EPCglobal Certificate Profile

Ratified Specification 1.0

March 8, 2006

Copyright Notice

© 2006, EPCglobal Inc.

All rights reserved. Unauthorized reproduction, modification, and/or use of this document is not permitted. Requests for permission to reproduce should be addressed to epcglobal@epcglobalinc.org.

Disclaimer

EPCglobal Inc.™ is providing this document as a service to interested industries. This document was developed through a consensus process of interested parties. Although efforts have been to assure that the document is correct, reliable, and technically accurate, EPCglobal Inc. makes NO WARRANTY, EXPRESS OR IMPLIED, THAT THIS DOCUMENT IS CORRECT, WILL NOT REQUIRE MODIFICATION AS EXPERIENCE AND TECHNOLOGICAL ADVANCES DICTATE, OR WILL BE SUITABLE FOR ANY PURPOSE OR WORKABLE IN ANY APPLICATION, OR OTHERWISE. Use of this document is with the understanding that EPCglobal Inc. has no liability for any claim to the contrary, or for any damage or loss of any kind or nature.

Copyright ©2006 EPCglobal®, All Rights Reserved.

Abstract

This document defines an X.509 certificate profile for use in the EPCglobal network.

The target audience for this specification includes:

- EPCglobal working groups using X.509 certificates in their specifications

Status of this document

This section describes the status of this document at the time of its publication. Other documents may supersede this document. The latest status of this document series is maintained at the EPCglobal. This document is the Ratified Specification representing EPCglobal Board of Governors ratification of the Recommended Specification. The Recommended Specification had been approved by both the Technical and Business Steering Committees before January 20th, 2006

Until this document is ratified by the EPCglobal Board of Governors, it is inappropriate to use EPCglobal as reference material or to cite them as other than "work in progress". This is work in progress and does not imply endorsement by the EPCglobal membership.

Comments on this document should be sent to the EPCglobal Software Action Group Security Working Group mailing list sag_security2@epclinklist.epcglobalinc.org.

Table of Contents

Copyright ©2006 EPCglobal®, All Rights Reserved.

51

Copyright ©2006 EPCglobal®, All Rights Reserved.

1 Introduction

The EPCglobal Architecture Framework document [ARCH] describes how security functions such as authentication, access control, validation, and privacy protection of individuals and corporations will be distributed across many of the roles/interfaces operating within the EPCglobal network. For example, EPCIS Interface responsibilities include a means for mutual authentication of two parties exchanging EPCIS data across that interface. Another example is the securing of communications between RFID readers and filtering/collection middleware, or reader management systems, when those elements are operating within an untrusted network environment.

The authentication of entities (subscribers, services, physical devices) operating within the EPCglobal network serves as the foundation of any security function incorporated into the network. The EPCglobal architecture allows the use of a variety of authentication technologies across its defined interfaces. It is expected, however, that the X.509 authentication framework will be widely employed within the EPCglobal network.

To ensure broad interoperability and rapid deployment while ensuring secure usage, this document defines a profile of X.509 certificate issuance and usage by entities in the EPCglobal network. The profiles defined in this document are based upon two Internet standards, defined in the IETF's PKIX Working Group, that have been well implemented, deployed and tested in many existing environments.

The first of these specifications is RFC3280 - *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* [RFC3280]. RFC3280 profiles the format and semantics of certificates and certificate revocation lists (CRLs) for the Internet PKI, and is itself a profile of the ITU X.509 [X509] standard.

The second is RFC 3279 - *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* [RFC3279]. This specification defines algorithm identifiers and ASN.1 encoding formats for digital signatures and subject public keys used in Internet PKI as defined in RFC3280.

The goals of this specification are as follows –

1. Ensure compatibility with, and thus fully leverage, existing deployed PKI infrastructure. As such, the intent of the profiles defined below is not to define any new functionality that may require updates to existing infrastructure, but to simply clarify and narrow (profile) functionality that already exists.
2. Ensure compatibility with existing deployed applications currently used "in the supply chain".
3. Define a minimum set of capabilities that SHALL be supported to ensure broad interoperability, while still allowing interested parties to extended and/or further refine to suit their individual requirements.

Certificate Authorities and applications conforming to this specification SHALL conform to all normative requirements as defined RFC3279 and RFC3280 unless otherwise indicated or clarified in this specification.

Copyright ©2006 EPCglobal®, All Rights Reserved.

