GUIDA AL CONTRATTO QUADRO
"SERVIZI DI GESTIONE DELLE IDENTITÀ DIGITALI
E
SICUREZZA APPLICATIVA"

(Servizi di cloud computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le pubbliche amministrazioni – Lotto 2)

INDICE

Sommario

1. PREMESSA

La presente Guida, ferma restando la documentazione integrale a corredo e sotto elencata, ha lo scopo di facilitare l'utilizzo del Contratto Quadro descrivendo le modalità operative per l'adesione delle Amministrazione Beneficiarie al Contratto Quadro "Servizi di gestione delle identità digitali e sicurezza applicativa" attraverso la sottoscrizione di specifici Contratti Esecutivi con il Fornitore aggiudicatario. La Guida fornisce inoltre la descrizione dei servizi offerti e i relativi prezzi definiti attraverso la procedura di gara svolta.

Documentazione contrattuale

- Contratto Quadro
- Schema di Contratto Esecutivo
- Capitolato tecnico Parte Generale
- Capitolato Tecnico
- Appendice 1 Capitolato Tecnico Indicatori di qualità della fornitura
- Appendice 2 Capitolato Tecnico Descrizione dei profili professionali
- Appendice 3 Capitolato Tecnico Servizi di monitoraggio
- Offerta tecnica RTI
- Offerta economica del RTI

N.B.

La presente guida non intende sostituire né integrare la documentazione contrattuale sottoscritta fra le Parti. Pertanto, le informazioni in essa contenute non possono costituire motivo di rivalsa da parte delle Amministrazioni contraenti nei confronti del Fornitore e/o di Consip né possono ritenersi prevalenti rispetto alla documentazione contrattuale.

2. OGGETTO DEL CONTRATTO QUADRO

Il Contratto Quadro definisce la disciplina normativa e contrattuale, comprese le modalità di conclusione ed esecuzione dei singoli Contratti Esecutivi, relativa alla prestazione da parte del Fornitore dei Servizi di gestione delle identità digitali e sicurezza applicativa in favore delle Amministrazioni Beneficiarie, nonché di ogni attività prodromica necessaria e funzionale alla corretta esecuzione di detti Servizi oggetto del Contratto.

Il Contratto Quadro è stipulato e sottoscritto tra Consip Spa ed il Fornitore. I singoli Contratti Esecutivi, nell'ambito del Contratto Quadro, vengono stipulati tra l'Amministrazione ed il Fornitore.

La sottoscrizione del Contratto Quadro vale per il Fornitore quale proposta irrevocabile, per la stipula dei singoli Contratti Esecutivi e, pertanto, con la stipula dello stesso, il Fornitore si obbliga irrevocabilmente a prestare i seguenti servizi:

a) servizi di gestione delle identità digitali;

b) servizi di firma digitale remota compresa della fornitura di certificati e di timbro elettronico;

c) servizi di sicurezza;

d) servizio di monitoraggio in ambito sicurezza (eventualmente, ove offerto dal Fornitore ed accettato da Consip);

tutto nella misura richiesta dalle Amministrazioni Beneficiarie con i Contratti Esecutivi e relativi allegati, sino alla concorrenza dell'importo massimo complessivo pari ad Euro 600.000.000,00= (seicentomilioni/00), al netto dell'IVA.

I predetti servizi dovranno essere prestati con le modalità ed alle condizioni stabilite nel Contratto Quadro e relativi allegati, ivi inclusi il Capitolato Tecnico e relative Appendici e l'Offerta Tecnica, nonché quelle stabilite nei singoli Contratti Esecutivi.

Consip S.p.A. ha la facoltà di richiedere al Fornitore, nel periodo di efficacia del Contratto Quadro, l'aumento delle prestazioni contrattuali, nei limiti in vigore per la Pubblica Amministrazione, agli stessi patti, prezzi e condizioni stabiliti nello stesso e nei suoi allegati, e quindi di incrementare il predetto importo massimo complessivo fino a concorrenza di un quinto.

2.1. Durata del Contratto Quadro

Il Contratto Quadro ha una durata di 60 (sessanta) mesi decorrenti dalla data di sua sottoscrizione.

I singoli Contratti Esecutivi avranno una durata decorrente dalla data di stipula del Contratto Esecutivo medesimo e sino al massimo alla scadenza ultima del Contratto Quadro. Tuttavia, le singole Amministrazioni Beneficiarie potranno richiedere una proroga temporale dei singoli Contratti Esecutivi al solo fine di consentire la migrazione dei servizi ad un nuovo fornitore al termine del Contratto Quadro, qualora l'aggiudicazione del nuovo fornitore subentrante, come meglio specificato nel Capitolato Tecnico, non sia intervenuta entro i 3 (tre) mesi antecedenti la scadenza del presente Contratto Quadro; la durata massima della predetta proroga non può superare i 6 (sei) mesi.

Sempre con riferimento alla durata del Contratto Esecutivo, si precisa che:

Per tutte le tipologie di servizio, l'ordine di acquisto del servizio deve avere una durata minima di 12 (dodici) mesi, 24 (ventiquattro) per i servizi di Identity Provider (IdP). Il Fornitore ha facoltà di accettare ordini per durate inferiori a quanto sopra indicato.

a) per i servizi con modalità di erogazione "progettuale": la durata coincide con la quella prevista dal progetto/attività e non potrà, in ogni caso, prolungarsi oltre la durata del Contratto Quadro;

b) per i servizi con modalità di erogazione "continuativa": la durata non può prolungarsi oltre il termine di durata massima del Contratto Quadro; la finestra d'ordine termina in considerazione della durata minima di ciascun singolo servizio come stabilita nel Capitolato Tecnico. Oltre tale

termine, è facoltà del Fornitore accettare l'esecuzione dei servizi anche per durate inferiori, alle medesime condizioni contrattuali (considerando il rateo della periodicità offerta).

Per tutte le tipologie di servizio che prevedono, in chiusura di Contratto Esecutivo, un passaggio di consegne (verso il fornitore entrante o l'Amministrazione Beneficiaria) nel corso degli ultimi 3 (tre) mesi del Contratto Esecutivo saranno svolte anche le necessarie attività di phase out.

Qualora per qualsiasi motivo cessi l'efficacia del Contratto Quadro o del singolo Contratto Esecutivo, il Fornitore è tenuto a prestare la massima collaborazione, anche tecnica, affinché possa essere garantita la continuità dei servizi oggetto della prestazione contrattuale.

2.2. Condizioni di utilizzo del Contratto Quadro

Le Amministrazioni che sulla base della normativa vigente hanno l'obbligo o la facoltà di utilizzare il Contratto Quadro, nei limiti di capienza dell'importo massimo complessivo, aderiscono al Contratto Quadro, come già precedentemente detto, mediante la stipula di uno o più Contratti Esecutivi.

Per la fruizione dei servizi, le Pubbliche Amministrazioni Beneficiarie dovranno essere interconnesse direttamente alla rete del Sistema Pubblico di Connettività (SPC) - o altre strutture equivalenti individuate da Consip S.p.A. e/o dell'Agenzia per l'Italia Digitale (AgID) - attraverso uno o più Fornitori di connettività, o attraverso Enti autorizzati.

Il singolo Contratto Esecutivo si perfeziona alla data di sottoscrizione dello stesso da parte del Fornitore e dell'Amministrazione Beneficiaria e nel rispetto della normativa vigente.

La Consip S.p.A. non potrà in alcun modo essere ritenuta responsabile per il mancato perfezionamento dei Contratti Esecutivi da parte delle Amministrazioni Beneficiarie e non sussiste in capo a Consip S.p.A. alcuna verifica dei poteri di acquisto attribuiti alle Amministrazioni sottoscrittrici del Contratto Esecutivo.

Ove il Fornitore ritenga di non poter procedere alla stipula del Contratto Esecutivo in quanto proveniente da un soggetto non legittimato ad utilizzare il Contratto Quadro, in base alla normativa vigente, , dovrà, tempestivamente, e comunque entro due giorni lavorativi dal ricevimento del documento stesso, informare l'Amministrazione e Consip S.p.A., motivando le ragioni del rifiuto.

Qualora il Contratto Esecutivo non sia completo in ogni sua parte necessaria o allegata, lo stesso non avrà validità ed il Fornitore non dovrà darvi esecuzione; quest'ultimo, tuttavia, dovrà darne tempestiva comunicazione alla Amministrazione, entro e non oltre due giorni lavorativi dal ricevimento del documento.

Per effetto della stipula del Contratto Esecutivo, il Fornitore è obbligato ad eseguire la prestazione dei servizi richiesta, nell'ambito dell'oggetto contrattuale. Le Amministrazioni Beneficiarie provvederanno, prima della stipula del singolo Contratto Esecutivo:

i. alla nomina del Responsabile del Procedimento, ai sensi e per gli effetti dell'art. 10 del D.Lgs. n. 163/2006 e del d.P.R. n. 207/2010;
ii. alla nomina del Direttore dell'esecuzione, che dovrà essere soggetto diverso dal Responsabile del procedimento, qualora ricorrano le condizioni di cui all'art. 300, comma 2, del d.P.R. n. 207/2010;
iii. ai sensi e per gli effetti dell'art. 3 della Legge 13 agosto 2010 n. 136 e s.m.i., degli artt. 6 e 7 del Decreto Legge 12 novembre 2010, n. 187 nonché della Determinazione dell'Autorità per la Vigilanza sui Contratti Pubblici n. 8 del 18 novembre 2010, alla indicazione sul medesimo Contratto Esecutivo del CIG (Codice Identificativo Gara) "derivato" rispetto a quello del Contratto Quadro e da esse richiesto, nonché del CUP (Codice Unico Progetto) ove obbligatorio ai sensi dell'art. 11 della Legge 16 gennaio 2003 n. 3.

Nel Contratto Esecutivo le Amministrazioni Beneficiarie sono inoltre tenute ad indicare l'avvenuta registrazione o meno alla "Piattaforma per la certificazione dei crediti" di cui ai Decreti Ministeriali 22/05/2012 e 25/06/2012, in conformità a quanto previsto dai Decreti stessi. Le Amministrazioni

obbligate alla registrazione alla “Piattaforma per la certificazione dei crediti” di cui ai Decreti Ministeriali 22/05/2012 e 25/06/2012 dovranno pertanto prima dell’emissione Contratto Esecutivo essere in regola con gli obblighi di registrazione. Contratti Esecutivi sprovvisti dell’indicazione relativa all’avvenuta registrazione di cui sopra saranno ritenuti incompleti ai sensi e per gli effetti di quanto sopra previsto.

2.3. Contributo a carico delle Amministrazioni

Ai sensi dell’art. 4, comma 3-quater, del D.L. 6 luglio 2012, n. 95, convertito con modificazioni in legge 7 agosto 2012, n. 135, si applica il contributo di cui all’art. 18, comma 3, D.Lgs. 1 dicembre 2009, n. 177, come disciplinato dal D.P.C.M. 23 giugno 2010. Pertanto, le Amministrazioni Beneficiarie sono tenute a versare a Consip S.p.A., entro il termine di trenta giorni solari dalla data di perfezionamento del Contratto Esecutivo ,il predetto contributo nella misura prevista dall’art. 2, lettera a) o lettera b), del D.P.C.M. 23 giugno 2010, in ragione del valore complessivo del Contratto Esecutivo. In caso di incremento del valore del Contratto Esecutivo ai sensi del precedente articolo 8, quest’ultima è tenuta a versare a Consip S.p.A., entro il termine di trenta giorni solari dalla predetta approvazione, un ulteriore contributo nella misura prevista dall’art. 2, lettera c), del D.P.C.M. 23 giugno 2010.

Le modalità operative di pagamento del predetto contributo sono descritte sul sito internet della Consip S.p.A. (www.consip.it).

3. DESCRIZIONE DEI SERVIZI

Sono disponibili alle Amministrazioni Beneficiarie i servizi come di seguito descritti.

- Servizi per la gestione delle identità digitali, erogati in modalità «*as a service*», in conformità anche all'art. 64 del CAD;
- Servizi di firma digitale remota comprensiva della fornitura di certificati e 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*» che 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 delle Unità Locali di Sicurezza o strutture equivalenti delle Pubbliche Amministrazioni.

I servizi «*as a service*» vengono erogati dal Fornitore attraverso Centri Servizi, di proprietà di quest'ultimo, obbligatoriamente dislocati su sedi ubicate sul territorio comunitario ed in ottempera la Direttiva 95/46/CE del Parlamento e del Consiglio Europeo, oggetto di certificazione ISO 27001 e dei requisiti tecnici come richiesti nel Capitolato Tecnico. Il Fornitore è obbligato a trattare, trasferire e conservare le eventuali repliche dei dati conservati dai suddetti Centri Servizi sempre all'interno del territorio comunitario. In particolare il RTI utilizza i Centri Servizi dislocati sul territorio italiano e di seguito elencati:

- Centro servizi FASTWEB di Via Caracciolo, 51 CAP 20155 Milano;
- Centro servizi FASTWEB di Via Bernina, 6 CAP 20158 Milano;
- Centro servizi Selex ES di Via Puccini, 2 – CAP 16151 Genova;
- Centro servizi e-Security di Via Enrico Mattei, 21 - CAP 66100 Chieti.

I Centri Servizi e le relative macchine fisiche sono condivisi esclusivamente con altre Pubbliche Amministrazioni in una logica di «*community cloud*». I servizi "on premise" vengono erogati attraverso risorse professionali del Fornitore utilizzando le infrastrutture di proprietà dell'Amministrazione Beneficiaria.

In figura 1 è riportato il catalogo dei servizi disponibili.

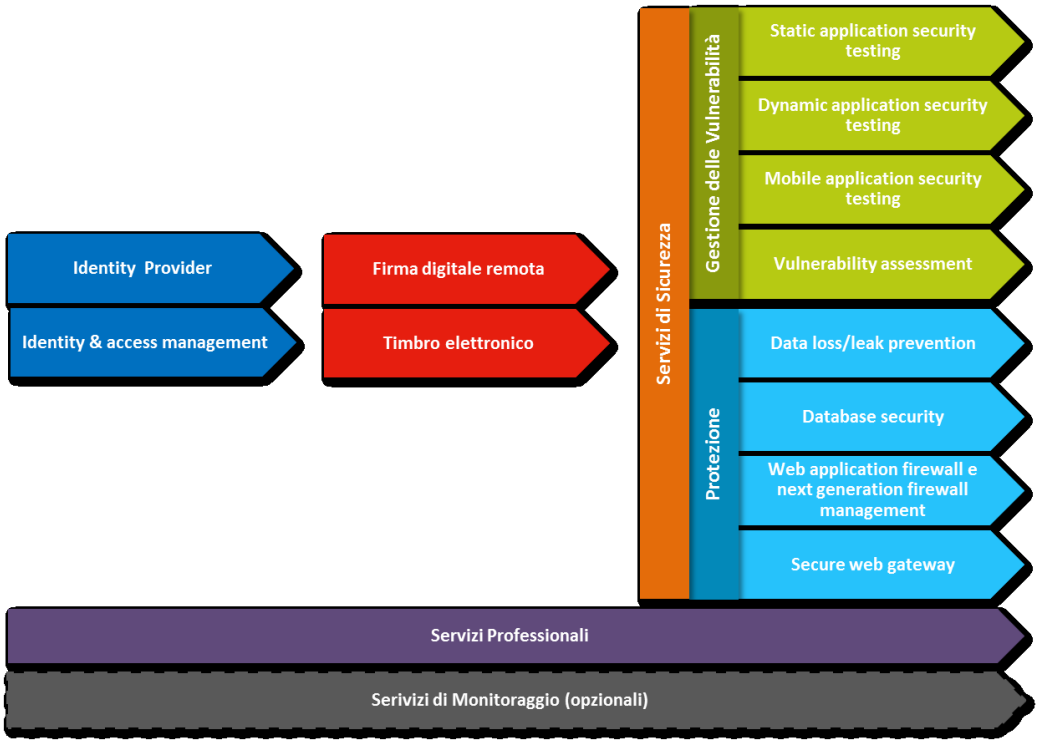


Fig. 1 Catalogo dei servizi

La descrizione dei servizi nella presente Guida è articolata secondo il seguente schema.

Introduzione	Architettura	Processi/Fasi	Flussi	Casi d'uso
Introduzione funzionale generale	Architettura tecnologica rappresentante: • Interfacce tra sistemi e utenti, • Dislocazione fisica • Flussi informatici • Tecnologie	Scomposizione delle metodologie adottate	Modellazione dell'erogazione dei servizi in fasi e attività	Descrizione testuale di dettaglio delle attività operative

Laddove possibile, gli argomenti sono stati trattati a livello generale nella macro famiglia e poi declinati nello specifico servizio, seguendo la seguente struttura ed in dipendenza dalla complessità (salvo le specificità dei Servizi Professionali e di Monitoraggio).

