POR CAMPANIA FESR 2007/2013 - Asse 5 - Obiettivo Operativo 5.1(Settore 02 Sistemi Informativi)- Progetto "Misurare e Conoscere per Governare"

CUP *H59C09000110002*
CIG 6274403925

GARA IN ECONOMIA PER L'AFFIDAMENTO DELLA FORNITURA
"INFRASTRUTTURA HW E SW PER IMPLEMENTAZIONE PROCESSO DI APPOSIZIONE FIRMA DIGITALE"
espletata utilizzando lo strumento di acquisto e di negoziazione telematico MePA
con predisposizione di RdO

DESCRIZIONE

1. OBIETTIVO

La Provincia di Salerno si pone l'obiettivo di implementare, all'interno del ciclo documentale in uso, un sistema di firma digitale sui tutti i documenti trattati da parte degli utilizzatori.

L'operatività della firma deve essere implementata a minimo rispetto al parco applicativo già istallato con la possibilità di poter realizzare i seguenti casi d'uso.

a. Firma digitale alla propria postazione

Il documento/i deve/devono essere firmato/i dal personale alla propria postazione client desktop con SO Windows. Il client di firma deve consentire la scelta se operare con firma locale (su smartcard o su USB token) o con firma remota.

b. Firma digitale in mobilità su tablet o smartphone

Il documento/i deve essere firmato dal personale in mobilità mediante dispositivi mobili come tablet e smartphone iOS/Android. L'operatività dell'utente finale deve essere guidata da wizard che vengono attivati in automatico dagli applicativi che possono essere residenti sullo stesso tablet/smartphone o su PC.

c. "Self-Service" enrollment e gestione dell'identità digitale locale e remota

L'utente deve essere in grado di gestire in autonomia le proprie identità digitali (coppie chiavi-certificati) a

2. OGGETTO DELLA FORNITURA

La Provincia desidera acquisire un'infrastruttura HW e SW da gestire autonomamente in house presso il proprio CED che implementa quanto in obiettivo.

In particolare nella fornitura sono richieste:

A. Nr. 2 appliance di rete specializzate per i processi di firma digitale e marcatura temporale con le seguenti caratteristiche funzionali:

- Firma *a Batch*, Firma automatica e massiva di documenti utilizzando identità digitali detenute centralmente dall'organizzazione a livello di reparto o di dipartimento/divisione. Le chiavi di firma possono essere tenuti in un HSM sicuro o in file software crittografate e mantenute in sicurezza nel database interno o esterno all'appliance.
- *Virtual smartcard*, Questa è la firma remota dei documenti da parte di utenti le cui chiavi di firma uniche sono tenute/gestite sull'appliance.
- Funzionamento in cluster ALTA AFFIDABILITA'
- Console amministrativa WEB
- Nr. 4 interfacce di rete alta velocità
- Interfaccia di servizio/utilizzo via web service
- Capacità di creare firme digitali secondo normativa vigente nei formati CADES, PADES
- Capacità di creare Marche temporali secondo normativa vigente
- Capacità di operare contemporaneamente con Identità digitali rilasciate da CA Qualificate iscritte all'albo AGID (ex DigitPA) e con Identità Digitali rilasciate da CA Interna per FEA.
- Implementazione di protocollo sicuro per operare con client sia in ambiente PC sia in ambiente Mobile

B. Nr. 240 licenze di SW client per l'emissione di firme digitali e marche temporali secondo i casi d'uso in Obiettivo. In particolare il software deve:

- essere installabile su postazioni utente desktop (dotate di sistema operativo Windows) o su dispositivi mobili iOS/Android.
- costituire la componente con cui l'utente finale si interfaccia direttamente nel corso dell'operazione di firma digitale. Si deve caratterizzare per essere un componente realizzato con tecnologie che garantiscono l'indipendenza dal browser utilizzato (devono essere supportati simultaneamente Internet Explorer, Firefox e Chrome) e soprattutto dalla Java Virtual Machine (JVM). Tale modulo deve costantemente essere attivo in background sulla postazione utente finché non viene intercettato, poiché scatenato dalle applicazioni di terze parti già presenti in azienda, un "intento" di autenticazione o di firma. A tal punto il modulo client deve presentare all'utente la propria interfaccia per permettere l'operazione di firma.
- consentire la visualizzazione del documento da firmare e del documento una volta firmato. I livelli di sicurezza raggiunti in questo modo sono decisamente elevati, semplificando al tempo stesso, la cosidetta *user experience*, dato che il processo di autenticazione risulta facile e veloce, sempre uguale indipendentemente dall'applicazione esterna a cui ci si sta collegando.
- permettere di autorizzare l'utilizzo delle Identità digitali solo a determinati gruppi di applicazioni.

C. Nr. 1 Sistema di *Identity Management* per la gestione in Self-Service da parte dell'utente finale da PC e da Mobile delle proprie Identità digitali locali o remote. Il Sistema deve garantire anche la prima emissione e la relativa associazione/registrazione dei dispositivi mobili utilizzati. In particolare, il sistema deve garantire in self-service le seguenti operazioni:

- generazione
- sospensione
- revoca
- abilitazione ai servizi (firma elettronica avanzata/digitale, autenticazione alle applicazioni, single sign-on, eventuali ulteriori aggiunti in successive estensioni del progetto)

D. Nr. 40 Certificati di firma digitale a validità legale.

E. Nr. 10 gg di Servizi professionali per la installazione, configurazione, formazione e tutto quanto necessario alla messa in esercizio dell'infrastruttura.

3. CARATTERISTICHE TECNICHE

Di seguito sono specificate le caratteristiche tecniche minime richieste per le componenti sopra elencate:

A. Appliance di rete specializzate per i processi di firma digitale e marcatura temporale

CPU	Intel Core2Duo E7400 / 2.8 GHz (1066 MHz) 2M/1M L2 Cache
RAM	2 x 240-pin DDR III 1066 DIMM Sockets, up to 4GB Non-ŒŒECC DDR3 SDRAMmemory max. 4GB
Chipset	Intel G41 and ICH7R
HSM	High performance Hardware Secure Module validated for FIPS 140-2 Level 3 and Common Criteria EAL4+
LAN Bypass	4
Velocità	10/100/1000
LAN Chip	10/100/1000 LAN 4
LCD display	2 X 16 Characters
Indicatori	HDD access/Power/LAN status/Bypass status
Alimentazione	200W ATX Power Supply
Form Factor	1U
Certificationi	CE/FCC Class A/UL

Formati e standard supportati: PDF – PadES – CadES – XadES - PKCS#7 - PKCS#1 -S/MIME

B. SW Client

Deve supportare i seguenti standard, funzionalità e piattaforme

- ETSI standards (CAdES, PAdES, XAdES)
- Countersignature: un firmatario convalida la firma emessa precedentemente da un altro firmatario.
- Parallel signature: un firmatario aggiunge la firma a un documento firmato da un altro a firmatario.
- File Destruction: un document viene distrutto senza possibilità di *recovery*
- Verification of a signature: verifica della firma e della marca con CRL e con OCSP
- Timestamping: marcatura temporale

- Windows 7/8
- Mac OS X 10.7.x or later
- Linux
- IOS
- Android

- Certificate profiles: X.509, ETSI TS 101 862 V1.3.2
- Signature Formats: XAdES (ETSI TS 101 903 V1.3.2), CAdES (ETSI TS 101 733 V1.7.4), PAdES (ETSI TS 102 778-1 V1.1.1, TS 102 778-2 V1.2.1, TS 102 778-3 V1.1.1, TS 102 778-4 V1.1.1, TS 102 778-5 V1.1.1)
- Hashing Alghoritms :SHA-256, SHA-1
- Keylenght: 2048/1024
- Verification: CRL, OCSP
- Encryption Alghoritms: AES-256, 3-DES
- Encoding: ASN.1-DER (ISO 8824, 8825), BASE64 (RFC 1421)
- Time stamped data: RFC 5544

C. Sistema per la gestione delle identità locali e remote in modalità self-service

Tale componente deve consentire di avere a disposizione un'infrastruttura PKI senza l'onere della complessità tipica di questi sistemi.
Inoltre deve permettere tramite un'interfaccia disponibile su browser web di gestire tutte le identità digitali emesse sia dal componente CA che da una CA esterna connessa, tra quelle iscritte all'albo AGID.
Il sistema di Identity Management offerto deve comprendere un sistema di Card e Key Management System.
Deve occuparsi della gestione centralizzata dei certificati, dei dispositivi, delle identità a supporto dell'organizzazione.