2 Algorithm Profile

This section defines a profile of RFC3279.

2.1 Subject Public Key Algorithm Support

Certificate Authorities and applications conforming to this profile SHALL support the RSA asymmetric algorithm.

2.2 Signature Algorithm

Certificate Authorities conforming to this profile SHALL issue certificates using the `sha1WithRSAEncryption` algorithm.

Applications conforming to this profile SHALL, at a minimum, support the `sha1WithRSAEncryption` algorithm. Applications MAY also support the `md5WithRSAEncryption` to ensure backwards compatibility with existing deployed infrastructure; however this profile strongly discourages its use.

2.3 Key Length

To ensure the long term security of data within the EPCglobal network, this profile recommends that certificates issued in conformance with this profile have the following minimum key size [RSAKeySize]:

For Certificates Expiring	Before 2010	Before 2030	After 2030
Minimum RSA key size	1024 bits	2048 bits	3072 bits

Table 1 – Minimum RSA Key Size

3 Certificate Profile

3.1 General

This section applies to all certificate profiles defined in this specification.

3.1.1 Version

As specified in Section 4.1.2.1 of [RFC3280].

3.1.2 Serial Number

As specified in Section 4.1.2.2 of [RFC3280].

3.1.3 Issuer and Subject Distinguished Name (DN) Attribute Support

As specified in Section 4.1.2.4 of [RFC3280].

Note that this profile does not mandate which or how many attributes should appear in certificates, but simply defines a minimum that SHALL be supported by applications.

Copyright ©2006 EPCglobal®, All Rights Reserved.

See Section 3.2 for details as to which DN attributes should appear in certificates bound to entities in the EPCglobal network.

3.1.4 Validity

As specified in Section 4.1.2.5 of [RFC3280].

3.1.5 Extensions

CAs conforming to this profile SHALL support extensions as defined in Section 4.2 of [RFC3280].

At a minimum, applications conforming to this profile SHALL support the following extensions:

- subject key identifier,
- authority key identifier,
- certificate policies,
- subject alternative name,
- basic constraints,
- extended key usage
- CRL distribution point

Applications SHOULD support the authority information access extension which indicates where OCSP information is available.

Applications MAY support additional extensions as defined in [RFC3280].

Applications SHALL fail gracefully (i.e. not crash) when they encounter an unknown critical extension.

Note that this section does not mandate which or how many of these extensions should appear in certificates, but simply defines a minimum that SHALL be supported by applications to ensure a baseline of interoperability.

3.1.6 Including a GLN in a Certificate

The GLN (Global Location Number) provides a standard means to identify legal entities, trading parties and locations to support the requirements of electronic commerce. [GLNImp] As such, it is sometime useful to include a GLN in a certificate.

This section defines a new subject alternative name form of “otherName”, called globalLocationNumber, to convey a GLN.

Implementations MAY use this subject alternative name form to convey a GLN within a certificate.

The globalLocationNumber is identified as follows.

Copyright ©2006 EPCglobal®, All Rights Reserved.

```
 epcglobal OBJECT IDENTIFIER ::=
    {iso(1) org(3) dod(6) internet(1) private(4)
       enterprise(1) epcglobal(22695) }

epcgSecurity   OBJECT IDENTIFIER ::= { epcglobal (3) }
epcgPKI        OBJECT IDENTIFIER ::= { epcgSecurity (1) }
epcgOtherNames OBJECT IDENTIFIER ::= { epcgPKI (1) }
epcg-on-gln    OBJECT IDENTIFIER ::= { epcgOtherNames (1) }

-- e.g. 1.3.6.1.4.1.22695.3.1.1.1 in decimal notation

globalLocationNumber    ::= IA5String
```

The globalLocationNumber if present SHALL include the 13 digit GLN, tagged as an IA5String.

See Appendix A for additional informative information and an example encoding of this extension.

3.1.7 Path Validation

Applications claiming conformance with this profile SHALL support certificate path validation as defined in Section 6 of [RFC3280].

3.2 Identification of EPCglobal Entities

The purpose of a certificate is to bind a strongly authenticated *identity* to an asymmetric key pair. Within the EPCglobal Network it is envisioned that there are at least three different entities that may need to be securely identified via certificates. At a high level these entities are: Users, Services and/or Servers and Readers and/or Devices. The requirements for the identification of these entities differ slightly, and thus will be defined separately in this profile.

