Sécurité Applicative

Infrastructure de gestion de clefs et certificats X.509 (temps conseillé : 20 mn)

1. Pour le certificat « A » (voir annexe):
   1.1 Donnez le nom de son autorité de certification.
   1.2 Donnez le nom de son propriétaire.
   1.3 Ce certificat peut-il être utilisé pour :
   - Vérifier la signature d'un email ? OUI/NON
   - Chiffrer un email ? OUI/NON
   - S'authentifier sur un site web HTTPS ? OUI/NON
   - Chiffrer des données sur son disque ? OUI/NON
   - Vérifier la signature d'un certificat X509 ? OUI/NON
   - Vérifier la signature d'une liste de révocation (CRL) ? OUI/NON

   1.4 Ce certificat est-il valide ?

2. Pour les certificats B, C, D, E, F et les CRL G, H (voir annexe) :
   2.1 Quel(s) est(sont) le(s) certificat(s) racine(s) ? Dans la suite de cet exercice, nous considèrerons que ce(s) certificat(s) est(sont) considéré(s) comme « de confiance ».
   2.2 Donnez les chemins de certification des certificats présentés (ex: X signé par Y signé par Z, M signé par N, ...). Présentez ces chemins sous forme de graphique.
   2.3 Quel(s) certificat(s) ne sont pas ou plus valides ? Expliquez pourquoi ?
   2.4 Quelles sont les conséquences pour la sécurité si un client logiciel accepte ce type de chemin de certification illicite? Comment est censé se comporter le client logiciel dans ce cas ?
   2.5 Que se serait-il passé sur la CRL H avait été la suivante ?

```
Certificate Revocation List (CRL):
      Version 1 (0x0)
      Signature Algorithm: sha1WithRSAEncryption
      Issuer: /C=fr/O=Inconnu/OU=AC/CN=AC Racine
      Last Update: Oct 15 07:00:09 2009 GMT
      Next Update: Apr 16 07:00:09 2011 GMT
Serial Number: 12
      Revocation Date: Apr 18 14:15:38 2008 GMT
            CRL entry extensions:
            X509v3 CRL Reason Code:
                  Cessation Of Operation
```

Annexe

- Certificat « A »

```
Certificate:
  Data:
    Serial Number: 24
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=FR, ST=IdF, L=Paris, OU=IT, CN=AC1
    Validity
      Not Before: Dec  8 07:00:30 2008 GMT
      Not After : Dec  8 07:00:30 2010 GMT
    Subject: C=FR, ST=IdF, OU=IT, CN=paul
    X509v3 extensions:
      X509v3 Basic Constraints: CA:FALSE
      X509v3 Key Usage: Digital Signature, Non Repudiation, Key Encipherment
      X509v3 Subject Key Identifier:
        6B:33:D5:A1:2E:3C:0B:44:86:52:C2:8B:9B:30:8E:72:AE:F2:0D:05
      X509v3 Authority Key Identifier:
        keyid:7D:27:1A:71:C2:04:79:A0:6C:CF:19:AA:0C:7D:80:97:7A:49:61:34
```

- Certificat « B »

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=FR, O=Inconnu, OU=AC, CN=AC Utilisateur
        Validity
            Not Before: Sep 21 09:56:26 2007 GMT
            Not After : Sep 21 09:56:26 2009 GMT
        Subject: C=FR, O=Inconnu, OU=Utilisateur, CN=DURAND Francois
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:e5:9a:8b:95:12:ac:38:03:89:9c:1f:88:73:5c:
                    a7:da:c6:87:f2:4b:51:5b:a0:01:8b:4e:fa:b3:b7:
                    df:49:2a:e4:66:00:4a:33:e9:7a:15:b1:a6:2e:ff:
                    ef:59:4e:d7:a1:c9:71:3a:d8:bd:e1:fd:d6:22:f0:
                    da:23:ef:90:af:b0:1a:ab:07:9f:48:5e:2d:57:95:
                    6f:f2:c0:22:12:54:8d:68:8a:03:51:a6:21:16:6b:
                    23:51:24:8e:6b:36:43:93:b1:78:ac:3b:5f:8e:18:
                    57:6a:69:fd:c4:07:59:53:2e:23:02:fd:06:37:1b:
                    9c:6f:79:49:2e:ff:33:59:b5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                F9:15:DD:82:56:E9:5A:4A:6F:BA:18:45:DC:E5:75:4F:39:B8:98:A1
            X509v3 Authority Key Identifier:
                keyid:48:1F:62:5B:D3:A4:54:EB:28:D3:C1:A4:3B:72:7A:4A:AF:42:28:BC

