CA ICBPI

Policy per i Certificati Qualificati con limitazioni d'uso e di valore

Redatto da:	**Galoni Enrico** RP(Responsabile Progetto)	_____	_____ Data
Verificato da:	**Granier Umberto** RU(Responsabile Ufficio)	_____	_____ Data
Approvato da:	**Martinoli Alberto** RS(Responsabile Servizio)	_____	_____ Data

Il documento è :

- ***REDATTO*** *se provvisto della/e firma/e di redazione,*
- ***VERIFICATO*** *se provvisto anche della firma di verifica,*
- ***APPROVATO*** *se provvisto di tutte le firme*

Codice documento: CA ICBPI - 010 - 01

Progetto *N. Doc* *Versione*

Distribuzione: PUBBLICA

STORIA DELLE MODIFICHE APPORTATE

Non applicabile, poiché questa è la prima versione del documento.

LEGENDA DI COPERTINA

Stato del documento

Le firme sulla copertina del presente documento fanno riferimento allo standard interno di ICBPI per la gestione della documentazione del Sistema Qualità: hanno lo scopo di permetterne il controllo di configurazione e di indicarne lo stato di lavorazione.
Si segnala che la firma di approvazione autorizza la circolazione del documento limitatamente alla lista di distribuzione e non implica in alcun modo che il documento sia stato revisionato e/o accettato da eventuali Enti esterni.
In particolare, il documento è da intendersi **REDATTO** se provvisto della/e firma/e di chi lo ha redatto; **VERIFICATO** se ha superato con esito positivo la verifica interna e quindi provvisto della/e firma/e di verifica che ne autorizza il rilascio alla GESTIONE DELLA CONFIGURAZIONE. Nel caso in cui la revisione abbia esito negativo il documento viene modificato e verificato, con un nuovo numero di versione e una nuova data di emissione. Il documento è da intendersi **APPROVATO** se provvisto della firma di approvazione che si aggiunge alle altre.
Un documento sprovvisto di firme è in uno stato indefinito, e non può essere messo in circolazione.

Distribuzione

La distribuzione di un documento può essere:
- **PUBBLICA**, se il documento può circolare senza restrizioni;
- **INTERNA**, se il documento può circolare solo all'interno di ICBPI;
- **RISERVATA,** se il documento è distribuibile ad un numero limitato di destinatari;
- **CONTROLLATA**, se il documento è distribuibile ad un numero limitato di destinatari e ogni copia è controllata.

SOMMARIO

1. GENERALITÀ 4
1.1 Scopo del documento 4
1.2 Riferimenti alle norme di legge 4
1.3 Convenzioni di lettura 5
1.4 Riferimenti agli standard 5
1.5 Definizioni ed acronimi 6
2. PROFILO DEL CERTIFICATO 7
3. INTEGRAZIONI AL MANUALE OPERATIVO 7

1. GENERALITÀ

1.1 Scopo del documento

Questo documento è la policy dei certificati qualificati di firma digitale con limitazioni d'uso, emessi da ICBPI in conformità al Manuale Operativo dei Certificati Qualificati [MO].

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 dei Certificati Qualificati [MO].

1.2 Riferimenti alle norme di legge

[CAD] Decreto Legislativo 7 marzo 2005, n. 82: "Codice dell'amministrazione digitale", pubblicato nella Gazzetta Ufficiale. n. 112 del 16 maggio 2005.

[DIR] Direttiva del Parlamento europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche (Gazzetta Ufficiale delle Comunità europee L. 13 del 13 dicembre 1999).

[DPCM] Decreto del Presidente del Consiglio dei Ministri (DPCM) 30 marzo 2009, "Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici", pubblicato sulla Gazzetta Ufficiale n.129 del 6 giugno 2009.

[DPR445] Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445, "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", pubblicato sul Supplemento Ordinario alla Gazzetta Ufficiale n. 42 del 20 febbraio 2001.

[DLGS196] Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", pubblicato nel Supplemento Ordinario n.123 della G.U. n. 174, 29 luglio 2003.

[DLGS82] Decreto Legislativo 7 marzo 2005, n. 82: "Codice dell'amministrazione digitale", pubblicato nella Gazzetta Ufficiale. n. 112 del 16 maggio 2005.

[DLB45/09] Deliberazione CNIPA n.45 del 21 maggio 2009, "Regole per il riconoscimento e la verifica del documento informatico", Pubblicato nella G.U. n. 282 (serie generale) del 3 dicembre 2009, e successive modifiche e integrazioni.

[DM] Decreto 2 luglio 2004, "Competenza in materia di certificatori di firma elettronica" pubblicato nella Gazzetta Ufficiale n.199, 25 agosto 2004.

[DM 591] Decreto Ministeriale 30 novembre 1993, N. 591, "Regolamento concernente la determinazione dei campioni nazionali di talune unità di misura del Sistema Internazionale (SI) in attuazione dell'art. 3 della Legge 11 agosto 1991, n. 273", Pubblicato in Gazzetta Ufficiale 15 febbraio 1994, n. 37.

[DLGS159] Decreto legislativo 4 aprile 2006, n. 159 "Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale", pubblicato in G.U. 29 aprile 2006, n.99.

