Capitolato tecnico della manifestazione di interesse: servizio triennale di firma digitale remota mobile e della marcatura temporale di Telecom Italia Trust Technologies presso l'Università degli Studi di Genova

1 Quadro generale di riferimento

1.1 Il Contesto

Ricordando che:

- **la Firma Elettronica Qualificata** è un particolare tipo di Firma Elettronica Avanzata basata su un certificato qualificato emesso da un Certificatore Accreditato e basata sull'utilizzo di un dispositivo sicuro per la creazione della firma.
- la **Firma Remota** è una particolare procedura di Firma Elettronica Qualificata, o di Firma Digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse

secondo la normativa in vigore, la firma digitale è una firma elettronica che possieda **tutti i requisiti seguenti**:

a) basata su un certificato qualificato;
b) generata mediante un dispositivo sicuro per la creazione di una firma;
c) basata sulla crittografia asimmetrica a chiave pubblica e a chiave privata.

In particolare la forma remota mobile consente di non avere dispositivi da collegare ad un computer, ma di usare il proprio cellulare/smartphone, indipendentemente dal provider usato.

1.2 Quadro normativo di riferimento

Le norme ad oggi in vigore, su cui si fonda la regolamentazione normativa della firma digitale, sono elencate nella tabella sottostante che riporta anche una breve descrizione dei contenuti e dei punti rilevanti della norma stessa.

Norma
Legge 15 marzo 1997, n. 59 (G.U. del 17 marzo 1997, n. 63), "Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della PA e per la semplificazione amministrativa"
D. Lgs. del 7 marzo 2005, n. 82 (G.U. del 16 maggio 2005, n. 93), "Codice dell'amministrazione digitale (CAD)" e successive modifiche
DPCM 30 MARZO 2009 *"Regole Tecniche in materia di generazione, apposizione e verifica delle firma digitali e validazione temporale dei documenti informatici."* (G.U. del 6 giugno 2009, n. 129)

Tale quadro normativo è completato dalla documentazione prodotta dall'ente di vigilanza (Circolari, Raccomandazioni e Norme Integrative emesse da DigitPA/Agid)

2 Descrizione del servizio

Il servizio richiesto è il servizio, fornito da Telecom Italia Trust Technologies srl, di Firma Digitale, nella declinazione di Firma Remota Mobile che permette di apporre firme digitali utilizzando il proprio telefono cellulare. **Il sistema remoto** garantisce al titolare della firma che l'operazione sia effettuata in modalità sicura e con un'autenticazione forte. Il telefono cellulare dell'utilizzatore occorre per effettuare le operazioni seguenti:

- **autenticazione forte dell'utente (strong authentication);**
- **autorizzazione diretta della firma da parte dell'utente.**

Un apposito **HSM** (hardware security module) custodisce in maniera sicura i certificati digitali e le chiavi private dei clienti.

Agli utenti viene fornito un certificato di firma digitale mediante un preventivo processo di registrazione. Tale operazione di identificazione è effettuato dagli incaricati di Trust Telecom presso l'Università degli Studi di Genova, che hanno quindi la responsabilità dell'identificazione di chi richiede un certificato digitale e della corretta registrazione dei dati.

Tra le informazioni acquisite in fase di attivazione del servizio, è compresa **l'associazione tra utente e numero di telefono cellulare.**

Durante la registrazione viene comunicato al cliente il suo PIN personale ed un codice segreto per la sospensione cautelativa del proprio certificato in caso di emergenza.

Il servizio consente di soddisfare i seguenti requisiti:

- **Identificazione certa ed autenticazione sicura del titolare remoto**: l'autenticazione avviene tramite telefonata ad un sistema (numero verde) che riconosce il CLI (caller ID) da cui proviene la chiamata.
- **Associazione univoca dell'operazione di firma con uno specifico documento:** la chiamata allo specifico numero di Rete Intelligente e la digitazione del codice OTP fornito dal sistema di autenticazione consentono di associare univocamente e temporaneamente la chiamata all'operazione di firma di "quel" documento.
- **Controllo "esclusivo" dell'operazione di firma da parte del titolare:** l'associazione dei passi precedenti alla protezione mediante PIN personale permette di apporre la firma digitale allo specifico documento in sicurezza.

Il servizio di rilascio dei certificati è un sistema applicativo web in modalità Saas, fornito con il servizio di firma digitale remota mobile di Telecom Italia Trust Technologies, chiamato sistema di provisioning.

Dimensionamento del servizio

Oggi i certificati :

- attivi presso l'Università di Genova sono 2.000;
- disponibili ma non ancora attivati sono 300.

La previsione nel prossimo triennio è pari a un incremento annuale di circa 200 certificati rilasciati.

Per quanto riguarda i certificati di firma attivi e non scaduti Unige richiede il mantenimento del servizio fino alla loro scadenza naturale e al rinnovo.

Poiché la normativa vigente non prevede la certificazione di chiavi che siano state già certificate, pertanto allo scadere del periodo di validità del certificato è necessaria la sostituzione delle chiavi con nuove coppie di chiavi e quindi l'emissione di un nuovo certificato. La sostituzione delle chiavi si svolge in modo analogo alla prima emissione. In particolare, se i dati utilizzati per l'emissione del certificato e per le comunicazioni con il titolare non sono variati, non è necessario né effettuare una nuova registrazione né produrre una nuova documentazione di accompagnamento. L'emissione del nuovo certificato è richiesto normalmente dal titolare.

