CAPITOLATO TECNICO

ACQUISIZIONE DI CERTIFICATI DIGITALI PER SSL SERVER E CODE SIGNING PER SOGEI

INDICE

1 PREMESSA

1.1 DEFINIZIONI

Nel corpo del documento, ai termini di cui appresso, viene attribuito il significato riportato a fianco di ciascuno di essi:

- CONSIP: la società che, in qualità di stazione appaltante, affida le attività oggetto del presente Capitolato;
- SOGEI: la Società Generale di Informatica S.p.A., beneficiaria del servizio;
- Capitolato tecnico: il presente documento che enuncia le specifiche tecniche alle quali dovrà conformarsi il servizio;
- Contratto: il contratto che verrà stipulato tra la SOGEI e l'impresa che enuncia le regole giuridiche alle quali si dovrà conformare il servizio;
- Fornitura: il complesso delle attività oggetto del presente Capitolato;
- Società: la società aggiudicataria del servizio;
- Responsabile delle attività contrattuali: la persona individuata dalla Società come interlocutore di Sogei e responsabile di tutte le attività contrattuali;
- Sistema Informativo: il sistema informativo della fiscalità con sede in Via Mario Carucci 99.

1.2 ACRONIMI

- **CA** Certificate Authority;
- **SSL** Secure Socket Layer;
- **CRL** Certificate Revocation List;
- **OID** Object Identifier;

1.3 RIFERIMENTI

[1] Baseline Requirements. Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates (v. 1.6.7); CAB Forum

[2] Baseline Requirements for the Issuance and Management of Code Signing Certificates (v. 1.2); CAB Forum

[3] RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List

(CRL) Profile; Internet Engineering Task Force

[4] RFC 8555 - Automatic Certificate Management Environment (ACME); Internet Engineering Task Force

2 REQUISITI DELL'AUTORITÀ DI CERTIFICAZIONE E MODALITÀ DI EROGAZIONE DEL SERVIZIO

I certificati SSL Server dovranno essere emessi da una CA rispondente ai requisiti specificati dal CAB Forum (vedi par. 1.3 punto [1]).

I certificati Code Signing dovranno essere emessi da una CA rispondente ai requisiti specificati dal CAB Forum (vedi paragrafo 1.3 punto [2]).

Le CA emittenti dovranno inoltre rispondere ai seguenti requisiti:

- presenza del certificato di CA tra le "Root Certification Authorities" preinstallate nelle seguenti applicazioni:
  - Apple: Mac OS X 10.6 e successivi, iOS 5.0;
  - Microsoft: Internet Explorer 8 e successivi, Windows Mobile 6 e successivi, Windows Phone 7 e successivi;
  - Mozilla Foundation: Firefox 38.5.0 ESR e successivi;
  - Opera: Opera 11 e successivi;
  - Sun: Java Runtime Environment (JRE) 6.0 e successive;
  - Android 3.0 e successivi;
- disponibilità costante delle liste di revoca aggiornate su internet alla URL indicata nell'estensione CRL Distribution Points presente nel certificato emesso;

Dovrà essere garantito l'adeguamento delle caratteristiche dei certificati richiesti all'evoluzione degli standard tecnici e della normativa applicabile. In relazione a quest'ultimo aspetto si chiarisce che si fa riferimento all'algoritmo con cui la CA firma i certificati emessi per le tipologie richieste. Ad esempio se durante il periodo di validità del contratto fosse emanata una legge nazionale o una direttiva europea che preveda che i certificati server SSL debbano essere firmati con RSA/SHA512, i certificati già emessi e firmati con RSA/SHA256 debbono poter essere sostituiti senza spese aggiuntive.

La Società dovrà emettere i certificati entro 4 ore lavorative dalla ricezione della richiesta di Sogei, pena l'applicazione delle penali di cui al successivo paragrafo 6.