[DPR117] Decreto del Presidente della Repubblica 2 marzo 2004, n. 117, "Regolamento concernente la diffusione della Carta Nazionale dei Servizi, a norma dell'articolo 27, comma 8, lettera b), della legge 16 gennaio 2003, n. 3." (G.U. n. 105 del 6 maggio 2004).

[LGCNS]	"Linee guida per l'emissione e l'utilizzo della Carta Nazionale dei Servizi", Ufficio standard e metodologie d'identificazione, CNIPA, Versione 3.0, 15 maggio 2006.
[L. 48]	Legge 18 marzo 2008, n.48, "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno" pubblicato nella Gazzetta Ufficiale n.80 del 4 aprile 2008
[MO]	Manuale Operativo ICBPI S.p.A. (codice documento CA-ICBPI-001).

1.3 Convenzioni di lettura

Nel resto del documento, l'azienda ICBPI S.p.A., erogatrice del servizio di certificazione qui descritto e disciplinato, è indicata semplicemente con "ICBPI".

Col termine "Manuale Operativo" si intende sempre fare riferimento alla *versione corrente* del Manuale Operativo (vedere la sezione **Errore. L'origine riferimento non è stata trovata.**).

I riferimenti alla normativa e agli standard sono riportati tra parentesi quadre. In particolare, in alcuni dei titoli e sottotitoli di questo documento è riportato tra parentesi l'articolo, il comma e la lettera di riferimento del [DPCM].

1.4 Riferimenti agli standard

[LDAP3]	Wahl, M., Kille, S. and T. Howes, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.
[PKCS1]	B. Kaliski, "PKCS#1: RSA Encryption - Version 1.5", Internet RFC 2313, March 1998.
[PKCS10]	B. Kaliski, "PKCS#10: Certification Request Syntax - Version 1.5", Internet RFC 2314, March 1998.
[X500]	ITU-T Recommendation X.500 (1997 E), "Information Technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services", August 1997.
[X509]	ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.
[RFC 3161]	Adams, C., Cain, P., Pinkas, D. and Zuccherato, R., "Time-Stamp Protocol (TSP)", RFC 3161, August 2001.
[RFC 5816]	Santesson, S., Pope, N., "ESSCertIDv2 Update for RFC 3161", RFC 5186, March 2010.
[RFC 5280]	Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.
[ETSI 280]	ETSI TS 102 280 v 1.1.1 – "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons", March 2004.
[ETSI 862]	ETSI TS 101 862 v.1.3.2 – "Qualified Certificate profile", June 2004.

1.5 Definizioni ed acronimi

Il seguente elenco riporta il significato di acronimi ed abbreviazioni usati in questo documento:

CCIAA	Camera di Commercio, Industria, Artigianato ed Agricoltura
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
CNS	Carta Nazionale dei Servizi
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DN	Distinguished Name
DNS	Domain Name System
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
ETSI	European Telecommunications Standards Institute
GPS	Global Positioning System
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IEN	Istituto Elettrotecnico Nazionale
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
OID	Object IDentifier
PA	Pubblica Amministrazione
PDF	Portable Document Format
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman
SSL	Secure Sockets Layer
TST	Time Stamping Token
URL	Uniform Resource Locator

2. PROFILO DEL CERTIFICATO

L'indicazione che il certificato è qualificato e che la chiave privata, corrispondente alla chiave pubblica presente nel certificato qualificato, è memorizzata su un dispositivo sicuro per la generazione della firma è rappresentata, rispettivamente, dai valori id-etsi-qcs-QcCompliance (OID: 0.4.0.1862.1.1) ed id-etsi-qcs-QcSSCD (OID: 0.4.0.1862.1.4) presenti nell'estensione qcStatements.

L'estensione CertificatePolicies (OID: 2.5.29.32) del certificato contiene l'OID 1.3.159.1.5.1 che identifica il manuale operativo e l'URL che punta al manuale operativo nel rispetto del quale il certificatore ha emesso il certificato.

Nell'attributo ExplicitText del campo UserNotice dell'estensione CertificatePolicies possono essere indicati i limiti d'utilizzo del certificato che il Certificatore è tenuto ad inserire se richiesti dal titolare o dal Terzo Interessato.

Relativamente ai limiti di utilizzo, il valore dell'attributo ExplicitText, previo accordo contrattuale, può assumere i seguenti diversi valori (riportati in corsivo):

- "*La presente firma digitale ed il certificato ad essa collegato hanno validità solo <finalità>. Ogni altro utilizzo è escluso*". La <finalità> è costituita dal testo, concordato con il cliente, che descrive la finalità di utilizzo, limitata, della firma digitale e del relativo certificato.
- "*Il presente certificato è valido solo per firme apposte con procedura automatica. La presente dichiarazione costituisce evidenza dell'adozione di tale tipo di procedura in relazione ai documenti firmati*".

Infine, nel valore id-etsi-qcs-QcLimitValue dell'estensione qcSatements possono essere inseriti anche eventuali limiti al valore dei negozi per il quale il certificato può essere utilizzato.

L'estensione non è marcata critica.

3. INTEGRAZIONI AL MANUALE OPERATIVO

Nessuna.

FINE DOCUMENTO