3.1. Servizio L2.S1.1 - Identity provider

Il modello Logico

Lo I&AM consiste di una composizione di persone, processi e tecnologie che permettono la gestione delle identità e l'accesso alle risorse basate sul politiche di business, regole e standard al fine di aumentare il livello di efficienza e di sicurezza.

Il modello di riferimento I&AM è composto da componenti dello I&AM stesso, da fonti autoritative e sistemi di destinazione, servizi di gestione dei dati e della sicurezza e servizi di infrastruttura condivisa.

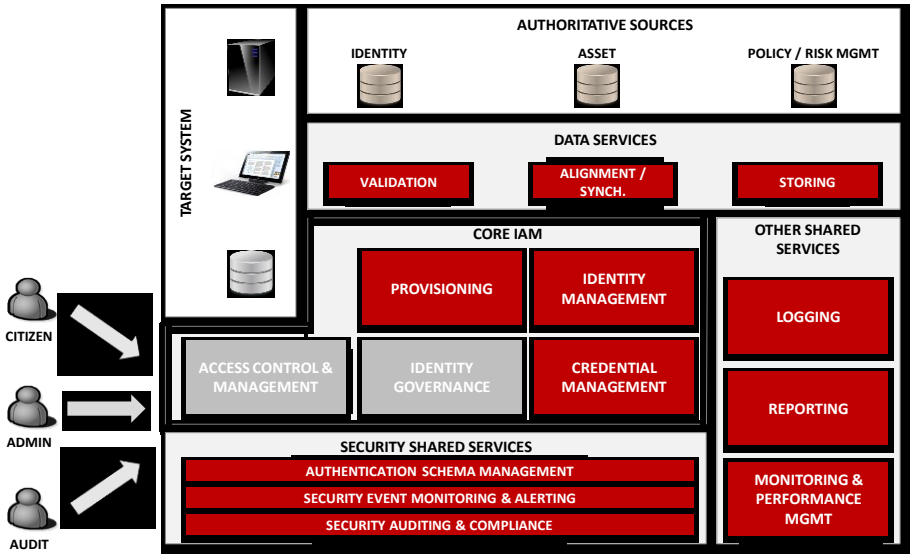


Fig. 2 Modello logico I&AM

Nei paragrafi seguenti sono descritte le componenti funzionali relative ai moduli inerenti il servizio di Identity Provider (in rosso).

Descrizione Componenti

Di seguito una breve descrizione delle principali componenti di una soluzione di Identity & Access Management:

- Core I&AM: è il core dei sistemi I&AM, responsabile di fornire le funzioni principali di Identity e Access Management. È principalmente costituito dai seguenti sotto-componenti:
  - Identity Management: è responsabile per la gestione del ciclo di vita delle identità digitali, gestisce la creazione, la modifica o la cancellazione delle identità, i loro attributi e il rapporto tra identità e attributi all'interno del sistema I&AM;
  - Identity Governance: è responsabile per la gestione del ciclo di vita dei ruoli e dei diritti di accesso per gestite le risorse di amministrazione;
  - Provisioning: è responsabile della propagazione delle identità e delle informazioni associate (attributi, i diritti di accesso, etc.) sui sistemi di destinazione;
  - Access Control & Management: è responsabile di gestire l'assegnazione dei diritti di accesso alle identità e l'esecuzione, in caso contrario la convalida, dei diritti di accesso su sistemi finali;
  - Credential Management: è responsabile per la gestione del ciclo di vita delle credenziali delle identità e la gestione dei relativi eventi, come la creazione, blocco, sblocco, etc.
- Security Shared Services: sono i servizi infrastrutturali di sicurezza, di supporto o utilizzati dal sistema I&AM. Si dividono in:

- Authentication Schema Management: gestisce gli schemi di autenticazione utilizzati sul sistema I&AM (gestione delle password, OTP Token, Smart Card, etc.);
- Security Event Monitoring & Alerting: raccoglie e monitora gli eventi di sicurezza ed i relativi sistemi di allarme;
- Security Auditing & Compliance: supporta il controllo della sicurezza e le attività di compliance.

- Other Shared Services: queste sono le applicazioni o i servizi che supporta il sistema I&AM:
  - Reporting: è responsabile di raccogliere le informazioni necessarie a fini amministrativi o di controllo;
  - Logging: è il componente responsabile di raccogliere, correlare e normalizzare tutte le informazioni gestite dal sistema I&AM per generare rapporti per uso amministrativo o di revisione contabile;
  - Monitoring & Performance Management: è responsabile di monitorare le prestazioni e il corretto funzionamento dei componenti del sistema I&AM a livello di applicazioni o di sistema;
- Authoritative Sources: questa componente raccoglie tutte le fonti che possono inserire dati all'interno del sistema I&AM (identity provider esterni, attribute provider, service provider, etc);
- Target System: ciascun sistema (directory, database sistema di gestione degli accessi web, applicazioni, endpoint, Portale dell'Identità Digitale, etc), in cui l'informazione disposizioni del sistema I&AM sulle identità digitali.

Identity Management

La componente Identity Management è l'unica responsabile per determinare l'identità sulla base di fonti esterne attendibili (fonti autoritative) o su un provider di informazioni (amministratori sul sistema Identity Management). La componente è progettata per:

- raccogliere informazioni sul sistema di identità;
- correlare e confrontare le informazioni di identità già esistenti sul sistema;
- provvedere e risolvere le differenze tra le variazioni e incongruenze nelle informazioni raccolte.

Il sistema d'identità definisce e gestisce sia manualmente sia automaticamente le identità e le relative informazioni correlate d'identificazione (attributi anagrafici, attributi giuridici, etc.).

Entità gestite

Nel sistema Identity Management ogni entry è considerata come un'identità digitale, che è la rappresentazione digitale di una persona fisica o giuridica o di un'entità virtuale (applicazione, servizio, etc.) definita e gestita all'interno nel sistema.

Le categorie d'identità che sono gestite dalla soluzione I&AM sono contenute nella tabella seguente:

Tipologie Identità	Descrizione
Cittadino - Persona Fisica	Identità associata al cittadino
Cittadino - Persona Giuridica	Identità associate a una società e rappresentata da una Persona Fisica
Amministrazione	Identità associate a un'entità virtuale (ad es. utenze per gestire le interazioni tra sistemi) o di amministrazione
Audit	Identità associate a personale di controllo e verifica dei dati

Tabella 1: Categorie Identità

Management Model

Le Identità digitali sono definite da informazioni recuperate da fonti autoritative (migrazione d'identità da Pubblica Amministrazione) o inserite direttamente nel sistema I&AM dalla sua interfaccia amministrativa (ad esempio, nel caso di una creazione identità da parte del cittadino stesso, il Portale dell'Identità Digitale).

Le Informazioni legate all'identità sono rappresentate nel sistema I&AM con una serie di attributi che possono essere recuperati direttamente dalla fonte autoritativa, dall'interfaccia amministrativa o generata dal sistema I&AM basandosi su regole definite. Questi attributi sono utilizzati per:

- identificare e descrivere univocamente l'utente (attributi identificativi - nome, cognome, codice di identificazione, ragione sociale, etc);
- l'autenticazione utente su sistemi legacy (ID univoco, password, etc);
- autorizzare l'uso sui sistemi terminali (titolo di lavoro, gruppo di appartenenza, settore, etc.)

Ogni utente ha un insieme minimo di attributi obbligatori (identificativi e parte dei non identificativi) e altri popolati in base alle esigenze specifiche, come ad esempio la necessità di accedere a un sistema specifico.

Identity Identification Schema

Uno schema d'identificazione rappresenta l'insieme delle informazioni utilizzate per identificare univocamente un soggetto e si compone di un insieme di attributi relativi all'utente / servizio.

Tale insieme di attributi sono scelti tenendo in considerazione le seguenti linee guida:

- zero o almeno estremamente bassa frequenza modifica durante l'intero ciclo di vita del soggetto
- zero o almeno estremamente bassa probabilità di collisione
- dizionario di possibili valori ben definito per impedire differenti interpretazione degli essi

Di conseguenza, lo schema d'identificazione è progettato per limitare il numero di collisioni all'interno di un dominio specifico; uno schema ben definito è un equilibrio tra il numero e la complessità delle informazioni raccolte, al fine di garantire l'unicità ed evitare duplicazioni.

Identity Status

Lo stato di un'identità è un attributo particolare che determina lo stato di un'identità digitale in un lasso di tempo definito (ad esempio attivo, sospeso). Quest'attributo cambia nel tempo, al fine di descrivere l'intero ciclo di vita delle identità ed è calcolato dal sistema I&AM in base a regole predefinite.

Attribute Authorities

Le fonti autoritative sono fonti di dati che contengono determinate informazioni sulla identità gestite. Possono essere sistemi in cui sono creati i valori degli attributi d'identità (ad esempio numero Carta Identità, Codice Fiscale, etc.) o sistemi in cui gli utenti devono andare a inserire le proprie informazioni (ad esempio, numero di cellulare).

Le fonti autoritative possono essere classificati in base ai seguenti criteri:

- Affidabilità delle informazioni gestite:
  - Trusted: se le informazioni *sono affidabili*, complete e corrette;
  - Untrusted: se le informazioni *non sono affidabili*, complete e/o corrette;
- Modello Autoritativo:
  - Un'unica fonte autoritativa: per ciascun'identità digitale c'è solo una fonte autoritativa attraverso la quale è possibile creare, modificare ed eliminare / disattivare l'identità;
  - Diverse fonti autoritative: le identità digitali possono avere più di una fonte autoritativa.

Nella presente piattaforma si considerano fonti autoritative affidabili e trusted che saranno definite da Consip successivamente.

Architettura Logica

Nella figura seguente è indicato il modello operativo logico del componente Identity Management.

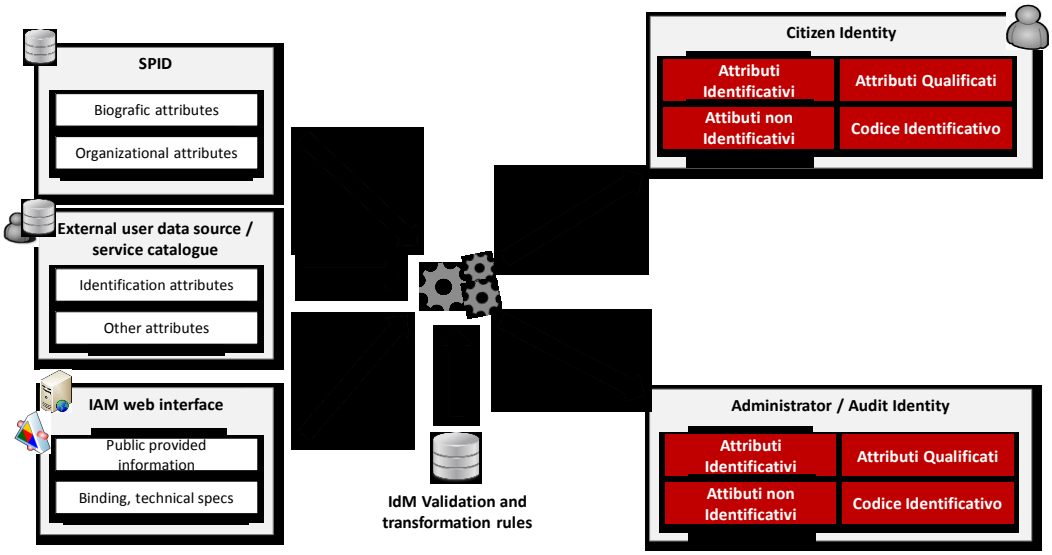


Fig. 3 Modello logico I&AM – Identity Management

Provisioning

La componente di provisioning è la responsabile per la fornitura delle identità e dei relativi permessi sui target system, in modo da consentire all'utente l'accesso richiesto alle risorse.

L'entità principale gestita dalla componente Provisioning è l'account, che è la trasposizione dell'identità nel target system.

Systems managed classification

I sistemi gestiti dalla componente Provisioning sono chiamati "*target system*" e possono essere di differente natura. Nella piattaforma corrente i "*target system*" oggetto di connessione sono i seguenti:

- Portale dell'Identità Digitale
- Portali delle P.A.

Architettura Logica

Nella figura seguente è rappresentato il modello operativo logico del componente Provisioning.

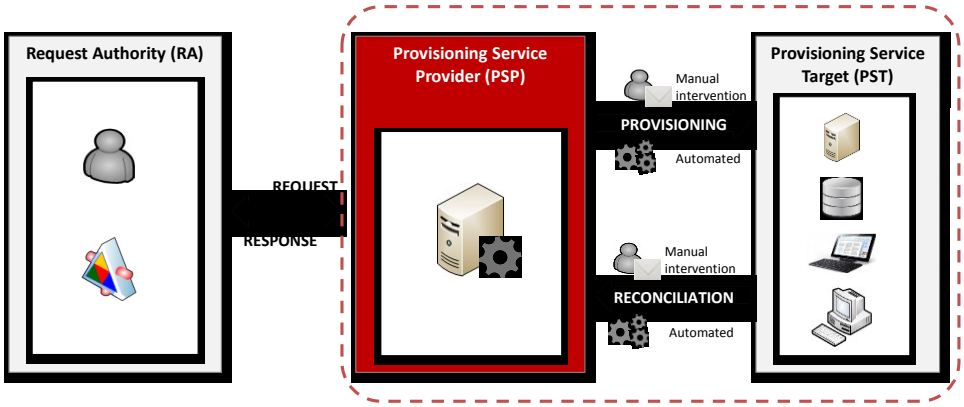


Fig. 4 Modello logico I&AM – Provisioning

Credential Management

La componente Gestione Credenziali si occupa delle seguenti attività:

- dare un interfaccia unica per altri componenti I&AM per la gestione e la creazione di diversi schemi di autenticazione (ad esempio OTP, certificato digitale, etc);
- implementare i processi per la gestione degli eventi (ad esempio creazione, modifica, blocco, etc) con la notifica degli stessi quando richiesto.

Di seguito gli schemi di autenticazione implementati:

Schemi di autenticazione
UserID + password
UserID + PIN + OTP
Certificato Digitale + PIN Certificate

Tabella 2: Schemi di autenticazione

Status and Password Synchronization

La componente Credential Manager ha lo scopo di propagare la sincronizzazione dello stato e delle password ai differenti target system che per esigenze particolari necessitano di mantenere in locale le credenziali e gli attributi anche parziali (delle single identità).

Strong Authentication

La Strong Authentication è una procedura di autenticazione che coinvolge almeno due delle tre categorie di schemi di autenticazione:

- "*Una cosa che conosci*", per esempio una password o il PIN.
- "*Una cosa che hai*", come un telefono cellulare, una carta di credito o un oggetto fisico come un token.
- "*Una cosa che sei*", come l'impronta digitale, il timbro vocale, la retina o l'iride, o altre peculiarità di riconoscimento attraverso caratteristiche uniche del corpo umano (biometria).

In accordo quindi alle direttive SPID è possibile definire i tre livelli di Strong Authentication secondo i seguenti paradigmi:

- *Primo Livello*: secondo lo standard ISO/IEC DIS 29115 corrisponde al Level of Assurance LoA2 che definisce un sistema di autenticazione a un fattore (ad es. la password)
- *Secondo Livello*: secondo lo standard ISO/IEC DIS 29115 corrisponde al Level of Assurance LoA3 che definisce un sistema di autenticazione a due fattori non necessariamente basati su certificati digitali
- *Terzo Livello*: secondo lo standard ISO/IEC DIS 29115 corrisponde al Level of Assurance LoA4 che definisce un sistema di autenticazione a due fattori basati su certificati digitali e le cui chiavi private seguono le direttive di custodia relative alla direttiva europea 1999/93/CE.

Logical architecture

Nella figura seguente sono evidenziate le principali interazioni tra la componente Gestione credenziali e le altre componenti logiche della soluzione I&AM.

