AGID

Agenzia per l'Italia Digitale

Direzione Pubblica Amministrazione e Vigilanza

Area Soluzioni per la Pubblica Amministrazione

Profilo dei Certificati

Versione 1.0

Redatto da:	Area Soluzioni per la Pubblica Amministrazione
Approvato da:	Francesco Tortorelli

DISTRIBUZIONE : PUBBLICA

Sommario

STORIA DELLE MODIFICHE

Descrizione delle modifiche	Versione	Data
Prima emissione	1.0	13/07/2021

1 INTRODUZIONE

Il presente documento descrive i Profili dei certificati del servizio di certificazione (SPKI).

2 PROFILO DEI CERTIFICATI, CRL E OCSP

2.1 Certificato della CA emittente

Il certificato della CA emittente deve avere il seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	<8 random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	CN = TBD O = TBD L = TBD C = TBD
Validity	10 anni
Subject	CN = TBD OU = TBD O = Agenzia per l'Italia Digitale L = Roma C = IT
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit>
SignatureValue	<firma della Root CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true, pathLen=0
AuthorityKeyIdentifier (AKI)	<valore dell'estensione della Root CA>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: keyCertSign, cRLSign
CertificatePolicies	PolicyOID = XXXXXXX CPS-URI = **<**URL del CPS sul sito dell'AgID**>**
NameConstraints	<come stabilito dalla Root CA>
ExtendedKeyUsage (EKU)	<come stabilito dalla Root CA>
SubjectAlternativeName (SAN)	<assente>
AuthorityInformationAccess (AIA)	<indirizzo HTTP del servizio OCSP >
CRLDistributionPoints (CDP)	<indirizzo HTTP della ARL> <indirizzo LDAP della ARL>

2.2 Certificato di Firma

Il certificato di Firma deve avere il seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	<8 random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<Subject della CA emittente>
Validity	<3 anni>
Subject	**C** = <paese dove ha sede l'organizzazione> **ST** = <provincia dove ha sede l'organizzazione> **L** = <località dove ha sede l'organizzazione> **O** = <nome ufficiale dell'organizzazione> OU = <opzionale > **CN** = <nome comune del titolare>
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit>
SignatureValue	<firma della CA emittente>
Estensione	**Valore**
Basic Constraints	(assente)
AuthorityKeyIdentifier (AKI)	<valore dell'estensione SKI della CA emittente>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica secondo RFC5280>
KeyUsage	critico: digitalSignature
ExtendedKeyUsage (EKU)	emailProtection (1.3.6.1.5.5.7.3.4)
CertificatePolicies	PolicyOID = XXXXXXXXXXX CPS-URI = <URL del CPS sul sito dell'AgID>
SubjectAlternativeName (SAN)	rfc822Name=<indirizzo di posta elettronica di proprietà / sotto il controllo dell'organizzazione titolare del certificato>
CRLDistributionPoints (CDP)	<indirizzo HTTP di accesso alla CRL> <indirizzo LDAP di accesso alla CRL>

2.3 Certificato per Autenticazione

Il certificato per autenticazione deve avere il seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	<8 random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<Subject della CA emittente>
Validity	<3 anni>
Subject	**C** = <paese dove ha sede l'organizzazione> **ST** = <provincia dove ha sede l'organizzazione> **L** = <località dove ha sede l'organizzazione > **O** = <nome ufficiale dell'organizzazione> OU = <opzionale > **CN** = <…>
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit>
SignatureValue	<firma della CA emittente>
Estensione	**Valore**
Basic Constraints	(assente)
AuthorityKeyIdentifier (AKI)	<valore dell'estensione SKI della CA emittente>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica secondo RFC5280>
KeyUsage	critico: digitalSignature, keyEncryption
ExtendedKeyUsage (EKU)	clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4)
CertificatePolicies	PolicyOID = XXXXXXXXX CPS-URI = <URL del CPS sul sito dell'AgID>
SubjectAlternativeName (SAN)	rfc822Name=<indirizzo di posta elettronica di proprietà / sotto il controllo dell'organizzazione titolare del certificato>
CRLDistributionPoints (CDP)	<indirizzo HTTP di accesso alla CRL> <indirizzo LDAP di accesso alla CRL>

2.4 Certificato per Sito Web

Il certificato per sito web (SSL Server) deve avere il seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	<8 random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<Subject della CA emittente>
Validity	<1 anno>
Subject	**C** = **IT** **ST** = <nome della provincia dove ha sede l'organizzazione> **L** = <località dove ha sede l'organizzazione> **O** = <nome ufficiale dell'organizzazione> OU = <opzionale> **CN** = <FQDN contenuto nella estensione SAN>
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit>
SignatureValue	<firma della CA emittente>
Estensione	**Valore**
Basic Constraints	(assente)
AuthorityKeyIdentifier (AKI)	<valore dell'estensione SKI della CA emittente>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica secondo RFC5280>
KeyUsage	critico: digitalSignature, keyEncipherment
ExtendedKeyUsage (EKU)	serverAuth (1.3.6.1.5.5.7.3.1), clientAuth (1.3.6.1.5.5.7.3.2)
CertificatePolicies	Policy OID = XXXXXXXXXX CPS-URI = <URL del CPS sul sito dell'AgID>
SubjectAlternativeName (SAN)	<Uno o più FQDN, in conformità a [BR]>
AuthorityInformationAccess (AIA)	<indirizzo HTTP del servizio OCSP >
CRLDistributionPoints (CDP)	<indirizzo HTTP di accesso alla CRL> <indirizzo LDAP di accesso alla CRL>
EmbeddedSCTList (1.3.6.1.4.1.11129.2.4.2)	Elenco di Signed Certificate Timestamps secondo RFC 6962

2.5 Profilo delle CRL

Le CRL emesse dalle CA emittenti devono essere conformi alla specifica pubblica RFC 5280 [CPROF].

2.6 Profilo OCSP

Il servizio OCSP erogato per le CA emittenti deve essere conforme alla specifica pubblica RFC 6960 [OCSP].