



2 EPCglobal Certificate Profile

3 Ratified Specification with Approved, Fixed Errata
4 May 14, 2008

5
6 This version: 1.0.1
7 Previous version: 1.0

9 Disclaimer

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

20 Copyright notice

21 © 2008, EPCglobal Inc.

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

25
26 EPCglobal Inc.™ is providing this document as a service to interested industries. This document
27 was developed through a consensus process of interested parties. Although efforts have been to
28 assure that the document is correct, reliable, and technically accurate, EPCglobal Inc. makes NO
29 WARRANTY, EXPRESS OR IMPLIED, THAT THIS DOCUMENT IS CORRECT, WILL NOT
30 REQUIRE MODIFICATION AS EXPERIENCE AND TECHNOLOGICAL ADVANCES DICTATE,
31 OR WILL BE SUITABLE FOR ANY PURPOSE OR WORKABLE IN ANY APPLICATION, OR
32 OTHERWISE. Use of this Document is with the understanding that EPCglobal Inc. has no liability
33 for any claim to the contrary, or for any damage or loss of any kind or nature.

34 **Abstract**

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

36

37 The target audience for this specification includes:

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

39

40 **Status of this document**

41 This section describes the status of this document at the time of its publication. Other
42 documents may supersede this document. The latest status of this document series is
43 maintained at the EPCglobal. This document is the Ratified Specification modified to
44 correct for errata as identified. This document had completed Standards Development
45 Process steps for errata and was approved by the EPCglobal President on May 14, 2008.

46 Comments on this document should be sent to the EPCglobal Software Action Group [and](#)
47 addressed to Mark Frey MFrey@epcglobalinc.org .

48 **Fixed Errata**

Section#	Line #	Description	Disposition
Cover Page		Cover Page does not match other EPCglobal Standards	Added Dsclaimers, 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

49 **Table of Contents**

50 EPCglobal Certificate Profile 1

51 This version: 1.0.1 1

52 Previous version: 1.0 1

53 1 Introduction 4

54 2 Algorithm Profile 5

55 2.1 Subject Public Key Algorithm Support 5

56 2.2 Signature Algorithm 5

57 2.3 Key Length 5

58 3 Certificate Profile 5

59 3.1 General 5

60 3.1.1 Version 5

61 3.1.2 Serial Number 5

62 3.1.3 Issuer and Subject Distinguished Name (DN) Attribute Support 5

63 3.1.4 Validity 6

64 3.1.5 Extensions 6

65 3.1.6 Including a GLN in a Certificate 6

66 3.1.7 Path Validation 7

67 3.2 Identification of EPCglobal Entities 7

68 3.2.1 Users 7

69 3.2.2 Services/Servers 8

70 3.2.3 Readers and Devices 8

71 4 Certificate Validation Mechanisms 9

72 5 References 9

73 5.1 Normative 9

74 5.2 Informative 9

75 Appendix A. Example globalLocationNumber 10

76 A.1 Example 1 10

77 A.2 Example 2 11

78

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.

119 **2 Algorithm Profile**

120 This section defines a profile of RFC3279.

121 **2.1 Subject Public Key Algorithm Support**

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

124 **2.2 Signature Algorithm**

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

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

131 **2.3 Key Length**

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

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

135 **Table 1 – Minimum RSA Key Size**

136 **3 Certificate Profile**

137 **3.1 General**

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

139 **3.1.1 Version**

140 As specified in Section 4.1.2.1 of [RFC3280].

141 **3.1.2 Serial Number**

142 As specified in Section 4.1.2.2 of [RFC3280].

143 **3.1.3 Issuer and Subject Distinguished Name (DN) Attribute**
144 **Support**

145 As specified in Section 4.1.2.4 of [RFC3280].

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

148
149

150 **3.1.4 Validity**

151 As specified in Section 4.1.2.5 of [RFC3280].

152 **3.1.5 Extensions**

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

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

- 157 • subject key identifier,
- 158 • authority key identifier,
- 159 • certificate policies,
- 160 • subject alternative name,
- 161 • basic constraints,
- 162 • extended key usage
- 163 • CRL distribution point

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

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

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

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

172 **3.1.6 Including a GLN in a Certificate**

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

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

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

180 The globalLocationNumber is identified as follows.

181

```

182     epcglobal OBJECT IDENTIFIER ::=
183         {iso(1) org(3) dod(6) internet(1) private(4)
184             enterprise(1) epcglobal(22695) }
185     epcgSecurity    OBJECT IDENTIFIER ::= { epcglobal (3) }
186     epcgPKI        OBJECT IDENTIFIER ::= { epcgSecurity (1) }
187     epcgOtherNames OBJECT IDENTIFIER ::= { epcgPKI (1) }
188     epcg-on-gln    OBJECT IDENTIFIER ::= { epcgOtherNames (1) }
189     -- e.g. 1.3.6.1.4.1.22695.3.1.1.1 in decimal notation
190     globalLocationNumber ::= IA5String
191

```

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

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

196 3.1.7 Path Validation

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

199 3.2 Identification of EPCglobal Entities

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

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

213 3.2.1 Users

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

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

- 219 • CN = <Name>
- 220 • O = <Organizational Affiliation>

221 Additional identifying attributes MAY also be present, as specified in Section 3.1.3.
222 If an RFC822 email address is to be used as an identifying attribute for a user, it SHALL be
223 placed in the subjectAltName.rfc822Name extension.

