PKI : Public Key Infrastructure

IUT de Béziers, dépt. R&T © 2009 - 2017
http://www.borelly.net/
Christophe.BORELLY@iutbeziers.fr

Généralités

- PKI (Public Key Infrastructure)
- IGC (Infrastructure de Gestion de Clés)
- Gestion de certificats X.509 (RFC 3280 - 5280 - 6818)
- Clé publique + informations (CN, OU, O, L, ST, C, durée de validité, utilisations possibles de la clé, …) signées par une “autorité”
- RFC 4212 PKIX

Exemple (1)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            01:00:00:00:00:01:1c:7b:96:3a:0b
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: OU=Extended Validation CA, O=GlobalSign, CN=GlobalSign Extended
Validation CA
        Validity
            Not Before: Sep 19 17:09:14 2008 GMT
            Not After : Sep 20 17:09:09 2010 GMT
        Subject: 2.5.4.15=V1.0, Clause 5.(b)/serialNumber=C2759208/1.3.6.1.4.1.3
11.60.2.1.3=US/1.3.6.1.4.1.311.60.2.1.2=California, C=US, ST=California, L=Mount
ain View/streetAddress=1981 Landings Dr., OU=Mozilla Add-ons, O=Mozilla Corporat
ion, CN=addons.mozilla.org
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:dd:54:3b:ea:8a:e5:96:88:72:af:de:71:79:d1:
                    ....
```

Exemple (2)

