ALLEGATO A

CAPITOLATO TECNICO E RELATIVE APPENDICI

CAPITOLATO TECNICO

Lotto 2

PROCEDURA RISTRETTA PER L'AFFIDAMENTO DEI SERVIZI DI CLOUD COMPUTING, DI SICUREZZA, DI REALIZZAZIONE DI PORTALI E SERVIZI ONLINE E DI COOPERAZIONE APPLICATIVA PER LE PUBBLICHE AMMINISTRAZIONI (ID SIGEF 1403).

Realizzato da azienda con sistema di gestione per la qualità certificato ISO 9001:2008

1. PREMESSA

In questo capitolo si forniscono l'elenco e la descrizione dei servizi che costituiscono il Lotto 2 della presente procedura.

Il Lotto 2 della presente procedura comprende le seguenti tipologie di servizi:

- *servizi per la gestione delle identità digitali,* erogati in modalità "as a service", in conformità anche all'art. 64 del CAD;
- *servizio di firma digitale remota comprensiva della fornitura di certificati e servizio di timbro elettronico*, erogati in modalità "as a service", volti a favorire la dematerializzazione dei documenti e la digitalizzazione dei processi amministrativi;
- *servizi di sicurezza*, erogati sia in modalità "as a service" attraverso i Centri Servizi del Fornitore sia in modalità "on premise", atti a garantire la sicurezza applicativa e a supportare le Amministrazioni nella prevenzione e gestione degli incidenti informatici e nell'analisi delle vulnerabilità dei sistemi informativi; i servizi di sicurezza includono anche servizi professionali a supporto delle attività erogati presso i centri delle Pubbliche Amministrazioni.

Le modalità di attivazione ed erogazione dei servizi devono avvenire secondo quanto specificato al capitolo 7 del Capitolato Tecnico – Parte Generale.

Le scadenze temporali relative ai servizi offerti, laddove non espressamente specificate nel presente Capitolato Tecnico, saranno definite nei relativi Piani di Attuazione, come descritto nel Capitolato Tecnico - Parte Generale.

Sono da considerarsi parte integrante del presente Capitolato Tecnico le Appendici di seguito indicate:

Appendice 1: Indicatori di qualità della fornitura;

Appendice 2: Descrizione dei profili professionali;

Appendice 3: Servizi di monitoraggio.

1.1. Tipologia servizi L2.S1 – Servizi per la gestione delle identità digitali

Per una piena diffusione dei servizi telematici, sia nelle transazioni tra soggetti privati e imprese che nell'interazione tra le pubbliche amministrazioni ed i cittadini, un aspetto particolarmente critico è rappresentato da una corretta e sicura gestione delle identità digitali dei soggetti che si presentano in rete. L'importanza di questa tematica ha avuto giusto riconoscimento sul piano normativo dal DL 69 del 21/6/2013 che all'articolo 17-ter istituisce un sistema per la gestione delle identità digitali - denominato SPID - valido ai sensi di legge nell'ambito pubblico e privato.

I servizi di identità digitale hanno lo scopo di realizzare le componenti previste dal modello proposto dalle specifiche SAML, che rappresenta ormai lo standard de-facto, universalmente adottato dai vari operatori tecnologici di mercato, per la tematica relativa alla gestione delle identità digitali in rete. Lo scenario di riferimento parte dal profilo di *single sign-on* originariamente proposto dalle prime versioni di SAML per estenderlo ad un ambito di sistema, al fine di arrivare alla definizione di una vera e propria infrastruttura finalizzata alla gestione delle identità e degli attributi riferibili ai soggetti operanti in rete.

In questo contesto generale gli attori previsti sono i seguenti:

- i *titolari dell'identità digitale* identificati nei soggetti che accedono ai servizi telematici, erogati da un *fornitore di servizi*, fornendo la propria identità digitale;
- i *fornitori di servizi* rappresentati dai soggetti privati o dalle pubbliche amministrazioni che erogano servizi in rete per cui la cui fruizione è richiesta l'identificazione e l'autenticazione degli utenti;
- i *gestori dell'identità digitale* costituiti dalle persone giuridiche che creano, rendono disponibili e gestiscono gli attributi necessari al fine di dimostrare l'identità digitale dei soggetti operanti in rete;
- i *gestori di attributi qualificati* rappresentati dagli enti aventi per legge l'obbligo di certificare il possesso e la validità di attributi qualificati, abilitazioni professionali, poteri di rappresentanza o altri attributi dei soggetti operanti in rete.

Le relazioni tra i suddetti attori si evidenziano nelle interazioni necessarie al completamento delle attività che, a partire da una richiesta avanzata da un soggetto titolare di un identità digitale, portano alla autorizzazione o al diniego alla fruizione di

un servizio telematico, messo a disposizione da un fornitore di servizi. Tali interazioni portano alla produzione di certificazioni da parte di alcune entità e l'utilizzo delle stesse da parte di altre.

La figura riportata nella pagina seguente illustra i passi previsti:

1. il soggetto *titolare dell'identità digitale* richiede l'accesso ad un servizio collegandosi telematicamente al sito o al portale del *fornitore dei servizi*;

2. il *fornitore dei servizi* rimanda il soggetto *titolare dell'identità digitale* presso il proprio *gestore dell'identità digitale*;

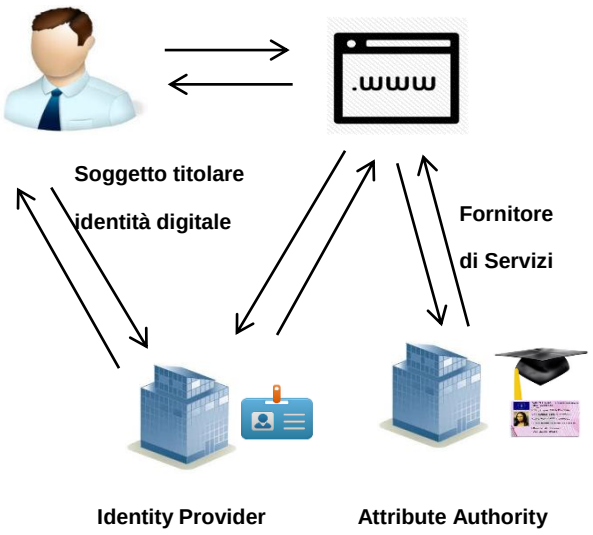
3. *il gestore dell'identità digitale* verifica l'identità del soggetto sulla base di credenziali da lui accettate ed esibite dal soggetto. Se la verifica ha esito positivo viene emessa a favore dell'erogatore del servizio una certificazione (asserzione di autenticazione SAML) di autenticazione e rimanda il soggetto presso il *fornitore dei servizi*;

4. il *fornitore dei servizi* pur avendo adesso contezza dell'identità dell'utente può avere la necessità di verificare ulteriori attributi qualificati eventualmente presenti nel profilo utente e richiesti dalle policy di sicurezza che regolano l'accesso al servizio. In questo caso:

5. individuati i *gestori di attributi qualificati* in grado di attestare la validità degli attributi necessari inoltra agli stessi un richiesta di attestazione degli stessi presentando i riferimenti dell'identità digitale per la quale si richiede la verifica:

6. il risultato della richiesta è l'emissione di una certificazione (asserzione di attributo SAML) emessa a favore del *fornitore dei servizi*;

7. Il *fornitore dei servizi* raccolte tutte le certificazioni (asserzioni SAML) di identità e di attributi qualificati presenti nel profilo necessarie per l'applicazione delle policy di sicurezza relative al profilo utente del soggetto che richiede l'erogazione può verificarne la sussistenza e decidere se soddisfare o rigettare la richiesta di servizio avanzata.



Il modello proposto, come già detto, è basato sullo standard SAML v 2.0 sia per il formato delle certificazioni (nella nomenclatura SAML asserzioni nelle due varianti di *asserzione di autenticazione* e *asserzione di attributo*) sia per i protocolli sottesi alle interazioni previste (SAML *binding*).

I servizi di identità digitali previsti dal presente capitolato sono quelli che realizzano le entità necessarie a realizzare tutte le entità previste dal modello e sono i seguenti:

- "Identity Provider"
- "Identity & Access management"

Nei paragrafi seguenti relativi ai suddetti servizi, si descrivono i requisiti dei servizi in oggetto e i relativi parametri di dimensionamento, da considerarsi minimi.

1.1.1. Servizio L2.S1.1 - Identity provider

Descrizione del servizio

Il servizio di "Identity Provider" prevede la messa a disposizione di un sistema tecnologico e amministrativo che realizzi complessivamente le funzionalità di *gestore dell'identità digitale*, garantendo la compatibilità con quanto previsto dall'articolo 17-ter del DL 69 del 21/6/2013 e successive norme attuative ed esecutive.

Il servizio dovrà prevedere due componenti:

- l'*autorità di registrazione* avente il compito di effettuare la registrazione dei soggetti per i quali il servizio gestisce l'identità digitale, l'associazione di questi a credenziali riconosciute e la gestione del ciclo di vita dell'identità creata;
- l'*autorità di autenticazione* avente il compito, a seguito di richieste provenienti da un *fornitore di servizi* o dall'utente stesso, di autenticare telematicamente i soggetti registrati verificandone le credenziali e rilasciando al richiedente una asserzione di autenticazione riportante gli attributi associati all'identità digitale.

Il servizio potrà gestire un numero di identità digitali non superiore a 12.000.000 (dodici milioni) ed è sostanzialmente concepito per agevolare la migrazione delle identità digitali attualmente già detenute da una amministrazione verso un identity provider esterno con il quale si è stabilita una relazione di fiducia (trust) nell'ottica della realizzazione di una gestione federata delle identità.

