3GPP TSG SA WG3 Security — S3#30 **S3-030530**
6 –10 October 2003
Povoa de Varzim, Portugal

Source: **Nokia**

Title: **Subscriber Certificate Profiles**

Document for: **Information**

Agenda Item: **7.9 GAA and Support for subscriber certificates**

1. INTRODUCTION

SA3 has agreed that the subscriber certificate profiles are based on WAP certificate and CRL profiles specification [WAPCert] (later referred as “WAP profile”). WAP profile was selected to be the profile for the subscriber certificates because WAP profile has been defined for the wireless world in mind, 3GPP should reuse the work already done in OMA, and 3GPP should not define yet another certificate profile.

This contribution gives a brief historical background of the relevant certificate profiles, and introduces the WAP profile in more detail.

2. CERTIFICATE PROFILES

A *Certificate Profile* defines the format and the semantics of certificates for certain PKIs. For example, “Internet X.509 PKI: Certificate and CRL profile” [RFC 3280] does this for the Internet PKI, as the WAP profile does it for the WPKI [WPKI]. Different groups have been defining certificate formats, which include X.509, SPKI [SPKI], OpenPGP [OpenPGP], and EDIFACT [EDIFACT]. In this paper we concentrate on X.509 certificate formats and formats that have been derived from it.

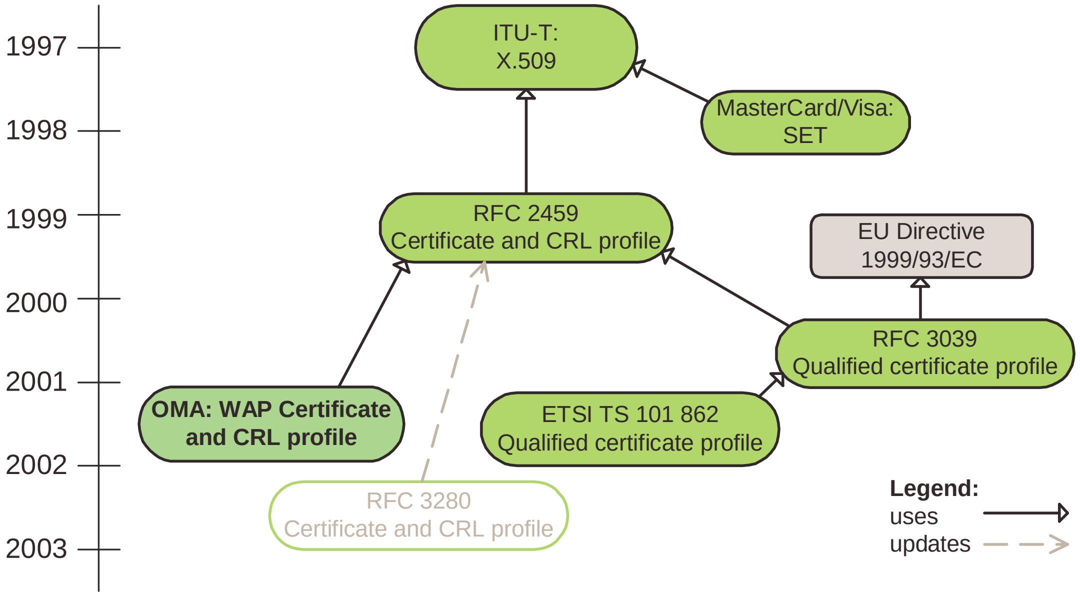
1997
1998
1999
2000
2001
2002
2003
ITU-T:
X.509
MasterCard/Visa:
SET
RFC 2459
Certificate and CRL profile
EU Directive
1999/93/EC
RFC 3039
Qualified certificate profile
OMA: WAP Certificate and CRL profile
ETSI TS 101 862
Qualified certificate profile
RFC 3280
Certificate and CRL profile
Legend:
uses
updates

Figure 1. Certificate profiles based on X.509 format.

Figure 1 depicts relationships between the well-known certificate profiles that are derived from X.509 version 3 certificate format. One exception to this is the EU Directive on electronic signatures [DIR], which states merely requirements on a certificate profile and does not define any format.

X.509 defines a X.509 version 3 public key certificate format in [X509-97] and [X509-00]. It has gained the most momentum in current PKI standards, profiles, and frameworks. Although X.509 defines certain requirements associated with the standard fields and extensions of a certificate, other issues still must be further refined in specific profiles to fully address interoperability considerations.

