Profilo di certificato digitale per l'autenticazione mediante Carta Nazionale dei Servizi (CNS)

Per ragioni di chiarezza nell'interpretazione del profilo il testo è stato redatto secondo le indicazioni della specifica pubblica RFC 2119.

1 Scopo

Nel presente documento viene definito il profilo del certificato di autenticazione per l'utilizzo nell'ambito dell'emissione della Carta Nazionale dei Servizi (CNS) [9].

Il profilo proposto consente di individuare lo specifico circuito di emissione che ha generato il certificato.

2 Riferimenti

I seguenti documenti contengono definizioni e indicazioni di riferimento che sono citate all'interno del testo e che costituiscono parte integrante della proposta.
I riferimenti sono specifici (identificati dalla data di pubblicazione e/o numero di versione o dal numero di versione) oppure non specifici. Per i riferimenti specifici le revisioni successive non sono applicabili mentre lo sono per i riferimenti non specifici.

[1] CIRCOLARE n. AIPA/CR/24, "Linee guida per l'interoperabilità tra i certificatori iscritti nell'elenco pubblico di cui all'articolo 8, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513", 19 giugno 2000, (G.U. 30 giugno 2000, Serie generale n. 151).

[2] RFC 1778, "The String Representation of Standard Attribute Syntaxes", IETF, March 1995.

[3] RFC 2119, "Key words for use in RFCs to Indicate Requirement Levels", IETF, March 1997.

[4] RFC 2246, "The TLS Protocol Version 1.0", IETF, January 1999.

[5] RFC 2255, "The LDAP URL Format", IETF, December 1997.

[6] RFC 2560, "Online Certificate Status Protocol – OCSP", IETF, June 1999.

[7] RFC 3039, "Qualified Certificates Profile", IETF, January 2001.

[8] RFC 3280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, IETF, April 2002 (rende obsoleto l’RFC 2459).

[9] CNS/CIE, documentazione tecnica per la Carta d’Identità Elettronica (CIE) e per la Carta Nazionale dei Servizi (CNS), http://www.cartaidentita.it, http://www.cnipa.it .

3 Introduzione

Le parole chiave “*DEVE*”, “*DEVONO*”, “*NON DEVE*”, “*NON DEVONO*”, “*E’ RICHIESTO*”, “*DOVREBBE*”, “*NON DOVREBBE*”, “*RACCOMANDATO*”, “*NON RACCOMANDATO*” “*PUO’*” e “*OPZIONALE*” nel testo del documento debbono essere interpretate come descritto nel seguito, in conformità alle corrispondenti traduzioni contenute nel documento IETF RFC 2119 [3].

Le parole chiave “*DEVE*” o “*DEVONO*” o “*E’ RICHIESTO*” stanno a significare che l’oggetto in questione è un requisito assoluto della definizione.
Le parole chiave “*NON DEVE*” o “*NON DEVONO*” stanno a significare che l’oggetto in questione è un divieto assoluto per la definizione.
Le parole chiave “*DOVREBBE*” o “*RACCOMANDATO*” stanno a significare che, in particolari circostanze, possono esistere valide motivazioni per ignorare la particolare specifica, ma le complete implicazioni di tale scelta debbono essere comprese e pesate con cautela prima di scegliere per un’altra soluzione.
Le parole chiave “*NON DOVREBBE*” o “*NON RACCOMANDATO*” stanno a significare che, in particolari circostanze, possono esistere valide motivazioni perché la specifica sia accettabile o anche utile, ma le complete implicazioni debbono essere comprese e pesate con cautela prima di implementare una soluzione corrispondente.
Le parole chiave “*PUO’*” o “*OPZIONALE*” stanno a significare che una specifica è puramente opzionale. Un soggetto può scegliere di includere l’oggetto perché un particolare mercato lo richiede o perché ritiene che il prodotto finale ne risulti migliorato, mentre è possibile che un altro soggetto ometta tale oggetto. Un’implementazione che non include una particolare opzione, *DEVE* essere preparata ad interoperare con un’altra implementazione che la include, anche se con ridotte funzionalità. Allo stesso modo, un’implementazione che include una particolare opzione, *DEVE* essere preparata ad interoperare con un’altra implementazione che non la include (eccetto per la particolare funzionalità che l’opzione consente).