Requisiti del servizio

Il *servizio di "Identity provider"* deve soddisfare le seguenti specifiche:

1. Le identità digitali gestiti dal servizio dovranno essere rappresentate per mezzo di un insieme di attributi;

   1.1. Gli attributi che rappresentano le identità digitali sono classificati secondo le seguenti categorie:

      1.1.1. *Attributi Identificativi*: nome, cognome, luogo e data di nascita, sesso per le persone fisiche, ovvero ragione o denominazione sociale, sede legale per le persone giuridiche, nonché il codice fiscale e gli estremi del documento d'identità utilizzato ai fini dell'identificazione;

      1.1.2. *Attributi non Identificativi*: il numero di telefono, l'indirizzo di posta elettronica, il domicilio fisico e digitale, nonché eventuali altri *attributi* individuati dall'*AgID;*

1.1.3. *Attributi non qualificati*: le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi altro tipo di *attributo* attestato da un *gestore di attributi qualificati*;

1.2. Le identità digitali rilasciate all'utente contengono obbligatoriamente il codice identificativo, gli attributi identificativi e almeno un attributo secondario, funzionale alle comunicazioni tra il gestore dell'identità digitale e l'utente;

1.3. Le identità digitali possono contenere gli attributi qualificati e ulteriori attributi registrati su richiesta dell'utente nell'ambito delle categorie individuate dall'AgID. Gli attributi qualificati possono essere anche forniti direttamente dal gestore di attributi qualificati al fornitore di servizi su consenso dell'utente;

2. La componente di servizio autorità di registrazione dovrà gestire il ciclo di vita delle identità Digitali;

2.1. La componente di servizio *autorità di registrazione* dovrà gestire la registrazione dei soggetti per i quali il servizio gestisce l'identità digitale;

2.1.1. Il rilascio dell'identità digitale da parte del gestore del servizio deve avvenire a seguito della verifica dell'identità personale del soggetto richiedente;

2.1.1.1. la verifica dell'identità personale deve avvenire in uno dei seguenti modi:

2.1.1.1.1. riconoscimento tramite esibizione a vista di un valido documento d'identità;

2.1.1.1.2. riconoscimento effettuato attraverso una sessione audio/video durante la quale l'identità del soggetto è verificata tramite il riscontro di un documento di riconoscimento in corso di validità, purché leggibile e munito di fotografia recente e riconoscibile del soggetto, firma autografa e timbro, rilasciato da un'Amministrazione dello Stato

2.1.1.1.2.1. l'incaricato del gestore ha la facoltà di rifiutare il riconoscimento a causa dell'inadeguatezza della qualità della sessione audio/video al fine del riconoscimento del soggetto o di dubbi sulla reale identità del soggetto.

2.1.1.1.2.2. durante la registrazione il soggetto dichiara la volontà di essere dotato dell'identità digitale.

2.1.1.1.2.3. la registrazione audio-video, da cui è individuabile l'incaricato del gestore che ha effettuato il riconoscimento, è conservata in forma protetta per la durata prevista al par. 2.1.1.4.

2.1.1.1.3. riconoscimento a distanza mediante autenticazione informatica tramite documenti digitali di identità, TS-CNS, CNS o carte ad essa conformi, validi ai sensi di legge;

2.1.1.1.4. mediante sottoscrizione di un apposito modulo di richiesta con firma elettronica qualificata o con firma digitale rilasciata a seguito di riconoscimento a vista del titolare;

2.1.1.2. il gestore del servizio dovrà conservare i dati utilizzati per la verifica dell'identità personale di ciascun utente a seconda dei casi sopra previsti. In particolare relativamente al punto 2.1.1.1.1, gli estremi e la copia per immagine del documento di riconoscimento, relativamente al punto 2.1.1.1.2 copia dei log di transazione e relativamente al punto 2.1.1.1.3, il modulo di adesione firmato digitalmente;

2.1.1.3. i dati personali raccolti per la verifica dell'identità personale sono trattati e conservati nel rispetto della normativa in materia di tutela dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.

2.1.1.4. i dati personali raccolti per la verifica dell'identità personale dovranno essere conservati per un periodo non inferiore ai venti anni decorrenti dalla scadenza, dalla disattivazione o dalla revoca dell'identità digitale. Il gestore del servizio dovrà quindi conservarli per tutta la durata contrattuale e trasmetterli alla scadenza del contratto all'Agenzia per l'Italia Digitale o a soggetto da lei indicato;

2.1.2. il gestore del servizio dovrà individuare nell'ambito della propria struttura organizzativa il responsabile delle attività di verifica dell'identità personale qui descritte;

2.1.3. Il gestore del servizio dovrà assicurare che, nei casi previsti dalla legge, l'Autorità giudiziaria ed il Garante per il trattamento dei dati personali possano conoscere, per il tramite del gestore del servizio stesso, l'identità personale dell'utente;

2.1.4. I gestori dell'identità digitale, ricevuta la richiesta di adesione, effettuano la verifica degli attributi identificativi del richiedente sulla base di documenti, dati o informazioni ottenibili da fonti affidabili e indipendenti, secondo i criteri e le modalità stabilite dall'Agenzia per l'Italia Digitale;

2.2. La componente di servizio *autorità di registrazione* dovrà gestire l'associazione dei soggetti per i quali il servizio gestisce l'identità digitale a credenziali riconosciute sia già in possesso del soggetto sia appositamente prodotte e rilasciate agli stessi;

2.2.1. le credenziali di autenticazione associate alle identità digitali registrate sono rilasciate dal gestore del servizio mediante consegna in modalità sicura.

2.2.2. Il servizio dovrà esser in grado di garantire per l'autenticazione i livelli di sicurezza (Level of Assurance) LoA2, LoA3 e LoA4 definiti dallo standard dello standard ISO/IEC DIS 29115. In particolare:

2.2.2.1. per il livello corrispondente al Level of Assurance LoA2 dello standard ISO/IEC DIS 29115, il servizio dovrà rendere

disponibili sistemi di autenticazione informatica a un fattore (password o parola chiave);

2.2.2.2. per il livello corrispondente al Level of Assurance LoA3 dello standard ISO/IEC DIS 29115, il servizio dovrà rendere disponibili sistemi di autenticazione informatica a due fattori, non basati necessariamente su certificati digitali le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo;

2.2.2.3. per il livello corrispondente al Level of Assurance LoA4 dello standard ISO/IEC DIS 29115, il servizio dovrà rendere disponibili sistemi di autenticazione informatica a due fattori basati su certificati digitali, le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo;

2.2.2.4. nel caso in cui i fornitori di servizi per i quali viene richiesta l'autenticazione siano pubbliche amministrazioni dovranno essere consentite solo i livelli di sicurezza LoA3 e LoA4.

2.3. La componente di servizio autorità di registrazione dovrà garantire il tempestivo aggiornamento delle Identità Digitali;

2.3.1. gli utenti sono obbligati a informare tempestivamente il gestore dell'identità digitale di ogni variazione degli attributi previamente comunicati. Quest'ultimo provvede tempestivamente ai necessari aggiornamenti, avendo verificato le informazioni fornite sulla base di documenti, dati o informazioni ottenibili da fonti affidabili e indipendenti, secondo i criteri e le modalità stabilite dall'Agenzia per l'Italia Digitale;

2.3.2. l'utente può chiedere al gestore dell'identità digitale, in qualsiasi momento la revoca della propria identità digitale ovvero la modifica delle proprie credenziali di accesso. A tali richieste il gestore dell'identità digitale provvede tempestivamente.

2.3.3. Il gestore dell'identità digitale revoca l'identità digitale se riscontra l'inattività della stessa per un periodo continuativo superiore a ventiquattro mesi o se viene a conoscenza del decesso della persona fisica o dell'estinzione della persona giuridica attivando opportune e documentate verifiche delle informazioni ricevute.

2.4. La componente di servizio *autorità di registrazione* dovrà garantire tempestivamente la revoca e il disconoscimento delle Identità Digitali;

2.4.1. Il soggetto titolare di una Identità digitale, nel caso in cui ritenga che la propria identità digitale sia stata utilizzata abusivamente o fraudolentemente da un terzo, può disconoscere la propria identità digitale inviando a mezzo posta elettronica, una dichiarazione di disconoscimento al gestore del servizio di identità digitale;

2.4.1.1. La dichiarazione di disconoscimento se non firmata digitalmente deve avere in allegato copia di un documento di riconoscimento in corso di validità.

2.4.1.2. il gestore dell'identità digitale sospende immediatamente l'identità digitale disconosciuta per un periodo massimo di trenta giorni.

2.4.1.3. Se nel predetto periodo di trenta giorni il gestore riceve dal soggetto titolare dell'Identità Digitale disconosciuta copia della denuncia penale presentata all'Autorità Giudiziaria per gli stessi fatti su cui è basata la dichiarazione di disconoscimento Identità digitale la medesima viene revocata

2.4.1.4. Se nel predetto periodo di trenta giorni il gestore non riceve dal soggetto titolare dell'Identità Digitale disconosciuta copia della denuncia penale presentata all'Autorità Giudiziaria per gli stessi fatti su cui è basata la dichiarazione di disconoscimento Identità digitale la medesima viene ripristinata;

2.5. Il soggetto titolare di una identità digitale può chiedere, attraverso i referenti delle Amministrazioni, al gestore del servizio di identità digitale di conoscere gratuitamente i propri dati personali, in conformità con la normativa vigente.

2.6. Il gestore del servizio di identità digitale, su richiesta dell'utente, gli segnala ogni avvenuto utilizzo delle credenziali di accesso, inviandone gli estremi ad uno degli attributi non identificativi a tale scopo indicato dall'utente stesso, secondo le regole tecniche definite con i regolamenti di cui all'articolo 4.

2.7. Il gestore del servizio di identità digitale dovrà prevedere, su richiesta, la presa in carico e la migrazione delle identità gestite dall'amministrazione, direttamente o tramite un terzo fornitore;

3. La componente di servizio *autorità di autenticazione* dovrà gestire le richieste di autenticazione provenienti da un fornitore di servizi o dall'utente stesso, verificando le credenziali presentate e rilasciando al richiedente una asserzione di autenticazione riportante gli attributi associati all'identità digitale.

3.1. Le interazioni dovranno essere conformi allo standard SAML v2.0 come descritto nelle specifiche OASIS:

[SAML-TechOv] OASIS Security Services (SAML) TC, Security Assertion Markup Language (SAML) V2.0 Technical Overview, Draft 3, 20 febbraio 2005.

https://www.oasis-open.org/committees/download.php/11511/sstc-saml-tech-overview-2.0-draft-03.pdf

[SAML-Core] OASIS Security Services (SAML) TC, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005

[SAML-Bindings] OASIS Security Services (SAML) TC, Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005

[SAML-Profile] OASIS Security Services (SAML) TC, Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005.

[SAML-Metadata]OASIS Security Services (SAML) TC, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005

[SAMLAuthContext]OASIS Security Services (SAML) TC, Authentication Context for The OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005.

3.2. La componente di servizio autorità di autenticazione dovrà essere in grado di realizzare il profilo SAML "Web Browser SSO" come specificato in ([SAML-TechOv] sez. 4.1) prevedendo le due versioni "SP-Initiated": "Redirect->POST binding" e "POST->POST binding" in cui il meccanismo di autenticazione è innescato dalla richiesta inoltrata dall'utente (tramite il suo User Agent) ad un fornitore di servizi, il quale a sua volta si rivolge all'autorità di autenticazione in modalità "pull".