3 OGGETTO DEL CAPITOLATO

Il presente Capitolato disciplina il servizio di registrazione ed emissione di certificati SSL Server e Code Signing presso una Certification Authority ufficiale, da utilizzare per l'emissione di certificati per i servizi esposti su reti pubbliche per un periodo massimo di **60 (sessanta) mesi** da erogarsi in favore della SOGEI, ivi comprese tutte le attività connesse allo svolgimento delle prestazioni medesime così come regolamentate, oltre che dal presente Capitolato, anche dallo Schema di contratto e dalle Condizioni Particolari di RdO, ed in particolare riguarda i servizi di:

- Registration Authority, finalizzati a verificare le richieste di certificati digitali da emettere
- Certification Authority, finalizzati all'emissione ed alla gestione di n. 1400 certificati digitali da utilizzare per server SSL o Code Signing.

I 1400 certificati digitali da emettere e gestire dovranno essere così ripartiti:

- n. 1398 per server SSL;
- n. 2 per Code Signing.

I certificati saranno utilizzati nell'ambito dei servizi gestiti da Sogei e ad essa intestati, ma potranno essere anche intestati a Pubbliche Amministrazioni clienti Sogei.

I certificati potranno essere richiesti, anche singolarmente, nel corso della validità stabilita per il contratto, secondo le esigenze espresse da Sogei e dalle Pubbliche Amministrazioni, fino al raggiungimento dei valori massimali sopra indicati.

Si evidenzia che il costo di un certificato SSL server con nomi DNS multipli non potrà essere superiore a quello di un certificato SSL server che presenti un singolo nome DNS moltiplicato per il numero di nomi DNS richiesti nel certificato. La riemissione di un certificato revocato che non modifichi la data di scadenza non comporterà ulteriori oneri.

3.1 CERTIFICATI SSL SERVER

I certificati SSL Server dovranno rispondere ai requisiti specificati al precedente paragrafo 1.3 punto [1] per i certificati "Organization Validated".
I Certificati SSL Server potranno contenere uno o più nomi DNS.
I Certificati SSL server dovranno avere validità annuale.
I certificati SSL server dovranno indicare nell'estensione Certificate Policies la rispondenza ai requisiti richiesti dal CAB Forum per i certificati "Organization Validated" presentando l'OID: {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baselinerequirements(2) organization-validated(2)} (2.23.140.1.2.2).

I Certificati SSL server dovranno presentare l'estensione CRL Distribution Points valorizzata con L'URL dove la CA pubblica le CRL.
I Certificati SSL server dovranno presentare l'estensione Extended Key Usage valorizzata con l'OID id-kp-serverAuth (vedi parafrafo 1.3 punto [3])
Il numero dei certificati richiesti (1398), indica la somma di certificati principali e SAN.
Nei certificati SSL sono compresi certificati con SAN; verranno richiesti certificati SSL server per un numero complessivo di nomi DNS pari a 1398, indipendentemente da come verranno "raggruppati" nei certificati. Al momento non è possibile stimare il numero di certificati con SAN previsti, né come saranno distribuiti per sottodomini.
Il numero N di SAN presenti in ogni singolo certificato richiesto lo stabilisce Sogei e può variare per ogni singolo certificato richiesto.
I certificati SSL server sono tutti della tipologia Organizzation Vetted (Autenticazione dell'Organizzazione).

3.2 CERTIFICATI CODE SIGNING

I certificati Code Signing dovranno poter essere utilizzati sia per la firma di codice java che di oggetti eseguibili per sistema operativo Microsoft e Apple.
I certificati Code Signing dovranno rispondere ai requisiti specificati dal CAB Forum (vedi paragrafo 1.3 punto [2]).
I certificati Code Signing dovranno avere validità triennale.
I certificati Code Signing dovranno indicare nell'estensione Certificate Policies la rispondenza ai requisiti richiesti dal CAB Forum presentando l'OID: {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) code-signing-requirements(4) code signing(1)} (2.23.140.1.4.1).

I certificati di tipologia Code Signing sono tutti della tipologia Organizzation Vetted (Autenticazione dell'Organizzazione).