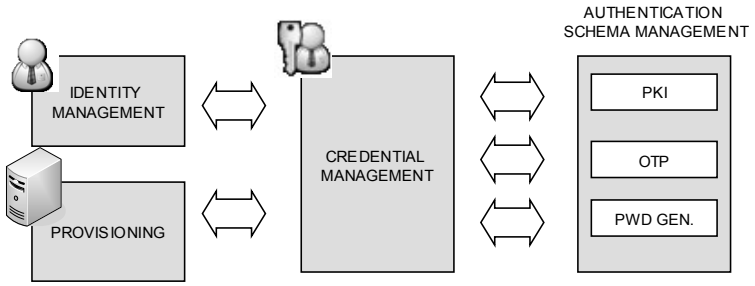


Fig. 5 Modello logico I&AM – Credential Management

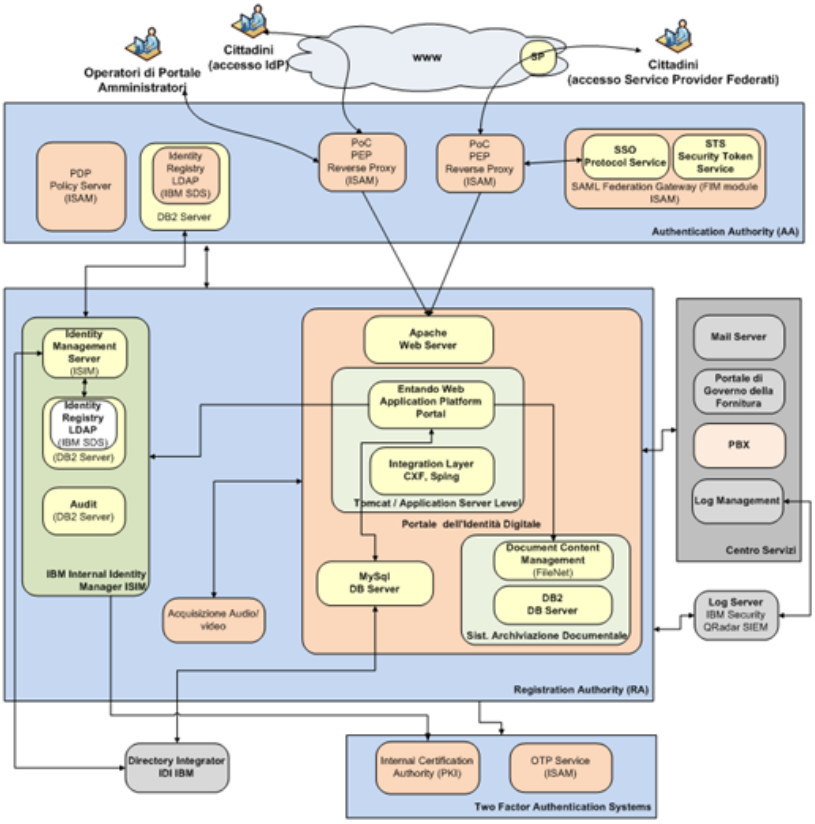


Figura 1 - Schema applicativo del sistema di IdP

Fig. 6 Schema sistema IdP

Tecnologie e prodotti di riferimento

Per la realizzazione del sistema di Identity Provider (IdP) sono utilizzati e personalizzati i seguenti prodotti:

- IBM Security Identity Manager for Web (ISIM), per le componenti di gestione identità digitali e relativo ciclo di vita. ISIM offre molte delle funzionalità attese di un prodotto di Identity e Governance Administration, tra cui richiesta di un utente, certificazione utenti, role mining, role modelling, analisi e report di conformità.
- IBM Security Access Manager for Web (ISAM), per le componenti di gestione utenti e profili e per la gestione delle policy di accesso;
- IBM Filenet, per l'implementazione del Sistema di gestione documentale. IBM FileNet P8 Content Manager è l'engine di gestione documentale e rappresenta il cuore della piattaforma di Enterprise Content Management di IBM. Esso gestisce la memorizzazione e la classificazione di contenuti in qualsiasi formato, mantenendo inalterato il contenuto stesso. Esso prevede la definizione di classi di documenti e di oggetti, secondo una struttura ad albero gerarchico: ogni classe eredita le proprietà (metadati e livelli di sicurezza e autorizzazioni) dalla classe gerarchicamente superiore, e definisce nuovi metadati specializzati. Il numero delle classi e la loro strutturazione non sono limitate a priori.
- Entando, per la componente Portale dell'Identità Digitale. Entando è una piattaforma portal leader e Open Source che consente la realizzazione di soluzioni interattive, user-centric e fruibili da diversi device. Come CMS la piattaforma offre nativamente una struttura a widget che consente una collocazione all'interno dello spazio utente delle differenti funzioni necessarie all'utilizzatore personalizzati grazie alla user experience.

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

L'Access Manager rappresenta un componente software che regola l'accesso alla risorsa gestita da un Service Provider (SP).

Il servizio I&AM ha quindi come finalità primaria la gestione delle attività d'identificazione ed autenticazione tramite Identity Provider accreditati e, in completa autonomia, la gestione delle autorizzazioni propedeutiche all'accesso da parte di utenti esterni (cittadini) ai portali delle Pubbliche Amministrazioni o ai servizi da essa erogati in rete garantendo piena compatibilità con quanto previsto dall'articolo 17-ter del DL 69 del 21/6/2013.

Al fine di rispondere ai requisiti SPID definiti (1)[1], il servizio I&AM implementa la specifica SAML nella parte relativa al Service Provider, permettendo quindi alle Pubbliche Amministrazioni che espongono servizi web per il cittadino di aderire alle regole tecniche definite da SPID senza dover realizzare e/o modificare le proprie infrastrutture tecnologiche. Il servizio mette quindi a disposizione delle PA una componente tecnologica in ambiente cloud che, inserendosi tra il cittadino e le risorse dell'Amministrazione, gestisce le richieste e, operando gli opportuni passi di identificazione e autorizzazione, permette l'accesso alla risorsa richiesta.

Secondo le regole tecniche SPID, il flusso tipo implementato è rappresentato nel diagramma seguente:

ID	DESCRIZIONE
1	Richiesta di servizi: il titolare dell'identità digitale richiede accesso ad un servizio per via telematica connettendosi al sito del fornitore dei servizi
2	Inoltro verso Identity provider: il fornitore dei servizi rimanda il titolare dell'identità digitale presso il proprio gestore dell'identità digitale
3-4	Richiesta e verifica credenziali: il gestore dell'identità digitale verifica l'identità del soggetto sulla base di credenziali da lui accettate ed esibite dal soggetto
5	Risposta: 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
6-7	Richiesta e verifica attributi: il fornitore dei servizi può avere la necessità di verificare ulteriori attributi presenti nel profilo utente e richiesti dalle policy di sicurezza che regolano l'accesso al servizio per cui, in questo caso, dopo aver individuato il gestori di attributi qualificati in grado di attestarne la validità, inoltra a questi richiesta di certificazione presentando i riferimenti dell'identità digitale per la quale si richiede la verifica. Il risultato della richiesta è l'emissione di una certificazione (asserzione di attributo SAML) emessa a favore del fornitore dei servizi
8	Verifica richiesta: il fornitore dei servizi raccolte tutte le certificazioni (asserzioni SAML) di identità e di attributi qualificati presenti nel profilo e necessarie per l'applicazione delle policy di sicurezza relative al profilo utente del soggetto richiedente l'erogazione del servizio può verificarne la sussistenza e decidere se soddisfare o rigettare la richiesta di servizio avanzata

[1] AgID – Regolamento recante le modalità attuative per la realizzazione dello SPID (art. 4, comma 2, DPCM 24/10/2014)

Nella figura seguente viene rappresentato come il servizio di Identity & Access Management proposto interagisce con tutti gli altri elementi e attori dell'intero processo di autenticazione e autorizzazione.

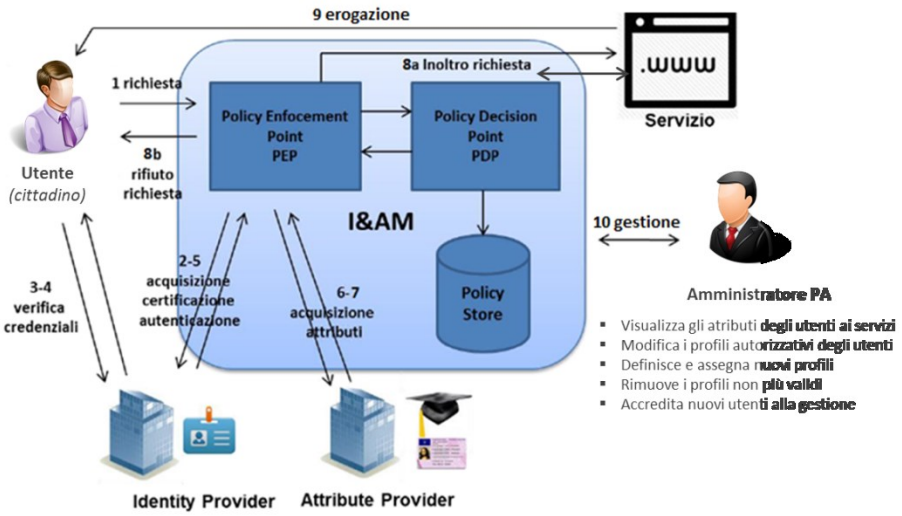


Fig. 7 Servizio di I&AM

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, e garantire la compatibilità con quanto previsto dall'articolo 17-ter del DL 69 del 21/6/2013.

Il servizio di I&AM, dovrà consistere nella gestione delle attività di identificazione, autenticazione ed autorizzazione all'accesso ai *portali* delle Amministrazione orientato ai propri utenti esterni.

Secondo il classico modello logico il sistema dovrà prevedere due sottosistemi:

- *Policy Enforcement*, che si interfaccia con il mondo esterno (*Identity Provider* e *Attribute Authority*) al fine di ricevere le richieste per l'applicazione delle policy di sicurezza associate alle risorse.

- *Policy Decision*, in grado di accedere ai i profili degli utenti e alle policy di sicurezza associate alle risorse per la verifica della legittimità della richiesta.

Per l'autenticazione dei propri utenti il servizio potrà fare ricorso ad un *Identity provider* esterno all'Amministrazione.

Per la verifica degli attributi associati al profilo di un utente, esterni all'Amministrazione, il servizio dovrà fare ricorso ad *Attribute Authority* esterne.

Il servizio comprende la gestione delle policy di accesso ai servizi e la gestione del ciclo di vita dei profili utente.

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

Il gestore del servizio di I&AM prevede, su richiesta, la presa in carico e la migrazione dei profili utente gestite dall'amministrazione.

Caso d'uso

ID	DESCRIZIONE
1	L'utente (cittadino), che vuole utilizzare i servizi resi disponibili da un'Amministrazione, si collega al portale della PA e iniziare la navigazione
2	Il Point of Contact (PoC) intercetta la richiesta dell'utente di accedere a risorse protette da autenticazione e gli presenta la lista degli IdP federati, tra i quali l'utente può individuare e selezionare il proprio
3	L'IdP, a seconda del livello di autenticazione richiesto, presenta all'utente il challenge di autenticazione (utente+password, oppure utente+password+OTP, oppure utente+password+certificato digitale) che inserirà le proprie credenziali.
4-7	Ad autenticazione avvenuta, l'IdP emette un'asserzione di SAML Authentication Response che viene inviata al Point of Contact e si verificano i seguenti tre casi: ○ Creazione Utente - nel caso di utente non registrato all'interno del servizio I&AM, si provvede alla creazione automatica del nuovo utente sul Policy Store ○ Aggiornamento Attributi - se l'utente è già presente, gli attributi dell'identità ricevuti dall'IdP disponibili dalla SAML Assertion sono aggiornati ○ Arricchimento (opzionale) – viene composta una query per le Attribute Authority qualificate. Tale passo è funzionalmente eseguito (indicato quindi come opzionale) se e solo se presenti eventuali attributi da validare tramite Attribute Authority certificate AgID
8	In base alla risposta dell'IdP, il Poc, tramite il Policy Decision Point, decide se concedere l'autorizzazione all'utente. In caso di permessi insufficienti il flusso s'interrompe senza erogazione del servizio.
9	Il PoC incapsula gli attributi dell'utente e i profili applicativi, li invia all'applicazione che erogherà il servizio
10	L'Amministratore della PA, tramite interfaccia Web, gestisce i profili utente, dalla loro creazione, modifica e rimozione.

Tecnologie e prodotti di riferimento

In questo paragrafo è descritta l'architettura applicativa del sistema di I&AM. Il componente principale di questo sistema è rappresentato dal prodotto IBM Security Access Manager (ISAM). Di seguito le componenti dell'architettura applicativa che costituiscono la piattaforma di erogazione servizio:

SAML Federation Gateway: realizzato tramite la soluzione IBM Security Federated Identity Manager, fornisce lo strato applicativo necessario per la gestione dei servizi utili alla realizzazione delle dinamiche dello standard SAML. Specificatamente il modulo SSO Security Service garantisce le primitive necessarie per allestire un Single Sign On federato e quindi il "trust" tra partner qualificati come Identity Provider o come Service Provider; il modulo STS Security Token Service consente la conversione di token di sicurezza, in particolare l'asserzione SAML proveniente dall'IdP nel token ISAM direttamente gestibile dal Web Reverse Proxy ISAM.

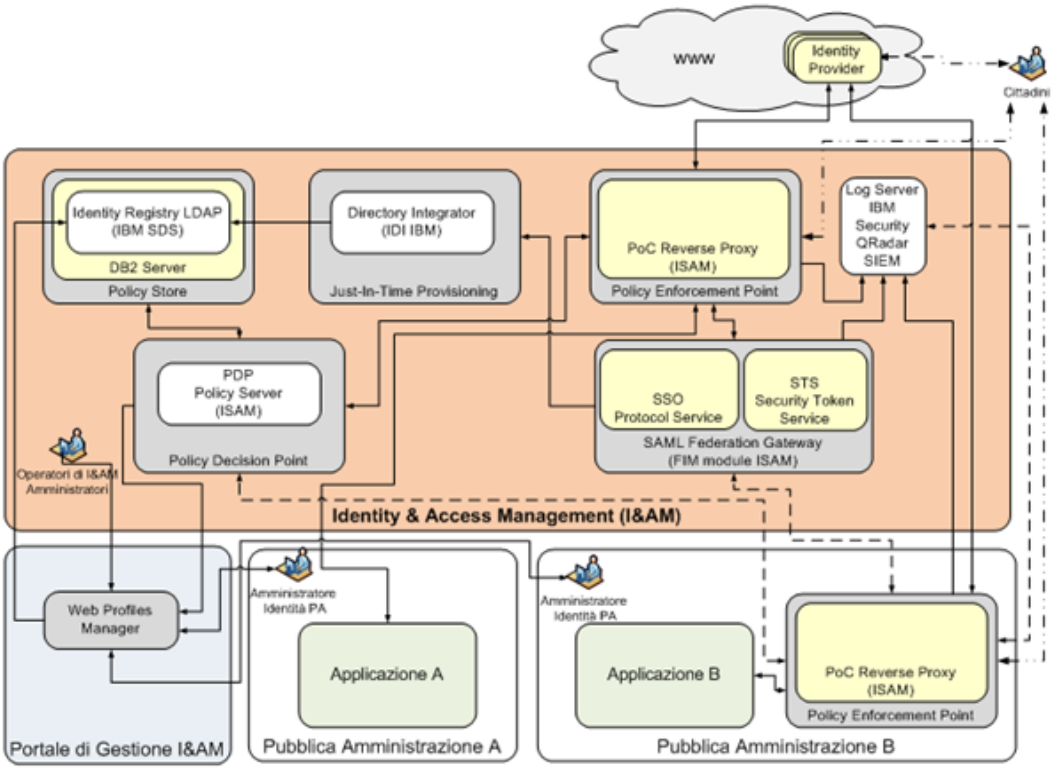


Figura 1 - Schema applicativo del Sistema di I&AM

Fig. 8 – Schema applicativo I&AM

Policy Enforcement Point (PEP): verifica le credenziali e applica le politiche di controllo relative alle richieste di accesso degli utenti, gestendo la sessione Web nel suo intero ciclo di vita. È realizzato tramite il componente WebSEAL del IBM Security Access Manager (ISAM) e applica le politiche di controllo accessi alle applicazioni Web di back-end delle Pubbliche Amministrazioni. Nell'ambito IA&M si applicano le seguenti funzioni:

- Autorizzazione: fornisce autorizzazione a "Grana Grossa" (a livello di URL) per l'accesso alle risorse; accede alla User Directory e al database delle policy per reperire gli attributi utente e decidere se consentire o negare gli accessi
- Session Management: per la gestione delle sessioni utente (controllo del tempo di vita della sessione, logout, ecc.) e le configurazioni in cluster (scalabilità orizzontale, HA)
- Single Sign-On: ISAM può integrare in vario modo le applicazioni di back-end e fornire il Web SSO; per ogni sistema di back-end viene configurata una "junction" che regola come le informazioni sull'utente vengono trasmesse all'applicazione: via HTTP header, BA authentication, Kerberos, LTPA, TAI, form authentication, etc.
- Audit: traccia tutte le richieste ricevute e processate ed è pienamente configurabile (livello di dettaglio dell'audit, periodo di retention, ecc..); può inviare gli eventi registrati ad un SIEM esterno
- Load Balancing: ISAM include una componente di Load Balancer allo scopo di semplificare le configurazioni in cluster (scalabilità, HA) e ridurre le dipendenze da componenti esterni di infrastruttura.