3.3. La richiesta di autenticazione SAML (basata sul costrutto <AuthnRequest>) può essere inoltrata da un fornitore di servizi (Relying Party) all'autorità di autenticazione (servizio di Identity Provider) usando il binding HTTP Redirect o il binding HTTP POST.

3.4. La relativa risposta SAML (basata sul costrutto <Response>) sarà inviata dall'Identity Provider al Relying Party tramite il binding HTTP POST.

3.5. Deve essere garantito il supporto a tutti i formati ammessi dallo standard SAMLv2.0 di cui al 3.1 in merito alle asserzioni, alle richieste di <AuthnRequest> con relative risposte <Response> e del binding.

4. Obblighi del gestore del servizio di Identità Digitale:

4.1. definiscono e applicano le procedure e i metodi di gestione delle attività svolte;

4.2. utilizzano sistemi affidabili che garantiscono la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo o internazionale;

4.3. adottano adeguate misure contro la contraffazione, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle credenziali di accesso;

4.4. effettuano un monitoraggio continuo al fine rilevare usi impropri (a titolo esemplificativo e non esaustivo *brute force attack*, accessi a indirizzi IP differenti) o tentativi di violazione delle credenziali di accesso dell'identità digitale di ciascun utente, procedendo alla sospensione dell'identità digitale in caso di attività sospetta. In tal caso il fornitore potrà procedere alla revoca del certificato, sulla base di policy precedentemente concordate; effettuano, con cadenza almeno annuale, un'analisi dei rischi i cui risultati dovranno essere messi a disposizione di AgID e Consip entro 30 giorni dalla richiesta;

4.5. definiscono il piano per la sicurezza dei servizi di "Identity Provider", da trasmettere ad AgID entro 30 giorni dalla richiesta e ne garantiscono l'aggiornamento;

4.6. allineano le procedure di sicurezza agli standard internazionali, la cui conformità è certificata da un terzo abilitato;

4.7. conducono, con cadenza almeno semestrale, "Penetration Test", i cui risultati dovranno essere messi a disposizione di AgID e Consip entro 30 giorni dalla richiesta;

4.8. effettuano ininterrottamente l'attività di monitoraggio della sicurezza dei sistemi, garantendo la gestione degli incidenti da parte di un'apposita struttura interna;

4.9. garantiscono la gestione sicura delle componenti riservate delle identità digitali degli utenti, assicurando che le stesse non siano rese disponibili a terzi, ivi compresi i fornitori di servizi stessi, neppure in forma cifrata.

Tipologia del servizio

Il servizio sarà erogato in modalità "as a service"; l'aggiudicatario predisporrà un sistema che realizza le funzionalità di gestore dell'identità digitale, a servizio di tutte le amministrazioni contraenti.

Parametri di valutazione economica

La modalità di remunerazione del servizio "Identity Provider" è: a canone.

Ai fini della valutazione economica del servizio "Identity Provider" deve essere presentata una quotazione – canone annuale per identità - per ciascuna delle seguenti fasce, definite in base al numero di identità digitali gestite:

- *Fascia 1:* fino a 1.000 identità gestite
- *Fascia 2:* da 1.001 a 10.000 identità gestite
- *Fascia 3:* oltre 10.000 identità gestite

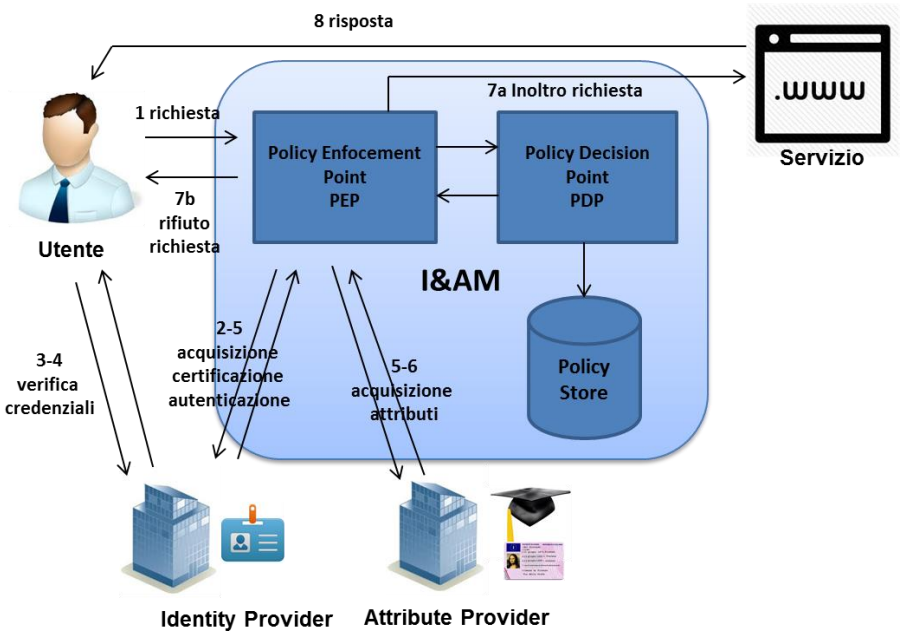
L'ordine di acquisto del servizio deve avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

1.1.2. Servizio L2.S1.2 - Identity & Access Management (I&AM)

Descrizione del servizio

Il servizio di "Identity & Access management" ha come finalità la completa gestione delle attività di identificazione, autenticazione ed autorizzazione propedeutiche all'accesso da parte di utenti esterni al portale dell'Amministrazione o ai servizi da essa erogati in rete. Il servizio dovrà essere condotto con modalità conformi ai requisiti di sicurezza richiesti dalle normative vigenti (si veda il Capitolato Tecnico - Parte Generale), e garantire la compatibilità con quanto previsto dall'articolo 17-ter del DL 69 del 21/6/2013.

Il servizio dovrà mettere a disposizione dell'amministrazione una componente tecnologica che frapponendosi tra l'utente esterno e le risorse disponibili - siano esse pagine web o servizi telematici - gestisca le richieste operando gli opportuni passi necessari all'autenticazione ed all'autorizzazione all'accesso; a seguito degli accertamenti operati, la richiesta sarà poi inoltrata dal sistema verso la risorsa richiesta o rigettata.



Secondo il classico modello logico il sistema dovrà prevedere due sottosistemi. Un componente, che espleta le funzionalità di *Policy Enforcement Point,* che si interfaccia con il mondo esterno comunicando con gli utenti e le entità di certificazione (*Identity Provider* e *Attribute Authority*) al fine di ricevere le richieste e collezionare tutte le certificazioni necessarie per l'applicazione delle policy di sicurezza associate alle risorse. Un secondo componente, con funzionalità di *Policy Decision Point,* in grado di accedere ai profili degli utenti e alle policy di sicurezza associate alle risorse e che, sulla base di questi e delle informazioni raccolte dal *Policy Enforcement Point,* verifica la legittimità della richiesta. Lo scambio di certificazioni tra il sistema e le entità esterne deve essere basato sullo standard OASIS Saml v2.0.

Oltre alla messa a disposizione della piattaforma di run-time in grado di operare come sopra il servizio dovrà provvedere a tutte le attività amministrative legate alla gestione del ciclo di vita dei profili utente e delle policy di accesso relative alle risorse controllate, interagendo con i responsabili delle amministrazioni.

Requisiti del servizio

Il *servizio di "Identity & Access Management"* deve soddisfare le seguenti specifiche:

1. Il servizio di I&AM dovrà consistere nella gestione delle attività di identificazione, autenticazione ed autorizzazione all'accesso ai portali delle

Amministrazione e alla fruizione dei servizi da esse erogati ai propri utenti esterni;

1.1. per l'autenticazione dei propri utenti il servizio potrà fare ricorso ad un Identity provider esterno all'Amministrazione;

1.1.1. l'utente esterno dovrà scegliere il proprio identity provider in grado di autenticarlo tra quelli presenti in una lista proposta dal sistema I&AM;

1.2. per la verifica degli attributi associati al profilo di un utente, non certificabili dalla stessa amministrazione contraente, il servizio dovrà fare ricorso ad Attribute Authority esterne;

1.2.1. l'individuazione dell'Attribute Authority dovrà essere fatta dal sistema in base al tipo di attributo referenziato nel profilo utente sulla base di lista di entità conosciute;

1.3. le fonti delle informazioni relative agli Identity Provider e alle Attribute Authority esterne da utilizzare per gli scopi specificati ai punti 1.1 e 1.2 sono indicate dall'amministrazione;

1.3.1. l'accesso alle suddette fonti potrà avvenire anche telematicamente secondo protocolli standard;

1.4. identificato l'utente e validato il suo profilo per mezzo delle attestazioni di autenticazione e di attributo acquisite secondo le modalità specificate ai punti 1.1 e 1.2, il sistema I&AM dovrà gestire le operazioni necessarie per la verifica dei diritti di accesso alle risorse richieste, sulla base delle policy di sicurezza a queste associate;

1.5. Le interazioni di cui ai punti precedente dovranno essere conformi allo standard SAML v2.0 come descritto nelle specifiche OASIS:

[SAML-TechOv] OASIS Security Services (SAML) TC, Security Assertion Markup Language (SAML) V2.0 Technical Overview, Draft 3, 20 febbraio 2005.

https://www.oasis-open.org/committees/download.php/11511/sstc-saml-tech-overview-2.0-draft-03.pdf

[SAML-Core] OASIS Security Services (SAML) TC, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005

[SAML-Bindings] OASIS Security Services (SAML) TC, Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005

[SAML-Profile] OASIS Security Services (SAML) TC, Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005.

[SAML-Metadata] OASIS Security Services (SAML) TC, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005

[SAMLAuthContext] OASIS Security Services (SAML) TC, Authentication Context for The OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005.

1.6. Il servizio di I&AM dovrà essere in grado di realizzare il profilo SAML "Web Browser SSO" come specificato in ([SAML-TechOv] sez. 4.1) prevedendo le due versioni "SP-Initiated": "Redirect->POST binding" e "POST->POST binding" in cui il meccanismo di autenticazione è innescato dalla richiesta inoltrata dall'utente (tramite il suo User Agent) al componente PEP del servizio I&AM dell'amministrazione, che a sua volta per l'autenticazione si rivolge all'autorità di autenticazione esterna in modalità "pull".

1.7. La richiesta di autenticazione SAML (basata sul costrutto <AuthnRequest>) può essere inoltrata da I&AM (Relying Party) all'autorità di autenticazione (servizio di Identity Provider) usando il binding HTTP Redirect o il binding HTTP POST.