IETF PKIX Working Group introduced such a profile in January 1999 with the publication of [RFC 2459]. In April 2002, this RFC was replaced with [RFC 3280]. OMA's WAP profile further develops the PKIX certificate profile for the mobile environment. Also, MasterCard/Visa's SET specifications [SET] uses X.509 version 3 public key certificate format.

The term *Qualified Certificate* describes a format for a certificate whose primary purpose is identifying a person with high level of assurance in public *non-repudiation* services [RFC 3039]. Qualified certificates are typically issued by government instances or national bodies, and the certification procedures must follow the EU Directive on electronic signature. For example, during the initial registration the person must be physically present at the registration office.

Current draft TS for subscriber certificates [S3-030488] uses the WAP profile with subscriber certificates. As can be seen from the figure this certificate profile is derived directly from IETF PKIX [RFC 3280] and ITU-T X.509 [X509-97] Certificate profiles.

3. WAP CERTIFICATE AND CRL PROFILES

WAP profile is based on IETF PKIX Certificate and CRL profile[1]. It specifies which attributes and extensions from PKIX profile are needed and what are the possible values for them. It also defines additional attributes and one new extension to be used with WAP certificates. This chapter gives a general level description of the profile.

3.1 Requirements and assumptions

WAP profile assumes that the WAP environment may be characterized in the following way:

- Limited bandwidth between WAP clients and WAP servers.
- Limited computational capabilities in WAP clients.
- Limited memory resources in WAP clients.

Additionally, a reasonable assumption is that WAP servers are connected to and inter-operating with the Internet. Therefore, the certificate profile should takes these characterization into account.

Because of these assumptions WAP profile must take into account possible reductions on certificate footprint, and limited processing requirements but also make sure that WAP certificates provide a secure binding between an entity and its public key, and ensure compatibility with existing PKI infrastructure.

3.2 Certificate profiles

WAP profile defines four types of certificates:

1. User certificates for authentication,
2. User certificates for digital signature (non-repudiation),
3. X.509-compliant server certificates (for authentication), and

[1] WAP Certificate and CRL profile actually refers to RFC 2459, which has been obsoleted by RFC 3280.

4. Authority certificates (i.e., CA certificates).

Appendix A presents the four profiles in greater detail. WAP Profile also mentions “role certificates” (i.e., attribute certificates [RFC 3281]), but does not define them.

Subscriber certificates are issued only to users. Therefore, only the user certificate and CA certificate profiles are relevant to subscriber certificate profiles. Server certificate profile is not required to be part of the subscriber certificate profiles.

3.3 CRL profile

As WAP Profile assumes, that Certificate revocation lists (CRLs) will not be sent over the air in WAP protocols, or stored (or processed) by UEs, it does not put any requirements on the format of these data structures, but recommends that CRLs are issued in conformance with the PKIX profile [RFC 3280].

3.4 Private attributes and extensions

WAP Profile extends the PKIX profile by defining private attributes and extensions.

3.4.1 serialNumber attribute

WAP Profile defines serialNumber attribute to be used within Issuer and Subject Names as a part of the distinguished name. It is used to shorten subject names, while maintaining distinguished name requirements (i.e., uniqueness). See more details in chapter 8.1.1 of [WAPCert].

3.4.2 domainInformation extension

WAP Profile defines domainInformation extension to carry information that pertain to the usage of this certificate and the domain in which is has been issued, such as:

- whether on-line status requests are required before using this certificate,
- the name of the domain root CA (optional), and
- an (optional) URL pointing to a resource containing a DER-encoded value of type *Extensions*, carrying more (non-critical) extensions linked to this certificate. The hash included in the certificate protects the integrity of this externally stored value.

This extension shall not be critical. See more details in chapter 10.1 of [WAPCert].

3.5 WTLS certificate format

OMA’s WTLS specification [WTLS] defines a WTLS certificate format, which has been optimised for size and have typically been issued only to WTLS servers. Since subscriber certificate profiles define the use of user certificates, the WTLS certificate format should not be included to subscriber certificate profiles.

4. CONCLUSION

This contribution described the WAP profile in detail. It was noted that both the server certificate profile (defined in [WAPCert]), and the WTLS certificate format (defined in [WTLS]) are not required to be part of subscriber certificate profiles. This should be stated in the TS SSC [S3-030488].