Policy Store: è realizzato mediante IBM Security Directory Server (SDS) e registra su un server LDAP le utenze associate all'identità digitale con gli eventuali gruppi ed attributi. Tali informazioni sono utilizzati dal PDP per validare le eventuali scelte autorizzative che vengono applicate dal PEP.

Policy Decision Point (PDP): le politiche di accesso sono governate centralmente attraverso il Policy Server dell'ISAM, che costituisce funzionalmente il "Policy Decision Point" della soluzione. Il Policy Server gestisce il Policy Store e permette agli amministratori del sistema:

- la definizione di utenti, gruppi e risorse
- la configurazione delle policy (ACL, POP, authorization rules) che regolamentano l'accesso alle risorse
- La distribuzione delle policy ai Reverse Proxy.

Just-in-time Provisioning: implementato essenzialmente dalla soluzione IBM Directory Integrator (IDI), è il tool programmabile per lo scambio di dati tra meta-directory interconnesse per mezzo di connettori predefiniti. Nello specifico la sua funzione è di implementare la logica di "Just-in-Time Provisioning" necessaria per la creazione dell'utente I&AM, nel dominio di sicurezza ISAM, in seguito alla prima autenticazione di una identità ed all'aggiornamento degli attributi contenuti all'interno delle asserzioni SAML ricevute dall'IdP. Lo stesso strumento IDI è utilizzato per il popolamento massivo, a tempo zero, del Policy Store nel momento in cui un'Amministrazione viene accreditata al servizio I&AM.

Web Profile Manager: la gestione delle autorizzazioni fatta a livello di URL (HTTP header) è resa disponibile attraverso le funzioni contenute all'interno del "Web Profile Manager" accessibile sia mediante l'infrastruttura dedicata al Sistema di Gestione e Governo della Fornitura della Fornitura sia dagli strumenti nativi delle soluzioni utilizzate.

Mediante tali funzionalità l'Amministratore di una PA e/o gli operatori RTI potranno gestire lo spazio di accesso a un'applicazione e gli utenti che accedono all'applicazione stessa.

L'Amministratore locale della PA avrà la possibilità di accedere a una interfaccia web con visibilità dei soli dati degli utenti profilati per applicazioni erogate dalla propria Amministrazione e per le quali è referente a livello di Contratto Esecutivo. Egli avrà facoltà di ricercare le proprie utenze nell'Identity Registry I&AM, di visualizzarne gli attributi identificativi, non identificativi e qualificati, già compilati dall'IdP e dal SP dello I&AM (gli attributi non saranno pertanto modificabili), e procedere autonomamente all'assegnazione dei profili applicativi.

L'operatore di RTI avrà la possibilità di dichiarare/definire nuovi profili applicativi e utilizzarli nelle assegnazioni, provvedendo a verificare la coerente mappatura sul profilo applicativo reale nell'applicazione target. Analogamente l'operatore di RTI avrà la possibilità di definire particolari ACL per un controllo capillare delle autorizzazioni sulle singole URL dell'applicazione web PA.

Le funzionalità disponibili su tale applicazione sono quindi le seguenti:

- Ricerca di utente accreditato all'Amministrazione, visualizzazione dei suoi attributi identificativi e non, qualificati e profili applicativi correntemente assegnati;
- Modifica dell'assegnazione dei profili applicativi;

Profilatura nuovo utente. In questa fase sarà necessario specificare solamente un identificativo univoco (esempio: codice fiscale). Se già presente nello I&AM, l'utente è visualizzato con tutti i suoi attributi e può essere aggiornato con l'assegnazione di nuovi profili. Se non ancora presente, l'utente è creato senza gli attributi personali, che saranno comunque valorizzati dall'IdP e dall'SP alla prima richiesta di accesso.

3.3. Servizio L2.S2.1 – Firma digitale remota e Sigillo elettronico

La Firma Digitale è l'equivalente informatico di una tradizionale firma autografa apposta su carta e consente quindi alle Amministrazioni di dare efficacia probatoria ai documenti informatici firmati digitalmente.

Possiede le seguenti caratteristiche:

- autenticità: la firma digitale garantisce l'identità del sottoscrittore

- integrità: la firma digitale assicura che il documento non sia stato modificato dopo la sottoscrizione
- non ripudio: la firma digitale attribuisce piena validità legale al documento, pertanto il documento non può essere ripudiato dal sottoscrittore

Per generare una firma digitale è necessario utilizzare una coppia di chiavi digitali asimmetriche attribuite in maniera univoca ad un soggetto, detto titolare. La chiave privata è conosciuta solo dal titolare ed è usata per generare la firma digitale da apporre al documento. Viceversa, la chiave da rendere pubblica è usata per verificare l'autenticità della firma. L'impiego della Firma Digitale pertanto, permette di snellire significativamente i rapporti tra Pubbliche Amministrazioni, i cittadini o le imprese, riducendo drasticamente la gestione in forma cartacea dei documenti, proprio come indicato nelle Linee Guida per l'utilizzo della Firma Digitale, emanate da AgID (Agenzia per l'Italia Digitale, ex DigitPA)

Nella sezione successiva vengono schematizzate le tipologie di Firma digitale oggetto del servizio.

Firma Digitale Remota

La Firma Remota è una modalità di firma digitale che, pur garantendo lo stesso grado di sicurezza e gli stessi effetti di legge, ha il certificato qualificato con relativa chiave privata residente su un dispositivo remoto (HSM).

Accedendo al Portale di firma e timbro della PA, l'utente deve autenticarsi al servizio utilizzando un sistema di autenticazione a due fattori (conoscenza e possesso):

- Il primo fattore è costituito da una password statica conosciuta solo dall'utente;
- il secondo fattore è costituito da un codice dinamico OTP (One-Time Password) che viene generato dall'utente grazie al possesso di un dispositivo (se hardware consegnato dall'operatore, se software scaricato ed installato sullo smartphone dall'utente) configurato in modo specifico e univoco per l'utente.

In aggiunta viene reso disponibile il servizio di Verifica della Marca temporale remota.

Sigillo elettronico

Con sigillo elettronico si intende un servizio perfettamente analogo a quello della firma digitale remota, con la differenza che il certificato digitale è rilasciato ad un soggetto giuridico anziché ad una persona fisica. Il servizio di sigillo elettronico è disponibile esclusivamente in modalità con SLA garantito.

Firma Digitale Remota Automatica

La Firma Automatica è una modalità di firma digitale che consente di firmare uno o più documenti in maniera automatica senza che il titolare della firma debba visualizzarli e sottoscriverli uno ad uno. Anche in questo caso il certificato qualificato con relativa chiave privata è residente su un dispositivo remoto (HSM).

Il servizio è disponibile tramite i WEB service messi a disposizione dal sistema.

Firma Digitale Remota Verificata

La Firma Remota Verificata è una modalità di firma digitale remota che consente di ricevere un documento firmato digitalmente in cui la validità del certificato qualificato è stata già verificata al momento dell'apposizione della firma da parte del titolare del certificato stesso. Anche in questo caso il certificato qualificato con relativa chiave privata è residente su un dispositivo remoto (HSM).

Architettura

Tutti i sistemi a supporto del servizio di "Firma Digitale Remota" sono ospitati e gestiti nei Centri Servizi del RTI, ad eccezione dei servizi di emissione e gestione certificati in quanto, per rispetto della normativa, devono essere erogati da un certificatore accreditato.

I sistemi ospitati dai Centri Servizi del RTI interagiscono con i seguenti attori:

- amministratori dell'RTI, ossia coloro che censiscono ed abilitano le singole PA alla richiesta ed emissione di certificati di firma remota.
- referenti PA, ossia coloro che censiscono e gestiscono gli operatori di registrazione (ODR) afferenti alla PA medesima.
- operatori di registrazione (ODR), ossia coloro che sono incaricati - dalle proprie Amministrazioni di appartenenza - di svolgere le attività di identificazione e registrazione (attraverso il portale di emissione e gestione della firma) degli utenti di firma digitale remota;
- Certification Authority (per la richiesta e gestione dei certificati).

Lo schema mostra l'architettura logica del sistema di firma remota proposto, il quale sarà fruibile in modalità "as a service".

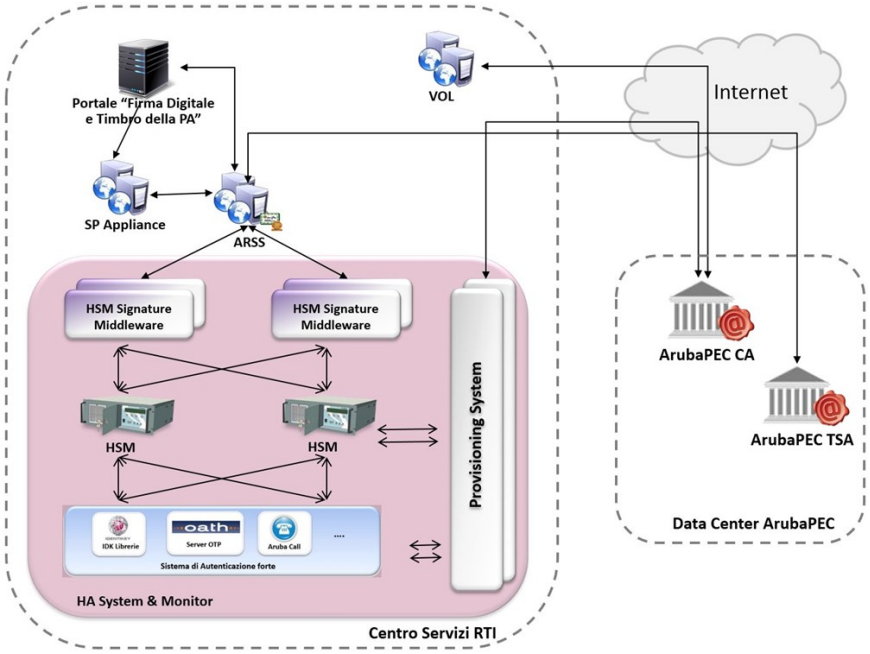


Fig. 9 Architettura servizio "firma digitale"

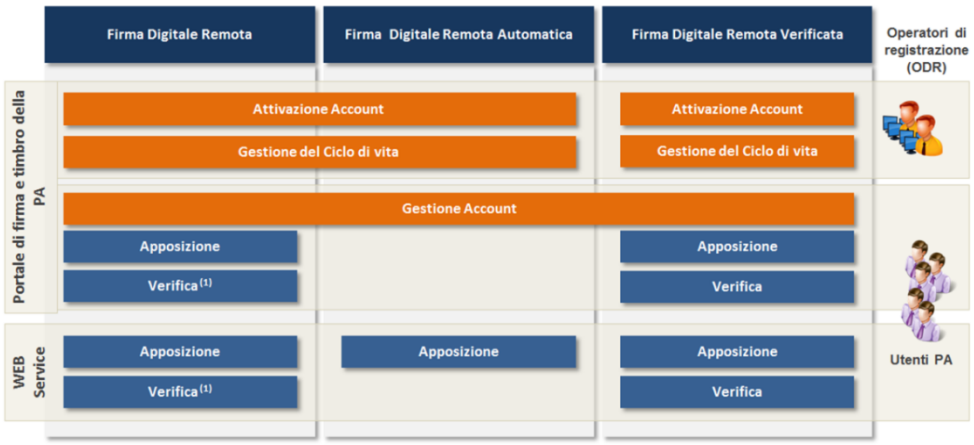
La soluzione si compone dei seguenti componenti architetturali:

- HSM – apparato crittografico hardware a norma di legge all'interno del quale sono generate e custodite le chiavi e i certificati digitali
- HSM Signature Middleware – software di gestione di tutte le richieste da e verso gli HSM
- Sistema di Autenticazione Forte – è formato da varie componenti che possono essere interfacciate agli HSM e che consentono un'autenticazione forte del Titolare per lo sblocco delle varie operazioni crittografiche sull'HSM stesso
- Provisioning System - software che orchestra il dialogo con gli HSM, col Sistema di Autenticazione Forte e con la Certification Authority (CA) ai fini dell'attivazione delle utenze di firma digitale remota
- HA System & Monitor - software, trasversale all'intero sistema di firma digitale remota, che consente il monitoraggio del sistema e che implementa tutte le funzioni necessarie a garantire l'alta disponibilità del servizio (fault tolerance)

- Aruba Remote Signing Server (ARSS) – componente software che espone tutte le funzionalità di firma remota con protocollo SOAP, consentendo quindi una semplice integrazione con gli applicativi ed i sistemi informativi delle PA (per integrazione diretta con applicazioni delle PA). Normalmente installato in configurazione ridondata al fine di garantire la continuità del servizio.
- SP Appliance – Componente software (a essa vi si può riferire anche attraverso il termine: SDS (Secure Doc Server)) che espone il servizio di Timbro digitale, secondo le modalità descritte nello specifico documento
- Portale di Firma Digitale e Timbro della PA (di seguito, per semplicità, anche "portale"): è un insieme di strumenti, fruibili da interfaccia web, che consentirà alla pubbliche amministrazioni di attivare e gestire il ciclo di vita del servizio di firma digitale remota/automatica e dei relativi certificati digitali. Apposite funzioni di profilazione consentono il censimento e la gestione di una o più unità operative (Enti) tra loro distinte. All'interno delle stesse l'operatività può essere distribuita su uno o più uffici.

Casi d'uso

Nello schema vengono riportati i processi afferenti il servizio che in questa presentazione sono declinati a Casi d'uso della Firma digitale remota con i rispettivi attori e fruitori coinvolti.



Tecnologie e prodotti di riferimento

In questo paragrafo viene riportato lo schema applicativo per l'erogazione del servizio di Firma Digitale, che raccoglie tutte le funzionalità necessarie per la Firma Digitale Remota, la Firma Automatica e le verifiche di: firme, marcature temporali o timbri.

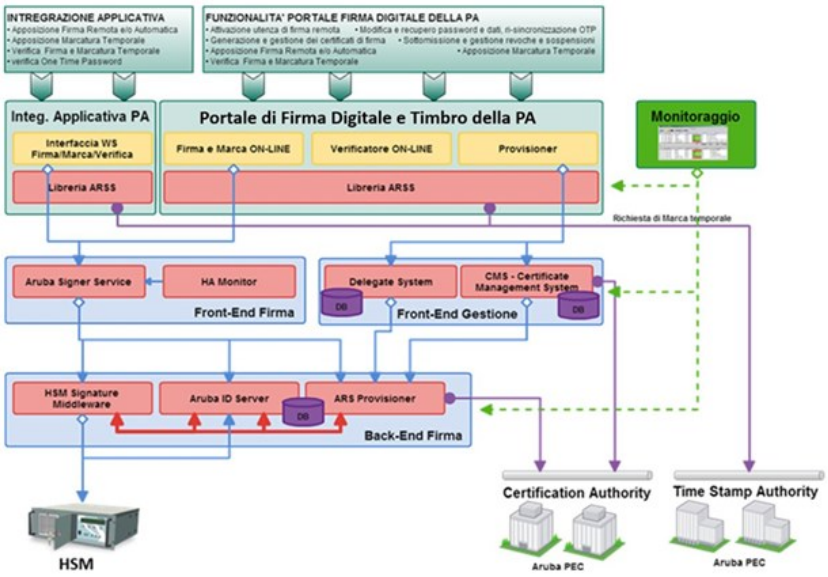


Figura 1 - Schema applicativo del Servizio di Firma digitale

Fig. 10 Schema applicativo servizio "firma digitale"

Le componenti SW su cui l'infrastruttura si basa sono di seguito descritte secondo il macrosistema di appartenenza:

Architettura Software di Firma Remota

- Integrazione applicativa – si tratta di componenti che espongono apposite interfacce Web service attraverso le quali è possibile effettuare tutte le operazioni di firma e relativa verifica, quest'ultima anche per la marcatura temporale. Queste componenti, installate presso il Centro Servizi oppure presso la sede ove operano le applicazioni che vi si interfacciano, hanno l'obiettivo di ottimizzare tutte le operazioni coinvolte. ARSS include le librerie crittografiche e provvede a far dialogare, su canale sicuro di comunicazione (HTTPS) con mutua autenticazione, le applicazioni ospitate nel Centro Servizi con il sistema di firma remota, esponendo verso di esse le funzionalità di firma digitale (ed altri servizi collegati, es. verifica firma, cifratura/decifratura, ecc.). Nel caso di operazioni relative alla marcatura temporale, ARSS si interfaccia direttamente con i servizi standard che erogano la Time Stamping Authority di Aruba PEC; la componente dedicata alla validazione effettua direttamente tutte le verifiche interrogando i servizi esterni necessari (CRL, VA, OCSP) delle CA coinvolte nella verifica.
- Portale di Firma Digitale della PA – Servizio web che s'interfaccia con l'infrastruttura di firma remota consentendone l'attivazione, l'utilizzo e la gestione del ciclo di vita del certificato, nonché della credenziale titolare ad esso associata.