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.12384.1.4.2
                  CPS: http://www-igc.inconnu.fr/pc/
                  User Notice:
                    Organization: Inconnu
                    Numbers: 2, 0
                    Explicit Text: Vous devez accepter la politique de
certification avant d'utiliser ce certificat.

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                email:francois.durand@inconnu.fr
            X509v3 CRL Distribution Points:
                URI:http://crl-ac-utilisateur.inconnu.fr/crl/ac-utilisateur.crl

            Authority Information Access:
                CA Issuers - URI:http://www-igc.inconnu.fr/ac/ac-utilisateur.cer
```

- Certificat « C »

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 3611 (0xe1b)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=FR, O=Inconnu, OU=AC, CN=AC Utilisateur
        Validity
            Not Before: Aug  3 08:16:02 2009 GMT
            Not After : Aug  4 08:16:02 2011 GMT
        Subject: C=FR, O=Inconnu, OU=Utilisateur, CN=DURAND Francois
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:ca:1a:b5:82:62:14:26:b9:fc:bf:fe:69:7c:49:
                    73:de:ba:e4:57:8f:2a:8e:72:f1:0b:d7:81:bc:d0:
                    dd:03:cf:cd:c3:44:de:ff:44:b6:fb:8c:d9:2c:60:
                    e0:aa:fd:a1:5d:e5:42:eb:af:f9:7d:c0:1c:6f:b9:
                    77:e7:c8:52:21:e2:8f:bc:70:6a:d3:9c:69:81:a6:
                    5d:23:4f:17:9a:64:e0:43:80:3f:91:fe:99:38:0b:
                    86:05:fc:3a:c5:bc:b0:61:2a:e4:d5:70:bc:4e:6f:
                    47:c3:e9:b1:39:8b:6e:30:4e:73:fa:2f:56:e0:e2:
                    3e:fb:7e:9c:18:4e:9b:68:f5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                EF:75:E8:92:B9:9A:D6:1C:5D:CC:8D:FA:FA:96:D8:F5:98:68:D2:53
            X509v3 Authority Key Identifier:
                keyid:48:1F:62:5B:D3:A4:54:EB:28:D3:C1:A4:3B:72:7A:4A:AF:42:28:BC

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.12384.1.4.2
                  CPS: http://www-igc.inconnu.fr/pc/
                  User Notice:
                    Organization: Inconnu
                    Numbers: 2, 0
                    Explicit Text: Vous devez accepter la politique de
certification avant d'utiliser ce certificat.

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                email:francois.durand@inconnu.fr
            X509v3 CRL Distribution Points:
                URI:http://crl-ac-utilisateur.inconnu.fr/crl/ac-utilisateur.crl

            Authority Information Access:
                CA Issuers - URI:http://www-igc.inconnu.fr/ac/ac-utilisateur.cer
```

- Certificat « D »