REFERENCES

[BOOK] Adams, C., and S. Lloyd, “Understanding PKI: Concepts, Standards, and Deployment Considerations”, 2nd Edition, Addison-Wesley, 2003.

[DIR] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[EDIFACT] ISO 9735, Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) specification.

[OpenPGP] OpenPGP.org, URL: http://www.openpgp.org/

[RFC 2459] Housley, R., Ford, W., Polk, W., and D. Solo, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, RFC 2459, January 1999. Obsoleted by RFC 3280.

[RFC 3039] Santesson, S., Polk, W., Barzin, P., and M. Nystrom, “Internet X.509 Public Key Infrastructure Qualified Certificates Profile”, RFC 3039, January 2001.

[RFC 3280] Housley, R., Polk, W., Ford, W., and D. Solo, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, RFC 3280, April 2002.

[RFC 3281] Farrell, S., and R. Housley, “An Internet Attribute Certificate – Profile for Authorization”, RFC 3281, April 2002.

[S3-030488] Draft 3GPP TS 33.109 v0.3.0 “Bootstrapping of application security using AKA and Support for Subscriber Certificates; System Description (Release 6)”.

[SET] MasterCard/Visa, Secure Electronic Transaction, URL: http://www.setco.org/

[SPKI] The Simple Public Key Infrastructure (SPKI) Charter,
URL: http://www.ietf.org/html.charters/spki-charter.html

[TS-101862] ETSI TS 101 862: “Qualified certificate profile”, V1.2.1 (2001-06).

[WAPCert] WAP Forum, “WAP Certificate and CRL Profiles”, WAP-211-WAPCert, 22-May-2001.

[WPKI] WAP Forum, “WPKI”, WAP-217-WPKI, 24-Apr-2001.

[WTLS] WAP Forum, “Wireless Transport Layer Security Specification”, WAP-199-WTLS, 06-Apr-2001.

[X509-00] ITU-T Recommendation X.509: Information Technology – Open Systems Interconnection – The Directory: Public Key and Attribute Certificate Frameworks, March 2000.

[X509-97] ITU-T Recommendation X.509 (1997 E): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, June 1997.

APPENDIX A: WAP CERTIFICATE PROFILES

Table 1 presents most of the requirements for the WAP profiles [WAPCert]. Static conformance requirements imposed on UE are stated in chapter C.1 of [WAPCert].

Attributes / Extensions	**User certificates (authentication and non-repudiation)**	**Server certificates (authentication)**	**CA certificates**
Certificate serial number	Avoid using longer than 8 bytes (63 bits, topmost bit cannot be set to 1)	Avoid using longer than 20 bytes (159 bits, topmost bit cannot be set to 1)	Same as for user certificates.
Signature (Algorithm)[1]	sha1WithRSAEncryption, ecdsa-with-SHA1	Same as for user certificates.	Same as for user certificates
Issuer (Name)	MUST recognize: countryName, organizationalName, organizationalUnitName, stateOrProviceName, commonName, domainComponent, serialNumber (private) SHOULD recognize: All the other attributes in section 4.1.2.4 of [RFC 3280].	Same as for user certificates.	Same as for user certificates
Subject (Name)	Same as for Issuer Name.	Same as for user certificates.	In self-signed certificate, the subject name shall be the same as the issuer name. Otherwice, same as for user certificates.
Subject Public Key[2]	rsaEncryption id-ecPublicKey	Same as for user certificates	Same as for user certificates
Certificate Extensions[3]	keyUsage[4]*, extKeyUsage*, certificatePolicies*, subjectAltName*, basicConstraints[5]*, domainInformation (private)*, nameConstraints, policyConstraints, authorityKeyIdentifier[6], subjectKeyIdentifier[3] * MUST be recognized by application server, others SHOULD be recognized	keyUsage*, extKeyUsage[7]*, authorityKeyIdentifier[8]*, subjectAltName[9]*, certificatePolicies[10], authorityAccessInfo * MUST be recognized by UEs, others SHOULD be recognized	Same as for user certificates, except: *keyUsage* should be present and must have at least the *keyCertSign* bit set if present. *basicConstraint* must be present, and shall be critical: the *cA* component of it must be set to true, and the *pathLenConstraint* component need not be present.

Table 1. WAP certificate profile.

[1] UE MUST support at least one of these algorithms. UEs that support server-authenticated TLS session MUST support *sha1WithRSAEncryption*. UEs MUST be able to process certificates signed with keys up to and including 2048 bits (RSA) and 233 bits (EC).