Per il monitoraggio dell'infrastruttura verranno fornite apposite chiamate applicative, richiamabili dalla piattaforma di monitoraggio prescelta: queste, attraverso un insieme di procedure che emulano le operazioni effettuate dalle applicazioni o dagli utenti tramite il portale, verificano il corretto funzionamento dei servizi segnalando eventuali anomalie totali del servizio o anche parziali, cioè di una singola componente.

Le componenti core dell'infrastruttura di Firma remota, che includono anche i servizi di firma automatica e Strong Authentication sono di seguito elencate:

Front-end di Firma

- Aruba Signer Service – Componente che, installato presso il Centro Sevizi del RTI, espone i servizi di firma. Tutte le richieste, opportunamente ottimizzate a monte dagli ARSS, vengono

collassate sul front-end, che le smista opportunamente verso la piattaforma di back-end sia per le operazioni di firma che per il servizio di Strong Authentication.

- HA Monitor - Componente software, specificatamente sviluppato per monitorare il funzionamento del sistema: è formato da vari moduli che interagiscono con le varie componenti del Sistema di Firma Digitale Remota al fine di verificare lo stato dell'intero sistema e la disponibilità del servizio erogato. In caso di failure, l'HA monitor rileva il malfunzionamento del componente e provvede alla notifica agli amministratori del sistema tramite vari canali di comunicazione opportunamente configurati.

Front-end di Gestione

- Delegate System – Il pannello di gestione delle deleghe serve per implementare correttamente il servizio di firma automatica consentendo agli utenti titolari dei certificati di firma automatica di "delegare" alcune applicazioni a firmare con la propria credenziale. L'utente, accedendo in maniera forte al pannello, avrà la possibilità di abilitare/disabilitare l'utilizzo del certificato di firma automatica da parte delle applicazioni delegate (switch on/off).
- Certificate Management System (Portale di emissione e gestione della firma): è la porta di accesso verso i "motori di CA" e supporta la generazione e gestione dei certificati (emissione, revoca, ricerca e reporting, ecc.); inoltre espone Web Services che consentono ai back-end di firma di richiedere ed ottenere le informazioni necessarie e i certificati pubblicati durante le fasi di provisioning automatizzate. Attraverso il portale si ha una chiara visione dei certificati emessi per ogni singolo ente ed è possibile seguirne il ciclo di vita. I dati relativi alle emissioni effettuate possono essere esportati in formato CSV, in maniera totale o per Ente.

Back-end di Firma

- HSM Signature Middleware - Componente software installato sul Back End al quale viene demandata la completa gestione delle connessioni verso le funzionalità di firma proprie dell'HSM. Il HSM Signature Middleware è in grado, oltre che di gestire più sessioni contemporanee, di bilanciare il carico sugli HSM in esso configurati consentendo una scalabilità orizzontale e verticale dell'infrastruttura.
- Aruba ID Server – implementa sia le funzionalità di Strong Authentication per il servizio di firma remota che di gestione della stessa.
- ARS Provisioner - Il Provisioning System è la componente software che gestisce le fasi necessarie all'attivazione del Servizio di Firma Remota. Si interfaccia con i sistemi per la verifica delle credenziali di attivazione, gestendo il dialogo con le componenti tra cui l'HSM Cosign, per la creazione (laddove richiesto) degli account e la Certification Authority per la generazione dei certificati digitali.

Nella figura sono anche evidenziate le componenti software che necessitano di un Database Management Systems (DBMS): si tratta in tutti i casi di database relazionali necessari per il funzionamento dei "motori di CA", quindi destinati a contenere tutte le informazioni di servizio relative alle CA, i profili dei certificati, i certificati emessi, le CRL, gli audit log, ecc. Come DBMS è possibile utilizzare anche soluzioni open source a condizione che abbiano un livello adeguato sia di affidabilità che prestazionale. I DBMS rientrano comunque nella lista di quei software di base/Middleware che sono di pertinenza del Centro Servizi e che verranno descritti nell'apposito capitolo.

3.4. Servizio L2.S2.2 – Firma digitale con smart card

La fruizione del servizio di firma digitale remota, necessita come pre-requisito della connessione, tramite rete internet o SPC, all'infrastruttura di firma remota così da consentire ai titolari dei certificati di firma di poter procedere alla sottoscrizione dei documenti informatici. Tale necessità è

intrinseca nel servizio di firma remota essendo quest'ultimo caratterizzato dal fatto di gestire i certificati di firma digitale centralmente, su dispositivi HSM conformi alla vigente normativa.

In determinati scenari, però, le Amministrazioni potrebbero avere l'esigenza di introdurre, nei loro processi o applicazioni, le funzionalità di firma digitale in modalità off-line, senza quindi la possibilità di connessione con l'infrastruttura di firma remota.

Il presente servizio consente di soddisfare questa esigenza, consentendo di fruire della soluzione di firma digitale su smart card, caratterizzata dal fatto di eseguire le operazioni di firma digitale dei documenti localmente, senza richiedere alcuna connessione con l'esterno.

La smart card, pienamente conforme a quanto previsto dalla vigente normativa sulla firma digitale, ospiterà oltre al certificato di firma digitale qualificata anche un certificato di autenticazione. Sarà lasciata la possibilità alle PA di richiedere che tale certificato di autenticazione sia conforme alle specifiche della Carta Nazionale dei Servizi (sia quindi un CNS) oppure sia un certificato di autenticazione "semplice", quindi non CNS.

In fase di definizione del Progetto dei Fabbisogni, il RTI dovrà altresì descrivere il processo che si intenderà adottare per soddisfare le richieste dell'Amministrazione in oggetto e gli eventuali vincoli, quali ad esempio la modalità di consegna delle smart card, e come realizzare la Registration Authority, se tramite personale della stessa Amministrazione o personale del RTI e/o della Certification Authority.

Si precisa che tale servizio potrà essere ordinato dalle Amministrazioni esclusivamente se abbinato ad almeno uno dei servizi complementari quali : firma digitale remota o marca temporale.

3.5. Servizio L2.S2.3 – Timbro elettronico

Il "Timbro elettronico" (o contrassegno elettronico o ancora glifo) estende il concetto di digital trust di un documento digitale anche a seguito della sua stampa su supporto cartaceo. Il servizio abilita quindi le Amministrazioni alla creazione di documenti informatici in formato elettronico che possano conservare la medesima validità legale anche dopo essere stati stampati su supporto cartaceo. Il processo permette difatti di recuperare il documento digitale originale firmato digitalmente partendo dalla scansione del documento cartaceo, verificandone l'integrità. È altresì disponibile una modalità che consente di leggere i contrassegni mediante applicazione mobile il che permette di verificare la validità di un documento mediante una semplice foto.

Le due modalità principali di apposizione del timbro sono:

- Modalità copia controllata

  Il timbro contiene una chiave di ricerca da utilizzare per recuperare il documento originale da un repository centralizzato: idonea laddove il documento da timbrare non ha un formato specifico come potrebbero essere i documenti prodotti da utenti finali. Questa modalità consente al sistema di astrarsi dal contenuto del documento. I documenti originali vengono depositati su di un repository documentale da dove vengono recuperati in fase di verifica.

- Modalità auto contenuta

  I dati del documento originale vengono inseriti all'interno del glifo e trasportati sul documento cartaceo: idonea per processi verticalizzati derivanti dall'interfacciamento con sistemi informativi che richiedono documenti ben definiti. In tal caso il processo prevede la totale elaborazione di un file XML fornito in ingresso, la sua firma, la creazione del relativo file PDF con l'applicazione contestuale del glifo. Tale modalità viene spesso utilizzata in ambiti dove è prevista l'emissione di certificati (es. certificati anagrafici).

<u>Architettura</u>

Nella prossima figura vengono descritti i processi del Timbro elettronico

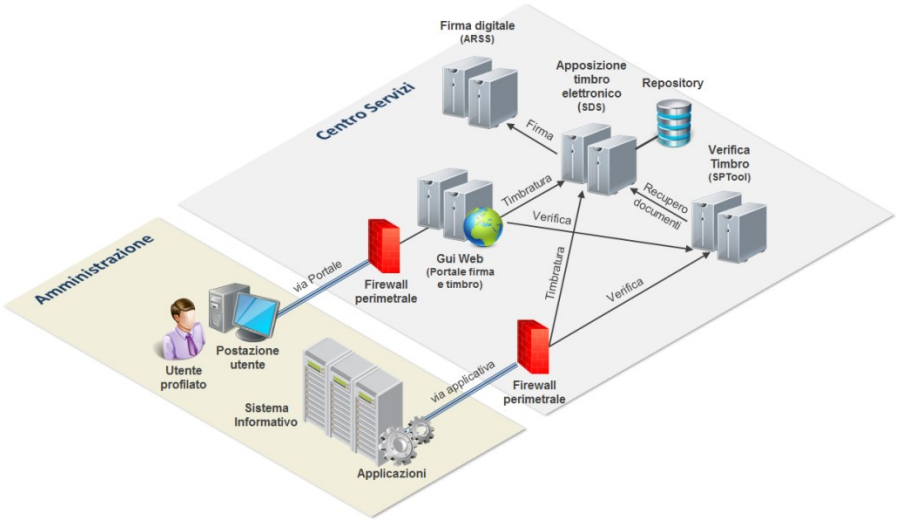


Fig. 11 Processi servizio "timbro elettronico"

Lo schema precedente esemplifica l'architettura logica e fisica per l'erogazione del servizio.

- Tutte le componenti risiedono presso il Centro Servizi e si evidenziano due flussi distinti relativi alle due modalità principali di apposizione del timbro, ossia copia conforme (o controllata) e auto contenuta.
- La prima modalità è normalmente utilizzata da una persona fisica dalla postazione di lavoro tramite l'accesso alla GUI Web del Portale di Firma Digitale e Timbro della PA, mentre il secondo è tipicamente utilizzata da una applicazione residente nel Sistema Informativo dell'amministrazione tramite i Web Service esposti in modo protetto.
- Entrambe le modalità afferiscono ai due processi di apposizione e verifica del timbro elettronico e interfacciamento agli HSM con la Firma digitale (ARSS) e condividono gli stessi componenti di Apposizione timbro elettronico (SDS) e Verifica timbro (SPTool).
- La modalità copia conforme utilizza uno storage (Repository) per il salvataggio dei documenti timbrati e il relativo recupero in fase di verifica.

Di seguito vengono descritti nel dettaglio i processi, anticipati in questa prima parte, che sottintendono il servizio.

Processi

Il processo viene attivato al momento della registrazione di un nuovo utente al servizio e prevede le seguenti attività:

- Registrazione
  Viene eseguita tramite portale all'apposita pagina di profilazione delle utenze.
- Identificazione della modalità
  Scelta della modalità più idonea alle esigenze dell'utente dell'applicazione del Contrassegno Elettronico, tra le seguenti:
  - Copia Conforme (o Controllata)
  - Auto contenuta
- Assegnazione e gestione
  Terminata la profilazione dell'utente, viene restituito all'utente un identificativo univoco (ID-Service) da utilizzare nella configurazione dei servizi di timbratura, qualora intenda

utilizzare i web Services. L'identificativo viene associato alle credenziali utente negli altri casi.

Viene creata una sola utenza applicativa, mentre vengono create utenze specifiche per ogni tipologia documentale.

Creazione e apposizione del Timbro elettronico

Il servizio di Timbratura elettronica prevede un'interfaccia integrata con quello di Firma digitale, nella quale l'utente registrato deve identificarsi attraverso le proprie credenziali. Il sistema, una volta verificato il profilo dell'utente , consente di apporre il timbro digitale sul documento fornito in ingresso in uno dei formati riconosciuti (XML/PDF) e secondo le modalità già descritte:

- Copia Conforme (o Controllata)
- Auto contenuta

Una semplificazione del processo consiste nell'uniformare i documenti forniti allo standard PDF 1/b (snellimento delle operazioni di normalizzazione dei documenti).

Verifica del Timbro elettronico

La fase di verifica del Timbro prevede la rilettura del contrassegno dal documento, la sua decodifica, la verifica di integrità e la visualizzazione del documento originale.

È possibile effettuare la verifica secondo quattro modalità, di seguito descritte:

1. Tool per PC (per documenti digitali e cartacei)
2. WEB tramite Portale di firma e timbro della PA
3. WEB service
4. APP per Smartphone (solo per Copia Conforme)

Per la verifica dei documenti sono presenti alcuni vincoli sulla qualità dei documenti da sottomettere al processo (in particolare per quanto riguarda la modalità di stampa e riacquisizione dei documenti, che richiedono che l'intero processo si svolga mantenendo una qualità di stampa e riacquisizione a 600dpi nel caso di documenti non-mobile, e di 300dpi nel caso di documenti mobile).

Tecnologie e prodotti di riferimento

Il presente paragrafo illustra i software verticali utilizzati per l'erogazione dei servizi di timbratura digitale e relativa verifica. Lo schema dell'architettura applicativa, relativa alle funzionalità di Timbratura e Verifica, è riportato in figura 12.

Il servizio viene erogato tramite il portale di accesso "Portale di Firma Digitale e Timbro della PA" .

Le componenti che costituiscono l'architettura applicativa sono le seguenti:

Componente di timbratura digitale

- GUI Web: la GUI web rappresenta la componente di interazione con l'utente finale, che si collega al portale integrato e viene autenticato dietro inserimento delle proprie credenziali. Si appoggia al layer HDBMS per la verifica delle stesse e per recuperare i dati utente. La GUI Web è esposta da un server web Apache 2 presente all'interno del server SDS su architettura Linux;
- Web Services: i web services consentono di erogare i servizi di timbratura nelle modalità descritte nelle pagine precedenti (auto contenuta e copia conforme). I Web Services si appoggiano sul DBMS e depositano eventuali file (modalità copia conforme) sullo storage; vengono esposti da un application server Apache Tomcat7;

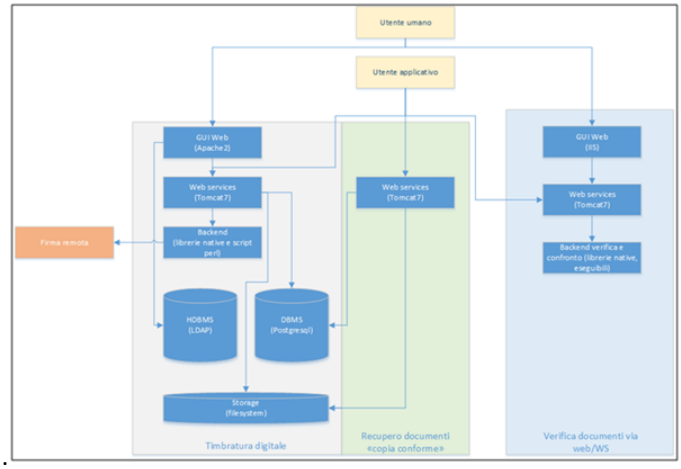


Fig. 12 Schema architettura "Timbro elettronico"

- Back end: il back end rappresenta il sistema centrale di timbratura ed è composto da un insieme di librerie scritte in linguaggio C, eseguibili e script perl. Il back end è interfacciato con il sistema di firma digitale automatica (ARSS) per firmare il contenuto dei glifi;
- HDBMS: il database gerarchico (LDAP) mantiene le informazioni locali legate ai profili utente del sistema e può essere utilizzato per la verifica delle credenziali di accesso. A livello applicativo il database locale LDAP è necessario per il corretto funzionamento del sistema;
- DBMS: il database relazionale tiene traccia delle configurazioni del sistema, oltre che mantiene la corrispondenza tra i documenti archiviati e la relativa chiave di ricerca. Il DBMS utilizzato è PostgreSQL v.9;
- Storage: lo storage da utilizzare per il salvataggio dei documenti timbrati in modalità copia conforme è esposto dall'infrastruttura VMware sotto forma di share NFS messa a disposizione per i nodi di timbratura.

Componente di recupero dei documenti in copia conforme

- Web Services: analogamente ai Web Services di timbratura, il layer Web Service di recupero documenti espone i metodi necessari al prelievo dallo storage dei documenti in copia conforme, sfruttando l'indicizzazione fatta dal DBMS. I Web Service vengono erogati da un application server Tomcat7;
- DBMS: si tratta del medesimo database del sistema di timbratura, utilizzato in sola lettura per prelevare le informazioni di indicizzazione che consentono di recuperare i documenti dallo storage;
- Storage: si tratta del medesimo storage del sistema di timbratura, acceduto in sola lettura per recuperare i documenti indicizzati.

