6qd2XyAE
GRMKAAYFAl4oXxoACgkQX6H51qs76nEGrwD/dgtG6/RTtFcBfSAZ9lhFAeqhfso7
x9ep2I9djK4et64A+gK9l2iHhCZeH0D7ezXqy+ntm9+A5E+UTlWMeGl4phVAxiwB
gO+IW0LstgyUMDpBTxVLulpmqjFJZM2uc3irsaq8wVthuQseuK1D9EclePt9E9V5
dgGA7IynNn4f1BHEbRFSgBn/3lXqcMraFHJxM7w6g5mdQFDqmX5MiyVqOMENMwnJ
ph6D
=UN+9
-----END PGP PUBLIC KEY BLOCK-----
```

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: Keybase OpenPGP v1.0.0
Comment: https://keybase.io/crypto

xcASBF4oXxoTBSuBBAAiAwMElLuaOjQRgffz/WlKDnxPaq9+X37w4cPj0loHE0bj
f2TGRNngFQUjr1u74QDlZuVS0zNpqkx8NBmHwBPJ2bLbCtoW7GuUCepcNk7XUvVN
PCRyfBCa5dutWuV+Fka4fiLG/gkDCA6kO3AT/1tNYNvBoDVWmVOYQPRNR/PdaBxl
4pKle2m0SvnPV3cDQuz5GbNRswHZFr7K9BQe70QND3gFYDZIzc1Qv++aE0bS+lfl
SmXUOfLUk9Z4C6nr7XYoLxhBmpzTzRN0ZXN0IDx0ZXN0QHRlc3QuZnI+wo8EExMK
ABcFAl4oXxoCGy8DCwkHAxUKCAIeAQIXgAAKCRBDvV7AW+qndg0AAX4nzUXt/Nr/
ksTIwee8UO4m1tf/u5Pj6HMjGJ9JhA2cZI4t4ddxXWxrN7Qts20QkMwBf1UyNNm+
prbRR83C5qkx13CZNAoPrduTEqSY+SxOc1DDHez6HY1ogibNbFNRk+Xt2selBF4o
XxoTCCqGSM49AwEHAgMElaYxz/DVHZTZIHp6959GUgLf25etD8BC4ZPsVwSVmge8
3G8TEnFD8AvWIh/OgdXBmlgeCSdkm5Qhn7KEtgFZef4JAwjUR609vFWE/GDp86fh
II3d5w8pqLdtH9c0mj1v9LOkqsA173TRtDFcjV2A5Bo5LPfYoE3f6zaDYka5kWvE
y3mFkkTSh+RnCeMs18yIk7duwsAnBBgTCgAPBQJeKF8aBQkPCZwAAhsuAGoJEEO9
XsBb6qd2XyAEGRMKAAYFAl4oXxoACgkQyh7tM7dq9S61kQEApg3AgSEWJ9MIXyyl
Z6G9l9AoU5KD8AnlBiYwmHIq2X4A+weBxSWyaJbZfGz34EBnIvw54NNVknpY991T
glvn/rzYhHIBgIpPU0F+HajAKxjyrrlvncoDh5BSRoxkCiyvSlUYGzAzBMAFb787
M4dEFmo5kvPw2gGAwTo2Hxd7BocrOfgkHdMr73Ol4OS4tlqKHibxRvq69xsb+uoQ
yMfTTy7jnNTz57C5x6UEXihfGhMIKoZIzj0DAQcCAwRfmmdynkLXkmXvIj5N3Cap
mU9DodtDk22LzMhfzh30YvMLDfrWBjdj1JPskzEsiTELkxi6f3CSbhWzW/xP91kE
/gkDCCabIp+0SR6MYE1hBsqO88ip3yutoCnyaaPleDeg2RbHeIUsAADNGV6IC1pL
hHWV2C0U3l8Sv5qYHffJGZjtb85oib93I+tbTyDq9Z4OnJXCwCcEGBMKAA8FAl4o
XxoFCQ8JnAACGy4AagkQQ71ewFvqp3ZfIAQZEwoABgUCXihfGgAKCRBfofnWqzvq
cQavAP92C0br9FO0VwF9IBn2WEUB6qF+yjvH16nYj12Mrh63rgD6Ar2XaIeEJl4f
QPt7NerL6e2b34DkT5ROVYx4aXimFUDGLAGA74hbQuy2DJQwOkFPFUu6WmaqMUlk
za5zeKuxqrzBW2G5Cx64rUP0RyV4+30T1Xl2AYDsjKc2fh/UEcRtEVKAGf/eVepw
ytoUcnEzvDqDmZ1AUOqZfkyLJWo4wQ0zCcmmHoM=
=ptt7
-----END PGP PRIVATE KEY BLOCK-----
```

GPG ?