The following sections provide a high level overview of what should be used to identify each of the entities in the EPCglobal network and where this information is to be made available in the subject name of the certificate. The identities listed below are intended to be used by relying parties to authorize and control access to resources in their domain. The following recommendations simply define a minimum set of DN attributes that SHALL be present in certificates to ensure a base level of interoperability. These definitions may be extended further by EPCglobal working groups based on their particular usage scenarios.

3.2.1 Users

These entities include people in the EPCglobal network. Certificates issued to users can be used by other users, services/servers, and readers. Generally users are identified by attributes such as Name, Organizational Affiliation and email address.

User certificates issued in conformance with this profile SHALL, at a minimum, include the following subject DN attributes

- CN = <Name>
- O = <Organizational Affiliation>

Copyright ©2006 EPCglobal®, All Rights Reserved.

Additional identifying attributes MAY also be present, as specified in Section 3.1.3.

If an RFC822 email address is to be used as an identifying attribute for a user, it SHALL be placed in the subjectAltName.rfc822Name extension.

3.2.2 Services/Servers

These entities include service or server components in the EPCglobal network, including AS1 and AS2 servers, EPC-IS, ONS and other so-called “Middleware”-components.

Certificates issued to these entities can be used for authentication purposes by other services/servers, users and readers. Generally certificates associated with services and/or services are identified by attributes such as Service Description (i.e. fully qualified domain name (FQDN), organizational Function (CTO, Accounting, etc), organizational affiliation and in some cases a GLN.

Service/Server certificates issued in conformance with this profile SHALL, at a minimum, include the following subject DN attributes –

- CN = <Service Description>; or CN = <FQDN>
- O = <Organizational Affiliation>

The exact semantics of <Service Description> is not defined by this specification. Additional identifying attributes MAY also be present, as specified in Section 3.1.3.

If an FQDN or GLN is to be used as an identifying attribute for a server/service, it SHALL be placed in the subjectAltName as follows.

- subjectAltName.dNSName=<FQDN>
- subjectAltName.globalLocationNumber=<GLN>

3.2.3 Readers and Devices

These entities include tag readers and devices. Certificates associated with these entities can be used to authenticate readers to services and/or servers, other readers or even tags. Generally certificates associated with readers and devices are identified by attributes such as a FQDN, Serial Number, MAC Address, EPC and a manufacturer.

Reader and device certificates issued in conformance with this profile SHALL, at a minimum, include the following subject DN attributes

- CN = <FQDN>; and/or CN = <MAC>; and/or SN = <Serial Number> or CN=<Serial Number>
- O = <Manufacturer>

Additional identifying attributes MAY also be present, as specified in Section 3.1.3

If an FQDN or is to be used as an identifying attribute for a device/reader, it SHALL be placed in the subjectAltName as follows.

- subjectAltName.dNSName=<FQDN>

Copyright ©2006 EPCglobal®, All Rights Reserved.

4 Certificate Validation Mechanisms

This version of this specification does not mandate a profile for CRL's or OCSP. As such, EPCglobal implementations using CRL's SHALL conform to Section 5 of [RFC3280]. Implementations using OCSP SHALL conform to [RFC2560].

Further profiling of these mechanisms may be further defined in future versions of this specification.

5 References

5.1 Normative

[RFC3279] Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, http://www.ietf.org/rfc/rfc3279.txt

[RFC3280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, http://www.ietf.org/rfc/rfc3280.txt

[GLNImp] Global Location Number (GLN) Implementation Guide, http://www.uc-council.org/ean_ucc_system/pdf/GLN.pdf

[RSAKeySize] TWIRL and RSA Key Size, http://www.rsasecurity.com/rsalabs/node.asp?id=2004

[IANA] IANA Enterprise Number Registry http://www.iana.org/assignments/enterprise-numbers

5.2 Informative

[ARCH] K. Traub, G. Allgair, H. Barthel, L. Burstein, et al. , "The EPCglobal Architecture Framework", EPCglobal Public Document, July 2005.

[ONS] M. Mealing, "EPCglobal Object Name Service (ONS)", Working Draft August 2005.

[EPCIS] K. Traub, J. Chang, G. Gilbert, et al. , "EPC Information Services (EPCIS) Version 1.0 Specification", Working Draft, June 2005.

[TDS] M. Harrison, V. Sundhar, T. Osinski, "EPCglobal Tag Data Standard", Working Draft, April 2005.

