
 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	<i>Versione 3.5</i> <i>Data 24/07/15</i>

Ente Certificatore Postecom S.p.A.


Servizio Postecert Certificati Server

Manuale operativo


 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	<i>Servizio Postecert Certificati Server</i>	<i>Versione 3.5</i> <i>Data 24/07/15</i>

Sommar

1	Introduzione	4
1.1	Contesto	4
1.2	Identificazione del documento	5
1.3	Modifiche introdotte rispetto alle emissioni precedenti	5
1.4	Tabella di Acronimi e Abbreviazioni	6
1.5	Comunità ed applicabilità	6
1.6	Responsabile del Manuale Operativo	9
2	Condizioni generali di erogazione del servizio	10
2.1	Obblighi	10
2.2	Responsabilità della CA	11
2.3	Pubblicazione e directory	11
3	Processi operativi	17
3.1	Generazione della richiesta di certificazione	17
3.2	Registrazione del Richiedente	17
3.3	Modalità di pagamento	19
3.4	Verifica dei dati	19
3.5	Generazione del certificato	19
3.6	Pubblicazione del certificato	20
3.7	Accettazione del Certificato	20
3.8	Installazione del certificato	20
3.9	Variazione dei dati di registrazione	20
3.10	Revoca del certificato	20
3.11	Circostanza per la revoca	21
3.12	Richiesta di revoca da parte del richiedente	21
3.13	Richiesta di revoca da parte della CA	21
3.14	Gestione degli archivi	22
3.15	Livelli di servizio	22
3.16	Compromissione e disaster recovery	22
4	Aspetti di sicurezza	23

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	<i>Servizio Postecert Certificati Server</i>	<i>Versione 3.5</i> <i>Data 24/07/15</i>

4.1	Protezione fisica dei locali	23
4.2	Sicurezza del sistema di certificazione	23
4.3	Sicurezza del modulo crittografico	24
4.4	Sicurezza dei sistemi di emissione	24
4.5	Sicurezza della rete	25
5	Profilo dei certificati	26
5.1	Certificato 'Postecert Certificati Server'	26
5.2	Certificato 'Postecom CS2'	27
5.3	Certificato 'Postecom CS3'	28
5.4	Certificato per web server	29

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5 Data 24/07/15

1 Introduzione

1.1 Contesto

Il protocollo TLS/SSL (Transport Layer Security / Secure Sockets Layer) è diventato lo standard *de facto* per la sicurezza delle comunicazioni tra un web server ed un browser. Il protocollo utilizza tecnologie crittografiche a chiave pubblica e fornisce le seguenti funzionalità di sicurezza:

- Riservatezza del messaggio
- Integrità del messaggio
- Autenticazione del web server
- (opzionale) Autenticazione del browser


Il protocollo è strutturato per rendere i suoi servizi di sicurezza trasparenti all'utente finale. Affinché possa essere stabilita una comunicazione TLS/SSL, almeno il web server deve essere dotato di una coppia di chiavi crittografiche e deve avere a disposizione il certificato della sua chiave pubblica.

Il grado di affidabilità che un utilizzatore di un browser può attribuire al certificato della chiave pubblica del web server, e quindi all'associazione tra la chiave pubblica e "l'identità" del web server, dipende da un insieme di fattori che nell'insieme devono contribuire a fornire fiducia sulla affidabilità delle informazioni.

La descrizione di questi fattori è contenuta nel Manuale Operativo, documento che comprende l'insieme delle norme operative utilizzate da una Certification Authority (CA) nell'emissione dei certificati. Il Manuale Operativo rappresenta la "dichiarazione delle procedure utilizzate da un Certificatore nel rilascio dei certificati". Le informazioni presenti all'interno dei certificati sono definite dalle policy, un insieme di regole che indicano l'applicabilità del certificato a ben determinate comunità di utenti e/o classi di applicazioni con requisiti di sicurezza comuni.

Ogni nuova versione del Manuale Operativo annulla e sostituisce le precedenti versioni, che rimangono tuttavia applicabili ai certificati emessi durante la loro vigenza e fino alla scadenza degli stessi.

Questa versione del Manuale Operativo recepisce l'adozione dell'algoritmo SHA-256 in sostituzione dello SHA-1 nelle policies di emissione dei certificati TLS/SSL.

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5 Data 24/07/15

1.2 Identificazione del documento

Il presente documento costituisce il Manuale Operativo di Postecom S.p.A. per l'emissione dei certificati del servizio di certificazione per i web server e prende il nome di:

➔ Servizio "Postecert Certificati Server".

Il Manuale Operativo è identificato attraverso il numero di versione 3.4. Il corrispondente file elettronico è identificabile dal nome "CPS_PCS_01" ed è consultabile per via telematica a partire dall'indirizzo Internet: <http://postecert.poste.it/manualioperativi/index.shtml>


Questo Manuale è referenziato dai seguenti OID (Object Identifier Number):

➔ 1.3.76.11.1.1.3.1 – Certificato di Certificazione per web server: "Postecert Certificati Server" a partire dal 23/02/2005 "Postecom CS2" ed a partire dal 09/03/2011 "Postecom CS3"

➔ 1.3.76.11.1.1.4.1 – Certificati di chiavi pubbliche per web server

1.3 Modifiche introdotte rispetto alle emissioni precedenti

Versione	Pagina n.	Motivo della revisione	Data
1.0		Approvazione	21/05/2002
1.1	10, 23	Ridefinizione aspetti organizzativi	01/07/2002
1.2	23, 24	Aggiornamento allegato 2	03/10/2002
3.0	1,5,6,8,9,11,21,22	Aggiornamento relativo all'utilizzo del nuovo certificato di CA	22/02/2005
3.1	8,23,24	Aggiornamento contatto telefonico servizio di call center Inserimento indirizzo Certificate Revocation List Distribution Point Inserimento indirizzo puntuale Manuale Operativo	07/07/2009
3.2	5,6,7,10,11,12, 18,22,23,24	Aggiornamento relativo all'utilizzo del nuovo certificato di CA Postecom CS3	21/03/2011
3.3	22,27,28,29	Aggiornamento a 2048 della lunghezza prevista per la chiave pubblica del web sever	12/12/2013
3.4		Aggiornamento del profilo del certificato con introduzione della estensione Subject Alternative Name e dell'indirizzo per l'oscp responder	30/07/2014
3.5		Sostituzione dell'algoritmo di hashing SHA-1 con SHA-256	02/07/2015