Componente di verifica dei documenti via web

- GUI Web: la GUI Web consente all'utente finale di effettuare l'upload del documento da verificare e scaricare il file con i risultati finali. Viene erogata su piattaforma Microsoft IIS;
- Web Services: I Web Service di verifica e confronto servono per interfacciare la componente di back end con la componente di invocazione utente, sia essa gestita dalla GUI Web o mediante accesso diretto ai WS stessi. L'application server è nuovamente Tomcat7;
- Back end di verifica e confronto: consiste in un insieme di librerie di basso livello e di un'applicazione command line, utilizzata per effettuare tutte le operazioni. Questo strato applicativo necessita di un sistema operativo Microsoft Windows 2008/2012 a 64bit.

3.6. Servizio L2.S2.4 – Certificati SSL Server e Client

Il protocollo SSL (Secure Sockets Layer) consente alle applicazioni di trasmettere informazioni in modo sicuro mediante l'instaurazione di un tunnel cifrato ed autenticato. Tale protocollo si basa sull'utilizzo di certificati digitali sia lato server che, se richiesto, lato client.
Il certificato SSL, emesso da una Certification Authority (CA) accreditata al CA/Browser Forum (CAB Forum) e quindi ritenuto valido e riconosciuto world-wide dai principali browser e sistemi operativi, garantisce un alto grado di affidabilità e sicurezza della comunicazione tra l'applicativo Server ed la controparte Client.
Considerati quindi i servizi presenti all'interno del presente Contratto Quadro, caratterizzati da soluzioni che utilizzano certificati digitali, timbri digitali ed in generale che espongono servizi ad utenti sia interni alla Amministrazioni che ai cittadini, il presente servizio di certificati SSL completa l'offerta consentendo alle Amministrazioni di di garantire un livello di sicurezza e affidabilità alle proprie applicazioni ed ai sistemi convolti.
Come previsto dalle regole del CAB Forum, saranno resi disponibili alle Amministrazioni tutte le tipologie di certificati SSL Server che, differenziandosi per le procedure di identificazione previste, consentiranno di soddisfare tutte le esigenze delle PA.
Sempre nell'ambito dei certificati generati dalla CA "trustata" secondo le regole del CAB Forum, a completamento dell'offerta, sarà possibile per le Amministrazioni richiedere certificati per la firma del codice, detti CodeSign.

3.7. Servizio L2.S2.5 – Marca Temporale

La Marca Temporale è il risultato della procedura informatica, con cui si attribuisce, ad uno o più documenti informatici un preciso riferimento temporale opponibile ai terzi, grazie al quale è possibile dimostrare che quel documento informatico è stato generato in quel preciso orario e data. (Cfr. Art. 20, comma 3 Codice dell'Amministrazione Digitale D.lgs. 82/2005).
Il servizio di Marca Temporale offre la possibilità a tutti gli enti pubblici/amministrazioni di garantire l'apposizione di un riferimento temporale certo (legalmente valido) sia a documenti firmati digitalmente sia a documenti non firmati, oltre che l'estensione della validità legale dei propri documenti firmati digitalmente nel tempo.
In definitiva il servizio di Marca Temporale "certifica nel tempo" un documento e permette di:

- dimostrare che lo specifico documento elettronico esisteva in quella firma alla specifica data;
- estendere la validità di un documento informatico, firmato digitalmente, oltre la data di scadenza del certificato di firma digitale.

3.8. 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.

Modalità di erogazione:

- "as a service", mediante il Centro Servizi del Fornitore con l'ausilio degli strumenti (hardware e software) messi a disposizione da quest'ultimo. Il Fornitore può 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.

Il Fornitore, in fase di attivazione dei servizi "as a service", 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 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 3 – Livelli di severità

Il Fornitore ha 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 ha facoltà di poter richiedere in qualunque momento e senza oneri aggiuntivi l'aggiornamento e la modifica delle policy di sicurezza.

Il fornitore dovrà periodicamente consegnare all'Amministrazione i seguenti prodotti (come meglio descritti nel Capitolato Tecnico):

- 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.

Nell'ambito dei servizi di protezione, 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 come riportato nella tabella sotto, pena l'applicazione delle penali di cui all'Appendice 1 - Indicatori di qualità Lotto 2.

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

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 4 – Tempistica e gestione escalation

3.9. Servizi di Gestione delle vulnerabilità

I Servizi di Gestione delle Vulnerabilità forniscono le scansioni delle applicazioni e dell'infrastruttura delle Amministrazioni per rappresentare lo stato di criticità e il livello di esposizione delle applicazioni al rischio di sicurezza.

I Servizi di Gestione delle Vulnerabilità includono i seguenti Servizi di sicurezza:

- Static Application Security Testing (SAST);
- Dynamic Application Security Testing (DAST);
- Mobile Application Security Testing (MAST);
- Vulnerability Assessment (VA).

Essi sono volti alla rilevazione delle eventuali vulnerabilità delle applicazioni tramite analisi, eliminazione di falsi positivi, classificazione e reporting. Tali servizi sono erogati centralmente dal Centro Servizi e sono fruibili attraverso il Portale di fornitura. Sono inoltre utilizzati all'interno del ciclo di vita delle Applicazioni delle Amministrazioni in due momenti temporalmente distinti:

- prima del rilascio delle applicazioni in produzione;
- periodicamente, per verifica del livello di sicurezza delle applicazioni in produzione.

L'esito delle verifiche di analisi e scansione delle vulnerabilità, le "remediation" definite e l'ampia collezione di best practice di settore, continuamente aggiornata, costituiscono una base dati incrementale in grado di apportare valore all'intero ciclo di vita delle applicazioni delle Amministrazioni.

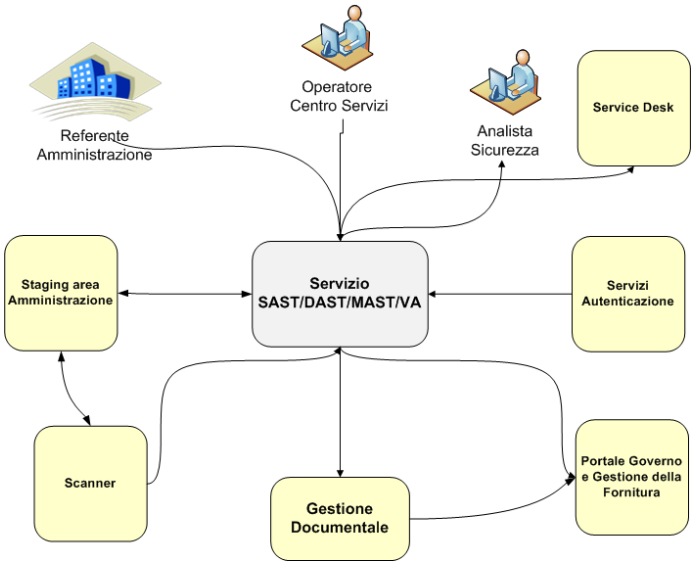


Fig. 13 Schema logico Servizi gestione vulnerabilità

- Il Service Desk è la piattaforma di comunicazione operativa con l'Amministrazione per la gestione dell'intero ciclo di vita del servizio. Attraverso il modulo web di Information Gathering, si raccolgono le informazioni tecniche necessarie alla configurazione dei template di scansione, le schedulazioni degli scanner, l'ambito tecnologico di erogazione del servizio
- I Servizi di Autenticazione sono utilizzati per la protezione dei dati dell'Amministrazione nell'ambito dei servizi attivati. Centralmente la componente LDAP contiene i profili dei Referenti delle Amministrazioni e degli Operatori del Centro Servizi assegnati ad ogni Contratto Esecutivo
- La Staging Area Amministrazione è un'area protetta di lavoro dedicata ad ogni singola Amministrazione, utilizzata per la condivisione delle configurazioni applicative, del codice sorgente, delle best practice di sviluppo sicuro e dei relativi report di vulnerabilità
- Il Portale di Governo e Gestione della Fornitura (SIGGF) rende disponibile in modalità unificata ed integrata le funzionalità operative di presentazione e condivisione dei contenuti informativi relativi a pianificazione, andamento, rendicontazione e monitoraggio dei servizi oggetto della fornitura
- La Gestione Documentale consente l'archiviazione, conservazione e indicizzazione dei documenti mediante l'associazione di apposite classi documentali e relativi metadati e li rende disponibili per la consultazione in funzione del profilo di appartenenza
- Lo Scanner rappresenta la componente di scansione specifica per ogni singolo servizio di vulnerabilità.

Processi

Tutti i Servizi di Gestione delle vulnerabilità coinvolgono attori e strumenti comuni, e seguono logiche di attivazione e terminazione medesimi, descritti nella tabella sotto. Le relative attività saranno rappresentate nei diagrammi di flusso e descritte nel dettaglio di seguito.

Item	Descrizione
Attori coinvolti	• Amministrazione: è il fruitore dei servizi che inizializza le richieste di scansione e riceve i report; • Operatore di Sicurezza: (del Centro servizi) gestisce i profili utente delle Amministrazioni, effettua le operazioni di scansione e predispone la reportistica di servizio; • Analista Sicurezza: (del Centro servizi) configura e analizza le scansioni, elimina i falsi positivi ed effettua la generazione e la pubblicazione dei report.
Strumenti	• Service Desk: gestione delle richieste accessibile da Portale dei Servizi di sicurezza
	• AppScan Suite: Sistemi di Gestione Vulnerabilità del Centro Servizi
Eventi che attivano il processo	Il processo è attivato a fronte di Service Request all'interno del processo di Request Fulfillment dagli utenti dell'Amministrazione Cliente definiti come referenti Amministrazione.
Eventi che terminano il processo	Il processo è terminato con la chiusura definitiva della Service Request e la consegna dei Deliverables.
Interazioni con altri processi	I processi con i quali interagiscono i Servizi di Gestione delle Vulnerabilità sono i seguenti: • Request Fulfillment • il Service Level Management.
Input al processo	Gli input al processo di Request Fulfillment, in dipendenza della tipologia del servizi, sono alcuni tra i seguenti: • informazioni di dettaglio relative al contratto esplicitate nella Service Request • informazioni tecniche di dettaglio inserite nella Web Form da parte dell'Amministrazione • Community dell'Amministrazione per download Source Code; • SLAs (Service Level Agreements); • aggiornamento degli stati delle richieste.

Architettura

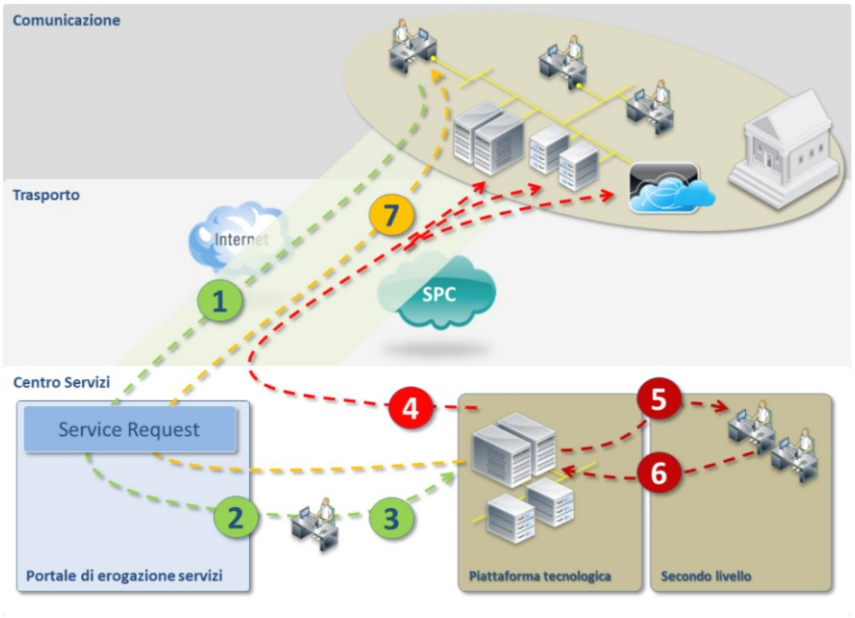


Fig. 13 Schema logico Servizi gestione vulnerabilità

Architettura logica comune per i servizi di Gestione del Vulnerabilità di interfacciamento fra il Centro Servizi e l'Amministrazione

	Azione	Descrizione
1	Richiesta di scansione	Il referente dell'Amministrazione (utente) richiede la scansione tramite Portale web, inserendo in appositi form tutte le informazioni richieste (software package o artefatto nel caso di analisi statica o mobile, URL o link nel caso di analisi dinamica o mobile);
2	Ricezione della richiesta	Il Centro Servizi prende in carico la richiesta e registra l'avanzamento, sempre disponibile all'utenza ed aggiornato in tempo reale;
3	Conferma della schedulazione	L'utente riceve conferma o notifica di nuova pianificazione;
4	Esecuzione delle scansioni	All'avvio della scansione l'utente viene avvisato via e-mail ed il relativo stato di completamento viene reso disponibile sul portale in tempo reale;
5	Esecuzione dell'analisi di secondo livello	Terminata la scansione è aggiornato lo stato del ticket e si avvia l'analisi di secondo livello per la verifica delle vulnerabilità riscontrate all'interno del contesto specifico dell'Amministrazione, per ottenere il miglioramento continuo del livello di affidabilità delle analisi.
6	Miglioramento Efficacia del servizio	Tale obiettivo è perseguito nel tempo lavorando per cicli successivi attraverso la manutenzione delle liste di esclusione al fine di migliorare l'efficacia del servizio;
7	Produzione della reportistica e consegna dei Rapporti	In aggiunta a quanto prodotto e reso disponibile al termine delle singole scansioni dei vari servizi, saranno pubblicati e resi disponibili all'Amministrazione i report integrati. A seguito di tale azione si considererà chiusa la richiesta e ne sarà data comunicazione ai referenti dell'Amministrazione attraverso il Portale e via e-mail.

Tecnologie e prodotti di riferimento

Da un punto di vista applicativo i servizi SAST, DAST, MAST e VA sono realizzati utilizzando le seguenti piattaforme:

Componenti applicative	Sotto-componenti applicative
IBM AppScan Suite	IBM Security AppScan Standard Edition IBM Security AppScan Enterprise Edition IBM Security AppScan Source Edition
IBM Qradar Vulnerability Manager	IBM QVM console IBM QVM scanner

Tabella 5 - Architettura Applicativa servizi Gestione delle Vulnerabilità

Per la realizzazione del sistema di Gestione delle Vulnerabilità sono configurate le componenti applicative illustrate di seguito.

IBM Security AppScan Source: utilizzato per verificare la corretta applicazione delle politiche di sicurezza al codice sorgente. Gli analisti di analisi statica del codice utilizzano le componenti IBM Security AppScan Source per eseguire le scansioni di codice sorgente, eseguire le procedure di test applicando le verifiche ed i controlli sviluppati dai centri di ricerca IBM e condivisi a livello mondiale. IBM Security AppScan Source offre assistenza sulle azioni di remediation di ogni vulnerabilità, tra cui la possibilità di isolare la riga di codice corrispondente al rischio per la sicurezza.

IBM Security AppScan Enterprise Server: consente la gestione centralizzata di tutti i risultati dei test e del rischio relativo alle vulnerabilità riscontrate. La sua architettura scalabile permette di gestire un numero elevato di scanner, attraverso connessioni sicure HTTPS, seguendo le richieste delle amministrazioni.

La componente SQL Server rappresenta il repository centrale per le informazioni raccolte durante la scansione: statistiche, scan logs, polling per gli eventi di scansione. Inoltre, rappresenta il mezzo di comunicazione tra Enterprise Console e gli scanner di analisi dinamica.

IBM AppScan Standard: è la componente utilizzata dagli analisti di sicurezza per effettuare test dinamici e automatizzati detti “black box”, per rilevare nuove vulnerabilità legate al Web 2.0 ed applicazioni Internet complesse, come quelle basate su Ajax e Adobe Flash.

IBM Rational License Key Server: gestisce le licenze di utilizzo degli scanner; le licenze sono organizzate tramite un pool da cui attingono i diversi client di scansione.

IBM Qradar Vulnerability Manager (QVM): componente utilizzata a supporto del servizio di Vulnerability Assessment. Consente di combinare l'automatismo delle scansioni di vulnerabilità con la conoscenza delle configurazioni dei dispositivi testati, la topologia di rete e i modelli di traffico. Questo rende possibile attivare misure di protezione proattive. Oltre a eseguire la scansione, fornisce un’interpretazione intelligente dei risultati. Riceve aggiornamenti giornalieri delle nuove vulnerabilità attraverso il servizio IBM X-FORCE Threat Intelligence. Il servizio aggiunge dinamicamente i dati delle minacce Internet alle funzionalità di analytics di IBM QRadar Security Intelligence Platform, per aggiornare il database delle vulnerabilità sullo stato dell’arte della sicurezza sulla rete. Questa funzionalità consente di identificare le nuove minacce più rapidamente, ottenere informazioni più dettagliate, definire le priorità degli incidenti di sicurezza e prevenire o ridurre gli attacchi.