Expéditeur
Message en clair
Chiffrement du message avec la clé publique du destinataire
Hash du message
Signature du message avec la clé privée de l'expéditeur
Envoi du message chiffré et signé
Déchiffrement du message avec la clé privé du destinataire, et vérification de l'empreinte avec la clé publique de l'expéditeur
Message en clair
Destinataire

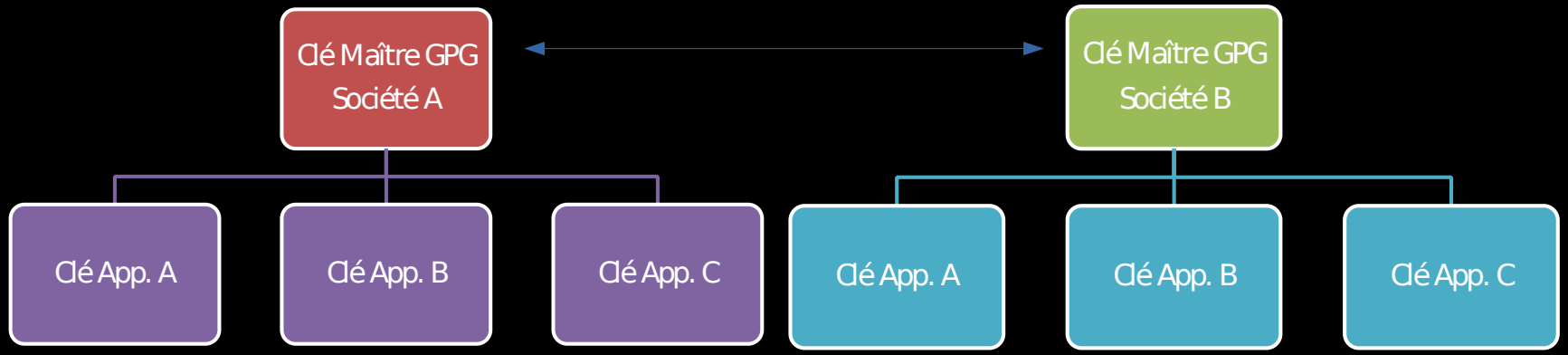
GPG ?

- Liste complète : https://rm-it.fr/gpg-cheatsheet/ && https://github.com/tzkuat/Ressources/blob/master/gpg-cheatsheet.md
- Commandes :
  - `gpg -k = list public keys`
  - `gpg -K = list private keys`
  - `gpg —-full-gen-key`
  - `gpg -r ID_KEY -e -a file`
  - …

```
gpg.conf
 -default-key ID_KEY
 -personal-cipher-preferences AES256 AES 3DES
 -personal-digest-preferences SHA512 SHA384 SHA256
 -personal-compress-preferences ZLIB BZIP2 ZIP Uncompressed
 -default-preference-list SHA512 SHA384 SHA256 AES256 AES 3DES
  ZLIB BZIP2 ZIP Uncompressed
```

Signer des clés ?

gpg --sign-key ID_KEY_TO_SIGN
gpg --edit-key ID_KEY_
> check



PKI ?

Public Key Infrastructure

Une infrastructure à clés publiques, est un ensemble de composants physiques, de procédures humaines et de logiciels destiné à gérer les clés publiques des utilisateurs d'un système.

Définition du besoin

- Combien de clé allez vous gérer ?
- Externe et/ou interne ?
- Est-ce que vous avez des besoins spécifiques ?
  - CSR signée par un tier ?
  - Certificat client ?
  - Certificat pour les utilisateurs (RGS, etc.) ?
  - GPG ?
- Politique cryptographique de l’entreprise ?
- Certification ?

Les grandes fonctionnalités

- Génération des clés privées, CSR & certificats
- Support des différents algorithmes/protocoles
- Gérer les alertes
- Gérer la segmentation des droits & l’attribution
- Mise à disposition des éléments
- Renouvellement des éléments

Les nouvelles fonctionnalités

- Génération & renouvellement automatique
- Découverte automatique de l’existant
- Déploiement automatique
- Gestion des environnements conteneurisés

Si fortes contraintes

- Politique de gestion des clés ++
- Utilisation de HSM (Hardware Security Module)
- Référent de confiance

Les solutions clés en main

- Sectigo Certificate Manager
- GlobalSign Plate-forme Managed PKI
- Digicert PKI Platform