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5 Data 24/07/15

1.4 Tabella di Acronimi e Abbreviazioni


CA	Certification Authority
CN	Common Name
MO	Manuale Operativo
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
ITSEC	Information Technology Security Evaluation Criteria
PKI	Public Key Infrastructure
RA	Registration Authority
RSA	Rivest-Shamir-Adleman
SSL	Secure Sockets Layer
TCSEC	Trusted Computer System Evaluation Criteria
TLS	Transport Layer Security

1.5 Comunità ed applicabilità


Certification Authority (CA)

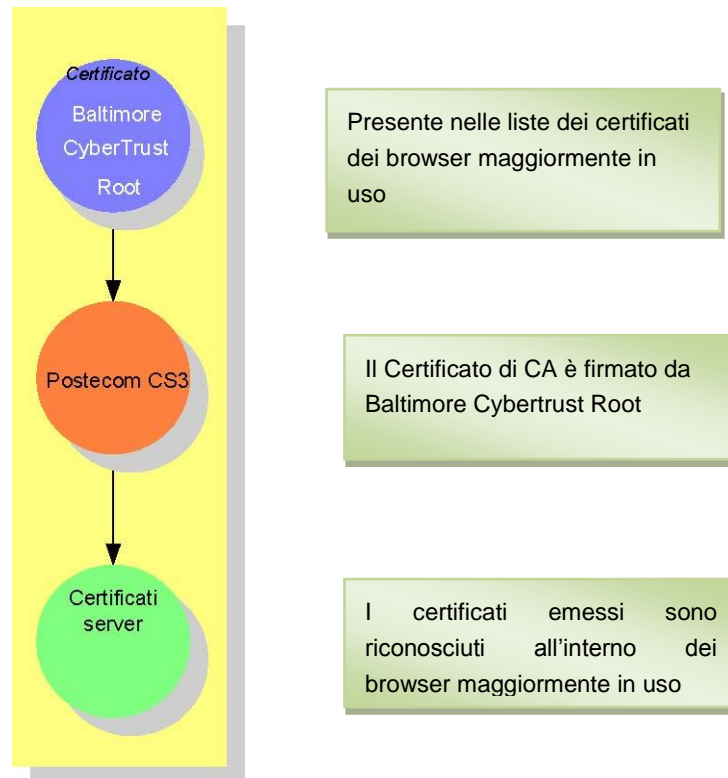
Per l'erogazione di certificati di chiave pubblica rivolti a soddisfare esigenze di sicurezza in Internet, Postecom prevede l'utilizzo di una CA che consente il riconoscimento dei certificati emessi agli utenti finali con i browser maggiormente in uso (*i.e.* Internet Explorer, Chrome, Mozilla Firefox).

A partire dal 9 marzo 2011, Postecom utilizza una nuova chiave di certificazione per l'erogazione dei certificati web server denominata "Postecom CS3". La nuova chiave di CA con la quale vengono emessi i singoli certificati per web server, è stata firmata utilizzando il certificato di Root Baltimore CyberTrust Root *Certificate*, inserito nella lista dei certificati accreditati presente nei browser più comuni ormai da un tempo sufficientemente lungo da garantire la diffusione di tale lista sulla quasi totalità dei browser attualmente in uso. Ciò permette di rendere trasparente all'utente finale che naviga in Internet, il sito protetto con un certificato rilasciato da Postecom, facendo riconoscere in automatico dai browser la pagina web accessibile in connessione sicura. Tale caratteristica viene

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	<i>Versione 3.5</i> <i>Data 24/07/15</i>

mantenuta inalterata anche per l'intero periodo di validità dei certificati web server emessi con la precedente chiave di CA "Postecom CS2".

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5
		Data 24/07/15




I certificati per web server rilasciati da Postecom permettono l'instaurazione di una connessione sicura a 128 bit. In seguito alla liberalizzazione dell'uso della crittografia forte, per attivare tale funzionalità può essere necessario aggiornare il proprio browser/sistema operativo installando l'apposita patch messa a disposizione da Microsoft.

Registration Authority (RA)

La funzione di verifica della documentazione fornita dal Richiedente è svolta da "Provisioning Servizi" della Struttura "Servizi al Cliente" di Postecom S.p.A.

Richiedente

Il servizio di certificazione è svolto da Postecom S.p.A. a favore di enti privati o enti pubblici, i quali siano legittimi proprietari di un dominio internet regolarmente registrato e siano in grado di fornire una documentazione ufficiale comprovante l'identità o l'iscrizione presso pubblici registri o la fonte normativa, amministrativa o negoziale dei poteri del richiedente. Il Richiedente dovrà provvedere ad espletare le fasi di registrazione al servizio come descritto nel paragrafo Registrazione del Richiedente individuando, nell'ambito dei propri dipendenti, il Responsabile dell'Organizzazione, quale persona che interfaccia il Richiedente con Postecom S.p.A. e che comunica, secondo le modalità indicate nel presente Manuale

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5 Data 24/07/15

Operativo, per ogni richiesta, un Responsabile del Server il quale sarà di volta in volta il soggetto deputato alla generazione della coppia di chiavi e della richiesta di certificazione (Certification Signing Request o “CSR”).

Utente

È il soggetto terzo che, tramite il proprio browser, instaura una comunicazione SSL con il web server certificato.

Tipologia di certificati

Il presente Manuale Operativo si riferisce unicamente alla emissione e gestione di certificati per web server, nell'ambito del protocollo di comunicazione sicura SSL.

1.6 Responsabile del Manuale Operativo

Postecom S.p.A. è responsabile della definizione, pubblicazione ed aggiornamento del presente documento.

Per questioni riguardanti il presente documento ed il Servizio Postecert Certificati Web Server contattare:

R.S.O. Servizio Postecert Firma Digitale
 e-mail: postecertfirmadigitale@postecert.it


Assistenza telefonica

L'assistenza telefonica è disponibile al numero 803.160 codice 3 da rete fissa (gratuito) o al numero 199.100.160 da rete mobile (costi a seconda dell'operatore), dal lunedì al venerdì (dalle 9:00 alle 20:00) ed il sabato (dalle 9:00 alle 15:00).