1.8. La relativa risposta SAML (basata sul costrutto <Response>) sarà inviata dall'Identity Provider al PEP del servizio I&AM (Relying Party) tramite il binding HTTP POST.

1.9. la richiesta di attributo basata sul costrutto SAML < AttributeQuery > sarà inoltrata dal servizio dal PEP di I&AM (Relying Party) all'autorità di attributo usando il binding SOAP Over HTTP.

1.10. La risposta basata sul costrutto SAML < response > sarà inviata dall'autorità di attributo al PEP del servizio I&AM (Relying Party) usando il binding SOAP Over HTTP.

1.11. Deve essere garantito il supporto a tutti i formati ammessi dallo standard SAMLv2.0 di cui al 3.1 in merito alle asserzioni, alle richieste di <AuthnRequest> con relative risposte <Response> e del binding; L'Agenzia dell'Italia Digitale darà indicazioni al fornitore in merito all'effettiva attualizzazione dei contenuti.

2. Il servizio deve essere fornito in modo indipendente dai sistemi operativi ed applicativi utilizzati e dalle architetture di rete e prevede diversi profili.

3. Il servizio comprende la gestione delle policy di accesso dei servizi, la gestione del ciclo di vita dei profili utente (creazione dell'utenza, aggiornamento e cancellazione) con relativa assegnazione dei privilegi di accesso ai servizi/sistemi (attribuzione, sospensione, modificazione, revoca e cancellazione). Tali attività dovranno essere condotte secondo le direttive e sotto la supervisione dei responsabili delle amministrazioni.

4. Deve valere il principio che ogni operazione effettuata sui sistemi è riconducibile a soggetti correttamente identificati, autenticati ed autorizzati. Ne consegue che devono essere rilevati anche tutti i tentativi di accesso non autorizzato, anche inconsapevolmente o senza dolo intenzionale da parte degli utenti.

5. Deve essere prevista la suddivisione degli utenti in gruppi omogenei (categorie).

6. Le caratteristiche del sistema la configurazione e la collocazione degli apparati necessari, nonché le procedure organizzative e la delimitazione del contesto, dovranno essere descritti in un documento di analisi del rischio, che

l'Aggiudicatario dovrà predisporre di concerto con l'Amministrazione, entro 10 giorni lavorativi dalla richiesta dell'Amministrazione.

7. Il gestore del servizio di I&AM dovrà prevedere, su richiesta, la presa in carico e la migrazione dei profili utente gestite dall'amministrazione, direttamente o tramite un terzo fornitore;

Tipologia del servizio

Il servizio sarà erogato in modalità "as a service".

Parametri di valutazione economica

La modalità di remunerazione del servizio "I&AM" è: a canone.

Ai fini della valutazione economica del servizio "I&AM" deve essere presentata una quotazione – canone annuale per utente - per ciascuna delle seguenti fasce, definite in base al numero di profili utenti gestiti:

- *Fascia 1:* fino a 10.000 utenti gestiti
- *Fascia 2:* da 10.001 a 100.000 utenti gestiti
- *Fascia 3:* da 100.001 a 400.000 utenti gestiti
- *Fascia 4:* oltre 400.000 utenti gestiti

L'ordine di acquisto del servizio deve avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

1.2. Tipologia servizi L2.S2 – Servizi di firma digitale remota e timbro elettronico

I servizi di firma digitale remota e di timbro elettronico sono volti a favorire la dematerializzazione dei documenti e la digitalizzazione dei processi amministrativi. Di seguito si descrivono i requisiti richiesti, da considerarsi minimi.

Tali servizi devono essere resi dal Fornitore in modalità "as a service" e in modo da garantire la conformità alla normativa vigente (CAD).

Il Fornitore, nella sua Offerta Tecnica, dovrà illustrare con adeguato livello di dettaglio:

- le infrastrutture tecnologiche e le architetture previste per l'erogazione dei servizi;
- le modalità operative di attivazione ed erogazione dei servizi, gli strumenti finalizzati a supportare le Amministrazioni nella fruizione dei suddetti servizi in termini di semplicità di utilizzo, interfaccia grafica, integrazione con altre applicazioni.

1.2.1. Servizio L2.S2.1 – Firma digitale remota

Descrizione del servizio

Il servizio di "firma digitale remota" consente alle Amministrazioni di dare efficacia probatoria ai documenti informatici firmati digitalmente, favorendo così i processi di dematerializzazione e consentendo l'automazione e l'ottimizzazione dei processi aziendali.

Il servizio deve essere configurato come un servizio online nel quale la chiave privata del firmatario viene generata e conservata assieme al certificato di firma rilasciato da parte di un Certificatore accreditato, all'interno di un server remoto sicuro (basato su un HSM conforme alla normativa vigente in materia). E' quindi richiesto che venga utilizzato un sistema di autenticazione forte che preveda l'uso, oltre alla conoscenza di un codice segreto (es. PIN), di sistemi OTP fisici o logici (USB, telefono cellulare, token), eliminando in tal modo i problemi e i rischi relativi all'utilizzo delle sole password statiche.

Qualora il sistema di autenticazione preveda la fornitura di uno strumento fisico (es. OTP) ai titolari, la consegna è effettuata presso una sede dell'Amministrazione dalla stessa indicata. L'Amministrazione provvede alla consegna ai rispettivi titolari.

L'attività di verifica dell'identità dei titolari dei certificati di firma digitale, propedeutica al loro rilascio, è effettuata a cura e sotto la responsabilità dell'Amministrazione.

Il servizio deve essere reso in modo da garantire la conformità alla normativa vigente in materia di firme digitali (CAD d.lgs. 82 del 7 marzo 2005 e successive modifiche).

Nella fornitura del servizio di firma digitale remota deve essere applicata la Determinazione Commissariale n. 63/2014 dell'Agenzia per l'Italia Digitale.

Il servizio deve includere la fornitura dei certificati digitali rilasciati da un Ente Certificatore accreditato a norma e delle relative coppie di chiavi pubblica/privata con lunghezza minima di 2048 bit, necessarie alla generazione delle firme.

Requisiti funzionali

Il Fornitore, nell'ambito del presente servizio deve garantire per l'Amministrazione almeno la disponibilità delle seguenti funzionalità base / strumenti a supporto:

- firma digitale remota dei documenti in formato CAdES, PAdES e XAdES come previsto dalla normativa vigente in materia;
- inserimento di firme multiple nello stesso documento;
- verifica delle firme digitali apposte a documenti informatici e delle marche temporali ad essi associati;
- gestione delle credenziali immateriali[1] del sistema di autenticazione. Tali credenziali sono fornite ai titolari direttamente dall'Amministrazione;
- associazione degli strumenti fisici previsti dal sistema di autenticazione al singolo titolare;
- generazione e gestione delle richieste di emissione dei certificati di firma digitale;
- sottomissione e gestione delle richieste di revoca e sospensione dei certificati di firma digitale;
- firma digitale massiva automatica.

Requisiti tecnici

Dal punto di vista tecnico, il servizio dovrà prevedere almeno:

- alta disponibilità:
- messa a disposizione di un'interfaccia grafica;
- possibilità di integrazione con applicazioni tramite Web Services;
- funzionalità di verifica della firma compatibile con i principali formati di documenti (tra cui almeno .doc, .docx, .xls, .xslx, .pdf, .ppt, .pptx, .eml, .odt, .ods, .odp).

[1] La procedura di firma remota deve prevedere l'uso di un sistema di autenticazione a doppio fattore: conoscenza e possesso. Le credenziali immateriali costituiscono il primo fattore. A titolo di esempio possono consistere in password/PIN. Gli "strumenti fisici" costituiscono il secondo fattore di autenticazione.

Tipologia del servizio

Il servizio firma digitale remota sarà erogato in modalità continuativa di tipo "as a service".

Parametri di valutazione economica

La modalità di remunerazione del servizio "firma digitale remota" è: a canone.

Ai fini della valutazione economica del servizio "firma digitale remota" dovrà essere presentata una quotazione – canone annuale per utente - per ciascuna delle seguenti fasce:

- *Fascia 1:* fino a 50 utenti
- *Fascia 2:* da 51 a 200 utenti
- *Fascia 3:* da 201 a 1.000 utenti
- *Fascia 4:* oltre 1.000 utenti

L'ordine di acquisto del servizio deve avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

1.2.2. Servizio L2.S2.3 – Timbro elettronico

Descrizione del servizio

Il servizio di "timbro elettronico" consente alle Amministrazioni la creazione di documenti informatici che possano conservare la medesima validità legale anche dopo essere stati stampati su supporto cartaceo. Di seguito si descrivono i requisiti richiesti, da considerarsi minimi.

Il servizio in oggetto deve consentire la creazione di un codice grafico bidimensionale posizionato in un punto qualsiasi del documento, a scelta dell'utente, e generato a partire dal contenuto del documento e dalla firma digitale, ove presente. Nell'ambito di tale servizio si richiede inoltre la messa a disposizione degli strumenti necessari per la decodifica del timbro e la verifica di conformità rispetto al documento originale.

Il servizio deve essere reso in modo da garantire la conformità alla normativa vigente in materia di timbro elettronico (dell'art. 23-ter del CAD).

Requisiti funzionali

Il Fornitore, nell'ambito del servizio "timbro elettronico" deve garantire all'Amministrazione almeno la disponibilità delle seguenti funzionalità base / strumenti a supporto:

- creazione ed emissione del timbro elettronico;
- verifica del timbro elettronico e della conformità del documento stampato rispetto all'originale informatico; Questa funzionalità deve poter essere liberamente e pubblicamente resa disponibile all'Amministrazione per la verifica dei documenti prodotti:
- gestione delle credenziali e creazione di specifici profili deputati all'apposizione del timbro.

Requisiti tecnici

Dal punto di vista tecnico, il servizio deve prevedere almeno:

- alta disponibilità;
- funzionalità di verifica del timbro compatibile con i principali formati di documenti (tra cui almeno .doc, .docx, .xls, .xslx, .pdf, .ppt, .pptx, .eml, .odt, .ods, .odp).

Tipologia del servizio

Il servizio "timbro elettronico" sarà erogato in modalità continuativa di tipo "as a service".

Parametri di valutazione economica

La modalità di remunerazione del servizio "timbro elettronico" è: a consumo.