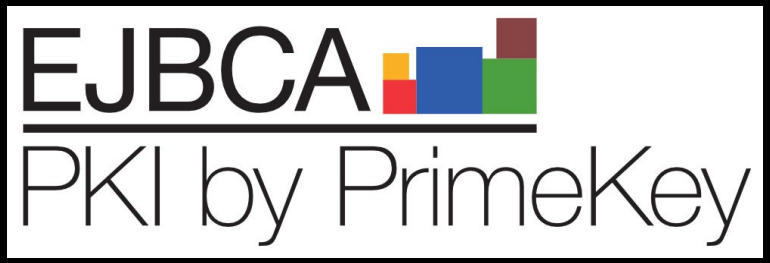
Managed PKI

- Les + et les -

Avantages	Inconvénients
Facilité/rapidité de mise en œuvre	Réversibilité
Intégration certificat pub.	Dépendance fournisseur
Solution maintenue	Pas adapté aux besoins
	Solution externe (SaaS ?)
	Coût

Les solutions Open Source

- EJBCA – PrimeKey
- Lemur – Netflix
- OpenCA
- XCA



NETFLIX

OpenSource PKI

- Les + et les -

Avantages	Inconvénients
Facilité/rapidité de mise en œuvre	Hébergement
Open Source	Durée de vie du projet
Internalisation	Coût (indirect)
Adaptabilité	Pas de support ?
Contribution (communauté)	

Solution “Maison”

Autre solution

- Microsoft AD CS
  - Utile si LDAPs & env. Microsoft
  - Difficile d’utilisation
  - Documentation catastrophique

Cryptographie quantique & post-quantique

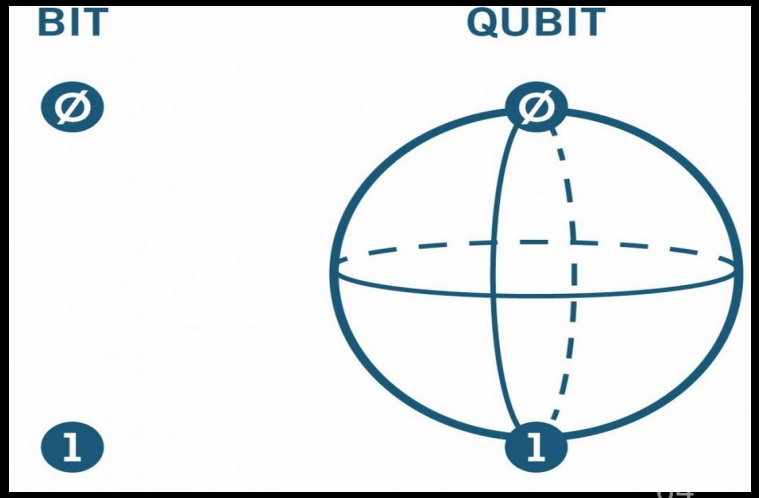
Informatique Quantique : Sous domaine de l’informatique basé sur les calculateurs quantiques (physique quantique).

Crypto Quantique vs Post Quantique

- Cryptographie post quantique
  - Branche de la cryptographie pour garantir la sécurité face à un calculateur quantique
- Cryptographique quantique
  - Vise à construire des algorithmes en utilisant des propriétés physiques et non mathématiques

Différence fondamentale

- Basé sur des qubits et non des bits
  - Un bits vaut 1 ou 0. Un qubits vaut 1 et 0.
- Les grands principes
  - La superposition quantique
  - L’intrication quantique
  - Les qubits