Documenti contrattuali di Servizio

La documentazione contrattuale di servizio “Modulo di Registrazione”, “Modulo nomina Responsabile”, “Modulo certificati Web Server” è disponibile al seguente indirizzo web:

<http://postecert.poste.it/certificatiws/download.shtml>

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5 Data 24/07/15

2 Condizioni generali di erogazione del servizio

La presente sezione disciplina e regola il rapporto contrattuale intercorrente tra Postecom ed il Richiedente il certificato per web server. La fornitura del servizio è regolata oltre che dal presente Manuale Operativo, dalle norme di legge vigenti e dal Contratto di cui al paragrafo Registrazione del Richiedente.

Il Richiedente prima di richiedere il servizio è tenuto a leggere il Manuale Operativo approvandone le condizioni generali di erogazione del servizio riportate all'interno dello stesso con la sottoscrizione del Contratto di cui al paragrafo Registrazione del Richiedente.

I contratti stipulati per l'erogazione dei servizi di certificazione per web server sono sottoposti alla legge italiana. Postecom, nell'erogazione dei propri servizi, è conforme alla normativa sul tema della protezione dei dati personali (privacy).

2.1 Obblighi

Obblighi della CA


Postecom si impegna a:

- Verificare, secondo quanto descritto all'interno del presente Manuale Operativo, la correttezza della documentazione fornita con la richiesta di certificazione;
- Rilasciare e rendere pubblico il certificato in accordo ai requisiti descritti nel presente Manuale Operativo;
- Dare tempestiva comunicazione, mediante pubblicazione nelle Liste di Revoca (CRL), della revoca dei certificati.

Obblighi del Richiedente

Il Richiedente è obbligato a:

- Fornire informazioni e documentazione veritieri in fase di registrazione;
- Generare e conservare la propria chiave privata in sicurezza, adottando le necessarie precauzioni per evitare danni, alterazioni o usi non autorizzati della stessa;
- Inviare la richiesta di certificazione con le modalità indicate nel presente Manuale Operativo;
- Installare il certificato digitale rilasciato da Postecom in base al presente Manuale Operativo unicamente sul web server corrispondente al dominio indicato nel medesimo certificato (relativo al campo CommonName);
- Informare tempestivamente Postecom nel caso in cui le informazioni presenti sul certificato rilasciato non siano più valide, richiedendo la revoca del certificato;

 GruppoPosteItaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5 Data 24/07/15

- Informare tempestivamente Postecom nel caso in cui ritenga che la sicurezza del web server su cui è stato installato il certificato possa essere compromessa, richiedendo la revoca del certificato stesso;
- Provvedere immediatamente a rimuovere dal web server il certificato per il quale è stata richiesta la revoca;
- Custodire con la massima cura il "codice di revoca".

2.2 Responsabilità della CA

Verso il Richiedente

Postecom non è responsabile nei confronti del Richiedente o di utenti terzi, per eventuali danni, di qualsiasi tipo, derivanti dalla mancata emissione del certificato o da un uso improprio del certificato. La responsabilità di Postecom, nei confronti del Richiedente o di terzi, è comunque limitata all'importo della tariffa di certificazione, fatti salvi i casi in cui l'art. 1229 del Codice Civile non consente tale limitazione.

2.3 Pubblicazione e directory


Informazioni sulla CA

Postecom, a partire dal 09/03/2011, utilizza un nuovo certificato di CA denominato "Postecom CS3" che sostituisce il precedente certificato "Postecom CS2" che ha sostituito l'ancora precedente "Postecert Certificati Server".

Per l'intero periodo di validità dei certificati web server emessi in conformità al presente Manuale Operativo, Postecom si impegna a pubblicare sul proprio sito web, postecert.poste.it, almeno le seguenti informazioni:

- I certificati delle chiavi di certificazione per firmare digitalmente i certificati per web server;
- Il presente Manuale Operativo.

Si riportano di seguito i dati salienti dei certificati di CA dedicati, nel tempo, al servizio descritto nel presente Manuale Operativo:

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5 Data 24/07/15

Postecert Certificati Server


Dato	Valore
Soggetto (Subject)	C = IT, O = Postecom s.p.a., OU = CA e Sicurezza, CN = Postecert Certificati Server
Emittente (Issuer)	C = US, O = GTE Corporation, CN = GTE CyberTrust Root
Periodo di validità	Dal 08/05/2002 al 23/02/2006

Postecom CS2

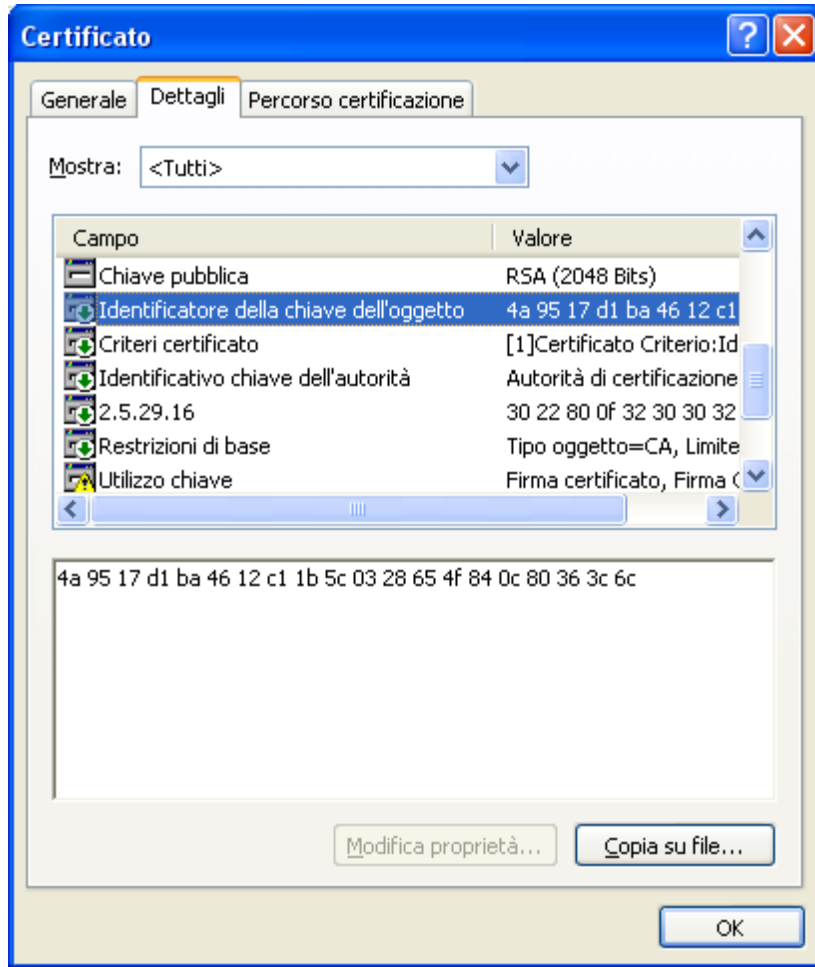
Dato	Valore
Soggetto (Subject)	C = IT, O = Postecom S.p.A., OU = Servizi Certification Authority, CN = Postecom CS2
Emittente (Issuer)	C = US, O = GTE Corporation, OU = GTE CyberTrust Solutions, Inc., CN = GTE CyberTrust Global Root
Periodo di validità	Dal 16/02/2005 al 17/02/2012