Il rinnovo del certificato, e quindi la sostituzione delle chiavi scadute, deve essere richiesto con un anticipo di almeno 30 giorni rispetto alla scadenza del periodo di validità del certificato. Nel servizio in oggetto sono comprese la sospensione e la revoca del certificato di firma digitale richieste da Unige e/o dal titolare del certificato.

Rispetto alla gestione attuale, l'Università di Genova richiederà, compreso nel servizio senza oneri aggiuntivi, l'uso delle "buste virtuali" con i codici segreti per l'utilizzo del servizio, questa innovazione semplificherà la gestione della distribuzione dei codici segreti.

Infine nel servizio complessivo della firma digitale dovrà essere compreso il servizio automatizzato di firma digitale "massiva" per sottoscrivere in tempi brevi grandi quantità di documenti elettronici, tramite procedure applicative: modelli CUD, cedolini, cartellini, fatture elettroniche,….In particolare dovrà essere garantita la firma massiva per almeno 50 documenti elettronici da firmare alla volta.

2.1 Servizio di Time Stamping (marcatura temporale)

La marca temporale è un importante strumento che assegna data ed ora certa ad un documento informatico.

Il servizio prevede che il soggetto che desidera una marca temporale trasmetta a Trust Technologies l'impronta dell'oggetto che intende marcare.

Il server di marcatura temporale aggiunge all'impronta l'informazione relativa alla data ed ora dell'istante in cui elabora la richiesta (per legge l'evasione del risultato non deve eccedere il minuto), quindi calcola su tale insieme di informazioni una firma digitale con una propria chiave di marcatura temporale dedicata.

Il server restituisce la marca temporale, che consiste nell'impronta originale, nell'informazione su data ed ora, nella firma digitale appena calcolata.

Il soggetto allega la marca temporale al documento. Poiché la marca contiene una firma digitale di un'autorità esterna e contiene altresì l'impronta del documento, non sarà più possibile negare l'esistenza del documento in tale data ed ora.

Dimensionamento del servizio

La previsione nel prossimo triennio di uso di marche temporali, oggetto della presente fornitura, è stimato per un numero complessivo di circa 80000 marche sul triennio.

2.2 Servizi accessori: integrazione con altri servizi

Il servizio di firma digitale potrebbe essere integrato con altri servizi, quali a titolo esemplificativo:

- la **Posta Elettronica Certificata (PEC)**;
- **lo sviluppo di eventuali interfacce software** necessarie all'integrazione automatizzata di applicativi esterni con il servizio, al momento né funzionanti, né censite.

2.3 Help Desk

I titolari del servizio devono potersi rivolgere ad un help desk in grado di risolvere problematiche di tipo tecnico. Il supporto deve essere erogato, infatti, da un team specialistico che aiuta il cliente in tutto il ciclo di vita del servizio, dai problemi che possono sorgere in fase di attivazione/configurazione del servizio fino ad interventi con carattere di urgenza quali, ad esempio, il ripristino del servizio oppure la sospensione cautelativa di un certificato.

L'Help Desk deve essere raggiungibile tramite il numero verde ed è erogato alle seguenti condizioni:

1. servizi di assistenza ai titolari: dal lunedì al sabato, dalle 8 alle 16.30, festivi esclusi;
2. servizi di segnalazione inconvenienti: 24 ore su 24, 7 giorni su 7;
3. servizi di sospensione cautelativa dei certificati: 24 ore su 24, 7 giorni su 7.

Le procedure di accesso ai servizi di assistenza tecnica prevedono l'identificazione del cliente mediante codici di riconoscimento e/o password. I tecnici provvederanno ad una prima analisi dell'anomalia segnalata (analisi di 1° livello), assegnando un grado di severità e un codice di priorità e all'apertura di uno specifico ticket. La mancata risoluzione del problema genererà l'intervento dell'assistenza di secondo livello.

Alla soluzione dell'anomalia il cliente verrà avvisato del ripristino completo del servizio e guidato nella verifica della funzionalità al fine di chiudere la segnalazione.

2.4 Caratterizzazione del servizio

2.4.1 Cosa comprende la fornitura

Nella fornitura del servizio sono compresi:

-la gestione completa dei servizi in oggetto per tutta la durata contrattuale, descritti in precedenza. Il fornitore avrà come riferimento per la formulazione dell'offerta le dimensioni di massima sopra esposti tenuto conto della situazione attuale e di una stima in base ai dati rilevati nell'arco del 2014.

-il servizio di Helpdesk sopracitato.

-le eventuali modifiche o migliorie delle componenti applicative in essere, che garantiscono l'interoperabilità con i sistemi informativi di CSITA, derivanti da variazioni nel funzionamento del servizio nella sua globalità oggetto della procedura, rispetto a quelle attualmente in uso presso Unige. Questo non dovrà indurre oneri economici per l'Amministrazione.

2.4.2 Esclusioni ed Opzioni

Nella fornitura del servizio è escluso qualunque servizio accessorio, elencati a titolo esemplificativo nel paragrafo 2.2.

2.4.3 Durata

Il servizio richiesto dovrà avere una durata triennale.