[2] RSA key should be 1024 bits or longer, EC public keys should be 160 bits or longer.

[3] UE certificate processing MUST NOT fail due to the presence of unrecognized, but non-critical, extensions. UEs MUST be able to process the basicConstraint and the subjectKeyIdentifier extension.

[4] <u>Authentication certificates:</u> If *keyUsage* extension is included, it shall have the *digitalSignature* bit set if the public is an RSA key. If the public key is an EC-DH key, it shall have the *keyAgreement* bit set. For RSA keys, the extension may also have the *keyEncipherment* bit set. Other bits must not be set. The *keyUsage* extension should be marked as critical. <u>Non-repudiation certificates:</u> If *keyUsage* extension is present (recommended), the only bits allowed to be are the *digitalSignature* bit and/or the *nonRepudiation* bit. Other bits must not be set. The *keyUsage* extension should be marked as critical.

[5] CAs should not include the *basicConstraints* extension.

[6] CAs should, if including the *subjectKeyIdentifier* and/or *authorityKeyIdentifier* extension, use the *KeyIdentifier* field, and calculate the value of that field in accordance with the procedure defined in 9.4.4 of WIM specification.

[7] For the *extKeyUsage* extension, UEs must recognize the *id-kp-serverAuth* object identifier.

[8] For the *authorityKeyIdentifier* extension, UEs must recognize the *keyIdentifier* field.

[9] For the *subjectAltName* extension, UEs must recognize the *dNSName* and the *iPAddress* choices of the *GeneralName* type.

[10] For the *certificatePolicies* extension, UEs must recognize the *CPSuri* qualifier and the *UserNotice* qualifier defined in [RFC 3280], and should be able to process (i.e., retrieve and display) information conveyed in them.

Povoa de Varzim, Portugal, 6-10 October 2003

CR-Form-v7

CHANGE REQUEST

⌘ **SpecNumber CR CRNum** ⌘**rev** **-** ⌘ Current version: **0.3.0** ⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☒ ME □ Radio Access Network □ Core Network ☒

Title:	⌘	Subscriber certificate profiles			
Source:	⌘	Nokia			
Work item code:	⌘	SEC1-SC	***Date:***	⌘	2003-09-30
Category:	⌘	**B**	***Release:***	⌘	Rel-6

Use one of the following categories:

F	*(correction)*
A	*(corresponds to a correction in an earlier release)*
B	*(addition of feature),*
C	*(functional modification of feature)*
D	*(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The TS does not contain details of the subscriber certificate profile.
Summary of change:	⌘	This pseudo-CR defines the subscriber certificate profiles, which are based on WAP Certificate and CRL profiles.
Consequences if not approved:	⌘	Subscriber certificate profiles are not defined in detail.

Clauses affected:	⌘	A.2.6				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

A.2.6 Subscriber Certificate Profile

Subscriber certificate profile shall be based on WAP Certificate and CRL Profiles [WAPCert], which in turn is based on profiles defined in [RFC3280] and [X.509]. A certificate profile defines the format and semantics of certificates in a specific context. WAP Certificate and CRL profiles specification defines four certificate profiles: two user certificate profiles – one for authentication and the other for non-repudiation purposes, server certificate profile for authentication, and authorization certificate profile (i.e., CA certificate). Since subscriber certificates are issued to users, and since services need CA certificate to validate subscriber certificates, the relevant WAP certificate profiles to be used with subscriber certificate profiles are the user certificate profiles, and CA certificate profile.

~~*Editor's note: Applicability of other certificate profile specifications, e.g. RFC 3281, ETSI QC profile is FFS.*~~

The following certificate extensions shall be filled with the information given by the UE in the certification request:

- Intended certificate usage (i.e., using keyUsage and/or extKeyUsage extensions [WAPCert]).
- Subscriber identities (i.e., subject name field, and possible additional identities defined in the subjectAltName extension [WAPCert]). Operator CA shall authorize each suggested subscriber identity.
- Proof of key origin (i.e., keyGenAssertion). Operator CA shall verify the proof of key origin if it is presented.

Note: It is not mandatory for Operator CA to insert these suggested extensions by UE to the certificate. Rather, Operator CA shall issue certificates based on its certification policies. It may write a certification practice statement (CPS) [RFC2527], where it describes the general requirements and steps taken during the certificate issuing.