IBM Rational Asset Manager: fornisce un’infrastruttura di gestione sicura di una libreria di asset, dedicati alle singole Amministrazioni a supporto dei servizi di Gestione della Vulnerabilità.

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

Il servizio consente l'identificazione delle vulnerabilità software all'interno del codice (sorgente) delle applicazioni nella fase iniziale del ciclo di vita in modo da poterle eliminare prima della distribuzione.

Il servizio, applica la metodologia OWASP (Open Web Application Software Project) e si compone delle seguenti funzionalità:

- **Data Validation**: verifica della presenza di vulnerabilità che possono riguardare eventuali dati corrotti in ingresso che possono portare a un comportamento anomalo dell'applicazione;
- **Controllo Semantico**: rilevazione di eventuali problematiche legate all'uso pericoloso di determinate funzioni o API (es. funzioni deprecate);
- **Verifica delle 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.
- **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;

Il servizio, compatibile con i principali linguaggi e framework di sviluppo, è prevalentemente orientato ad applicazioni in ambiente WEB. Su richiesta dell'Amministrazione può essere erogato anche su altri ambienti.

Processi

Information Gathering (avviamento al servizio)

Questa fase prevede il coinvolgimento dell'Amministrazione nella raccolta delle informazioni necessarie alla definizione della corretta profilatura del test. Il referente dell'Amministrazione, responsabile dello sviluppo dell'applicazione oggetto del test, compila il form di richiesta di attivazione del servizio inserendo tutte le informazioni necessarie alla corretta esecuzione.

Le informazioni riguardano:

- lo stack applicativo tecnologico dell'applicazione in analisi;
- le funzionalità principali dell'applicazione per meglio interpretare i flussi di dati durante l'analisi;
- i casi d'uso/abuso;
- framework di sviluppo comprensivo di librerie/dipendenze necessarie all'esecuzione del test;
- security policy.

Automated source code analysis (Operation)

Durante questa fase viene eseguita una build del codice ricevuto per la verifica della completezza delle informazioni raccolte. Lo strumento di scansione non sarà in grado di analizzare automaticamente le classi che non sono compilate. Questa attività permette di rilevare API e funzioni non presenti nel codice sorgente per permettere analisi dei flussi di dati. La risoluzione della maggior parte degli errori di compilazione è prerequisito alla corretta scansione.

Sulla base dei risultati dello scanning, l'analisi consiste nell'esecuzione delle seguenti attività:

- eliminazione dei falsi positivi;
- individuazione dei rischi scaturiti dalle vulnerabilità riscontrate;
- prioritizzazione delle vulnerabilità in base all'impatto sul business;
- stesura delle raccomandazioni di mitigazione del rischio.

Generazione dei report (output)

Durante questa fase sono rese disponibili sul Portale i deliverable del servizio, ovvero:

- Executive Summary, contenente:
  - application information background;
  - obiettivi del test;
  - sommario delle rilevanze del test;
  - valutazione del Security Risk;
  - sommario delle Vulnerabilità riscontrate.
- Technical report, contenente:
  - descrizione delle rilevanze riscontrate durante i test;
  - descrizione dell'impatto causato dallo sfruttamento della vulnerabilità riscontrata.
- Remediation Plan, contenente:
  - sommario dei punti di intervento e le opportune azioni correttive;
  - raccomandazioni, workaround, soluzioni di protezione.

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

Il servizio consente 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.

Il servizio, applica la metodologia OWASP (Open Web Application Software Project) e si compone delle seguenti funzionalità:

- 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 che prevedono tre diversi profili di erogazione del servizio - Bronze, Silver e Gold
- 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)

Il servizio è compatibile con i principali linguaggi e framework di sviluppo (tra cui .NET, PHP, C/C++, Java, J2EE, ASP)

<u>Bronze</u>

Applicazioni non critiche che consentono la visualizzazione di pagine di contenuto informativo (siti web statici)

<u>Silver</u>

Applicazioni costituite da più form (siti web dinamici) e con funzionalità di autenticazione. Le funzionalità aggiuntive sono le seguenti:

- Definizione di scansioni personalizzate
- Esecuzione di test di autenticazione multilivello
- PCI Compliance
- Esecuzione di test manuali sulle applicazioni in fase di esecuzione
-

<u>Gold</u>

Applicazioni critiche con funzionalità complesse e di tipo transazionale (ad esempio pagamenti). Le funzionalità aggiuntive sono le seguenti:

Definizione di scansioni personalizzate

- Esecuzione di test di autenticazione multilivello
- PCI Compliance
- Esecuzione di test manuali sulle applicazioni in fase di esecuzione
- Creazione personalizzata di business logic test
- Proof of concept delle vulnerabilità riscontrate

Vulnerabilità potenziali identificate e rilevate

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

Processi

Information Gathering (avviamento al servizio)

Questa fase prevede il coinvolgimento dell'Amministrazione nella raccolta delle informazioni necessarie alla definizione della corretta profilatura del test. Il referente dell'Amministrazione, responsabile dello sviluppo dell'applicazione oggetto del test, compila il form di richiesta di attivazione del servizio inserendo tutte le informazioni necessarie alla corretta esecuzione.

Le informazioni riguardano:

- lo scopo dell'applicazione;
- tipi di dati elaborati dall'applicazione;
- utenti indicati del sistema;
- i privilegi dell'applicazione sul server e sulla rete;
- gli input previsti dall'applicazione (es.: stringa, numeri interi, valori booleani);
- l'utilizzo e lo scopo dei nomi utente e delle password, se esistenti;
- le comunicazioni di rete dell'applicazione (es.: protocolli, porte, IP);
- altre applicazioni su cui si basa l'applicazione (es.: database, backend, middleware).

Automated source code analysis (Operation)

Si esegue il test di un potenziale attacco da un utente esterno senza privilegi o da un utente interno con credenziali di accesso e conoscenza delle applicazioni:

- si determinano e quantificano tutti i campi della sicurezza delle applicazioni,
- si valutano i punti di forza e di debolezza dei controlli di sicurezza esistenti;
- si identificano le mancanze nella progettazione e nella struttura delle applicazioni;

- si valutano i livelli di sicurezza esistenti, incluse le politiche di progettazione e sviluppo delle applicazioni di base;
- si effettua una analisi puntuale basata su controlli suggeriti dalle best practice internazionali sulle seguenti aree:
    - Sicurezza delle trasmissioni
    - Autenticazione
    - Gestione delle sessioni
    - Gestione delle password
    - Divulgazione delle informazioni
    - Validazione dati di Input
    - Flusso logico dei dati
    - Autorizzazione.

Generazione dei report (output)

Durante questa fase sono resi disponibili i seguenti deliverable di servizio:

Executive Summary contenente:

- Application information background;
- Obiettivi del test;
- Sommario delle rilevanze del test;
- Valutazione del Security Risk;
- Sommario delle vulnerabilità riscontrate;
- Sommario dei punti di intervento e delle opportune azioni correttive.

Technical report contenente:

- Descrizione delle rilevanze riscontrate durante i test;
- Descrizione dell'impatto causato dallo sfruttamento della vulnerabilità riscontrata;
- Raccomandazioni, workaround, soluzioni di protezione;
- Prioritizzazione delle raccomandazioni tattico/strategiche (vulnerabilità critiche/non critiche)

Remediation plan:

- Remediation Plan, contenente:sommario dei punti di intervento e le opportune azioni correttive;
- raccomandazioni, workaround, soluzioni di protezione.

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

Il servizio consente 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.

Il servizio, applica la metodologia OWASP (Open Web Application Software Project) e si compone delle seguenti funzionalità:

- 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.
- 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);
- analisi e gestione delle policy di accesso ai dati e alle funzioni del dispositivo).

Il servizio è compatibile con i sistemi operativi Android, Blackberry, iOS e Microsoft Windows.

La piattaforma fornisce gli strumenti per l'esecuzione di test mirati alle applicazioni di tipo mobile e permette la rilevazione delle vulnerabilità di sicurezza che possono essere sfruttate da un attaccante per compromettere i dati delle mobile app, la logica di business o il framework del

dispositivo mobile identificando qualsiasi minaccia che mette a rischio l'applicazione e/o l'infrastruttura.

La piattaforma tecnologica afferisce al servizio di Mobile Analysis Security Testing (MAST) e le tecnologie a supporto sono le suite IBM Security AppScan Source e AppScan Standard, integrate con altre piattaforme verticali che ne estendono le funzionalità nello specifico ambito dell'analisi Mobile.

AppScan Mobile esegue un'analisi completa sulle app richieste in quanto copre tre differenti tipologie di test:

- analisi statica: è necessario fornire il codice sorgente dell'app mobile da testare, comprensivo di tutte le eventuali informazioni aggiuntive necessarie per il processo di build,
- analisi dinamica: è possibile eseguire test specifici sulle "web app" che prevedono l'accesso ad un sito web da un device mobile. In questo caso è necessario fornire come input le informazioni relative a URL da testare, agent da simulare e credenziali di eventuali utenti;
- test di emulazione: la piattaforma tecnologica utilizza come input l'app stessa; il test consiste nel caricamento della app in un emulatore per effettuare un'analisi definita runtime. Il back-end dell'ecosistema mobile è analizzato ricercando gli specifici URL coinvolti nelle transazioni client-server.

Processi

Information Gathering (avviamento al servizio)

Questa fase prevede il coinvolgimento dell'Amministrazione nella raccolta delle informazioni necessarie alla definizione della corretta profilatura del test. Il referente dell'Amministrazione, responsabile dello sviluppo dell'applicazione oggetto del test, compila il form di richiesta di attivazione del servizio inserendo tutte le informazioni necessarie alla corretta esecuzione in particolare:

- dati riguardanti la progettazione e la programmazione dell'applicazione dal punto di vista dello sviluppatore di applicazioni;
- dati sulla configurazione del dispositivo mobile e sulle politiche di sicurezza previste;
- approfondimenti sulle differenze di sviluppo sui diversi dispositivi o OS per valutare la configurazione dell'ambiente di test più idoneo;
- copia valida del package di download dell'applicazione disponibile sul provider o una build utile per il test
- modelli di progettazione dell'applicazione.

Automated source code analysis (Operation)

Questa fase ha lo scopo di valutare il livello delle misure di sicurezza adottate durante lo sviluppo di applicazioni mobile, individuare i punti deboli e le vulnerabilità e fornire suggerimenti e linee guida di bonifica. La valutazione è condotta dal punto di vista potenziale di un attaccante.

Le attività svolte sono:

- Impostazione dell'ambiente di prova secondo l'architettura applicativa
- Esecuzione del test statico
- Esecuzione del test delle applicazioni dinamiche validando il flusso logico dei dati dell'applicazione in fase di esecuzione
- Verifica uso di chiamate sensibili
- Valutazione di fonti di dati e osservazione della reazione in fase di esecuzione
- Convalida di un uso corretto e sicuro dei paradigmi per le applicazioni mobile, della crittografia e di altri modelli di progettazione della sicurezza di rete per garantire la riservatezza dei dati scambiati

- Analisi della progettazione e delle politiche di sviluppo affinché non introducano perdita di dati riservati su storage locale, su sistemi di archiviazione e su backup esterni
- Valutazione delle applicazioni di backend (da eseguire mediante la sottoscrizione del servizio L2.S3.1)
- Valutazione dei punti di forma e di debolezza dell'architettura di backend e della tecnologia adottata (da eseguire mediante la sottoscrizione de servizio L2.S3.1)
- Verifica che ciascun sistema contattato dal client mobile sia protetto da attacchi verso applicazioni web (la verifica dinamica dell'applicazione web è eseguita mediante la sottoscrizione del servizio L2.S3), garantendo allo stesso tempo che gli input vengano analizzati correttamente dai parser remoti
- Analisi dei risultati e classificazione del livello di rischio.

Il servizio fornisce una classificazione dei risultati con esclusione dei falsi positivi, in modo che le vulnerabilità cruciali e sensibili ricevano un'adeguata attenzione e visibilità nella relazione finale.

Generazione dei report (output)

La documentazione sarà prodotta attraverso Durante questa fase sono resi disponibili sul Portale dei Servizi di Sicurezza i deliverable del servizio quali:

Executive Summary, contenente:

- Application information background
- Obiettivi del test
- Sommario delle rilevanze del test
- Valutazione del Security Risk
- Sommario delle Vulnerabilità riscontrate.

Technical report, contenente:

- Descrizione delle rilevanze riscontrate durante i test
- Descrizione dell'impatto causato dallo sfruttamento della vulnerabilità riscontrata

Remediation Plan, contenente:

- Sommario dei punti di intervento e le opportune azioni correttive;
- Raccomandazioni, workaround, soluzioni di protezione.

3.9.4. Servizio L2.S3.4 – Vulnerability assessment

Il servizio deve consentire una verifica dinamica della sicurezza dei dispositivi di rete 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 sono presenti strumenti automatizzati al fine di rilevare le potenziali vulnerabilità.

Il servizio si compone delle seguenti funzionalità:

- individuazione delle vulnerabilità attraverso l'esecuzione di test che consentano accertare le vulnerabilità individuate.
- assegnazione automatica delle priorità/severità ai rischi di sicurezza sulla base delle policy concordate.
- 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).

Il servizio consente di eseguire scansioni su perimetri estesi attraverso test dal livello network a quello applicativo.

Architettura

La piattaforma fornisce gli strumenti per la gestione delle vulnerabilità relative ai servizi, all'architettura e alle configurazioni dei sistemi oggetto dell'analisi, eseguendo una serie di test in grado di coprire le esigenze di sistemi complessi. La soluzione è basata su una componente centralizzata di gestione che governa e raccoglie i flussi informativi provenienti dalle istanze scanner dedicate alla realizzazione dei test. La soluzione si basa su IBM QRadar Vulnerability Manager quale componente specializzato della piattaforma IBM Qradar, posizionata come leader nel Gartner Magic Quadrant 2014 delle piattaforme SIEM.

Sono previste le seguenti fasi:

- Raccolta delle informazioni: realizzando la scansione del perimetro indicato rilevando la presenza di asset (discovery) e identificando tipologie e caratteristiche hardware e software,
- Individuazione delle vulnerabilità: collezionando le vulnerabilità presenti nelle varie componenti del sistema target eseguendo test dal livello network al livello applicativo,
- Prioritizzazione delle vulnerabilità: organizzando le vulnerabilità rilevate in funzione del rischio che esse rappresentano per l'Amministrazione. Ai fini di una appropriata classificazione, il RTI promuove una stretta collaborazione e comunicazione con l'Amministrazione sul tema, anche a supporto della realizzazione delle policy.

Tutte le scansioni saranno eseguite attraverso un canale sicuro instaurato tra gli apparati di sicurezza perimetrale del Centro Servizi e quelli del Cliente. Il deploy della Piattaforma tecnologica consente scenari compositi, ad esempio nel caso le scansioni siano effettuate attraverso lo scanner posizionato nel Centro Servizi e comunicante con gli IP esposti in DMZ, oppure, in funzione della numerosità dei target o per il loro posizionamento all'interno della rete cliente, l'Amministrazione potrà optare per collegare la VPN in prossimità dei target.

Processi

Information Gathering (avviamento al servizio)

Durante questa fase viene eseguita la raccolta automatica delle configurazioni e della topologia di rete per la definizione dei profili di scansione, ovvero:

- Operazione di network discovery della rete: rilevazione attiva e passiva di ogni nuovo dispositivo installato nella rete; questo riduce in maniera significativa il rischio associato alle risorse non protette e non governate dalle Amministrazioni collegate alla rete includendo apparati, porte, sistemi, servizi, applicazioni
- Valutazione di tutti gli indirizzi IP attivi e non attivi all'interno di un determinato intervallo
- Rilevazione di wireless access points
- Catalogazione di apparati di rete come firewall, IDS/IPS, router, switch, server, stampanti, telefoni VoIP.

Individuazione delle vulnerabilità (Operation)

In tale fase, vengono eseguite scansioni rapide condotte in tutta la rete (con cadenza periodica) per trovare le eventuali falle di sicurezza e ridurre i rischi di esposizione , evidenziando l'aderenza o meno alle normative vigenti tramite raccolta, correlazione e reportistica delle informazioni rilevate durante le scansioni. Le scansioni applicano una combinazione di controlli attivi (quali l'invio di pacchetti e l'analisi in remoto) e controlli di correlazione passiva.

In particolare, l'esecuzione di scansioni web complete aiuta a garantire il controllo della sicurezza della rete rilevando falle come ad esempio SQL Injection e Cross-Site Scripting nonché la presenza di errori nelle pagine web.