3.3 SERVIZIO DI REGISTRATION AUTHORITY

Il servizio di Registration Authority dovrà essere garantito fino alla naturale scadenza dell'ultimo certificato richiesto nel corso del periodo della durata del contratto.
Tale servizio dovrà rispondere ai seguenti requisiti:

- possibilità di gestire il ciclo di vita completo dei certificati;
- accesso da Internet;
- autenticazione forte (si riferisce alla modalità di autenticazione da parte del personale Sogei verso il servizio che permetterà di gestire i certificati oggetto della fornitura. Tale affermazione significa che, ad esempio, non è accettabile un'autenticazione con username e password);

- possibilità emissione di certificati SSL Server per server appartenenti a domini DNS afferenti a clienti Sogei. Le modalità di verifica della titolarità dei domini DNS dovranno essere comunicate a Sogei entro 15 (quindici) giorni dalla data di stipula;
- disponibilità del servizio 23x7;
- intervallo tra la firma del contratto e l'attivazione del servizio non superiore ai 15 (quindici) giorni solari;
- interfaccia web che esponga almeno le seguenti funzionalità:
  - emissione e revoca dei certificati;
  - visualizzazione del numero di licenze disponibili;
  - ricerca e visualizzazione dei certificati emessi;
  - generazione di report esportabili;
- disponibilità di un'interfaccia rispondente alle specifiche di cui al precedente paragrafo 1.3 punto [4] che consenta l'automazione delle operazioni di gestione del ciclo di vita dei certificati.

3.4 VERIFICA DI CONFORMITÀ

Entro 15 (quindici) giorni decorrenti dalla data stipula, Sogei avvierà la verifica di conformità, volta a certificare che le prestazioni contrattuali siano eseguite a regola d'arte sotto il profilo tecnico-funzionale.

La Società è tenuta a prestare alla Sogei, a propria cura e spese, l'assistenza tecnica necessaria e a mettere a disposizione della Sogei quanto necessario alle operazioni di verifica di conformità.

La Società potrà intervenire alla verifica di conformità, anche attraverso propri rappresentanti. In tal caso detti rappresentanti sono tenuti a sottoscrivere i documenti di verifica di conformità che verranno redatti da Sogei (verbali, certificato, ecc.)

In caso di esito negativo della verifica di conformità, ferma restando l'applicazione delle penali, di cui al successivo paragrafo 6, la Società dovrà provvedere, a propria cura e spese, entro il termine che le verrà comunicato dalla Sogei, alla eliminazione dei difetti e/o delle carenze riscontrati entro il termine massimo di 5 giorni lavorativi, oppure di 3 giorni lavorativi se il malfunzionamento segnalato riguarda problemi di sicurezza del prodotto, ovvero una vulnerabilità tecnica.

Dopo la comunicazione, da parte della Società, dell'avvenuta eliminazione dei difetti e/o delle carenze, la Sogei procederà a nuova verifica di conformità nei termini e con le modalità di cui ai commi precedenti.

In caso di ulteriore esito negativo della verifica di conformità, la Sogei avrà facoltà di risolvere il contratto e di fare eseguire tutta o in parte la fornitura a terzi in danno della Società e fatto salvo in ogni caso il diritto al risarcimento di tutti i danni comunque subiti.
A completamento della verifica positiva sarà prodotto il "Verbale di conformità" che dovrà essere sottoscritto dal Responsabile della Fornitura e dal Responsabile Sogei.

4 GESTIONE DEL CONTRATTO

Il contratto avrà efficacia dalla data della sua stipula, per **60 (sessanta) mesi** e, comunque, sino al completo adempimento di tutte le obbligazioni contrattuali.

4.1 RESPONSABILE DELLE ATTIVITÀ CONTRATTUALI

La Società dovrà comunicare a Consip, trasmettendolo con la documentazione per la stipula, il nominativo del Responsabile del Servizio, nonché un numero di telefono e un indirizzo e-mail al quale indirizzare eventuali comunicazioni. La Società deve provvedere in piena autonomia al coordinamento e all'organizzazione delle attività nel rispetto delle specifiche e dei tempi forniti da Sogei.

Sarà compito del Responsabile curare la gestione amministrativa del contratto e delle attività legate alla fatturazione e verificare il rispetto di tutti gli adempimenti contrattuali.