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=fr, O=Inconnu, OU=AC, CN=AC Racine
        Validity
            Not Before: Apr  3 17:33:11 2003 GMT
            Not After : Apr  1 17:33:11 2013 GMT
        Subject: C=fr, O=Inconnu, OU=AC, CN=AC Racine
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:dc:9e:a0:c6:92:f3:76:51:44:20:d2:9b:1d:e5:
                    2f:20:be:05:ea:f0:33:2b:2b:bf:bc:aa:23:1e:f9:
                    04:2c:f3:be:e3:d8:e3:b7:a9:1d:6e:38:cc:d8:24:
                    bc:fa:ea:61:44:dd:ae:43:5a:50:1f:c0:4f:2e:e9:
                    f2:4c:d7:85:9e:97:a9:71:58:08:63:39:8b:5a:68:
                    4b:07:6b:a1:1f:68:43:e0:9a:bb:0c:ee:9b:a7:f5:
                    16:07:bf:44:d3:e5:a5:32:51:be:dd:f2:eb:8a:00:
                    63:2e:91:96:16:8d:74:f8:e2:6c:56:4d:da:7d:90:
                    3d:54:94:50:84:85:c8:36:30:61:cd:b4:2c:d3:9d:
                    06:88:44:4e:90:9a:f4:c0:62:f4:bf:7b:fa:cc:09:
                    16:95:0c:6b:03:f3:46:90:50:75:d3:03:ce:19:50:
                    23:c3:a3:61:04:fb:69:ce:c1:88:5b:e6:e8:f9:01:
                    00:db:ce:0c:19:97:e0:c5:f5:65:a1:cd:0c:8d:7f:
                    f8:52:99:d2:7a:10:52:38:08:dd:1c:ac:1b:19:be:
                    f4:0c:4e:e9:fe:b9:ac:39:51:06:ad:fc:c8:60:cf:
                    54:5b:c6:37:09:d9:15:24:b7:8e:d2:75:ab:b7:13:
                    68:6e:53:a7:6b:f2:0e:18:55:e6:79:21:8f:81:05:
                    7b:47
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 CRL Distribution Points:
                URI:http://crl-ac-racine.inconnu.fr/crl/ac-racine.crl

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.12384.1.2
                  CPS: http://www-igc.inconnu.fr/pc/
                  User Notice:
                    Organization: Inconnu
                    Numbers: 2, 0
                    Explicit Text: Ce certificat est soumis a une Politique de
Certification qui en limite les garanties et responsabilites. Vous devez accepter
cette politique avant de l'utiliser.