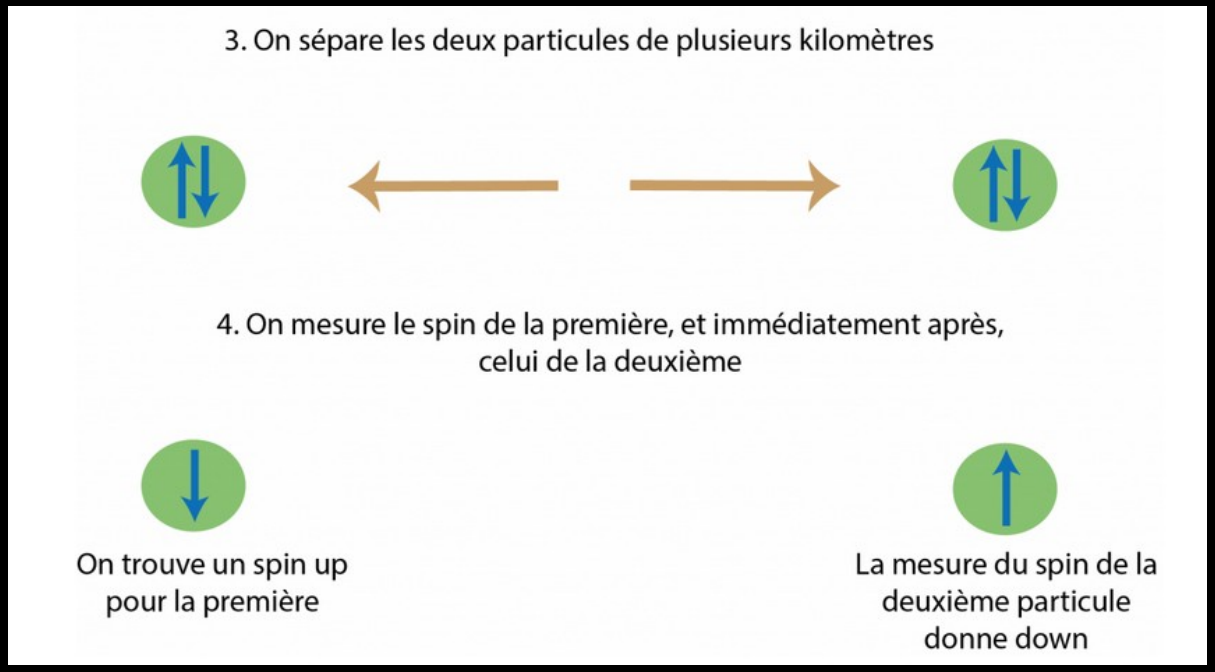


Superposition Quantique

- Une particule peut se trouver dans un état indéterminé avant toute mesure.
- Exemple :
  - Un ticket de loto
  - Le chat de Schrödinger

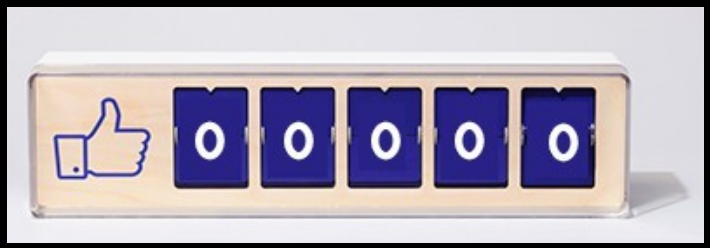
Intrication Quantique

- Liaison de deux objets quantiques a priori indépendants.
- Si une particule est dans un état positif, la seconde sera forcément négative.

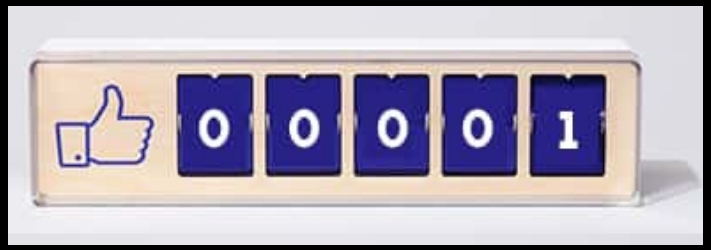


Les Qubits

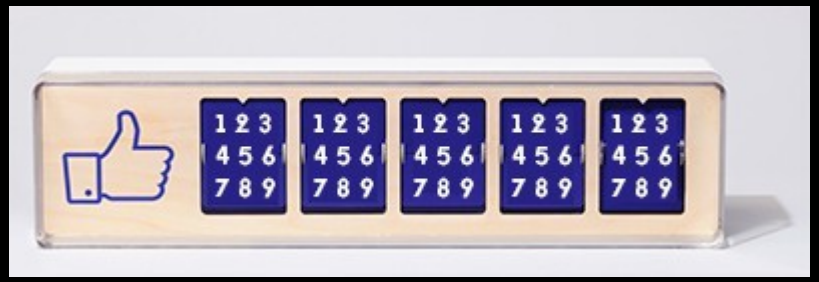
- Un qubits n’utilise pas 0 ou 1 mais une superposition de 0 et de 1
- Ex : Un compteur.



- Ordinateur classique :



- Ordinateur quantique :



La finalité

- Un ordinateur quantique à 4 qubits va calculer 16x plus vite qu'un ordinateur à 4 bits
- Il existe aujourd'hui des ordinateurs de 54 qubits
- Il existe des algorithmes quantiques capable de factoriser des entier plus rapidement (Shor)
- Exemple pour RSA : 6189 qubits + x portes logiques

Autres

- Sur la cryptographie quantique, l’intrication pourrait révolutioner les mécanismes d’échanges des clés
- Il est aujourd’hui très compliqué de garder un qubits dans un état quantique
- Les calculs génèrent un nombre d’erreur important, d’où la course au qubits
- Pour fonctionner un ordinateur quantique doit se trouver proche que 0 absolu (−273,15 °C)

Ressources

- Repo : https://repo.rm-it.fr/
- Lien 1 : https://rm-it.fr/crypto/
- Lien 2 : https://github.com/tzkuat/Ressources/blob/master/Crypto.md
- Shaarli : https://links.rm-it.fr/?

Merci à tous !
La partie pratique ?

Mickael Rigonnaux
Twitter : @tzkuat
mickael.rigonnaux@rm-it.fr
https://net-security.fr