La Certification Authority, C.A., di riferimento deve essere interna e, come detto, esterna come ad esempio un ente certificatore accreditato DigitPA (Agenda Digitale).
Il sistema deve consentire la gestione completa del ciclo di vita dei certificati (creazione, revoca, rinnovo...), delle anagrafiche correlate, di uffici di emissione, degli operatori ed amministratori, garantendo funzioni di organizzazione degli operatori in gruppi/sottogruppi o meglio unità organizzative.

Il singolo dipartimento/gruppo deve quindi avere un proprio ufficio con funzionalità e viste dedicate, a cui accede tramite semplice browser, ad esempio di immissione dati anagrafici.
Nello specifico il sistema deve fornire:

- Funzionalità completa per la gestione delle identità, con e senza smart card, PKCS#12, e più in generale dei certificati; emissione/sospensione/riattivazione e revoca dei certificati X.509v3, inserimento, aggiornamento e rimozione dei dati anagrafici
- End-user self-service
- Self-service 'wizard' che supporta gli utenti attraverso le più comuni funzioni: cambio/sblocco ID, recupero nuovi applet/credenziali, richiesta di sostituzione del certificato, etc.
- Supporto di qualsiasi Autorità di Certificazione in grado di fornire Credential Provider Interface API, comprese le CA riconosciute da AgiD.
- Permettere la gestione centralizzata di uffici di emissione distribuiti sul territorio

Relativamente alle funzionalità di Card e Key Management deve garantire:

- Registrazione
- Produzione
- Life-cycle management
- Azione : creazione/distribuzione/sospensione/riattivazione/revoca/rinnovo
- Modalità : Batch / Face to Face / Self service
- User Profile Management
- Certificate Profile Management
- Personalizzazione grafica (Graphical Customisation)
- Gestione dei profili (Profile Management)
- Generazione ed import dei codici segreti
- Gestione dei documenti accessori alle attività di registrazione

Per ciò che attiene agli aspetti di compatibilità con i sistemi in uso si richiama la sottostante lista con cui deve essere possibile nativamente interagire:

- Sistemi Operativi amministratore/utente: Microsoft Windows 2000/XP/Vista/7/8
- Web server: Microsoft Internet Information Services, Twisted, Apache
- Database: Microsoft SQL Server , Oracle®, Postgres SQL, MySQL
- Microsoft Windows Server 2003 Active Directory
- Autorità di certificazione (PKI): Cybertrust UniCERT™, Entrust® Authority™, Microsoft Windows Server 2003 Certificate Services, VeriSign® Managed PKI, smartSec CA
- Web browsers: Microsoft Windows Internet Explorer, Mozilla/Firefox

- Smart cards e USB token: Gemalto (Axalto), Gemalto (Gemplus), Giesecke & Devrient, Oberthur Card Systems ID-One™ Cosmo, ST Incard, BIT4ID smartToken
- Moduli di sicurezza hardware: nCipher™ netHSM, smartSEC HSM/SC
- Stampanti di smart card: Datacard® ImageCard IV, Magna, Select 2 (Datacard® IDWorks® license required), DIGITALID EDI/SECURE, evolis, DNP
- Lettori di smart card: Gemalto® (Gemplus®) GemPC™, OmniKey® CardMan™, SCM Microsystems® SCR, BIT4ID miniLector

Il sistema deve offrire il supporto ai seguenti standard:

- LDAPv3
- SSL, TSL
- PKCS#7, #10, #11, #12
- ISO 7816
- Global Platform
- Java Card