Ai fini della valutazione economica del servizio "timbro elettronico" deve essere presentata una quotazione – costo per timbratura - per ciascuna delle seguenti fasce:

- *Fascia 1:* fino a 1.000 timbrature
- *Fascia 2:* da 1.001 a 10.000 timbrature
- *Fascia 3:* da 10.001 a 100.000 timbrature
- *Fascia 4:* oltre 100.000 timbrature

L'ordine di acquisto del servizio deve avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

1.3. Tipologia servizi L2.S3 – Servizi di sicurezza

I servizi di sicurezza sono volti a supportare le Amministrazioni nella prevenzione e gestione degli incidenti informatici e nell'analisi delle vulnerabilità delle componenti hardware e software dei sistemi informativi.

Tali servizi saranno erogati secondo le seguenti modalità:

- "as a service", mediante il Centro Servizi del Fornitore con l'ausilio degli strumenti (hardware e software) messi a disposizione da quest'ultimo. Si precisa che, qualora lo ritenga opportuno ai fini dell'erogazione dei servizi, il Fornitore potrà richiedere l'autorizzazione ad installare una o più appliance e/o componenti/agent software dedicate presso l'Amministrazione;
- "on premise", mediante l'utilizzo degli strumenti in uso presso le Amministrazioni stesse con il supporto di figure professionali messe a disposizione dal Fornitore.

Le categorie di servizi "as a service" che il Fornitore si impegna ad erogare, sono le seguenti:

- static application security testing;
- dynamic application security testing;
- mobile application security testing;
- vulnerability assessment:
- data loss/leak prevention,
- database security;
- web application firewall management e next generation firewall management;
- secure web gateway.

Si precisa che per ciascuno dei servizi sopra indicati, il Fornitore, in fase di attivazione del servizio, dovrà concordare con l'Amministrazione la strategia e le policy di sicurezza che dovranno essere applicate per il blocco delle minacce e i livelli di criticità dei servizi erogati (critici e non critici).
La classificazione delle vulnerabilità e delle minacce deve tener conto dei livelli di severità definiti nella seguente tabella:

Severità	Descrizione
Livello 1 - Alta	Grave impatto sull'operatività e conseguente livello di compromissione di servizi e/o sistemi dell'Amministrazione. L'incidente presenta almeno una tra le seguenti condizioni: • impossibilità tecnica di fornire uno o più servizi classificati come critici dall'Amministrazione; • estesa infezione virale in grado di compromettere uno o più sistemi e di propagarsi nella rete; • compromissione di sistemi o di reti in grado di permettere accessi

Severità	Descrizione
	incontrollati a informazioni riservate; • violazione dei siti web; • rilevanti perdite di produttività per clienti interni (dipendenti-collaboratori) ed esterni (cittadini-partner-fornitori); • rischio di azioni legali; • frode o attività criminale che coinvolga servizi forniti dall'Amministrazione; • perdita di immagine e/o reputazione.
Livello 2 - Media	I servizi e/o sistemi sono parzialmente interrotti o seriamente degradati. L'incidente presenta una tra le seguenti condizioni: • compromissione di server e degrado delle prestazioni; • attacchi che provocano il funzionamento parziale o intermittente della rete/sistemi/applicazioni; • impossibilità tecnica di fornire servizi classificati dall'Amministrazione come non critici; • parziale perdita di produttività per un gruppo di clienti interni o esterni;
Livello 3 - Bassa	Modesto impatto sull'operatività e relativi ambienti per l'erogazione dei servizi. L'incidente presenta una tra le seguenti condizioni: • informazione (o segnalazione) del rischio di contaminazioni da virus; • informazione (o segnalazione) del rischio di intrusione da parte di un attaccante; • parziale perdita di produttività per un numero ristretto di clienti interni o esterni.

Tabella 1 – Livelli di Severità

Il Fornitore avrà l'obbligo di verificare almeno trimestralmente l'effettiva attuazione delle policy di sicurezza al fine di assicurare l'aderenza rispetto a quanto concordato con l'Amministrazione. L'Amministrazione si riserva la facoltà di poter richiedere in qualunque momento e senza oneri aggiuntivi l'aggiornamento e la modifica delle policy di sicurezza.

Si precisa inoltre che le attività di analisi, individuazione delle vulnerabilità ed esecuzione di test previste nell'ambito dei servizi di "static application security testing", "dynamic application security testing", "mobile application security testing" e

"vulnerability assessment" dovranno essere eseguite dal Fornitore sulle applicazioni in ambiente di produzione o collaudo, previo accordo con l'Amministrazione. Il Fornitore dovrà inoltre segnalare all'Amministrazione, tramite comunicazione formale, il perimetro che sarà interessato dall'attività di analisi e di test, la tipologia e la descrizione dei controlli effettuati e la valutazione dell'impatto potenziale.

Si precisa che, nell'ambito dei servizi professionali erogati in modalità "on premise", descritti nel paragrafo 1.3.9, tra gli altri servizi, l'Amministrazione potrà richiedere anche attività di supporto per la gestione del CERT e delle Unità Locali di Sicurezza o strutture equivalenti delle Pubbliche Amministrazioni per la prevenzione e gestione degli incidenti informatici e per l'analisi delle vulnerabilità dei sistemi hardware e software. Di seguito e nei paragrafi dedicati ai singoli servizi, si descrivono i requisiti di tutti i servizi richiesti, da considerarsi minimi.

Nell'ambito dell'offerta tecnica, il Fornitore dovrà illustrare con adeguato livello di dettaglio metodologia, processi, tecnologie e strumenti che intende utilizzare per l'erogazione dei servizi e l'esecuzione delle attività richieste ed in particolare:

- infrastrutture tecnologiche e architetture a supporto dei servizi offerti;
- eventuale necessità o meno, per ciascuno dei servizi richiesti, di installazione di appliance e/o componenti/agent software presso l'Amministrazione;
- modalità operative di attivazione ed erogazione dei servizi con particolare riferimento alla consegna del codice oggetto di analisi (ove applicabile), la scansione del codice, e la consegna dei deliverable richiesti;
- descrizione ed esempi del tipo di reportistica proposta per ciascuno dei servizi ove prevista;
- approccio e metodologie di riferimento per le attività di individuazione e analisi delle vulnerabilità;
- per i servizi di data "loss/leak prevention", "database security", "web application firewall" e "next generation firewall", "secure web gateway", le modalità operative e gli strumenti finalizzati a supportare da remoto le Amministrazioni nel caso di incidenti e/o attacchi ostili;
- caratteristiche tecniche delle soluzioni proposte, con particolare riferimento alla compatibilità verso un numero maggiore di sistemi/tecnologie/database rispetto a quanto richiesto nel presente Capitolato Tecnico;
- modalità organizzative e operative per la formazione delle risorse impegnate nei servizi "on premise" con particolare riferimento al piano formativo e ai giorni minimi di formazione proposti per ciascuna risorsa impiegata;

- eventuale proposta di miglioramento dei profili professionali richiesti nell'ambito dei servizi "on premise", in termini di incremento dell'anzianità lavorativa delle risorse impiegate, sia generale che nella funzione, rispetto a quanto richiesto nel presente Capitolato Tecnico;
- indicazione del numero di risorse per profilo professionale in relazione alle certificazioni possedute.

Prodotti della fornitura

Nell'ambito dei servizi di sicurezza, descritti nei paragrafi successivi, dovranno essere realizzati periodicamente i seguenti prodotti:

- un rapporto di sintesi, *executive summary*, destinato prevalentemente al management ed al personale non tecnico per una comprensione immediata dei problemi riscontrati;
- un rapporto tecnico, *technical report*, con tutte le indicazioni necessarie per la comprensione dei problemi riscontrati, per la loro classificazione in termini di severità e per l'identificazione delle misure più idonee da adottare per la loro risoluzione;
- un piano di rientro, *remediation plan*, con l'indicazione di tutte le possibili contromisure da porre in essere per eliminare le problematiche, le cause di non conformità e/o le vulnerabilità rilevate.

Al fine di assicurare la massima confidenzialità delle informazioni trattate, la consegna dei report e delle eventuali evidenze raccolte, dovrà avvenire per mezzo di un canale di comunicazione concordato con i referenti dell'Amministrazione.

Tali informazioni dovranno essere archiviabili mediante robuste tecniche di cifratura, e dovrà esserne consentito l'accesso al solo personale autorizzato mediante opportuni meccanismi di autenticazione. Dovrà inoltre essere evitata la conservazione su supporti rimovibili, e/o notebook, che sarà limitata al tempo strettamente necessario per le operazioni di elaborazione e di analisi.

Executive summary

L'executive summary dovrà illustrare in modo sintetico ma esaustivo i principali rischi a cui l'Amministrazione è esposta a causa delle vulnerabilità riscontrate. Nel documento, prodotto al termine delle attività di analisi, dovranno essere concentrati e riassunti i risultati esposti nel report tecnico, conservandone la sequenza e la struttura concettuale.

L'executive summary dovrà inoltre includere un piano di azione ad alto livello per illustrare, in base a specifiche classi di priorità (di breve, medio e lungo termine), le macro-categorie di problemi rilevati e definire le opportune azioni correttive/risolutive (piano di rientro).

Technical report

Il technical report dovrà fornire una precisa segnalazione di tutte le vulnerabilità riscontrate e/o punti deboli delle applicazioni e dovrà contenere le indicazioni sulle possibili soluzioni (in termini di patch, di configurazioni necessarie e suggerimenti migliorativi) al fine di mitigare i rischi potenziali generati dal loro sfruttamento.

Ogni problematica riportata dovrà essere descritta in una sezione specifica di approfondimento tecnico. Tale sezione descrittiva dovrà essere composta almeno da:

- descrizione di dettaglio della problematica rilevata (applicazione impattata, vulnerabilità, tipologia, descrizione, severità);
- suggerimenti provvisori realizzati dal team di analisi;
- workaround possibili, qualora applicabili;
- soluzioni di protezione, qualora applicabili.

In particolare, per il servizio di vulnerability assessment, per ogni vulnerabilità tecnica dovrà essere effettuata un'analisi del rischio "tecnica" (basata sullo standard CVSS) che prende in considerazione popolarità e semplicità dell'attacco commisurata al valore del sistema e al grado di compromissione raggiunto.

Remediation plan

Il remediation plan è il documento riportante l'indicazione, ad alto livello, delle possibili contromisure tecnologiche (applicative e/o infrastrutturali), organizzative e/o procedurali da porre in essere per eliminare le problematiche, le cause di non conformità e/o le vulnerabilità rilevate.