Copyright ©2006 EPCglobal®, All Rights Reserved.

Appendix A. Example globalLocatorNumber

This section contains two examples of the globalLocatorNumber extension as defined in section 3.1.6 above.

A.1 Example 1

The first example details the encoding of a single subject alternative name extension that contains a single globalLocatorNumber.

First - the raw DER encoding in hexadecimal encoding.

```
30 2a 06 03 55 1D 11 04 23 30 21 a0 1f 06 0c 2b
06 01 04 01 81 b1 27 03 01 01 01 a0 0f 16 0d 35
34 31 32 33 34 35 30 30 30 30 31 33
```

Second - the same DER hexadecimal encoding broken out for additional detail.

```
30 2a  -- SEQUENCE
   06 03  -- OID
      55 1D 11  -- subjectAltName OID
          04 23  -- OctetString
             30 21 -- General Name
                 a0 1f -- OtherName (constructed)
                    06 0c -- globalLocatorNumber OID
                       2b 06 01 04 01 81 b1 27 03 01 01 01
                    a0 0f -- EXPLICIT ANY (constructed)
                       16 0d -- IA5String = 5412345000013
                          35 34 31 32 33 34 35 30 30 30 30 31 33
```

Finally an ASN.1 dump (using the dumpasn1 tool) of the extension. First column is the offset and the second column is the length of the structure in decimal.

```
   0   42: SEQUENCE {
   2    3:   OBJECT IDENTIFIER subjectAltName (2 5 29 17)
   7   35:   OCTET STRING, encapsulates {
   9   33:     SEQUENCE {
  11   31:       [0] {
  13   12:         OBJECT IDENTIFIER '1 3 6 1 4 1 22695 3 1 1 1'
  27   15:         [0] {
  29   13:           IA5String '5412345000013'
         :           }
         :         }
         :       }
         :     }
         :   }
```


Copyright ©2006 EPCglobal®, All Rights Reserved.

A.2 Example 2

The second example details the encoding of a single subject alternative name extension that contains a three name forms: globalLocatorNumber, rfc822Name, domainName

First - the raw DER encoding in hexadecimal encoding.

```
30 55 06 03 55 1D 11 04 4e 30 4c a0 1f 06 0c 2b
06 01 04 01 81 b1 27 03 01 01 01 a0 0f 16 0d 35
34 31 32 33 34 35 30 30 30 30 31 33 81 11 61 6C
65 78 40 76 65 72 69 73 69 67 6E 2E 63 6F 6D 82
16 65 70 63 69 73 2E 65 70 63 67 6C 6F 62 61 6C
69 6E 63 2E 6F 72 67
```

Second - the same DER hexadecimal encoding broken out for additional detail.

```
30 55  -- SEQUENCE
   06 03  -- OID
      55 1D 11  -- subjectAltName OID
          04 4e  -- OctetString
             30 4c -- General Name
                 a0 1f -- OtherName (constructed)
                    06 0c -- globalLocatorNumber OID
                       2b 06 01 04 01 81 b1 27 03 01 01 01
                    a0 0f -- EXPLICIT ANY (constructed)
                       16 0d -- IA5String = 5412345000013
                          35 34 31 32 33 34 35 30 30 30 30 31 33
                    81 11 -- rfc822Name (primative) = alex@verisign.com
                       61 6C 65 78 40 76 65 72 69 73 69 67 6E 2E 63 6F 6D
                    82 16 -- domainName (primative)= epcis.epcglobalinc.org
                       65 70 63 69 73 2E 65 70 63 67 6C 6F 62 61 6C 69
                       6E 63 2E 6F 72 67
```

Finally an ASN.1 dump (using the dumpasn1 tool) of the extension. First column is the offset and the second column is the length of the structure in decimal.

```
   0   85: SEQUENCE {
   2    3:   OBJECT IDENTIFIER subjectAltName (2 5 29 17)
   7   78:   OCTET STRING, encapsulates {
   9   76:     SEQUENCE {
  11   31:       [0] {
  13   12:         OBJECT IDENTIFIER '1 3 6 1 4 1 22695 3 1 1 1'
  27   15:         [0] {
  29   13:           IA5String '5412345000013'
         :           }
         :         }
  44   17:       [1] 'alex@verisign.com'
  63   22:       [2] 'epcis.epcglobalinc.org'
         :       }
         :     }
         :   }
```


Copyright ©2006 EPCglobal®, All Rights Reserved.