Joseph Antonius Doekbrijder

Digitally signed by Joseph Antonius Doekbrijder
DN: CN = Joseph Antonius Doekbrijder, C = CH, O = SwissSign
Reason: I attest to the accuracy and integrity of this document
Location: Zürich
Date: 2004.07.09 09:50:59 +02'00'

Certificate Variables

A reply to the OFCOM request for comments on ZertES and related documents

SWISSSIGN DOCUMENT
CONFIDENTIAL

Author: Joseph A. Doekbrijder, SwissSign AG

Introduction

Over the years more and more people have found the need to work with information related to certain persons. If this information appeared to be compact and believed to be semi-static, many have jumped on the PKI-bandwagon. It appeared simple to put the information (ex: insurance policy, health information, (bank)account information, access rights or even social information like birthplace, residence, marital status, etc... liability, legal stipulations) into the certificate, since the certificate is a proven means of identifying individual persons (=subscribers). This is where the problem started. All this information should not be in the certificate, since this information is not really static and most of it is private and certificates are public.

Part of generally accepted PKI practice is, to make sure that all information in a certificate is correct and verified by the CA/RA. If some of these values change, either a new digital identity is necessary (ex: subject name change) or the certificate need to be "adjusted" (ex: new legal requirements). Still, the generally accepted practice holds and all information put into the certificate again needs to be verified by the CA/RA. The cost of registration simply becomes too high if the information that needs to be re-validated consists of too many elements. This is another good reason why one should not find private, semi-static information in a certificate.

The binding of non-certificate data to a certificate to data is not part of PKI. With a PKI the organization does no longer have to manage the users passwords and can allow a subscriber to be bound to many different services. If a subscriber is to be removed from accessing all these services it is only necessary to remove the link to the organizational data or to have the certificate revoked.

1 What to do with additional certificate content as proposed in 3.4.3.1.?

In general a certificate should contain as little information as necessary. With regard to point 3.4.3.1. of the "Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der electronischen Signatur" Version dated 1.6.04, we find a lot of semi-static information which should be put into the certificate. And we wonder why?

Using one (1) element in the certificate to point to a set of rules and regulations that apply to this certificate is clearly the preferred way to solve the issue.

Below we look at some of the proposed certificate variables, the SwissSign position on this variable and the proposed solution.

- SerialNumber

No Objections

- Subject

No objection, please consider the SwissSign document *"Certificate Content"* dated July 1st, 2004.

- Title

Not necessary, semi-variable, does not enhance the trustworthiness of the certificate because it can not be legally binding verified by the RA. This MUST not be included.

- SubjectAltName

Not necessary. For RFC conformity this variable MUST be included, but we MUST make sure that the content is verifiable by the RA. The preferred way to do this is to make sure the value of the SubjectAltName MUST be identical to information already contained in the subject. (i.e. email address, or canonical name)

- SubjectPublicKeyInfo

No objections

- Validity

No objections

- Issuer

The issuing party of a certificate should be clearly identified in the certificate. Since this is a trust related issue, and has strong implications with regard to liability. The only way to correctly identify the issuing party (=issuer), is through the digital signature of the issuing CA. This means that the subject-string of the signing CA MUST be present in the certificate. The subject-string of the signing CA MUST itself be compliant to the ZertES rules and regulations.

- CountryName

Not necessary as a special addition since does not enhance the trustworthiness of the certificate. Please consider our document *"Certificate Content"* from July 1st, 2004.

HOWEVER, if the variable "O" is used the following MUST apply:

- - The requester MUST provide documentation for the organizational or corporate name that should be included in the certificate (e.g. excerpt from the Federal Commercial Registry Office). The wording of the organizational or corporate name that should be included in the certificate MUST be identical to the wording in the documentation provided.
- - If the documentation does not identify the person applying for the organization or corporation as a legal representative for the organization or corporation, such a legal representative MUST, in person, authorize the request by supplying an official photo identity document (passport or national identity card) and authorize the request with a personal signature in the appropriate place on a registration form. The RA MUST create a high quality copy of the required supporting documentation.
- - If /O= is requested /C= must be supplied as well.
- - /OU= fields will only be permitted if a valid /O= is included in the request but this information can not legally binding be verified by the RA.

Thus, including a country name is very important if the name of an organization is included in the certificate. Reason: a company name may be used in other countries by a group of persons not related to the "original" holders of the organizational name.

- SignatureValue

No objections

- IssuerAltName

Strongly object. This variable MUST not be included.

The issuing party of a certificate should be clearly identified in the certificate. Since this is a trust related issue, and has strong implications with regard to liability. The only way to correctly identify the issuing party (=issuer), is through the digital signature of the issuing CA. This means that the subject-string of the signing CA MUST be present in the certificate. The subject-string of the signing CA MUST itself be compliant to the ZertES rules and regulations.

Including an alternative issuing party or, more importantly, indicating to the untrained reader of certificate information that alternative issuers could exist, may create confusion about which party is actually responsible for issuing the certificates and lead to liability claims that are incorrect and unnecessary costly.

The proposed solution is to use one (1) element in the certificate to point to a set of rules and regulations that apply to this certificate. This one element should be an OID which can be used to identify a policy. It is good to create a policy (with an OID) that stipulates that the certificate in question has been recognized by the following authorities: EA, SAS, KPMG as having been issued according to the stipulations of the Swiss digital signature law ZertES.

- KeyUsage

No objections

- CrlDistributionPoints

No Objections

- QCStatements (3 times)

Strongly object. This variable MUST not be included.