```
X509v3 extensions:
          X509v3 Authority Key Identifier:
             keyid:34:B1:F9:C9:8C:6B:35:44:CC:08:69:0A:EE:E3:A3:B9:5C:BF:16:E0
          Authority Information Access:
              CA Issuers - URI:http://secure.globalsign.net/cacert/extendval1.crt
          X509v3 CRL Distribution Points:
              URI:http://crl.globalsign.net/ExtendVal1.crl
          X509v3 Subject Key Identifier:
              EC:5E:7B:F5:E4:7F:D4:B1:32:1E:A5:19:B5:7E:EA:4D:C2:EE:4A:9F
          X509v3 Basic Constraints:
              CA:FALSE
          X509v3 Key Usage: critical
              Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
          X509v3 Extended Key Usage:
              TLS Web Server Authentication, TLS Web Client Authentication,
              Microsoft Server Gated Crypto, Netscape Server Gated Crypto
            ...
    Signature Algorithm: sha1WithRSAEncryption
        ad:80:3d:9f:94:38:15:ab:51:14:b6:f4:cb:10:2f:6f:87:29:
        ....
```

Utilisation des certificats

- SSL/TLS (identification serveur ou client)
- S/MIME (signature – chiffrement de mails)
- Signature de code (Applets, drivers, …)
- CA/CRL signing : Signature de nouveaux certificats
- OCSP helper : Vérification en ligne
- Online Certificate Status Protocol
- ...

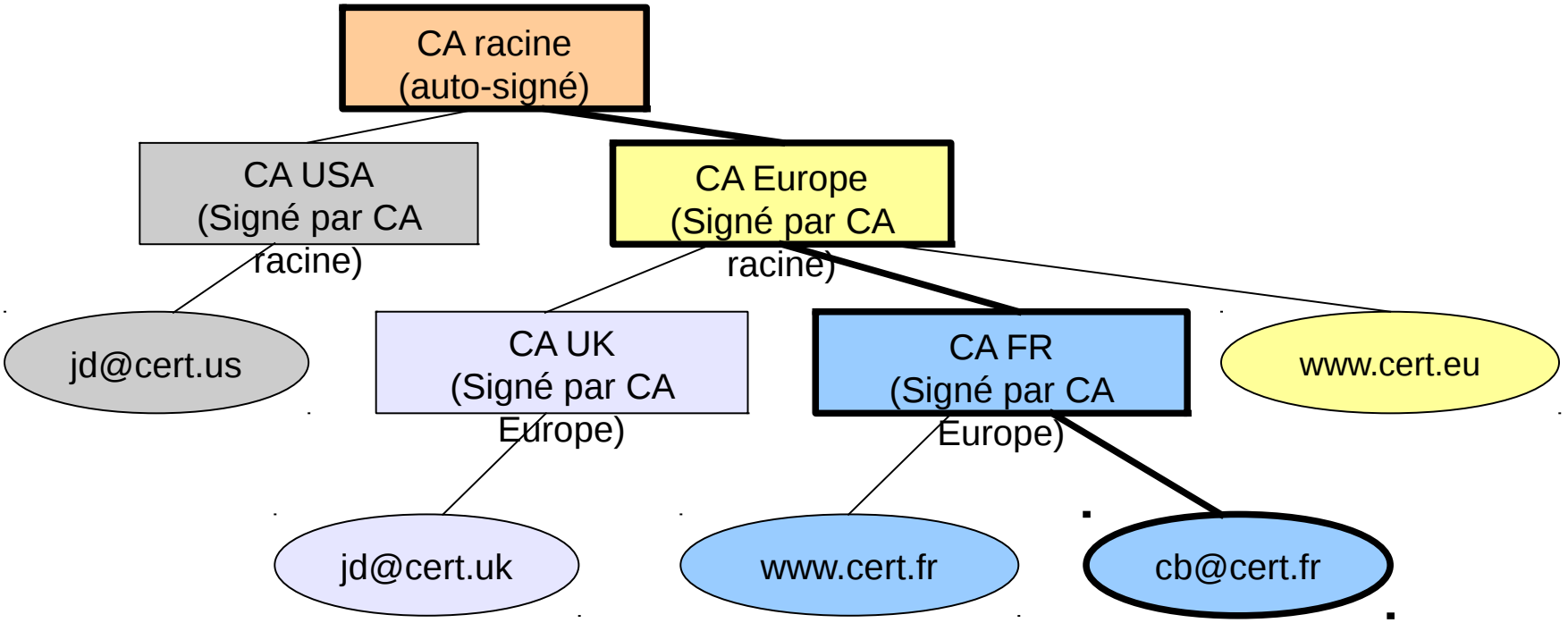
Usages de la clé

- Ils sont décris dans la RFC 5280 pages 29-31
- Chapitre : 4.2.1.3. Key Usage
- Il y existe 9 usages de clé prédéfinis :
  - digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, cRLSign, encipherOnly, decipherOnly

Usages étendus de clé (1)

- Ils sont décris dans la RFC 5280 pages 44-45
- Chapitre : 4.2.1.12. Extended Key Usage
- Il en existe 6 :
  - ServerAuth, clientAuth, codeSigning, emailProtection, timeStamping, OCSPSigning
- Il est conseillé d'associer ces usages étendus avec certains usages de clés simples...

Vérification des certificats



Services d'une PKI

- Identification et authentification des utilisateurs (administrateurs ou utilisateurs qui accèdent à l'IGC)
- Enregistrements des demandes de signature (CSR)
- Génération de certificats (CRT - P12)
- Renouvellement de certificats
- Révocation de certificats
- Publication de certificats
- Publication des listes de révocation (CRL)
- Archivage, séquestre et recouvrement des clés (option)

Protocoles

- CMP : Certificate Management Protocol - RFC 2510
- CMC : Certificate Management Using CMS - RFC 2797
- SCEP : Simple Certificate Enrollment Protocol (Cisco)
- XKMS : XML Key Management System (W3C)
- ISAKMP : Internet Security Association and Key Management Protocol - RFC 2408
- IKE : Internet Key Exchange - RFC 4306
- OCSP : Online Certificate Status Protocol - RFC 2560
- ...

PKCS (Public-Key Cryptography Standards)

- RSA laboratories (http://www.rsa.com/rsalabs/)
- PKCS #1: RSA Cryptography Standard
- PKCS #3: Diffie-Hellman Key Agreement Standard
- PKCS #5: Password-Based Cryptography Standard
- PKCS #6: Extended-Certificate Syntax Standard
- PKCS #7: Cryptographic Message Syntax Standard
- PKCS #8: Private-Key Information Syntax Standard
- PKCS #9: Selected Attribute Types
- PKCS #10: Certification Request Syntax Standard
- PKCS #11: Cryptographic Token Interface Standard
- PKCS #12: Personal Information Exchange Syntax Standard
- PKCS #13: Elliptic Curve Cryptography Standard
- PKCS #15: Cryptographic Token Information Format Standard

Références

- http://fr.wikipedia.org/
- https://tools.ietf.org/html/rfcXXXX
- The Open–source PKI Book