224 **3.2.2 Services/Servers**

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

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

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

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

236 The exact semantics of <Service Description> is not defined by this specification.

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

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

- 240 • subjectAltName.dNSName=<FQDN>
- 241 • subjectAltName.globalLocationNumber=<GLN>

242 **3.2.3 Readers and Devices**

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

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

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

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

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

- 255 • subjectAltName.dNSName=<FQDN>

256 **4 Certificate Validation Mechanisms**

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

259 Implementations using OCSP SHALL conform to [RFC2560].

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

262 **5 References**

263 **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>

264

265 **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.

266

267 Appendix A. Example globalLocationNumber

268

269 This section contains two examples of the globalLocationNumber extension as defined in
270 section 3.1.6 above.

271 A.1 Example 1

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

274

275 First - the raw DER encoding in hexadecimal encoding.

276

```
277 30 2a 06 03 55 1D 11 04 23 30 21 a0 1f 06 0c 2b  
278 06 01 04 01 81 b1 27 03 01 01 01 a0 0f 16 0d 35  
279 34 31 32 33 34 35 30 30 30 30 31 33
```

280

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

282

```
283 30 2a -- SEQUENCE  
284 06 03 -- OID  
285 55 1D 11 -- subjectAltName OID  
286 04 23 -- OctetString  
287 30 21 -- General Name  
288 a0 1f -- OtherName (constructed)  
289 06 0c -- globalLocationNumber OID  
290 2b 06 01 04 01 81 b1 27 03 01 01 01  
291 a0 0f -- EXPLICIT ANY (constructed)  
292 16 0d -- IA5String = 5412345000013  
293 35 34 31 32 33 34 35 30 30 30 30 31 33  
294
```

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

297

```
298 0 42: SEQUENCE {  
299 2 3: OBJECT IDENTIFIER subjectAltName (2 5 29 17)  
300 7 35: OCTET STRING, encapsulates {  
301 9 33: SEQUENCE {  
302 11 31: [0] {  
303 13 12: OBJECT IDENTIFIER '1 3 6 1 4 1 22695 3 1 1 1'  
304 27 15: [0] {  
305 29 13: IA5String '5412345000013'  
306 : }  
307 : }  
308 : }  
309 : }  
310 : }
```

311

312

A.2 Example 2

313

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

314

315

First - the raw DER encoding in hexadecimal encoding.

316

```

317 30 55 06 03 55 1D 11 04 4e 30 4c a0 1f 06 0c 2b
318 06 01 04 01 81 b1 27 03 01 01 01 a0 0f 16 0d 35
319 34 31 32 33 34 35 30 30 30 30 31 33 81 11 61 6C
320 65 78 40 76 65 72 69 73 69 67 6E 2E 63 6F 6D 82
321 16 65 70 63 69 73 2E 65 70 63 67 6C 6F 62 61 6C
322 69 6E 63 2E 6F 72 67

```

323

324

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

325

```

326 30 55 -- SEQUENCE
327 06 03 -- OID
328 55 1D 11 -- subjectAltName OID
329 04 4e -- OctetString
330 30 4c -- General Name
331 a0 1f -- OtherName (constructed)
332 06 0c -- globalLocationNumber OID
333 2b 06 01 04 01 81 b1 27 03 01 01 01
334 a0 0f -- EXPLICIT ANY (constructed)
335 16 0d -- IA5String = 5412345000013
336 35 34 31 32 33 34 35 30 30 30 30 31 33
337 81 11 -- rfc822Name (primitive) = alex@verisign.com
338 61 6C 65 78 40 76 65 72 69 73 69 67 6E 2E 63 6F 6D
339 82 16 -- domainName (primitive)= epcis.epcglobalinc.org
340 65 70 63 69 73 2E 65 70 63 67 6C 6F 62 61 6C 69
341 6E 63 2E 6F 72 67

```

342

343

Finally an ASN.1 dump (using the dumpasn1 tool) of the extension. First column is the

344

offset and the second column is the length of the structure in decimal.

345

```

346 0 85: SEQUENCE {
347 2 3: OBJECT IDENTIFIER subjectAltName (2 5 29 17)
348 7 78: OCTET STRING, encapsulates {
349 9 76: SEQUENCE {
350 11 31: [0] {
351 13 12: OBJECT IDENTIFIER '1 3 6 1 4 1 22695 3 1 1 1'
352 27 15: [0] {
353 29 13: IA5String '5412345000013'
354 : }
355 : }
356 44 17: [1] 'alex@verisign.com'
357 63 22: [2] 'epcis.epcglobalinc.org'
358 : }

```

359 : }
360 : }
361