

**LISIT S.p.A.**  
**Policy Certificati di Autenticazione e Cifra**

<b>Codice documento:</b>	<b>LISIT-CA-PRC#04</b>		
<b>Revisione:</b>	<b>1</b>	<b>Stato:</b>	APPROVATO
<b>Data di revisione:</b>	<b>31/10/2008</b>		

	<b>NOME</b>	<b>DATA</b>
<b>Redatto da:</b>	Luigi Bongiorno	
<b>Approvato da:</b>	Marina Vianello	31/10/2008

<b>INDICE DEI CONTENUTI</b>
-----------------------------

<b>1</b>	<b>STORIA DELLE MODIFICHE APPORTATE .....</b>	<b>3</b>
<b>2</b>	<b>INTRODUZIONE .....</b>	<b>4</b>
2.1	SCOPO E CAMPO DI APPLICAZIONE DEL DOCUMENTO .....	4
2.2	VALIDITÀ .....	4
2.3	RIFERIMENTI NORMATIVI.....	4
2.4	STANDARD DI RIFERIMENTO .....	4
<b>3</b>	<b>PROFILO DEL CERTIFICATO .....</b>	<b>5</b>
<b>4</b>	<b>INTEGRAZIONI AL MANUALE OPERATIVO .....</b>	<b>7</b>

## 1 STORIA DELLE MODIFICHE APPORTATE

Numero versione	Data di emissione	Sintesi delle variazioni
1.0	31/10/2008	Prima emissione

## 2 INTRODUZIONE

---

### 2.1 Scopo e campo di applicazione del documento

Questo documento è la policy dei certificati di autenticazione e cifra emessi da LISIT in conformità al Manuale Operativo per il Servizio di Certificazione Digitale [5].

Questo documento, in particolare, descrive:

- il profilo del certificato;
- solo se applicabile, eventuali regole tecniche e/o organizzative aggiuntive o meglio dettagliate rispetto a quanto già descritto nel Manuale Operativo per il Servizio di Certificazione Digitale [5].

### 2.2 Validità

Questo documento ha validità per:

- LISIT (certificatore)
- gli utenti utilizzatori dei certificati del tipo qui descritto.

### 2.3 Riferimenti normativi

- [1] DPCM 13 gennaio 2004: Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 – Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici (Gazzetta Ufficiale n. 98 del 27 aprile 2004) e successive modifiche ed integrazioni
- [2] Deliberazione CNIPA 4/2005 del 17 febbraio 2005: Regole per il riconoscimento e la verifica del documento informatico
- [3] D.lgs n° 82/2005 [CAD]: Codice dell'amministrazione digitale
- [4] D. lgs n° 159/2006: Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n° 82 recante codice dell'amministrazione digitale
- [5] Manuale Operativo per il Servizio di Certificazione Digitale (codice documento LISIT-CA-PRC#01)

### 2.4 Standard di riferimento

I certificati descritti nel presente documento sono conformi agli standard di riferimento internazionali (X509, PKCS, RFC 3280), agli standard individuati dalla normativa italiana in materia di Firma Digitale ed agli standard dalla Commissione Europea.

## 3 PROFILO DEL CERTIFICATO

L'estensione CertificatePolicies (OID: 2.5.29.32) del certificato contiene l'OID 1.3.6.1.4.1.7790.1.2.10 che identifica il Manuale Operativo e la URL del Manuale Operativo del Certificatore LISIT. L'estensione non è marcata critica.

Di seguito è descritto il profilo del certificato in termini di attributi ed estensioni:

Attributi X.509v3	Significato	Valore
Version	Indica la versione del formato del certificato implementata della specifica ITU-T X.509.	V3
Serial Number	Codice numerico che identifica univocamente il certificato nell'ambito della CA	Numero di serie del certificato
Signature Algorithm	Specifica l'algoritmo utilizzato dalla CA per firmare il certificato; è dato dalla coppia hash-algoritmo	SHA1RSA
Issuer	<p>È il nome distintivo dell'autorità di certificazione che ha emesso il certificato, fornito secondo lo standard di naming X.500, ovvero un Distinguish Name articolato in vari sottocampi.</p> <p>Country (c): individua il paese di appartenenza della CA che emette il certificato</p> <p>Organization (O): Individua l'organizzazione o l'ente di appartenenza della CA che emette il certificato</p> <p>Organization unit (OU): individua l'eventuale unità organizzativa dell'organizzazione che emette il certificato</p> <p>Common Name (CN): individua il nome della CA</p>	<p>C= IT</p> <p>O= LISIT S.p.A.</p> <p>OU= Servizio di certificazione</p> <p>CN= LISIT Servizio di Certificazione per la Firma Digitale</p>
Validity Period	Specifica la data e l'ora di inizio e fine validità del certificato. Questo campo si compone degli elementi NotBefore e notAfter	Il certificato di sottoscrizione è valido 6 anni a partire dalla sua data di emissione
Subject	Nome del possessore del certificato fornito secondo lo standard di naming X.500, ovvero un Distinguished Name.	<p>C= IT</p> <p>O=&lt;Ragione sociale o denominazione dell'organizzazione che ha richiesto l'emissione del certificato per il titolare oppure "non presente"&gt;</p> <p>OU=&lt;organization unit a cui appartiene il titolare del certificato oppure "non presente"&gt;</p> <p>CN=Cognome/Nome/CF/Codice Unico</p> <p>Description= C=&lt;Cognome esteso&gt;/ N=&lt;Nome esteso&gt;/</p> <p>D=&lt;data di nascita nel formato gg-mm-aaaa &gt;/</p> <p>R=&lt;ruolo titolare&gt;</p> <p>E=indirizzoemail</p>
Subject public Key Info	Contiene il valore della chiave pubblica del possessore del certificato, l'algoritmo con cui	RSA (1024 bit)+Chiave

	tale chiave viene usata e la sua lunghezza	
--	--	--

Estensioni X.509v3	Critica/non Critica	Significato	Valore
Key Usage	CRITICA	Specifica le finalità per le quali la chiave viene utilizzata	DigitalSignature, Key Encipherment, Data Encipherment
Certificate Policies	NON CRITICA	Specifica la policy di riferimento del certificato ed il sito di distribuzione del manuale operativo	PolicyIdentifier (1.3.6.1.4.1.7790.1.2.10) + URL del CPS nel formato <a href="http://www.lisit.it/firmadigitale">http://www.lisit.it/firmadigitale</a>
CRL Distribution Points	NON CRITICA	L'estensione indica dove reperire la CRL	URL di accesso alla CRL/CSL
EnhancedKeyUsage	NON CRITICA	Fornisce possibili estensioni nell'utilizzo della coppia di chiavi	Client Authentication, E-mail Protection
Authority Key Identifier	NON CRITICA	Seleziona una chiave tra quelle utilizzate dal certificatore	Identificatore della chiave, keyIdentifier
Subject Key Identifier	NON CRITICA	Seleziona una chiave fra quelle a disposizione del titolare	Identificatore della chiave, keyIdentifier
Subject Alternative Name (RFC822Name)	NON CRITICA	Individua l'indirizzo E-mail del titolare	Indirizzo E-mail

## 4 INTEGRAZIONI AL MANUALE OPERATIVO

Nessuna.