Postecom CS3

Dato	Valore
Soggetto (Subject)	C = IT, S=IT, O = Postecom S.p.A., OU = Servizi di Certificazione, CN = Postecom CS3
Emittente (Issuer)	C = IE, O = Baltimore, OU = CyberTrust , CN = Baltimore CyberTrust Root
Periodo di validità	Dal 09/03/2011 al 09/03/2018

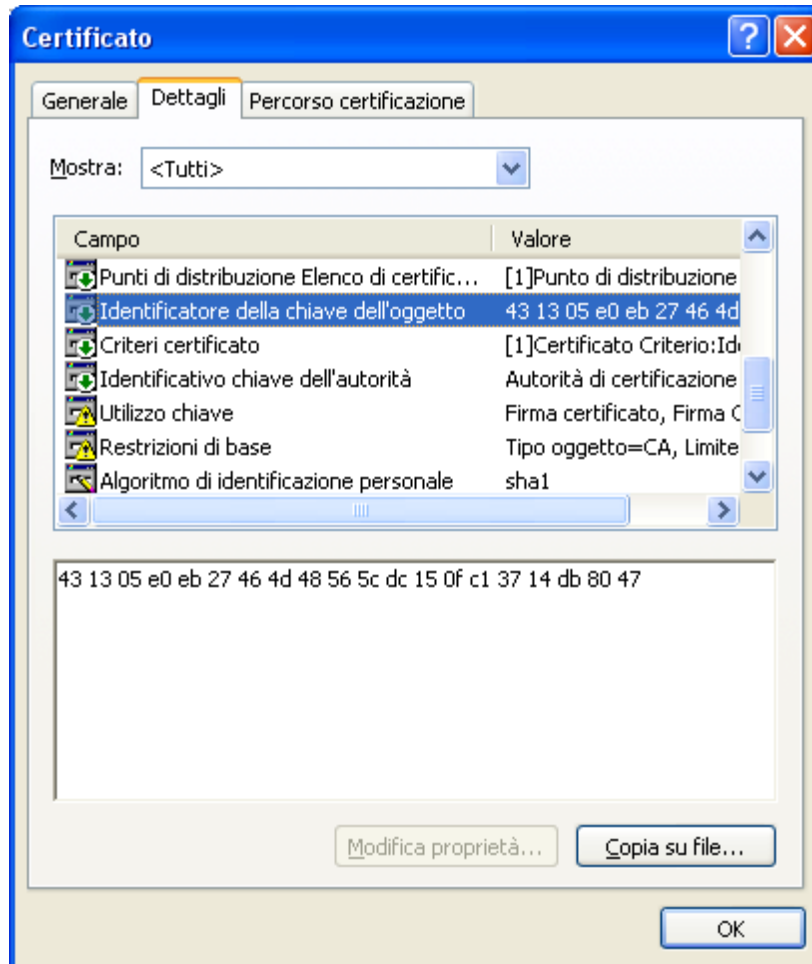
 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5
		Data 24/07/15


Postecert Certificati Server



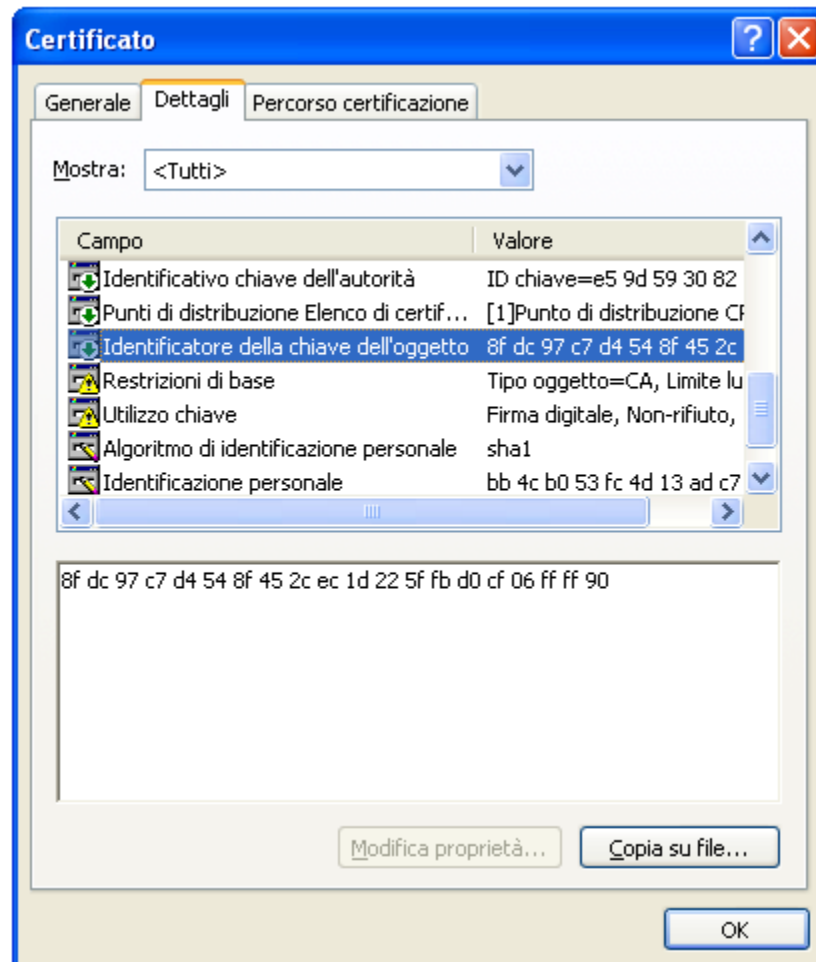
 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5
		Data 24/07/15


Postecom CS2



 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5
		Data 24/07/15

Postecom CS3



 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	<i>Versione 3.5</i> <i>Data 24/07/15</i>

Certificati e CRL


I certificati X.509v3 sono pubblicati in un directory server X.500 all'indirizzo: ldap://digicert.postecert.it accessibile mediante il protocollo LDAP v2 e v3.