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                2E:1F:95:BA:02:54:52:8C:28:AD:6F:D1:F7:8F:A0:54:56:93:28:91
            X509v3 Authority Key Identifier:
                keyid:2E:1F:95:BA:02:54:52:8C:28:AD:6F:D1:F7:8F:A0:54:56:93:28:91
```

- Certificat « E »

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 18 (0x12)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=fr, O=Inconnu, OU=AC, CN=AC Racine
        Validity
            Not Before: Sep 14 13:32:22 2007 GMT
            Not After : Apr  1 13:32:22 2013 GMT
        Subject: C=FR, O=Inconnu, OU=AC, CN=AC Utilisateur
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:a1:11:02:3a:e6:8f:ea:98:47:01:a6:62:5b:83:
                    ca:34:16:e1:9d:dd:d8:5e:83:21:0e:dc:da:93:15:
                    fc:9b:1c:55:cd:ca:cc:09:c3:86:3b:6b:16:18:f8:
                    2c:34:c2:2a:41:fc:d4:8c:28:24:89:3d:a9:4d:a0:
                    de:26:91:77:26:7c:95:b9:63:53:57:c3:c6:b9:74:
                    2f:35:b3:4d:a4:4a:9f:ca:84:c3:6d:98:d2:a7:6e:
                    2c:41:d7:00:e2:fd:f1:dc:e2:a1:a3:35:89:e7:19:
                    47:81:af:72:35:2f:68:00:81:ca:c7:51:6b:a0:6e:
                    8c:05:7c:45:62:6f:5f:18:c9:c0:2b:7a:9c:7f:8e:
                    74:f9:5e:85:b5:17:4d:a1:2a:ba:7f:7f:5b:cf:c7:
                    52:8b:51:63:c8:fe:02:a9:ef:fe:fd:87:61:00:c7:
                    1c:17:eb:34:2a:50:4b:4b:05:19:b6:dc:7b:56:4d:
                    72:e7:b3:5a:02:a6:38:6d:7e:9a:7d:77:22:1b:4d:
                    03:b8:05:fc:e1:e7:b2:43:29:ef:fa:b8:af:dd:4e:
                    8c:01:3d:e6:9b:2f:fa:c8:45:c8:a4:38:34:e2:25:
                    df:a2:f6:99:e9:29:81:99:8a:b2:3e:40:f3:ac:fa:
                    b5:51:1a:38:9a:73:28:6f:4c:cc:7e:24:a0:e8:13:
                    91:21
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 CRL Distribution Points:
                URI:http://crl-ac-racine.inconnu.fr/crl/ac-racine.crl

            Authority Information Access:
                CA Issuers - URI:http://www-igc.inconnu.fr/ac/ac-racine.cer

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.12384.1.4.1
                  CPS: http://www-igc.inconnu.fr/pc/
                  User Notice:
                    Organization: Inconnu
                    Numbers: 2, 0
                    Explicit Text: Vous devez accepter la politique de
certification avant d'utiliser ce certificat.

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                48:1F:62:5B:D3:A4:54:EB:28:D3:C1:A4:3B:72:7A:4A:AF:42:28:BC
            X509v3 Authority Key Identifier:
        keyid:2E:1F:95:BA:02:54:52:8C:28:AD:6F:D1:F7:8F:A0:54:56:93:28:91
```

- Certificat « F »

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 3612 (0xe1c)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=FR, O=Inconnu, OU=AC, CN=AC Utilisateur
        Validity
            Not Before: Aug  3 08:16:02 2009 GMT
            Not After : Aug  4 08:16:02 2011 GMT
        Subject: C=FR, O=Inconnu, OU=Utilisateur, CN=DURAND Francois
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:ca:1a:b5:82:62:14:26:b9:fc:bf:fe:69:7c:49:
                    73:de:ba:e4:57:8f:2a:8e:72:f1:0b:d7:81:bc:d0:
                    dd:03:cf:cd:c3:44:de:ff:44:b6:fb:8c:d9:2c:60:
                    e0:aa:fd:a1:5d:e5:42:eb:af:f9:7d:c0:1c:6f:b9:
                    77:e7:c8:52:21:e2:8f:bc:70:6a:d3:9c:69:81:a6:
                    5d:23:4f:17:9a:64:e0:43:80:3f:91:fe:99:38:0b:
                    86:05:fc:3a:c5:bc:b0:61:2a:e4:d5:70:bc:4e:6f:
                    47:c3:e9:b1:39:8b:6e:30:4e:73:fa:2f:56:e0:e2:
                    3e:fb:7e:9c:18:4e:9b:68:f5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                EF:75:E8:92:B9:9A:D6:1C:5D:CC:8D:FA:FA:96:D8:F5:98:68:D2:53
            X509v3 Authority Key Identifier:
                keyid:48:1F:62:5B:D3:A4:54:EB:28:D3:C1:A4:3B:72:7A:4A:AF:42:28:BC

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.12384.1.4.2
                  CPS: http://www-igc.inconnu.fr/pc/
                  User Notice:
                    Organization: Inconnu
                    Numbers: 2, 0
                    Explicit Text: Vous devez accepter la politique de
certification avant d'utiliser ce certificat.

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                email:francois.durand@inconnu.fr
            X509v3 CRL Distribution Points:
                URI:http://crl-ac-utilisateur.inconnu.fr/crl/ac-utilisateur.crl

            Authority Information Access:
                CA Issuers - URI:http://www-igc.inconnu.fr/ac/ac-utilisateur.cer
```