Così come definito in IETF RFC 3280 [8], si rammenta che per ogni estensione usata all’interno di un certificato va definito se essa vada marcata “critica” oppure “non critica”. Un sistema che utilizzi il certificato *DEVE* rifiutare il certificato stesso se esso incontra un’estensione marcata “critica” che non riconosce od interpreta correttamente, d’altra parte un’estensione non marcata “critica” può essere ignorata.

4 Certificato di autenticazione

Nel presente documento viene definito il profilo del certificato di autenticazione per l’utilizzo nell’ambito dell’emissione della Carta Nazionale dei Servizi (CNS) [9].

Il profilo del certificato di autenticazione è basato sugli standard IETF RFC 3039 [7] e RFC 3280 [8].

5 Certificato di autenticazione per CNS

5.1 Informazioni relative al titolare (subject)

Le informazioni relative al titolare del certificato *DEVONO* essere inserite nel campo Subject (Subject DN).
In particolare l'attributo commonName (Object ID: 2.5.4.3) *DEVE* contenere il codice fiscale del titolare (nel seguito: codiceFiscale). Esso *DEVE* inoltre contenere l'identificativo univoco del dispositivo (ID_Carta) e il valore dell'hash calcolato sul file elementare contenente i dati personali del titolare così come memorizzato nel dispositivo (EF_Dati_Personali).
La valorizzazione dei sottocampi relativi all'identificativo del dispositivo e ai dati personali DEVE essere effettuata in conformità con le specifiche della CNS e con lo scopo di garantire l'interoperabilità con la CIE.
In conformità con quanto definito per la CNS e per compatibilità con i certificati inseriti all'interno della CIE (CNS/CIE [9]), il carattere separatore dei sottocampi codiceFiscale e ID_Carta dell'attributo commonName *DEVE* essere il carattere "/" (slash, ASCII 0x2F) mentre il carattere separatore dei sottocampi ID_Carta e hashDatiPersonali *DEVE* essere il carattere "." (dot, ASCII 0x2E).
(ad es.: "DMMRNT63H14H501T/123322123123.cd3fdfdfeH2Duoewf5oasookDHo=" è un valore corretto per il commonName).
L'attributo countryName DEVE contenere il *Country Code* ISO 3166 dello Stato in cui è residente il titolare.
L'attributo organizationalUnitName DEVE contenere la denominazione dell'Amministrazione che ha rilasciato la carta.
La valorizzazione di altri attributi nel Subject DN *DEVE* essere eseguita in conformità allo RFC 3280 [8].

5.2 Estensioni del certificato

Le estensioni che *DEVONO* essere presenti nel certificato di autenticazione sono:

Key Usage, Extended Key Usage, Certificate Policies, CRL Distribution Points, Authority Key Identifier, Subject Key Identifier;

L'estensione Basic Constraints *NON DEVE* essere presente.

La valorizzazione delle estensioni elencate per il profilo descritto è riportata nel seguito.

L'estensione Key Usage (Object ID: 2.5.29.15) *DEVE* avere attivato il bit di digitalSignature (bit 0) e *DEVE* essere marcata critica. L'estensione *PUO'* contenere altri bit attivati corrispon-

denti ad altri Key Usage, purché ciò non sia in contrasto con quanto indicato in RFC 3280 [8] e in RFC 3039 [7]. L'estensione *NON DEVE* avere attivato il bit di nonRepudiation (bit 1).

L'estensione Extended Key Usage (Object ID: 2.5.29.37) *DEVE* contenere l'object id previsto per lo scopo di "TLS WWW Client Authentication" (Object ID 1.3.6.1.5.5.7.3.2) e *NON DEVE* essere marcata critica. L'estensione *PUO'* contenere altri valori che indicano altri scopi, purché non in contrasto con quanto indicato in RFC 3280 [8].