Le CRL sono pubblicate in un web server il cui indirizzo è <http://postecert.poste.it/postecomcs3/crl.crl> e attraverso un server ocsf all URL=<http://postecert.poste.it/ocsp>

Le CRL sono aggiornate in occasione della revoca di un certificato e, in ogni caso, almeno una volta al giorno.

Legge applicabile e Foro Competente

Le presenti Condizioni Generali sono soggette alla legge italiana. Per le controversie che dovessero insorgere tra le parti in relazione alle disposizioni del presente Manuale Operativo, competente a giudicare sarà esclusivamente il Foro di Roma.

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5 Data 24/07/15

3 Processi operativi

3.1 Generazione della richiesta di certificazione

Questo processo è a cura del richiedente. E' finalizzato a generare la coppia chiave privata/chiave pubblica del web server utilizzando gli appositi algoritmi crittografici, interni al web server, ammessi dal protocollo SSL e supportati dai browser più diffusi.


Al momento della generazione della richiesta di certificazione (CSR), il soggetto responsabile del web server autorizzato dal Contratto, di cui al paragrafo Registrazione del Richiedente del presente Manuale Operativo, deve adottare le necessarie precauzioni per generare la chiave privata del web server in sicurezza, ed evitare divulgazioni o usi non autorizzati della stessa.

Nel file CSR in particolare viene riportato il **nome del web server** da certificare (*CommonName*) che dovrà contenere il **dominio internet** intestato all'Organizzazione richiedente.

3.2 Registrazione del Richiedente

Questo processo è a cura del richiedente. La procedura da seguire è la seguente:


- 1) accedere alla apposita sezione on line di richiesta del certificato inserendo, ove richiesto, i dati relativi ai riferimenti organizzativi, amministrativi e tecnici del certificato per web server richiesto. Prima di accedere alle pagine web di registrazione, il richiedente deve aver provveduto a generare dal web server per il quale viene richiesta la certificazione il file CSR. Tra i dati previsti, sarà presente il campo denominato "codice di revoca" che permetterà di autenticare le richieste di revoca pervenute via assistenza telefonica;
- 2) firmare il Contratto, inviato precompilato all'indirizzo di casella postale elettronica inserita in fase di caricamento dati. All'interno del Contratto è individuato il Responsabile dell'Organizzazione. La copia aggiornata del Contratto è appositamente pubblicata presso il sito postecert.poste.it. Il soggetto autorizzato alla firma è il Legale Rappresentante o equivalente per le Società o Enti non iscritti alle Camere di Commercio ma comunque abilitati a richiedere il certificato.
- 3) Il Responsabile del Server (comunicato dal Responsabile dell'Organizzazione) dovrà firmare il Modulo di Registrazione, in facsimile in allegato 1, inviato alla casella di posta elettronica indicata in fase di registrazione on line;
- 4) Documentazione da allegare:

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5 Data 24/07/15

- ➔ Fotocopia del documento di identificazione, in corso di validità, del soggetto che firma il Contratto. Sono ammessi:
 - carta di identità (fronte retro);
 - patente di guida;
 - passaporto;
 - tessere di riconoscimento purché munite di fotografia e di timbro, rilasciate da un'Amministrazione dello Stato (fronte retro)
- ➔ Documento, su carta intestata, firmato dal Responsabile dell'Organizzazione recante gli estremi del nominativo del Responsabile del Server deputato ad effettuare la richiesta di certificazione del web server, e che firma il Modulo di Registrazione di cui al punto precedente
- ➔ A seconda della categoria di appartenenza, la seguente documentazione di competenza:
 - Visura camerale non antecedente 30 giorni per le imprese iscritte presso il Registro Imprese;
 - certificato di attribuzione della partita I.V.A., per le imprese non iscritte presso il Registro Imprese;
 - copia dell'atto costitutivo, per altri enti di diritto privato;
 - altra documentazione, in originale, idonea al conferimento dei poteri al soggetto incaricato della richiesta di certificazione secondo l'organizzazione interna della struttura di appartenenza, nel caso di enti ed organismi pubblici.

Il Contratto, la nomina del responsabile del Server ed il Modulo di Registrazione e la documentazione di cui al punto 4 possono essere inviati a mezzo:

- ➔ spediti via posta all'indirizzo: Postecom S.p.A., ~~Esercizio~~, Registration Authority CA, Viale Europa 175, 00144 Roma. Eventualmente possono essere anticipati via fax al seguente numero telefonico di Postecom S.p.A.: (+39) 06 59585049 ~~e (+39) 06 59585028~~;
- ➔ e-mail: il Richiedente potrà firmare digitalmente i previsti documenti purché sia in possesso di una carta con a bordo chiavi e certificati per la firma elettronica avanzata ed inviarli tramite posta elettronica al seguente indirizzo: registrazione@postecom.it.

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5 Data 24/07/15

3.3 Modalità di pagamento

Per usufruire del servizio il Richiedente è tenuto a pagare il corrispettivo previsto per il certificato e per i relativi servizi accessori richiesti. Per modalità e condizioni di pagamento si rinvia alle condizioni generali di servizio di volta in volta aggiornate sul sito postecert.poste.it

3.4 Verifica dei dati

Al ricevimento delle informazioni, Postecom provvederà a:

- Controllare il file con la richiesta di certificazione e verificare la coerenza con i dati contenuti nel Modulo di Registrazione, nel Contratto e nella documentazione cartacea allegata;
- Verificare la univocità del nome di tipo X.500 (Distinguished Name, DN) nell'ambito dei propri certificati emessi;
- Controllare l'attribuzione del dominio internet relativo al web server alla Società richiedente la certificazione;
- Effettuare un controllo telefonico, tramite un database terzo.

Se tutte le verifiche avranno avuto esito positivo, la Registration Authority trasmetterà il file con la richiesta di certificazione alla CA, autorizzando la generazione del certificato.