Il remediation plan deve contenere, come minimo, le seguenti informazioni:

- la descrizione della problematica rilevata;
- l'indicazione della root-cause;
- la descrizione dell'attività da porre in essere per risolvere la problematica;
- una stima temporale dell'intervento;

- una stima qualitativa (alto, medio, basso, sulla base di criteri concordati con il referente dell'Amministrazione) dell'impatto economico, organizzativo e tecnologico dell'intervento;
- la priorità di implementazione dell'intervento.

Gestione degli incident

Nell'ambito dei servizi di "data loss/leak prevention", "database security", "web application firewall" e "next generation firewall", "secure web gateway", descritti nei successivi paragrafi, oltre alle attività di identificazione e di blocco delle minacce, il Fornitore è responsabile anche delle attività di analisi e gestione degli allarmi.

In particolare, nel caso di rilevazione di attività ostili, il Fornitore deve garantire la realizzazione delle seguenti attività:

- analisi degli allarmi, al fine di discriminare i falsi positivi;
- identificazione del livello di severità;
- nel caso di incidenti con severità 1, notifica al responsabile dell'Amministrazione, alle ULS e/o a terzi da essi designati, tramite posta elettronica o telefono, dell'incidente rilevato e delle azioni da intraprendere;
- apertura di un ticket di "incidente di sicurezza" con indicazione del tipo di incidente. Si precisa che i tempi di reazione del Fornitore per l'apertura del ticket e la gestione dell'escalation variano in funzione della severità dell'incidente e dovranno essere i seguenti, pena l'applicazione delle penali di cui all'Appendice 1 - Indicatori di qualità Lotto 2:

Severità	Tempistica - Escalation
Livello 1 - Alta	Apertura del ticket entro 15 minuti dall'identificazione dell'evento. In questo caso deve essere prevista l'adozione di una procedura di escalation "avanzata" che include un aggiornamento ogni 30 minuti con indicazione dei risultati e delle azioni previste dal piano di risoluzione (o di rimedio).
Livello 2 - Media	Apertura del ticket entro 30 minuti dall'identificazione dell'evento. In questo caso deve essere prevista l'adozione di una procedura di escalation che include un aggiornamento ogni ora con indicazione dei risultati e delle azioni previste dal piano di risoluzione (o di rimedio).
Livello 3 - Bassa	Apertura del ticket entro 40 minuti dall'identificazione dell'evento. In questo caso non è prevista l'adozione di una procedura di escalation.

Tabella 2 - Tempistiche della procedura di escalation degli incident

In ogni caso alla chiusura del ticket il Fornitore deve rendere disponibile all'Amministrazione un report di sintesi (technical report), descritto nel seguente paragrafo, in cui dovranno essere indicate le seguenti informazioni:

- sorgente, tipologia, descrizione, severità dell'evento/allarme;
- istante temporale in cui l'evento si è verificato;
- azioni intraprese (es. modifiche alle policy) per la risoluzione o mitigazione del problema.

Nei paragrafi seguenti si riporta la descrizione dei servizi richiesti.

1.3.1. Servizio L2.S3.1 – Static application security testing

Descrizione del servizio

Il servizio di "static application security testing" deve consentire alle Amministrazioni l'identificazione delle vulnerabilità software all'interno del codice (sorgente o binario) delle applicazioni nella fase iniziale del ciclo di vita in modo da poterle eliminare prima della distribuzione.

Più in generale, il perimetro di applicazione del servizio comprende l'analisi statica del codice sorgente o binario delle seguenti categorie: sviluppo custom interno/esterno, open source, software/librerie di terze parti.

Il Fornitore nell'Offerta Tecnica dovrà specificare il tipo di supporto che sarà richiesto all'Amministrazione per l'erogazione del servizio, con esplicita indicazione delle singole attività per cui si richiede supporto ed effort stimato, con particolare riferimento alle tempistiche e alle modalità di consegna del codice oggetto di analisi.

L'attività di analisi statica del codice deve essere svolta dal Fornitore secondo le best practice internazionali, ed almeno secondo quanto previsto dalla metodologia OWASP, e dovrà includere almeno i seguenti controlli:

- *Data Validation*: verifica della presenza di vulnerabilità che possono riguardare eventuali dati corrotti in ingresso che possono portare a un comportamento anomalo dell'applicazione;
- *Control Flow*: verifica dei rischi collegati all'assenza di specifiche sequenze di operazioni che, se non eseguite in un certo ordine, potrebbero portare a violazioni sulla memoria o l'uso scorretto di determinati componenti;
- *Semantico*: rilevazione di eventuali problematiche legate all'uso pericoloso di determinate funzioni o API (es. funzioni deprecate);

- *Configurazioni*: verifica dei parametri intrinseci di configurazione dell'applicazione;
- *Buffer Validation:* verifica della presenza di buffer overflow exploitabile attraverso la scrittura o lettura di un numero di dati superiore alla reale capacità del buffer stesso.

Si precisa che pur essendo il servizio prevalentemente orientato ad applicazioni in ambiente web, il Fornitore, previo accordo con l'Amministrazione, potrà erogarlo anche su altre tipologie di ambienti, utilizzando il medesimo modello di pricing di seguito definito.

Requisiti funzionali

Il Fornitore nell'ambito del servizio "static application security testing" deve individuare le vulnerabiltà critiche come SQL injection, cross-site scripting (XSS), buffer overflow, condizioni di errore non gestite e potenziali back-door.

Di seguito un elenco delle funzionalità base / strumenti a supporto:

- identificazione delle vulnerabilità attraverso l'analisi del codice sorgente o binario e indicazione puntuale delle sezioni di codice relative alle vulnerabilità riscontrate;
- verifica dei risultati, individuazione e rimozione dei falsi positivi;
- prioritizzazione delle vulnerabilità individuate e definizione del piano delle azioni correttive (remediation plan*);*
- produzione di reportistica di sintesi (executive summary) e di dettaglio (technical report) sulle analisi eseguite e rappresentazione delle informazioni qualitative e dimensionali sugli applicativi analizzati, con indicazioni sulle possibili ottimizzazioni da apportare.

Requisiti tecnici

Dal punto di vista tecnico, nel caso in cui il servizio utilizzi il codice sorgente, deve prevedere almeno:

- compatibilità con i principali linguaggi e framework di sviluppo largamente diffusi (tra cui almeno .NET, PHP, C/C++, Java, J2EE, ASP);
- integrazione con almeno due dei seguenti repository del software: SVN - Subversion, CVS - Concurrent Versions System, Git, TFVC - Team Foundation Version Control.

Tipologia del servizio

Il servizio "static application security testing" sarà erogato in modalità continuativa di tipo "as a service".

Parametri di valutazione economica

La modalità di remunerazione del servizio "static application security testing" è a corpo nel caso in cui il servizio sia erogato in modalità *one time* (unica scansione) e a canone nel caso in cui il servizio sia erogato in modalità *continua* (scansioni periodiche).

Ai fini della valutazione economica del servizio "static application security testing", deve essere presentata una quotazione - costo per singola applicazione - per la modalità *one time* ed una quotazione – canone annuale per applicazione - per la modalità *continua* per ciascuna delle seguenti fasce definite in base al numero di applicazioni:

- *Fascia 1:* fino a 5 applicazioni
- *Fascia 2*: da 6 a 10 applicazioni
- *Fascia 3:* oltre 10 applicazioni

L'ordine di acquisto del servizio – per la modalità continua - deve avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

1.3.2. Servizio L2.S3.2 – Dynamic application security testing

Descrizione del servizio

Il servizio di "dynamic application security testing" consente alle Amministrazioni l'identificazione delle vulnerabilità all'interno delle applicazioni Web in fase di esecuzione e l'analisi dell'esposizione al rischio di attacchi informatici ai sistemi informativi mediante l'utilizzo di tecniche di analisi dinamica.

L'analisi per l'individuazione delle vulnerabilità dovrà essere comprendere almeno gli ambiti di seguito riportati.

- *Configurazione:* identificazione delle directory e delle pagine web interessate dal workflow applicativo.
- *Autenticazione:* analisi delle funzionalità di autenticazione per verificare che al loro interno non siano presenti problematiche di sicurezza in particolare:
    - che le credenziali di accesso fornite dagli utenti viaggino attraverso canali di comunicazioni considerati come sicuri e che siano utilizzati dei meccanismi di protezione tali da non favorire la conduzione di attacchi sofisticati;

- che siano presenti dei meccanismi di enforcing delle credenziali di accesso cioè se il meccanismo di autenticazione e di provisioning dell'applicazione impedisca agli utenti finali l'utilizzo di determinate password classificate comunemente come deboli;
- che all'interno dell'applicazione siano presenti dei meccanismi di protezione da "attacchi a dizionario"[2]. Qualora tali meccanismi siano presenti andrà verificato che non siano aggirabili;

- *Autorizzazione:* verifica della presenza di problematiche di sicurezza legate alla possibilità di elevare i privilegi e i ruoli delle utenze applicative o di accedere a sezioni dell'applicazione protette aggirando i meccanismi di autenticazione e autorizzazione esistenti.
- *Validazione dei dati:* verifica della validazione degli input degli utenti al fine di garantire che non siano presenti eventuali criticità di sicurezza.

I controlli effettuati dovranno consentire almeno di:

- verificare i meccanismi di gestione delle sessioni e della loro robustezza;
- analizzare il sistema di gestione degli errori dell'applicazione;
- controllare, laddove applicabile, i meccanismi di crittografia;
- verificare i meccanismi di logging e il metodo di gestione delle informazioni;
- verificare le comunicazioni dell'applicativo con soggetti esterni come client, DB, LDAP ecc..

Dovranno inoltre essere identificate e rilevate almeno le seguenti tipologie di vulnerabilità potenziali:

- *Accesso abusivo a funzionalità aggiuntive;*
- *Gestione non controllata degli input;*
- *Cross-Site Scripting;*
- *Cross-Site Request Forgery;*
- *Format String;*
- *Integer Overflows;*

[2] Tecnica di attacco alla sicurezza di un sistema o sottosistema informatico mirata a decifrare un codice o una determinata password utilizzando una lista di parole probabili (detta dizionario).

- *LDAP Injection;*
- *Mail Command Injection;*
- *Null Byte Injection;*
- *Path Traversal;*
- *Remote File Inclusion;*
- *SSI Injection;*
- *SQL Injection;*
- *XPath Injection;*
- *XML Attribute Blowup;*
- *XML Bombing;*
- *XML External Entities;*
- *XML Injection;*
- *XQuery Injection.*

Il servizio dovrà essere svolto secondo le best practice internazionali, e almeno secondo quanto previsto dalla metodologia OWASP.

