EPCglobal Certificate Profile Specification

Version 2.0

EPCglobal Ratified

June 10, 2010

Recommended Specification-Approved by TSC

Previous version: 1.0.1

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.

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 has completed the Certificate Profile Working Group review and was approved as the Last Call Working Draft (LCWD) on February 11, 2010. On March 31st an EPCglobal Software Action Group ballot advanced this document to Candidate Specification. On May 13th the Candidate Specification was advanced to Recommend Specification by the Technical Standards Committee, since it was considered not necessary by the WG to conduct a Prototype test event on this specification. On June 10th this standard was ratified by the EPCglobal Board.

Comments on this document should be sent to the EPCglobal Software Action Group and addressed to GS1help@gs1.org.

Fixed Errata

Section#	Line #	Description	Disposition
Cover Page		Cover Page does not match other EPCglobal Standards	Added Disclaimers, Copyright notice, revision date and GS1/EPCglobal Logo.
Status		Update status box	List nature of changes to document included
Appendix A1	238, 240, 244, 260 etc.	globalLocatorNumber is wrong terminology.	changed to globalLocationNumber
Appendix A2	285, 303	globalLocatorNumber is wrong terminology.	changed to globalLocationNumber

Table of Contents

1 Introduction

The EPCglobal Architecture Framework document 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.

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

To ensure the long term security of data within the EPCglobal network, this profile requires that certificates issued in conformance with this profile SHALL be generated using the following algorithm [RSA][SHS]:

For Certificates Expiring	On or before December 31, 2010	After December 31, 2010
Algorithm	sha1WithRSAEncryption sha2WithRSAEncryption	sha2WithRSAEncryption

Table 1 – Algorithm

It should be noted that, while SHA-1 is a single hash algorithm, SHA-2 is in fact a family of algorithms named after their digest lengths (in bits): SHA-224, SHA-256, SHA-384, and SHA-512. A certificate in conformance with this profile MAY use any of the members of the SHA-2 family.

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, certificates issued in conformance with this profile SHALL have the following minimum key size [RSAKeySize]:

For Certificates Expiring	On or before December 31, 2009	After December 31, 2009 and on or before December 31, 2030	After December 31, 2030
Minimum RSA key size	1024 bits	2048 bits	3072 bits

Table 2 – 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. 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 an EPC URI in a Certificate

The EPCglobal EPC (Electronic Product Code) URI (Uniform Resource Identifier) provides a standard means of identify various objects within the EPCglobal system for identifying products within e-commerce and supply chain management applications. As such, it is sometime useful to include an EPC URI in a certificate. The subset of EPC URI's to be supported are the "pure identity" EPC URIs beginning with `urn:epc:id:`.

This section defines a new permanent identifier as per [RFC 4043] called ePCURI, to convey an EPC URI.

Certificates in conformance with this profile MAY use this permanent identifier form to convey an EPC URI within a certificate. If an EPC URI is to be included in a certificate, it SHALL be included according to this profile.

The EPC URI is identified as defined in the EPC Tag Data Standard [TDS].

The AssignerID of the permanent identifier SHALL be the OID `epcgURI` as defined below:

```
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) }
epcgAssignerID OBJECT IDENTIFIER ::= { epcgOtherNames (2) }
epcgURI        OBJECT IDENTIFIER ::= { epcgAssignerID (1) }

-- i.e. 1.3.6.1.4.1.22695.3.1.1.2.1 in decimal notation
```

The IdentifierValue of the permanent identifier SHALL be the EPC URI:

```
ePCURI      ::= 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>

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.

In an EPCglobal environment, users MAY also be identified with a GSRN, GDTI, or other EPC-compliant identification key as required by the application. If an EPC URI is to be used as an identifying attribute for a user, it SHALL be placed in the subjectAltName as specified in Section 3.1.6.

3.2.2 Services/Servers

These entities include service or server components in the EPCglobal network, including AS1 and AS2 servers, EPCIS, 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.

In an EPCglobal environment, servers/services MAY also be identified with a GLN, GSRN, or other EPC-compliant identification key as required by the application. If an EPC URI is to be used as an identifying attribute for a server/service, it SHALL be placed in the subjectAltName as specified in Section 3.1.6.

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

In an EPCglobal environment, readers/devices MAY also be identified with a GLN, GSRN, or other EPC-compliant identification key as required by the application. If an EPC URI is to be used as an identifying attribute for a device/reader, it SHALL be placed in the subjectAltName as specified in Section 3.1.6.

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

[RFC4043] Internet X.509 Public Key Infrastructure Permanent Identifier,

http://www.ietf.org/rfc/rfc4043.txt

[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

[RSA] PKCS#1 v2.1 RSA Cryptography Standards, RSA Laboratories, June 14, 2002. http://www.rsa.com/rsalabs/node.asp?id=2125

[SHS] FIPS Pub 180-3, Federal Information Processing Standards Publication, Secure Hash Standard (SHS) National Institute of Standards and Technology, Gaithersburg, MD 20899-8900 October 2008. http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf

[TDS] EPC Tag Data Standard, http://www.epcglobalinc.org/standards/tds/

5.2 Informative

[ARCH] EPCglobal, "The EPCglobal Architecture Framework", EPCglobal Final Version 1.3, March 2009.

[ONS] EPCglobal, "EPCglobal Object Naming Service (ONS), Version 1.1", EPCglobal Ratified Standard, May 2008, http://www.epcglobalinc.org/standards/ons/ons_1_0_1-standard-20080529.pdf.

[EPCIS] EPCglobal, "EPC Information Services (EPCIS) Version 1.0.1 Specification", EPCglobal Ratified Standard, September 2007, http://www.epcglobalinc.org/standards/epcis/epcis_1_0_1-standard-20070921.pdf.

[TDS] EPCglobal, "EPCglobal Tag Data Standards Version 1.4", EPCglobal Ratified Standard, June 2008, http://www.epcglobalinc.org/standards/tds/tds_1_4-standard-20080611.pdf.

Appendix A. Example ePCURI

In this section, an example of a PermanentIdentifier is provided at three levels of detail describing structure and DER encoding for a single subject alternative name extension for OtherName, as described above and in "Internet X.509 Public Key Infrastructure Permanent Identifier" (*RFC 4043 ref here*).

First, a symbolic description is provided using the dumpasn format of a subjectAltName ASN object example for a permanent identifier value. The example contains a Global Location Number as an SGLN EPC Pure Identity URI [TDS]. The **epcgURI** OID identifies GS1 as the naming authority for identifier values, as described previously.