Il Certificatore procede nella verifica della documentazione inviata solo in seguito alla ricezione della prova di pagamento per la stessa.

Postecom non darà corso all'emissione del certificato qualora i dati comunicati non risultino corretti o siano incompleti in base ai riscontri delle verifiche poste in essere.

3.5 Generazione del certificato

Una volta ricevuta l'approvazione della RA, la CA verificherà che il formato PKCS#10 della richiesta sia corretto. Se le verifiche previste hanno esito positivo, la CA genera il certificato in accordo al profilo descritto nel paragrafo "Profilo dei certificati". Il DN apparirà come valore del campo *subject* del certificato.

Se le verifiche non hanno esito positivo, Postecom, tramite la RA, notifica al richiedente l'evento, richiedendo la generazione di una nuova richiesta di certificazione.

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5 Data 24/07/15

3.6 Pubblicazione del certificato

Il certificato viene pubblicato nel Directory Server X.500 ed inviato, a cura del Servizio di Certificazione, all'indirizzo di posta elettronica del Responsabile del Server autorizzato.

3.7 Accettazione del Certificato

Una volta generato il certificato, questo viene inviato all'indirizzo di posta elettronica del Responsabile del Server indicato nel Modulo di Registrazione. Nel caso il Richiedente riscontri eventuali imprecisioni o difetti del certificato, questi è tenuto ad informare immediatamente Postecom tramite comunicazione all'indirizzo di posta elettronica registrazione@postecom.it. Altrimenti, il certificato verrà ritenuto accettato dal Richiedente.

Accettando il certificato, il Richiedente dichiara di accogliere i termini e le condizioni contenute nel presente Manuale Operativo e nel Contratto di cui al paragrafo Registrazione del Richiedente.

3.8 Installazione del certificato

Al ricevimento del certificato, il Richiedente potrà installarlo sul web server, seguendo le istruzioni dello specifico prodotto utilizzato.


3.9 Variazione dei dati di registrazione

Il Richiedente deve informare tempestivamente Postecom nel caso in cui ci siano delle variazioni dei dati contemplati nel paragrafo Registrazione del Richiedente. Se le variazioni riguardano dati presenti sul certificato, il Richiedente deve altresì richiedere la revoca del certificato.

Postecom si riserva la facoltà di revocare il certificato del Richiedente nel caso in cui la variazione dei dati di registrazione lo richieda.

3.10 Revoca del certificato

La revoca di un certificato si completa con la sua pubblicazione nella lista di revoca firmata dal Certificatore (CRL). Il certificato revocato non ha più validità ed il Richiedente deve provvedere immediatamente a rimuovere il certificato relativo dal web server associato.

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5 Data 24/07/15

3.11 Circostanza per la revoca

Postecom procede alla revoca del certificato su richiesta da parte del Richiedente secondo le modalità ed i tempi previsti nel presente Manuale Operativo.

Il Certificatore può procedere alla revoca di propria iniziativa, se si verificano alcune precise condizioni, quali riscontri un utilizzo non conforme a quanto stabilito nel presente Manuale Operativo.

3.12 Richiesta di revoca da parte del richiedente

Il Richiedente deve richiedere la revoca del certificato nelle seguenti circostanze:

- ➔ nel caso in cui voglia cessare il rapporto contrattuale con Postecom;
- ➔ nel caso in cui le informazioni presenti sul certificato rilasciato non siano più valide;
- ➔ nel caso in cui ritenga che la sicurezza del web server su cui è stato installato il certificato sia stata compromessa.

Quest'ultima circostanza deve essere prontamente rilevata e comunicata; in ogni caso Postecom non assume alcuna responsabilità per l'uso improprio della chiave privata associata alla chiave pubblica certificata.

Per richiedere la revoca, il Richiedente deve inviare un fax su carta intestata e appositamente sottoscritto al numero +39 06 59585049 ovvero +39 06 59585028, in cui venga esplicitamente richiesta la revoca del certificato per web server con l'indicazione almeno della Ragione Sociale del Richiedente e del nome del web server (il valore che compare nel campo **Nome del Web Server da certificare** dell'Allegato 1) da revocare. In seguito alla ricezione del fax, l'area Registrazione di Postecom provvederà ad effettuare un controllo telefonico in cui verranno richieste al Richiedente alcune informazioni necessarie contenute nel Modulo di Registrazione di cui al paragrafo "Registrazione del Richiedente", per autenticare la sua richiesta di revoca.


La richiesta di revoca sarà verificata dalla Registration Authority che, in caso di verifica positiva, inoltrerà la richiesta alla CA.

Il Certificato revocato sarà inserito nella CRL (vedi Certificati e CRL).

Il servizio per richiedere la revoca è attivo dal Lunedì al Venerdì, dalle ore 8:30 alle ore 18:00.

3.13 Richiesta di revoca da parte della CA

Postecom può revocare il certificato di un Richiedente solamente nelle seguenti circostanze:

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5 Data 24/07/15

- certezza della variazione dei dati contenuti nel certificato;
- certezza dell'uso improprio del certificato.

In ambedue i casi, Postecom, dopo aver effettuato la revoca, lo comunica al Richiedente.

3.14 Gestione degli archivi

Postecom mantiene traccia dei record informatici relativi alla:

- Richiesta di generazione del certificato,
- Emissione del certificato,
- Revoca del certificato.

Postecom mantiene i record sopra elencati per un massimo di due anni dal termine della scadenza del certificato.

Viene effettuato un backup completo giornaliero di tutti gli archivi contenenti i record sopra elencati. Postecom conserva altresì tutta la documentazione cartacea ricevuta per un massimo di due anni dal termine della scadenza del certificato, salvo termini diversi per la documentazione di tipo fiscale.

3.15 Livelli di servizio

La generazione del certificato avviene entro 3 (tre) giorni lavorativi dal ricevimento del file con la richiesta di certificazione e delle informazioni previste nel paragrafo "Registrazione del Richiedente".


La revoca del certificato avviene entro 4 (quattro) ore dal ricevimento della richiesta, entro il periodo di disponibilità del servizio (dal Lunedì al Venerdì, dalle 8:30 alle 18:00).

L'accesso al Directory Server ed alle CRL è disponibile 7 giorni su 7, 24 ore su 24, salvo i fermi per manutenzione programmata.