L'estensione Certificate Policies (Object ID: 2.5.29.32) *DEVE* contenere l'object id della Certificate Policy (CP) e l'URI (Uniform Resource Identifier) che punta al Certificate Practice Statement (CPS) nel rispetto del quale il certificatore ha emesso il certificato. Detto object id è definito e pubblicizzato dal certificatore. A far data dal mese di maggio 2005 l'estensione DEVE inoltre contenere l'object id "1.3.76.16.2.1" e il qualifier "userNotice" di tipo "explicitText" con il seguente contenuto: "Identifies X.509 authentication certificates issued for the italian National Service Card (CNS) project in according to the italian regulation".
Considerato che la regione Lombardia, nell'ambito del progetto CRS SISS, ha già emesso certificati di autenticazione e smart card comunque conformi alle norme sulla CNS, che dette carte costituiscono quindi delle CNS, si rendono pubblici i valori che l'object id può assumere nei suddetti certificati: "1.3.159.6.1.3.2.10" e "1.3.76.12.1.1.10.2.2.10".
Nel caso specifico di certificati emessi per il circuito della CNS la correttezza del valore contenuto nel campo codiceFiscale viene sempre verificata dall'ente emettitore (la Pubblica Amministrazione) come specificato in CNS/CIE [9].L'estensione Certificate Policies *NON DEVE* essere marcata critica.

L'estensione CRL Distribution Points (Object ID: 2.5.29.31) *DEVE* contenere l'URI che punta alla CRL/CSL pubblicata dal certificatore e utilizzabile per effettuare la verifica del certificato. In conformità a quanto definito in IETF RFC 3280 [8] par. 4.2.1.14 e par. 5.2.5, l'URI *DEVE* configurare un percorso assoluto per l'accesso alla CRL e non un percorso relativo ed inoltre *DEVE* specificare anche il nome del server.
Lo schema da utilizzare per l'URI *DEVE* essere l'http oppure l'ldap (IETF RFC 1778 [2] e RFC 2255 [5]) e consentire il download anonimo della CRL.
Costituiscono esempio valido i seguenti valori possibili:

"http://www.cns_crl.it/CRL/Autenticazione/crlauth"
"ldap://dir.cns_crl.it/cn=CA%20Autenticazione,o=Servizi%20di%20Certificazione,c=IT?certificateRevocationList;binary"

L'estensione CRL Distribution Points *NON DEVE* essere marcata critica.

L'estensione Authority Key Identifier (Object ID: 2.5.29.35) *DEVE* contenere almeno il campo keyIdentifier e *NON DEVE* essere marcata critica.
L'estensione Subject Key Identifier (Object ID: 2.5.29.14) *DEVE* contenere almeno il campo keyIdentifier e *NON DEVE* essere marcata critica.

Se il certificatore mette a disposizione delle cosiddette "relying parties" (i terzi che effettuano la verifica della validità del certificato) un sistema di Online Certificate Status Protocol (OCSP, definito in IETF RFC 2560 [6]), ha la necessità di indirizzarle correttamente sui sistemi che forniscono tali informazioni (OCSP Responders).
In tal caso il certificato *DEVE* contenere l'estensione Authority Info Access (Object ID: 1.3.6.1.5.5.7.1.1). Tale estensione *DEVE* contenere almeno un campo AccessDescription valorizzato con l'OID 1.3.6.1.5.5.7.48.1 (id-ad-ocsp) nel campo accessMethod e l'URI che punta all'OCSP Responder del certificatore, utilizzabile per effettuare la verifica del certificato stesso, nel campo accessLocation. In conformità a quanto definito in IETF RFC 3280 [8] par. 4.2.2.1 e IETF RFC 2560 [6], l'URI *DEVE* configurare un percorso assoluto per l'accesso all'OCSP Responder ed inoltre *DEVE* specificare anche il nome del server.
Lo schema da utilizzare per l'URI *DEVE* essere almeno l'http e consentire l'interrogazione mediante il protocollo OCSP definito in IETF RFC 2560 [6].
Nel caso vengano valorizzati più di un AccessDescription per l'estensione, tali indicazioni deb-