4.2 ADEMPIMENTI PER LA SICUREZZA

La Società s'impegna a porre in essere quanto necessario a garantire l'esecuzione delle attività in piena aderenza con le disposizioni del D. Lgs. 81/2008 "Testo Unico sulla sicurezza durante il lavoro", cooperando e coordinandosi, in particolare, con i referenti della Committente e degli uffici dell'Amministrazione Finanziaria presso cui dovranno essere svolte le attività contrattuali, ai fini degli adempimenti di cui al comma 2 dell'art. 26 del citato decreto.

Si evidenzia che le attività di cui al presente capitolato rientrano nelle fattispecie di cui al comma 3-bis del suddetto articolo, per le quali non sussiste l'obbligo di redigere il DUVRI (Documento Unico di Valutazione dei Rischi da Interferenze).

4.3 MODALITÀ DI COMUNICAZIONE

La Società si impegna a comunicare a Consip, contestualmente alla presentazione della documentazione per la stipula, un numero di fax, un indirizzo e-mail, un indirizzo pec e un numero di telefono al quale rivolgersi, senza alcun limite sul numero di chiamate, per ogni comunicazione relativa alla fornitura.

Resta inteso che, per tutta la durata contrattuale, la Società dovrà garantire la piena funzionalità dei suddetti mezzi di comunicazione comunicando tempestivamente a Sogei eventuali modifiche.

4.4 LINGUA

Tutte le attività e la documentazione sarà in lingua italiana.

4.5 RISERVATEZZA

Tutte le informazioni trattate e tutti i documenti, anche parziali, scambiati tra la Società e Sogei sono riservati, pertanto è richiesta la massima attenzione per il loro utilizzo, in particolare se questo avviene al di fuori delle sedi Sogei.

La Società non potrà utilizzare, a nessun titolo, la documentazione ricevuta o prodotta, al di fuori delle attività oggetto del presente capitolato.

La Società non potrà utilizzare, a nessun titolo, la documentazione e i moduli software forniti da Sogei o realizzati per il servizio, al di fuori delle attività oggetto del presente capitolato.

5 MODALITA' DI CONSUNTIVAZIONE E FATTURAZIONE

La Società potrà consuntivare al termine di ciascun trimestre i certificati emessi nel periodo di riferimento. Il prospetto trimestrale riassuntivo, approvato dal Responsabile Sogei, dovrà essere allegato alla fattura di riferimento.

La modalità di fatturazione è trimestrale posticipata e ciascuna fattura dovrà essere di importo pari al numero di certificati effettivamente emessi nel trimestre di riferimento e dovrà riportare i seguenti riferimenti:

- Numero di repertorio
- CIG.

6 PENALI

Sogei applicherà le penali, secondo le modalità previste in contratto, nei seguenti casi:

- in caso di esito negativo della verifica di conformità di cui al paragrafo 3.4, si applicherà una penale pari all'1‰ (uno per mille) dell'importo contrattuale, per ogni giorno intercorrente tra la data del verbale negativo e quello positivo.
- in caso di ritardo rispetto ai tempi emissione del certificato di cui al precedente paragrafo 2, si applicherà una penale pari all'1‰ (uno per mille) dell'importo contrattuale, per ogni ora di ritardo successivo a quello indicato.

Nell'ipotesi in cui l'importo delle penali applicabili superi l'ammontare del 10% (diecipercento) dell'importo contrattuale complessivo, la Sogei avrà il diritto di risolvere, totalmente o parzialmente, il contratto in danno della Società, salvo il diritto dell'eventuale maggior danno.

7 ULTERIORI SPECIFICHE

Si evidenzia quanto segue:

- in relazione alla possibilità di intestare un unico servizio di gestione dei certificati a Sogei come Registration Authority, non è possibile dichiarare un legame "societario" tra Sogei e gli enti clienti;

- non è ammessa una configurazione che preveda diversi ambienti di gestione dei certificati (diversi servizi di Registration Authority) per i diversi clienti di SOGEI;

- non è ammessa la disponibilità di un contatto organizzativo dell'Ente cliente per poter procedere alla nomina di Registration Authority;

- non deve essere prevista nessuna limitazione all'installazione di un certificato su più server.