```
SEQUENCE {
  OBJECT IDENTIFIER subjectAltName (2 5 29 17)
  OCTET STRING, encapsulates {
    SEQUENCE {
      [0] {
        OBJECT IDENTIFIER id-on-permanentIdentifier (1 3 6 1
5 5 7 0 18 8 3)
        OCTET STRING, encapsulates {
          SEQUENCE {
            OBJECT IDENTIFIER epcgURI  (1 3 6 1 4 1 22695 3 1
1 2 1)
            UTF8String 'urn:epc:id:sgln:0614141.12345.0'
            }
          } } } } }
```

Second, here is a mixed symbolic and encoded description, associating DER octets that encode types and lengths with values in a readable format, again produced by a modified dumpasn1.cfg file to describe the GS1 OIDs used in this example. [The dumpasn1 Object Identifier configuration file is at http://www.cs.auckland.ac.nz/~pgut001/dumpasn1.cfg]

```
<30 4B>
SEQUENCE {
<06 03>
  OBJECT IDENTIFIER subjectAltName (2 5 29 17)
<04 44>
  OCTET STRING, encapsulates {
<30 42>
    SEQUENCE {
<A0 40>
      [0] {
<06 0A>
        OBJECT IDENTIFIER id-on-permanentIdentifier (1 3 6 1
5 5 7 0 18 8 3)
<04 32>
        OCTET STRING, encapsulates {
<30 30>
```

```
            SEQUENCE {
<06 0D>
              OBJECT IDENTIFIER epcgURI  (1 3 6 1 4 1 22695 3 1
1 2 1)
<0C 1F>
              UTF8String 'urn:epc:id:sgln:0614141.12345.0'
              }
            }

          } } } }
```

Finally, here is the raw DER encoding of this example in a hexadecimal format of the DER binary encoding:

```
30 4B 06 03 55 1D 11 04 44 30 42 A0 40 06 0A 2B
06 01 05 05 07 00 12 08 03 04 32 30 30 06 0D 2B
06 01 04 01 81 B1 27 03 01 01 02 01 0C 1F 75 72
6E 3A 65 70 63 3A 69 64 3A 73 67 6C 6E 3A 30 36
31 34 31 34 31 2E 31 32 33 34 35 2E 30
```

Appendix B. Acknowledgement of Contributors and Companies Opted-in during the Creation of this Standard (Informative)

Disclaimer

Whilst every effort has been made to ensure that this document and the information contained herein are correct, EPCglobal and any other party involved in the creation of the document hereby state that the document is provided on an "as is" basis without warranty, either expressed or implied, including but not limited to any warranty that the use of the information herein with not infringe any rights, of accuracy or fitness for purpose, and hereby disclaim any liability, direct or indirect, for damages or loss relating to the use of the document.

Below is a list of active participants and contributors in the development of Certificate Profile 2.0. This list does not acknowledge those who only monitored the process or those who choose not to have their name listed here. Active participants status was granted to those who generated emails, submitted comments during reviews, attended face-to-face meetings, participated in WG ballots, and attended conference calls that were associated with the development of this standard.

Company	Name of Participant	Role
GS1 Canada	Kevin Dean	Co-Chair/Editor
GS1 EPCglobal	Mark Frey	Facilitator/Process Manager
AXWAY/formerly Cyclone	Dale Moberg	
Bristol Myers Squibb Company	Cindy Cullen	
GS1 France	Jean-Luc LeBlond	
GS1 Germany	Craig Alan Repec	
GS1 US	Sean Lockhead	
Ken Traub Consulting	Ken Traub	

The following list in corporate alphabetical order contains all companies that were opted-in to the Certificate Profile Working Group and have signed the EPCglobal IP Policy as of April 2, 2010.

Company Name
AXWAY/formerly Cyclone
Bristol Myers Squibb Company
GS1 Australia
GS1 Canada
GS1 EPCglobal, Inc.
GS1 France
GS1 Germany
GS1 Global Office
GS1 Switzerland
GS1 Taiwan
GS1 US
Ken Traub Consulting LLC
Supply Insight, Inc.