3.16 Compromissione e disaster recovery

Le risorse hw per l'erogazione del servizio di certificazione sono coperte da un contratto di manutenzione che garantisce l'intervento in 8 (otto) ore.

Lo stato della configurazione del sistema di emissione dei certificati, e ogni eventuale necessità di ripristino è garantito da un sistema di backup/restore dedicato.

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5 Data 24/07/15

4 Aspetti di sicurezza

4.1 Protezione fisica dei locali

I sistemi tecnologici coinvolti sono situati in un'area protetta il cui accesso è consentito esclusivamente al personale Postecom ed è controllato mediante dispositivi di riconoscimento di impronte digitali, lettori di smart card, telecamere a circuito chiuso. L'area è situata all'interno degli edifici di Poste Italiane, situati a Roma, Viale Europa 175. Gli edifici di Poste Italiane sono sorvegliati e protetti 24 ore su 24, 7 giorni su 7, e comprendono un presidio fisso della Polizia Postale e delle Comunicazioni.

4.2 Sicurezza del sistema di certificazione

La piattaforma di gestione delle attività di certificazione, composta da vari moduli appartenenti alla suite software UniCERT della Verizon Business, offre le seguenti funzioni di sicurezza:

Identificazione e autenticazione

- ➔ L'accesso ai moduli applicativi della piattaforma avviene mediante identificazione dell'utente. Il meccanismo di autenticazione è previsto anche per l'avvio e/o fermo del servizio legato al modulo applicativo.

Controllo accessi


- ➔ L'accesso ai moduli applicativi della piattaforma avviene mediante meccanismi di strong authentication. L'accesso ai moduli è consentito solo previa verifica del corretto inserimento della passphrase.

Tracciamento

- ➔ Tutte le applicazioni in esecuzione all'interno del sistema di certificazione del Certificatore mantengono traccia su appositi database delle operazioni effettuate.
- ➔ Sono prodotti dei log in formato testo ove vengono riportate informazioni relative all'avvio, fermo o allarmi relativi ai servizi legati ai moduli applicativi, nonché contenenti traccia di eventuali modifiche di configurazione apportate ai servizi. Ciascuna registrazione all'interno dei log è firmata digitalmente.

Integrità e non ripudio

- ➔ Firma digitale dei messaggi. Tutti i messaggi inviati dai singoli moduli sono firmati in modo digitale.

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5 Data 24/07/15

- ➔ Verifica dei messaggi: i moduli verificano tutti i messaggi che ricevono per assicurarsi della loro integrità ed autenticità.
- ➔ Archiviazione dei dati: tutti i dati e gli audit log sono registrati nel database relativo a ciascun modulo. Tali registrazioni sono firmate in modo digitale dai moduli proprietari del DB. Ogni registrazione ha un numero d'identificazione univoco.

Comunicazioni

- ➔ Le comunicazioni tra i moduli avvengono mediante il protocollo PKIX.

4.3 Sicurezza del modulo crittografico


Per la generazione delle firme digitali di Postecom viene utilizzato l'algoritmo RSA (Rivest-Shamir-Adleman).

Tutti i certificati emessi da Postecom – a partire dai certificati relativi alle chiavi di certificazione, fino ai certificati relativi alle chiavi pubbliche dei web server – vengono firmati utilizzando l'algoritmo RSA. Lo stesso algoritmo RSA deve essere utilizzato dall'utente per generare la propria coppia di chiavi. Le chiavi pubbliche dei web server hanno lunghezza pari a 2048 bit, le chiavi di certificazione sono lunghe 2048 bit. Ad oggi non esistono ancora sistemi di cripto-analisi in grado di compromettere chiavi della suddetta lunghezza. Poiché in futuro le probabilità di compromettere chiavi a 2048 bit potrebbero aumentare, Postecom si riserva il diritto di adeguare la lunghezza delle chiavi alle tecnologie future. Per quel che concerne le funzioni di hash, viene utilizzata la funzione definita nella norma ISO/IEC 10118-3:2004 per la generazione dell'impronta digitale: Dedicated Hash-Function 4, corrispondente alla funzione SHA-256.

4.4 Sicurezza dei sistemi di emissione

Il sistema operativo dei sistemi di emissione utilizzati nelle attività di certificazione, nella generazione dei certificati e nella gestione del registro dei certificati, è conforme almeno alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme ITCSEC. I sistemi sono configurati in modo tale da ridurre al minimo il rischio di alterazione delle configurazioni. Sono quindi previsti, nel normale uso dei sistemi stessi, profili con diritti di accesso non assimilabili a quelli amministrativi.

Gli operatori di CA adottano una modalità di autenticazione multi-fattore al sistema di certificazione delle chiavi che prevede il possesso di un certificato personale su token usb.


 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	<i>Servizio Postecert Certificati Server</i>	<i>Versione 3.5</i> <i>Data 24/07/15</i>

4.5 Sicurezza della rete

L'infrastruttura di rete prevede una prima linea costituita da un sistema firewall, configurato in alta affidabilità, che filtra il traffico da Internet verso la rete DMZ, dove risiedono i server che devono essere accessibili da Internet (come il Directory Server ed il web server che pubblica le CRL), ed una seconda linea che filtra il traffico tra rete DMZ e Secure LAN, dove sono invece installati i sistemi per la certificazione.

L'utilizzo di questa tecnologia offre la possibilità di utilizzare il NAT Network Address Translation per "mascherare" gli ip interni verso la rete Internet, permette di intercettare i tentativi di creare interruzioni al servizio con attacchi di tipo DoS SYN flood, impostare regole Anti-spoofing, limitare gli accessi in un arco temporale definibile in maniera granulare. Al fine di analizzare in tempo reale i pacchetti che viaggiano in rete e di attivare, laddove viene riscontrata una attività sospetta, le dovute protezioni (blocco di indirizzi IP, interruzione di connessioni, invio di trap) ed allarmi, è in utilizzo un sistema di Intrusion Detection che si basa su un database di vulnerabilità costantemente aggiornato.

I servizi in DMZ vengono erogati con copertura 24x7x365 con un presidio dal lunedì al venerdì dalle ore 8.00 alle ore 20.00 ed una copertura nelle ore non presidiate e festivi tramite una struttura di reperibilità a 2 livelli h24. Le segnalazioni di allarme vengono inviate tramite SMS e tramite chiamata telefonica da un sistema di monitoraggio centralizzato.