bono configurare diversi percorsi alternativi per lo stesso risultato, ossia l'interrogazione tramite OCSP dello stato del certificato al momento della richiesta.
Il valore "http://www.cns_ocsp.it/OSCPResponderOne" costituisce un esempio valido per l'accessLocation.

L'estensione Authority Info Access *NON DEVE* essere marcata critica.

L'aggiunta delle altre estensioni anche private non contenute in questo documento è *OPZIONALE* purché in conformità allo IETF RFC 3280 [8].

Appendice - Esempio

Nel seguito è riportato un esempio di certificato digitale di autenticazione conforme.

a. Certificato per CNS in versione annotata

L'esempio riporta un certificato per CNS, i valori in esso contenuti sono immaginari e utilizzati a puro scopo di esempio.

VERSION: 3
SERIAL: 7510 (0x1d56)
INNER SIGNATURE:
ALG. ID: id-sha1-with-rsa-encryption
PARAMETER: 0
ISSUER:
Country Name: IT
Organization Name: Certificatore accreditato
Organizational Unit Name: Servizi di certificazione
Common Name: Certification Authority Cittadini
VALIDITY:
Not Before: Oct 28, 03 09:59:55 GMT
Not After: Oct 27, 09 09:58:42 GMT
SUBJECT:
Country Name: IT
Organization Name: Nome convenzionale di progetto
Organizational Unit Name: Nome dell'amministrazione
Common Name:
LGRDNT63H14H501T/1234567890123456.hRfo7thkjYF45tF40v0t8DkgiIG=
PUBLIC KEY: (key size is 1024 bits)
ALGORITHM:
ALG. ID: id-rsa-encryption
PARAMETER: 0
MODULUS: 0x00a209b4 65f57559 1f699938 e29a27b3
13a30893 7379cb22 37a6380e 9dd48c4d
c9057d01 1039dd56 a55e9940 76c68c50
069a25b5 d777ffc4 d8c56ca2 fc3163e0
279d919f 0bb1d22d bb07d923 9e972ff3
252ed27a 4781bccd 99d7b76d 149d08cd
057f4b9d 9b04ddcb 76e1029e 16e0067f
f7407553 01aa513e 126ae6b1 2977ea16
b3
EXPONENT: 0x010001

EXTENSIONS:
Authority Information Access:
Method: id-ad-ocsp
Location:
Uniform Resource ID: http://www.capki.it/OCSP/ResponderOne
Certificate Policies:
Policy 1:
ID: 1.3.76.16.2.1
Qualifier 1: unotice (id-qt-unotice)
userNotice:
explicitText: Identifies X.509 authentication certificates issued for the italian National Service Card (CNS) project in according to the italian regulation
Policy 2:
ID: OID del Certificatore
Qualifier 1: cps (id-qt-cps)
CPS uri: https://www.capki.it/PrivateCA/CNSCPS
Key Usage*: Digital Signature
Extended Key Usage: Client Authorization
Authority Key Identifier: 0xea3e2ce0 c724083f 97563685 e8b85cbd 4bba9e30
CRL Distribution Points:
Distribution Point 1:
Uniform Resource ID: https://www.capki.it/Certificatore/CRL3
Subject Key Identifier: 0x44a0ff7c f5592ca6 63da6059 490ac1ce 337ecc2a
SIGNATURE:
ALG. ID: id-sha1-with-rsa-encryption
PARAMETER: 0
VALUE: 0x6c3e208d 1d9bea97 31757b54 b752678f
1002426b a5e403d5 f5368d51 fce72a97
4040731e e0601ead e1e34a46 a7d0c305

(*) estensione marcata critica.