Il servizio prevede tre diversi profili di erogazione, a seconda della tipologia di applicazione oggetto di analisi, come specificato nella seguente tabella:

Profilo	Tipologia applicazione
Bronze	Applicazioni non critiche che consentono la visualizzazione di pagine di contenuto informativo (siti web statici)
Silver	Applicazioni costituite da più form (siti web dinamici) e con funzionalità di autenticazione
Gold	Applicazioni critiche con funzionalità complesse e di tipo transazionale (ad esempio pagamenti)

Requisiti funzionali

Il Fornitore, nell'ambito del servizio "dynamic application security testing" deve garantire per tutti i profili di erogazione sopra citati, la disponibilità per l'Amministrazione almeno delle seguenti funzionalità base / strumenti a supporto:

- identificazione delle vulnerabilità attraverso l'esecuzione di scansioni;

- verifica dei risultati, individuazione e rimozione dei falsi positivi;
- assegnazione automatica delle priorità/severità ai rischi di sicurezza sulla base delle policy concordate con l'Amministrazione;
- correlazione dei risultati delle fasi precedenti e la definizione del piano di rientro (remediation plan);
- produzione di reportistica di sintesi (executive summary) e di dettaglio (technical report) sulle analisi eseguite e rappresentazione delle informazioni qualitative e dimensionali sugli applicativi analizzati, con indicazioni sulle possibili ottimizzazioni da apportare.

Inoltre per i profili Silver e Gold sono previste le seguenti funzionalità aggiuntive:

Funzionalità	Profilo Silver	Profilo Gold
Definizione di scansioni personalizzate	X	X
Esecuzione di test di autenticazione multilivello	X	X
PCI Compliance	X	X
Esecuzione di test manuali sulle applicazioni in fase di esecuzione	X	X
Creazione personalizzata di *business logic test*		X
Proof of concept delle vulnerabilità riscontrate		X

Requisiti tecnici

Dal punto di vista tecnico, il servizio deve prevedere almeno:

- compatibilità con i principali linguaggi e framework di sviluppo largamente diffusi (tra cui almeno .NET, PHP, C/C++, Java, J2EE, ASP).

Tipologia del Servizio

Il servizio "dynamic application security testing" sarà erogato in modalità continuativa di tipo "as a service".

Parametri di valutazione economica

La modalità di remunerazione del servizio "dynamic application security testing" è: a canone.

Ai fini della valutazione economica dovrà essere presentata una quotazione – canone annuale per applicazione - per ciascuna delle seguenti fasce, definite in base al profilo del servizio e al numero di applicazioni:

- *Fascia 1:* fino a 5 applicazioni
- *Fascia 2:* da 6 a 10 applicazioni
- *Fascia 3:* oltre 10 applicazioni

L'ordine di acquisto del servizio deve avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

1.3.3. Servizio L2.S3.3 – Mobile application security testing

Descrizione del servizio

Il servizio di "mobile application security testing" consente alle Amministrazioni di verificare il livello di sicurezza delle applicazioni per dispositivi *mobile* nel corso dell'intero ciclo di sviluppo software, attraverso tecniche di analisi statica e dinamica, come illustrato nei paragrafi precedenti.

Si noti esplicitamente che l'ambito del servizio deve includere non solo l'analisi del codice e l'esecuzione dell'applicazione ma deve anche riguardare tutte le interfacce verso altri sistemi e/o applicazioni così come altre risorse collegate che potrebbero avere un impatto sulla sicurezza globale del sistema.

Requisiti funzionali

Il Fornitore, nell'ambito del servizio "mobile application security testing" deve garantire la disponibilità per l'Amministrazione almeno delle seguenti funzionalità base / strumenti a supporto:

- individuazione delle vulnerabilità mediante tecnica di analisi statica e dinamica;
- verifica dei risultati, individuazione e rimozione dei falsi positivi;
- assegnazione automatica delle priorità/severità ai rischi di sicurezza sulla base delle policy concordate con l'Amministrazione;
- correlazione dei risultati delle fasi precedenti e la definizione del piano di rientro (remediation plan);

- produzione di reportistica di sintesi (executive summary) e di dettaglio (technical report) sulle analisi eseguite e indicazione delle possibili ottimizzazioni da apportare;
- analisi e gestione delle policy di accesso ai dati e alle funzioni del dispositivo.

Requisiti tecnici

Dal punto di vista tecnico, il servizio deve prevedere almeno:

- compatibilità con almeno due dei seguenti sistemi operativi: Android, Blackberry, iOS e Microsoft Windows Mobile.

Tipologia del Servizio

Il servizio "mobile application security testing" sarà erogato in modalità continuativa di tipo "as a service".

Parametri di valutazione economica

La modalità di remunerazione del servizio "mobile application security testing" è: a canone.

Ai fini della valutazione economica del servizio "mobile application security testing", deve essere presentata una quotazione – canone annuale per applicazione - per ciascuna delle seguenti fasce, definite in base al numero di applicazioni:

- *Fascia 1:* fino a 5 applicazioni
- *Fascia 2:* da 6 a 10 applicazioni
- *Fascia 3:* oltre 10 applicazioni

L'ordine di acquisto del servizio deve avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

1.3.4. Servizio L2.S3.4 – Vulnerability assessment

Descrizione del servizio

Il servizio di "vulnerability assessment" deve fornire alle Amministrazioni una panoramica dello stato di sicurezza dell'infrastruttura e dello stato di esposizione alle vulnerabilità attraverso la raccolta di informazioni concernente i servizi erogati, l'architettura e le configurazioni del sistema.

Il servizio deve inoltre consentire una verifica dinamica della sicurezza dei dispositivi di rete dell'Amministrazione allo scopo di identificare eventuali vulnerabilità,

configurazioni di sicurezza errate, carenze sui livelli di protezione attivi che espongano il contesto ad attacchi interni ed esterni.

Per la raccolta di tali informazioni il Fornitore potrà avvalersi di strumenti automatizzati al fine di rilevare le potenziali vulnerabilità. Gli strumenti dovranno essere configurati in modo da non risultare intrusivi (a meno che non espressamente concordato con l'Amministrazione).

Il servizio dovrà prevedere almeno le fasi sotto elencate.

- *Raccolta di informazioni*: fase svolta al fine di reperire il maggior numero di informazioni sulla struttura della rete delle componenti Hardware e Software dei sistemi oggetto di analisi.
- *Individuazione delle vulnerabilità*: fase svolta al fine di collezionare, tramite un set opportuno di strumenti automatizzati e correttamente configurati, una lista delle potenziali vulnerabilità note a cui potrebbero essere soggetti i sistemi analizzati. Tale fase dovrà adattarsi al contesto infrastrutturale specifico ed alle peculiari vulnerabilità associate allo specifico modello di trasporto.
- *Prioritizzazione delle vulnerabilità:* le vulnerabilità individuate dovranno essere prioritizzate secondo policy definite a monte dall'Amministrazione.

Requisiti funzionali

Il Fornitore, nell'ambito del servizio "vulnerability assessment", deve garantire la disponibilità per l'Amministrazione almeno delle seguenti funzionalità base / strumenti a supporto:

- individuazione delle vulnerabilità;
- esecuzione di test che consentano accertare le vulnerabilità individuate;
- assegnazione automatica delle priorità/severità ai rischi di sicurezza sulla base delle policy concordate con l'Amministrazione;
- correlazione dei risultati delle fasi precedenti e la definizione del piano di rientro (remediation plan);
- produzione di reportistica di sintesi (executive summary) e di dettaglio (technical report) sulle analisi eseguite e rappresentazione delle informazioni qualitative e dimensionali sugli applicativi analizzati, con indicazioni sulle possibili ottimizzazioni da apportare.

Requisiti tecnici

Dal punto di vista tecnico, il servizio deve prevedere almeno:

- compatibilità con i maggiori protocolli di rete di livello application quali FTP/SFTP/FTPS, HTTP/HTTPS, SMTP e di livello network e transport.

Tipologia del servizio

Il servizio "vulnerability assessment" deve essere erogato in modalità continuativa di tipo "as a service".

Parametri di valutazione economica

La modalità di remunerazione del servizio "vulnerability assessment" è a canone in modalità *continua*.

Ai fini della valutazione economica dovrà essere presentata una quotazione deve essere presentata una quotazione – canone annuale per indirizzo IP - per ciascuna delle seguenti fasce:

- *Fascia 1: n.* 1 indirizzo IP
- *Fascia 2:* da 2 a 15 indirizzi IP
- *Fascia 3:* oltre 15 indirizzi IP

L'ordine di acquisto del servizio deve avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

1.3.5. Servizio L2.S3.5 – Data loss/leak prevention

Descrizione del servizio

Il servizio di "data loss/leak prevention" (o DLP) deve consentire alle Amministrazioni la protezione dei dati da accessi non autorizzati o violazioni delle policy di sicurezza e riducendo il rischio di perdita, danno o svantaggio competitivo.

Il servizio deve garantire supervisione e controllo dei dati indipendentemente dal fatto che siano archiviati o in transito sulla rete, includendo attività di monitoraggio e protezione dei dati in-use (accesso tramite endpoint – desktop e laptop), in-motion (traffico rete), e at-rest (sui supporti di memorizzazione).

Si precisa inoltre che il servizio include anche l'attività di gestione degli incident descritta nel paragrafo 1.3.

Requisiti funzionali

Il Fornitore, nell'ambito del servizio "data loss/leak prevention" deve garantire la disponibilità per l'Amministrazione almeno delle seguenti funzionalità base / strumenti a supporto:

- rilevazione dei dati che transitano nell'organizzazione, ovunque siano archiviati, e valutazione del rischio di perdita di dati (*DLP Risk Assessment*);
- analisi e classificazione dei dati (*DLP Information classification*);
- possibilità di creare regole predefinite per la protezione dei dati, identificando i sistemi in cui sono memorizzati (ad esempio porte USB, CD, DVD, porte COM & LPT, dischi rimovibili, dispositivi di acquisizione immagini, modem) per assicurarsi che siano usati in conformità con le politiche di privacy e sicurezza (*DLP data at rest*);
- generazione automatica di alert nel caso in cui vengano violate le policy di sicurezza definite, visibilità e controllo sui dati in movimento, sia che si trovino in messaggi e-mail, nella mail sul Web, nell'instant messaging, e nei protocolli di rete (*DLP data in motion*);
- possibilità di generare report di sintesi (executive summary) e di dettaglio (technical report) sulle analisi svolte;
- generazione audit trail e gestione profili di audit.