 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5
		Data 24/07/15

5 Profilo dei certificati

5.1 Certificato 'Postecert Certificati Server'

Version	Versione 3
Serial Number	02 00 02 7c
Signature	sha-1, RSA
Issuer	Country : "US" Organization : "GTE Corporation"
Validity	Dal 08/05/2002 al 23/02/2006
Subject	Country : "IT" Organization : "Postecom s.p.a." Organization Unit : "CA e Sicurezza"
SubjectPublicKeyInfo	chiave pubblica 2048 bit algoritmo utilizzato: RSA
Estensioni	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
KeyUsage (critica)	Certificate Signing, CRL Signing
basicConstraints	CA true PathLenConstraint 1


Il valore dell'OID è 1.3.76.11.1.1.3.1

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio Postecert Certificati Server	Versione 3.5 Data 24/07/15

5.2 Certificato 'Postecom CS2'

Version	Versione 3
Serial Number	04 00 03 cc
Signature	sha-1, RSA
Issuer	Country : "US" Organization : "GTE Corporation" Organization Unit : "GTE CyberTrust Solutions, Inc. "
Validity	Dal 16/02/2005 al 17/02/2012
Subject	Country : "IT" Organization : "Postecom S.p.A." Organization Unit : "Servizi Certification Authority"
SubjectPublicKeyInfo	chiave pubblica 2048 bit algoritmo utilizzato: RSA
Estensioni	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
KeyUsage (critica)	Certificate Signing, CRL Signing
basicConstraints	CA true PathLenConstraint 1


Il valore dell'OID è 1.3.76.11.1.1.3.1

 GruppoPostelitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5 Data 24/07/15

5.3 Certificato 'Postecom CS3'

Version	Versione 3
Serial Number	07 27 52 62
Signature	sha-1, RSA
Issuer	Country : "IE" Organization : "Baltimore" Organization Unit : "CyberTrust" COMMON NAME : "Baltimore CyberTrust Root"
Validity	Dal 09/03/2011 al 09/03/2018
Subject	Country : "IT" State : "IT" Organization : "Postecom S.p.A." Organization Unit : "Servizi di Certificazione" COMMON NAME : "Postecom CS3"
SubjectPublicKeyInfo	chiave pubblica 2048 bit algoritmo utilizzato: RSA
Estensioni	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
KeyUsage (critica)	Digital Signature, Non Repudiation, Certificate Signing, CRL Signing
basicConstraints	CA true PathLenConstraint 0

Il valore dell'OID è 1.3.76.11.1.1.3.1


 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio <i>Postecert Certificati Server</i>	Versione 3.5 Data 24/07/15

5.4 Certificato per web server

Il formato effettivo del certificato, e la valorizzazione degli attributi e delle estensioni, sarà deciso in base alle esigenze sistemistiche del Richiedente. La validità dei certificati per web server è di 1 (un) anno. Di seguito, a titolo esemplificativo, vengono riportate tre tipologie di profili per certificati web server emessi utilizzando il certificato di CA "Postecom CS3".


Profilo di un certificato per Microsoft IIS

Version	Versione 3
Serial Number	Numero di Serie del certificato
Signature	sha-256, RSA
Issuer	Country : "IT" State : "IT" Organization : "Postecom S.p.A." Organization Unit : "Servizi di Certificazione"
Validity	1 anno
Subject	Country : "IT" Organization : "Organisation" Organization Unit : "Unit name" COMMON NAME : "web server domain name"
SubjectPublicKeyInfo	chiave pubblica 2048 bit algoritmo utilizzato: RSA
Estensioni	
Authority Key Identifier	SHA-1 160bit
Subject Key Identifier	SHA-1 160bit
Subject Alternative Names	DNSNames
Extended Key usage	Server Authentication, Microsoft Server Gated
Certificate policies	OID della policy: 1.3.76.11.1.1.4.1 URL della policy: http://postecert.poste.it/manualioperativi/
crlDistributionPoint	http://postecert.poste.it/postecomcs3/crl.crl
Authority Information Access	Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://postecert.poste.it/ocsp

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio Postecert Certificati Server	Versione 3.5 Data 24/07/15

Profilo di un certificato per Iplanet Netscape Server

Version	Versione 3
Serial Number	Numero di Serie del certificato
Signature	sha-256, RSA
Issuer	Country : "IT" State : "IT" Organization : "Postecom S.p.A." Organization Unit : "Servizi di Certificazione"
Validity	1 anno
Subject	Country : "IT" Organization : "Organisation" Organization Unit : "Unit name" COMMON NAME : "web server domain name"
SubjectPublicKeyInfo	chiave pubblica 2048 bit algoritmo utilizzato: RSA
Estensioni	
Authority Key Identifier	SHA-1 160bit
Subject Key Identifier	SHA-1 160bit
Subject Alternative Names	DNSName
Key usage	Key Encipherment
Netscape Certificate Type	SSLServer
Certificate policies	OID della policy: 1.3.76.11.1.1.4.1 URL della policy: http://postecert.poste.it/manualioperativi/
crlDistributionPoint	http://postecert.poste.it/postecomcs3/crl.crl
Authority Information Access	Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://postecert.poste.it/ocsp

 GruppoPosteitaliane	Manuale Operativo	CPS_PCS_01
	Servizio Postecert Certificati Server	Versione 3.5 Data 24/07/15

Profilo di un certificato web server generico

Version	Versione 3
Serial Number	Numero di Serie del certificato
Signature	sha-256, RSA
Issuer	Country : "IT" State : "IT" Organization : "Postecom S.p.A." Organization Unit : "Servizi di Certificazione"
Validity	1 anno
Subject	Country : "IT" Organization : "Organisation" Organization Unit : "Unit name" COMMON NAME : "web server domain name"
SubjectPublicKeyInfo	chiave pubblica 2048 bit algoritmo utilizzato: RSA
Estensioni	
Authority Key Identifier	SHA-1 160bit
Subject Key Identifier	SHA-1 160bit
Subject Alternative Names	DNSName
Key usage	Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
Extended Key usage	Web server Authentication, Web Client Authentication
Certificate policies	OID della policy: 1.3.76.11.1.1.4.1 URL della policy: http://postecert.poste.it/manualioperativi/
crlDistributionPoint	http://postecert.poste.it/postecomcs3/crl.crl
Authority Information Access	Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://postecert.poste.it/ocsp