The proposed solution is to use one (1) element in the certificate to point to a set of rules and regulations that apply to this certificate. This one element should be an OID which can be used to identify a policy. It is good to create a policy (with an OID which may be the very same OID as mentioned under “IssuerAltName”) that stipulates that the certificate in question should be used for transactions with a maximum financial value of xxxx CHF and is a qualified certificate as defined in yyyy and that the private key belonging to the public key in this certificate has been generated on a cryptographic chip (defined in documents zzzz) and has never left the cryptographic chip and is under the sole control of the person referred to in the subject string of the certificate.

In general, it can be said that the proposed certificate fields in section 3.4.3.1. of the “Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der electronischen Signatur” Version dated 1.6.04 do not enhance or increase security and/or trustworthiness. Any person can create a csr which contains these fields. Although this also holds true for the OID, the IOD policy MUST clearly state that it is illegal to include this OID in a certificate if one is not legally allowed to do so.

2 Certificate content an example

Below a print of a normal certificate to illustrate the current complexity of a plain certificate. SwissSign strives to make certificates simpler, not more complex.

```
Certificate:
  Data:
    Version: 3 (0x2)
      Serial Number:
        95:4f:f8:ee:61:60:21:4c
      Signature Algorithm: sha1WithRSAEncryption
      Issuer: CN=SwissSign Personal Gold CA/Email=gold@swisssign.com,
O=SwissSign, C=CH
```

```
      Validity
        Not Before: Dec 10 21:40:01 2003 GMT
        Not After : Dec 10 21:40:01 2004 GMT
      Subject: CN=Joseph Antonius
Doekbrijder/Email=joseph.doekbrijder@swisssign.com, O=SwissSign, C=CH
      Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (2048 bit)
           Modulus (2048 bit):
                    00:95:46:be:c1:5b:e1:47:ec:fb:e0:f8:73:14:e7:
                    bf:6c:87:be:62:e3:29:94:36:a9:f3:d3:ed:83:b6:
                    75:f7:df:65:b8:9b:6b:8a:a4:29:0f:31:2c:4d:39:
                    0f:51:2a:94:bb:d7:9b:ee:1d:46:4b:23:0e:1b:72:
                    3b:3c:19:79:66:a3:67:f4:c6:c0:f8:0f:de:35:ce:
                    51:19:6a:93:28:55:ad:7d:24:b7:91:33:5b:91:28:
                    91:c3:02:fc:08:ac:e3:6d:8b:aa:d2:79:92:ad:a7:
                    3a:f2:bb:34:66:2d:7a:f4:b4:a4:c6:c7:8b:93:59:
                    b6:45:94:c1:56:5a:46:38:ce:25:a4:c6:3b:6c:43:
                    :30:0e:75:82:32:23:cb:dd:10:87:9d:24:85:ba:
                    2c:61:c8:66:c6:23:23:ec:96:ee:c5:25:23:a8:42:
                    5e:1a:d5:9e:c9:9d:bb:fb:21:1b:f4:d3:b2:f0:d0:
                    51:6d:bc:62:5e:ff:97:fb:af:8a:41:6c:bb:2e:1e:
                    ac:32:83:1d:c6:ed:87:fc:4a:b0:8f:ca:91:f5:f8:
                    d2:31:aa:18:8d:12:95:0e:df:1c:1a:61:0f:06:e7:
                    6c:e2:89:25:2b:b5:c2:03:13:d5:db:ee:c0:bc:85:
                    10:1a:b2:7f:43:92:3d:94:4e:a4:ad:75:4f:77:76:
                    2d:d7
            Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Authority Key Identifier:
     keyid:F2:36:86:CF:BD:A4:D6:79:DF:32:99:8C:D0:59:69:1D:05:95:2C:86
  X509v3 Key Usage: critical
     Digital Signature, Non Repudiation, Key Agreement
  X509v3 Extended Key Usage:
     E-mail Protection, TLS Web Client Authentication, Microsoft
Smartcardlogin
  X509v3 Subject Alternative Name:
     msUPN:joseph.doekbrijder@swisssign.com
Signature Algorithm: sha1WithRSAEncryption
        65:35:01:a9:08:24:e6:70:7e:d1:6e:cc:a3:3b:ff:b8:3e:a5:
        46:ea:e3:66:15:92:86:cb:65:69:0e:37:aa:f5:47:72:c0:e0:
        6f:89:96:fd:bc:a7:95:af:41:0e:63:3f:36:c4:14:e3:76:6c:
        a0:5c:63:90:9b:31:14:2a:60:9b:90:6e:32:dd:4a:b8:3e:c5:
        48:72:74:9b:14:6c:c1:a1:9f:f6:61:f1:7e:d5:35:72:ef:d8:
        85:8f:c0:8e:bb:05:1c:49:ec:3c:76:5a:60:00:26:8d:c2:ae:
        9c:78:13:fb:27:24:bd:46:51:dd:14:03:92:05:44:e0:f4:37:
        62:9b:06:d4:43:ca:41:21:00:15:b9:96:01:de:3e:4f:12:66:
        b8:15:d3:84:33:3a:de:03:a4:63:84:3b:80:4d:5b:63:59:23:
        91:d4:65:27:64:d9:fe:03:88:b5:0d:c0:b1:fc:12:ee:6a:be:
        00:d6:27:50:1a:d6:92:b9:d4:77:ce:4d:9a:0c:ef:e7:2b:3b:
        cf:1b:b3:f6:da:7a:e2:f4:be:c5:85:bd:f2:6a:e2:ae:e1:a5:
        f6:cb:4d:fd:be:d2:6c:e1:53:b2:9f:12:52:6f:37:7b:da:8f:
        39:06:51:60:f4:ba:4d:86:0a:50:e6:e3:dc:b6:da:5c:91:08:
        a8:a0:f9:d4
```