Requisiti tecnici

Dal punto di vista tecnico, il servizio deve prevedere almeno:

- compatibilità con i maggiori protocolli di rete di livello application quali FTP/SFTP/FTPS, HTTP/HTTPS, SMTP e di livello network e transport;
- compatibilità con i sistemi operativi Windows e Linux e con almeno due dei seguenti: Android, Blackberry, iOS e Microsoft Windows Mobile.

Tipologia del servizio

Il servizio "data loss/leak prevention" deve essere erogato in modalità continuativa di tipo "as a service".

Parametri di valutazione economica

La modalità di remunerazione del servizio "data loss/leak prevention" è: a canone.

Ai fini della valutazione economica del servizio "data loss/leak prevention" deve essere presentata una quotazione – canone annuale per endpoint[3] - per ciascuna delle seguenti fasce :

- *Fascia 1:* fino a 500 endpoint
- *Fascia 2:* da 501 a 1.000 endpoint
- *Fascia 3:* oltre 1.000 endpoint

L'ordine di acquisto del servizio deve avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

1.3.6. Servizio L2.S3.6 – Database security

Descrizione del servizio

Il servizio di "database security" riguarda l'uso di una vasta gamma di controlli della sicurezza per la protezione del database nel suo complesso (dati, procedure o funzioni stored, il sistema di gestione, i server ed i collegamenti di rete associati) allo scopo di salvaguardarne la riservatezza, integrità e disponibilità.

Il servizio deve consentire alle Amministrazioni la protezione in tempo reale delle basi di dati da minacce esterne o interne. Il servizio deve inoltre consentire la difesa da eventuali exploit presenti nei database.

Nell'ambito di tale servizio, il Fornitore dovrà consentire alle Amministrazione almeno la realizzazione delle seguenti attività:

- monitoraggio dei database presenti all'interno dell'Amministrazione e delle applicazioni web che ne fanno uso;
- definizione di regole di sicurezza personalizzate e blocco di comportamenti non autorizzati;
- identificazione delle potenziali vulnerabilità e indicazione delle relative azioni correttive.

Si precisa inoltre che il servizio include anche l'attività di gestione degli incident descritta nel paragrafo 1.3.

Requisiti funzionali

[3] Per endpoint si intende qualunque workstation, laptop e punto di accesso della rete aziendale.

Il Fornitore, nell'ambito del servizio "database security" deve garantire la disponibilità per l'Amministrazione almeno delle seguenti funzionalità base / strumenti a supporto:

- analisi dei database e valutazione dei rischi mediante controlli di vulnerabilità;
- individuazione delle alterazioni dei dati, degli utenti e dei profili di accesso;
- creazione personalizzata di policy di sicurezza per soddisfare le normative del settore o gli standard internazionali;
- arresto in tempo reale delle sessioni che violano le policy, evitando che i dati vengano compromessi;
- controllo degli accessi ai dati, identificazione e arresto di comportamenti non autorizzati o dannosi;
- classificazione delle minacce per tipologia e/o livelli di severità;
- reporting di sintesi (executive summary) e di dettaglio (technical report) sulle vulnerabilità individuate e indicazione di script correttivi.

Requisiti tecnici

Dal punto di vista tecnico, il servizio deve prevedere almeno:

- compatibilità con almeno tre dei seguenti sistemi di database: Oracle, Microsoft SQL Server, IBM DB2, SAP Sybase e MySQL.

Tipologia del servizio

Il servizio "database security" sarà erogato in modalità continuativa di tipo "as a service".

Parametri di valutazione economica

La modalità di remunerazione del servizio "database security" è: a canone.

Ai fini della valutazione economica del servizio "database security" nel caso di modalità erogazione in modalità "as a service" dovrà essere presentata una quotazione – canone annuale per nodo[4] - per ciascuna delle seguenti fasce:

- *Fascia 1:* fino a 25 nodi
- *Fascia 2:* da 26 a 50 nodi
- *Fascia 3:* oltre 50 nodi

[4] Per "nodo" si intende qualsiasi tipo di dispositivo capace di elaborare dati e su cui sia presente almeno un'istanza di database.

L'ordine di acquisto del servizio deve avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

1.3.7. Servizio L2.S3.7 – Web application firewall management e next generation firewall management

Descrizione del servizio

Il servizio di "web application firewall management" deve consentire alle Amministrazioni di proteggere le applicazioni web da attacchi esterni agendo da filtro del traffico di rete dello strato applicativo, superando quindi le caratteristiche dei normali *intrusion detection system*.

Il servizio di "next generation firewall management" deve fornire una visione completa e in tempo reale di tutte le attività, con funzionalità avanzate di reporting.

Si precisa inoltre che il servizio include anche l'attività di gestione degli incident descritta nel paragrafo 1.3.

Requisiti funzionali

Il Fornitore, nell'ambito dei servizi di "web application firewall" e "next generation firewall" deve garantire la disponibilità per l'amministrazione almeno delle seguenti funzionalità base / strumenti a supporto:

- funzionalità standard firewall (es. policy enforcement, statefull inspection, packet filtering, NAT, VPN client-to-site e site-to-site);
- anti-malware e anti-spam;
- Intrusion Prevention (IPS) per il blocco delle minacce;
- monitoraggio del livello di sicurezza degli applicativi web;
- prevenzione avanzata contro le intrusioni e filtraggio dei contenuti;
- *deep packet inspection* per scansionare l'intero payload dei pacchetti;
- produzione di report personalizzabili di sintesi (executive summary) e di dettaglio (technical report), al fine di certificare la compliance a determinati standard o per consentire analisi sul livello di protezione delle applicazioni.

Requisiti tecnici

Dal punto di vista tecnico, il servizio deve prevedere almeno:

- compatibilità con i protocolli FTP/SFTP/FTPS, HTTP/HTTPS.

Tipologia del servizio

I servizi di "web application firewall" e "next generation firewall" sarà erogato in modalità continuativa di tipo "as a service".

Parametri di valutazione economica

La modalità di remunerazione dei servizi di "web application firewall" e "next generation firewall" è: a canone.

Ai fini della valutazione economica dei servizi "web application firewall" e "next generation firewall" dovrà essere presentata una quotazione – canone annuale - per ciascuna delle seguenti fasce, definite in base al throughput[5]:

- *Fascia 1:* throughput fino a 50 Mbps
- *Fascia 2:* throughput fino a 200 Mbps
- *Fascia 3:* throughput fino a 500 Mbps

L'ordine di acquisto del servizio deve avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

1.3.8. Servizio L2.S3.8 – Secure web gateway

Descrizione del servizio

Il servizio di "secure web gateway" deve consentire alle amministrazioni di bloccare l'accesso a siti web potenzialmente malevoli aggiornando la propria base dati in maniera automatica e di riconoscere il download di applicazioni potenzialmente dannose.

Si precisa inoltre che il servizio include anche l'attività di gestione degli incident descritta nel paragrafo 1.3.

Requisiti funzionali

Il Fornitore, nell'ambito del servizio "secure web gateway" deve garantire la disponibilità per l'amministrazione almeno delle seguenti funzionalità base / strumenti a supporto:

- analisi del traffico per bloccare malware, botnet , spyware e furto dei dati;
- identificazione dei comportamenti potenzialmente pericolosi e blocco dei siti potenzialmente malevoli o categorizzati come tali;

[5] Per throughput si intende la capacità di trasmissione della rete in una unità di tempo.

- aggiornamento automatico delle liste di siti malevoli;
- produzione di report di sintesi (executive summary) e di dettaglio (technical report) con l'analisi di tutti gli incidenti rilevanti in ambito sicurezza al fine di permettere una rapida risposta;
- gestione della navigazione tramite utilizzo di categorie di siti web e protocolli.

Requisiti tecnici

Dal punto di vista tecnico, il servizio deve prevedere almeno:

- compatibilità con i principali protocolli web (tra cui almeno FTP/SFTP/FTPS, HTTP/HTTPS).

Tipologia del servizio

Il servizio "secure web gateway" sarà erogato in modalità continuativa di tipo "as a service".

Parametri di valutazione economica

La modalità di remunerazione del servizio "secure web gateway" è: a canone.

Ai fini della valutazione economica del servizio "secure web gateway" dovrà essere presentata una quotazione – canone annuale per singola pdli (postazione di lavoro informatizzata) - per ciascuna delle seguenti fasce:

- *Fascia 1: fino a 100 pdli*
- *Fascia 2: da 101 a 1.000 pdli*
- *Fascia 3: da 1.001 a 5.000 pdli*
- *Fascia 4: oltre 5.000 pdli*

L'ordine di acquisto del servizio deve avere una durata minima di 12 (dodici) mesi. Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

1.3.9. Servizio L2.S3.9 – Servizi professionali

Il servizio ha come obiettivo quello di supportare le Amministrazioni nella realizzazione di attività nell'ambito della sicurezza applicativa, comprensive di quelle relative ai servizi di monitoraggio, attraverso l'utilizzo di specifiche figure professionali messe a disposizione dal Fornitore.

A titolo esemplificativo e non esaustivo, si riportano alcune delle attività che possono essere richieste al Fornitore:

- supporto per la gestione delle attività del CERT e delle Unità Locali di Sicurezza o strutture equivalenti delle Pubbliche Amministrazioni per la prevenzione e gestione degli incidenti informatici, per l'analisi delle vulnerabilità dei sistemi hardware e software;
- attività di supporto ai Security Operating Center (SOC) presso le Amministrazioni;
- penetration test di tipo applicativo e infrastrutturale;
- encryption dei dati memorizzati sulle postazioni di lavoro;

Si precisa che tali servizi saranno erogati esclusivamente nella modalità "on premise" con gli strumenti hardware e software presenti presso l'Amministrazione.

Le figure professionali utilizzate per l'erogazione di tali servizi devono essere caratterizzate dai requisiti minimi inderogabili indicati nell'Appendice 2.

Requisiti funzionali

Non applicabile ai "servizi professionali".

Requisiti tecnici

Non applicabile ai "servizi professionali".

Tipologia del servizio

I servizi sono erogati in modalità continuativa di tipo "on premise".

Parametri di valutazione economica

La modalità di remunerazione del servizio è "a corpo". Su richiesta dell'Amministrazione il Fornitore indicherà il numero di giorni per figura professionale necessari per l'erogazione del supporto richiesto.

Ai fini della valutazione economica dei servizi dovrà essere presentata una quotazione delle tariffe per giorno/uomo delle figure professionali, descritte nell'Appendice 2, deputate all'erogazione del servizio. Per particolari attività l'Amministrazione potrà

richiedere un supporto continuativo nelle 24 ore, per le quali dovrà essere presentata un ulteriore quotazione giorno per figura professionale.