Prioritizzazione delle vulnerabilità (Operation)

La prioritizzazione delle vulnerabilità avviene in ottica di risoluzione e mitigazione del rischio attraverso la comprensione dell'intero contesto di rete.

Il rischio di ogni vulnerabilità viene classificato tramite un algoritmo basato su fattori come impatto o sfruttabilità o compliance PCI (Protocol Control Information).

Le vulnerabilità scoperte possono essere filtrate per asset, rete, servizio o tipo di vulnerabilità permettendo di produrre reportistica personalizzata secondo le esigenze delle Amministrazioni.

Definizione reportistica personalizzata

Durante questa fase sono resi disponibili sul Portale dei Servizi di Sicurezza i deliverable del servizio quali:

Executive Summary, contenente:

- Ambito infrastrutturale
- Obiettivi del test
- Sommario delle rilevanze del test
- Valutazione del Security Risk
- Sommario delle Vulnerabilità riscontrate.

Technical report, contenente:

- Descrizione delle rilevanze riscontrate durante i test
- Descrizione dell'impatto causato dallo sfruttamento della vulnerabilità riscontrata

Remediation Plan, contenente:

- Sommario dei punti di intervento e le opportune azioni correttive;
- Raccomandazioni, workaround, soluzioni di protezione.

3.10. Servizi di Protezione

L'estrema eterogeneità tecnologica e delle applicazioni informatiche, in genere riscontrabile presso le Pubbliche Amministrazioni, determina uno scenario di rischio complessivamente elevato, aggravato dall'obsolescenza accelerata delle tecnologie e dal panorama delle minacce informatiche in costante evoluzione.

In questo contesto i Servizi di Protezione forniti sono finalizzati alla rilevazione di anomalie, minacce ed attacchi alle infrastrutture ed ai sistemi delle Amministrazioni. In funzione del contesto specifico e delle necessità dell'Amministrazione, è prevista la possibilità di installare componenti "on premise" presso l'Amministrazione o in modalità " as a service" all'interno del Centro Servizi.

I Servizi di Protezione includono i seguenti Servizi di Sicurezza:

- Data loss/leak prevention (DLP);
- Database security (DBS);
- Web application firewall e next generation firewall management (WAF);
- Secure web gateway (SWG).

Questi servizi sottintendono una medesima Architettura logica e due principali tipi di attività: Gestione Operativa e Gestione degli Incidenti.

Per garantire l'efficacia del servizio, in ottica di Segregation of Duty, tali attività saranno erogate da due team specializzati, dedicati e separati. Il team di Gestione Operativa si occuperà della gestione dei sistemi tecnologici e della relativa manutenzione per garantire la continuità operativa, della gestione delle policy per garantire la continua aderenza delle configurazioni alle policy concordate con l'Amministrazione e in ultimo del reporting.

La visione/richiesta di modifica delle policy potrà essere fatta dall'Amministrazione tramite il Portale o Help Desk.

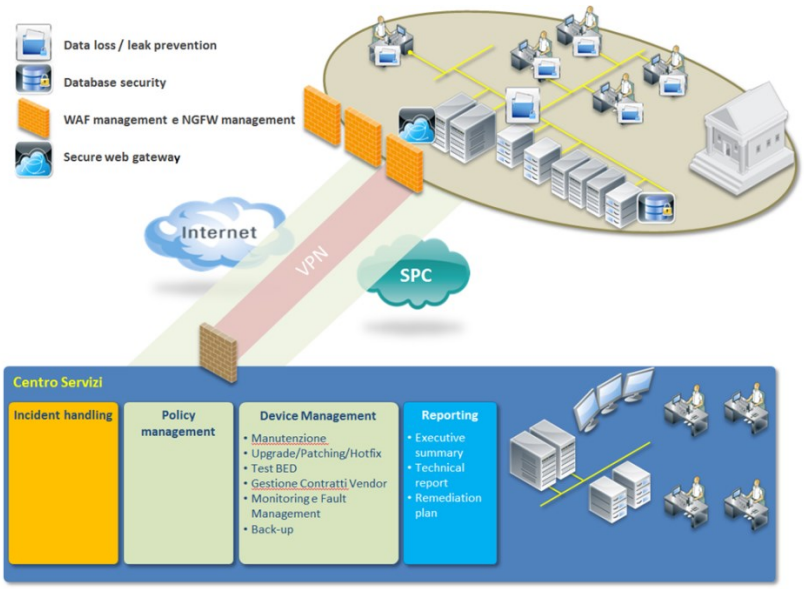


Fig. 14 Architettura logica comune dei Servizi di Protezione

Processi

A seguito di una richiesta da parte di un Utente della Pubblica Amministrazione, viene aperta una Service Request gestita dal Service Desk, secondo le tipologie di richiesta possibili seguenti.

Creazione/Modifica Privacy

Gestisce la creazione o la modifica di una policy di sicurezza, su uno specifico client o gruppi di client identificati tramite indirizzo IP o su uno specifico DBMS o gruppi di DBMS, a seconda del servizio.

Visione Policy

Gestisce la visualizzazione e l'esportazione delle policy in vigore

Reporting

Gestisce la generazione di report standard e personalizzati, corredati di statistiche e grafici ed esportabili in formato Excel o PDF.

Maintainance

Gestisce la manutenzione delle componenti impegnate nell'erogazione del servizio. Tali attività possono riguardare aggiornamenti software, hotfix, operazioni di riavvio di specifici processi applicativi, etc..

3.10.1. Servizio L2.S3.5 – Data loss/leak prevention (tecnologia Forcepoint Data Security)

Il servizio di "data loss/leak prevention" consente 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.

La soluzione è basata sulla tecnologia leader di mercato Forcepoint Data Security Suite (ex Websense), ed è in grado di effettuare il monitoraggio e la protezione dei dati at rest (sui supporti di memorizzazione), in use (accesso tramite endpoint), in motion (traffico di rete).

Il servizio di compone delle seguenti funzionalità:

- rilevazione dei dati che transitano all'interno dell'amministrazione, ovunque essi siano archiviati;
- analisi e classificazione dei dati facilitata da OCR e Machine Learning Documentale;
- possibilità di creare regole predefinite per la protezione dei dati, identificando i sistemi in cui sono memorizzati (ad es porte USB, DVD, porte COM & LPT, dischi rimovibili, etc..),
- 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 comunicazione;
- possibilità di generare report di sintesi (executive summary) e di dettaglio (technical report);

Il servizio prevede l'installazione di sw agent sugli endpoint distribuibili in maniera semi-automatica attraverso piattaforme di sw deployment dell'Amministrazione, è inoltre prevista l'installazione di gateway "on premise" per l'analisi del traffico in motion.

Architettura

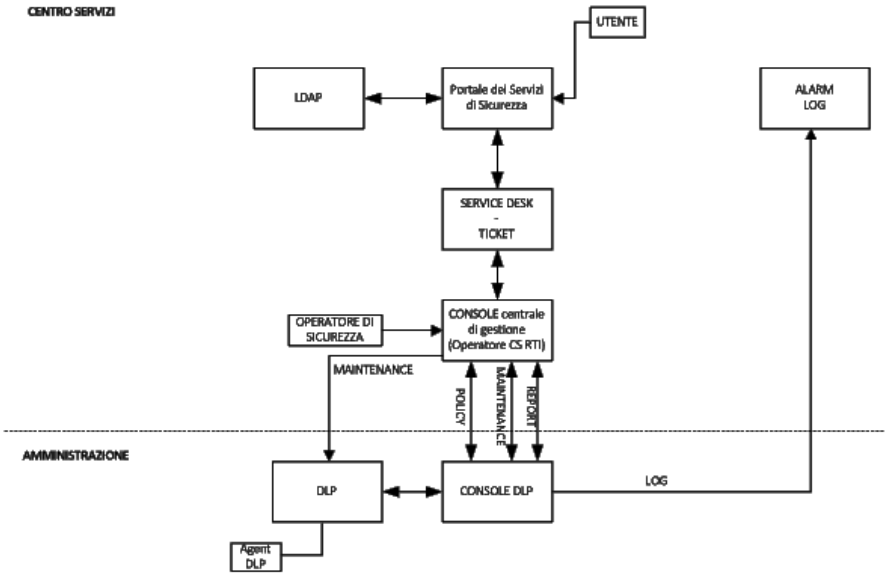


Fig 15 Architettura servizi Data loss/leak prevention

L'architettura è dislocata presso:

- Centro Servizi;
- Pubblica Amministrazione.

Presso il Centro Servizi sono dislocati:

- Portale dei Servizi di Sicurezza: per effettuare nuove richieste di servizi (es.: creazione o modifica di una policy);
- LDAP: per l'accesso ai servizi con utenza di dominio;
- Service Desk / Ticket: piattaforma di ticketing per la gestione delle richieste;
- Console centrale di gestione: postazione di gestione del servizio;
- Alarm log: per la raccolta degli eventi di sicurezza

Presso la Pubblica Amministrazione:

- Endpoint Controller (DLP): per il controllo e l'invio agli agent DLP delle policy di sicurezza;

- Console DLP: per il deploy delle policy di sicurezza;
- Agent DLP: per la protezione dei dati sulle PdL (Postazione di Lavoro).

Tecnologie e prodotti di riferimento

La figura seguente illustra l'architettura applicativa del servizio DLP, con indicazione dei prodotti utilizzati (tecnologia FORCEPOINT).

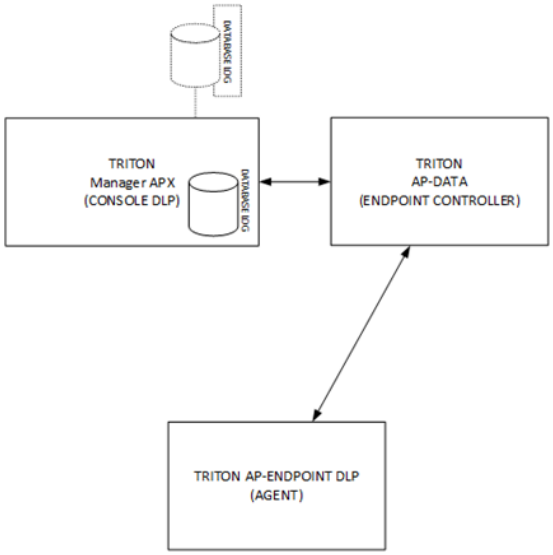


Figura 1 – Schema applicativo dei Servizi di Data Loss/Leak Prevention

Fig. 16 Schema applicativo servizi dta loss/leak prevention

Di seguito il dettaglio sui prodotti che costituiscono l'architettura applicativa:

- TRITON AP-DATA (Endpoint Controller) – si occupa della gestione degli endpoint, controlla la corretta connessione degli endpoint e applica l'enforcement delle policy inviate dal Triton Manager APX (Console DLP);
- TRITON Manager APX (Console DLP) – consente di applicare le policy di sicurezza inviandole al Triton AP-DATA (Endpoint Controller). La Triton Manager APX (Console DLP) è accessibile tramite Web Browser con connessione sicura SSL. La Triton Manager APX (Console DLP) genera logs di allarmi che vengono memorizzati sul DATABASE LOG;
- TRITON AP-ENDPOINT DLP (Agent) – Il Triton AP-ENDPOINT (Agent) monitora in tempo reale la violazione delle policy in vigore e genera log di allarme che vengono inviati al Triton Manager APX (Console DLP). Attraverso tale Agent è possibile controllare costantemente lo spostamento (inteso come copia/invio/ricezione) dei dati nella rete e/o attraverso le periferiche di una postazione di lavoro (pendrive usb, stampanti, cd/dvd, dischi esterni).

3.10.2. Servizio L2.S3.5 – Data loss/leak prevention (tecnologia Raptor)

La soluzione software RaPToR (Ransomware Prevention Toolkit and Rescue), di Cyber Intuition di seguito per brevità "Raptor o software", è una piattaforma software di sviluppo interamente italiano, che si pone come obiettivo la tutela dei dati, presenti all'interno delle memorie di massa della macchina sulla quale il software è installato, da infezioni locali.
RaPToR intercetta l'esecuzione dei Ransomware analizzando il comportamento dei processi in esecuzione della macchina e impedendo, ove possibile, la crittografia dei dati utente e di sistema e permettendo il recupero di eventuali dati crittografati mediante il ripristino da copie di

sicurezza generate costantemente.

Funzionalità

RaPToR previene la perdita dei dati dovuti alla crittografia da parte dei Ransomware e ne permette l'eventuale recupero da backup con tecnologia Shadow Copy create automaticamente a cadenza giornaliera o personalizzata qualora una nuova tipologia di Ransomware riesca a bypassare i sistemi di riconoscimento del motore comportamentale. Tale funzionalità, vero e proprio core del software, permette di ridurre al minimo la presenza di falsi positivi. Le funzionalità di base del software si compongono di due moduli distinti con compiti ben definiti:

- Motore di analisi comportamentale, con funzionalità di Memory Dump e Honeypot.
- Funzionalità di tutela e ripristino dei dati tramite Shadow Copy.

Tali funzionalità sono presenti all'interno di una componente agent, snella e leggera, da installarsi sulle macchine (client e server), che permette il monitoraggio dei processi e delle loro attività, e la rilevazione e il blocco degli attacchi.
Le funzionalità offerte a copertura dei requisiti sono le seguenti:

- rilevazione dei dati che transitano nell'organizzazione, ovunque siano archiviati, e valutazione del rischio di perdita di dati (DLP Risk Assessment); La piattaforma è in grado di monitorare e analizzare gli accessi che vengono effettuati sui dati da parte dei processi della macchina e degli utenti relativi a questi, classificando i processi stessi come malevoli e valutando real-time il rischio di perdita di informazioni; Questo viene fatto assegnando dei punteggi di rischio ai processi monitorati. Al superamento delle soglie predefinite, vengono attivate le procedure di protezione.
- analisi e classificazione dei dati (DLP Information classification); La piattaforma è in grado di analizzare e classificare i dati di interesse dei processi di tipo ransomware e suggerire una lista di aree/cartelle considerate ad alto rischio, che potrebbero contenere dati sensibili per l'utente.
- 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); La piattaforma è in grado di identificare l'accesso ai dati sensibili ovunque essi risiedano (porte USB, CD, DVD, porte COM & LPT, dischi rimovibili, …) e configurare delle policy. Esempi di configurazioni che possono essere eseguite tramite la piattaforma sono:
  - Indicazione di azioni automatiche in conseguenza di un attacco rilevato (es, shutdown temporizzato e forzato della macchina, riavvio esclusivo in modalità provvisoria, semplice notifica di avvenuta infezione).
  - Configurazione della cartella di destinazione utilizzata per il salvataggio dei file di dump.
  - Indicazione di cartelle specifiche classificate dall'utente come ad alto rischio.
- generazione automatica di alert nel caso in cui vengano violate le policy di sicurezza definite; - La piattaforma è in grado di generare alert in real-time in conseguenza di una rilevazione di possibile infezione ransomware. Gli alert possono essere visualizzati accedendo alla console.
- possibilità di generare report di sintesi (executive summary) e di dettaglio (technical report) sulle analisi svolte; E' possibile generare report di sintesi e di dettaglio tramite le funzionalità della console. In particolare è possibile ottenere (sotto forma di report tabellari e/o grafici):
  - Anagrafica e Report del parco macchine, rilevate all'interno della rete, organizzate secondo gruppi definiti dagli operatori che utilizzeranno la console.
  - Anagrafica e Report degli Stati, per ciascuna macchina sulla quale è installato il software; gli stati di funzionamento tra attivo, allarme, errore, inattivo.
  - Anagrafica e Report delle Versioni del SW e stato dell'Aggiornamento.

- generazione audit trail e gestione profili di audit: - La piattaforma è in grado di gestire la generazione di log in modalità nativa sulle piattaforma windows. Tali log delle attività rilevate, sono memorizzate in un registro dedicato all'interno del sistema operativo Microsoft, e sono visualizzabili anche tramite la console di gestione. All'interno della console sono configurabili dei profili di audit per l'accesso a questi log, che possono a loro volta essere memorizzati in un archivio interno.
- compatibilità con i maggiori protocolli di rete di livello application quali FTP/SFTP/FTPS, HTTP/HTTPS, SMTP e di livello network e transport; La piattaforma, lavorando a livello di endpoint, è in grado di intercettare qualsiasi tipo di accesso ai dati o trasmissione degli stessi.
- compatibilità con i sistemi operativi Windows e Linux: la piattaforma è compatibile con i sistemi operativi Microsoft Windows. Alcune componenti della console sono anche fruibili su sistema operativo Linux, tra cui, a titolo esemplificativo, la WebGUI per l'accesso tramite web browser alle funzionalità di visualizzazione dei log.

La soluzione è installabile sulle seguenti piattaforme:

Versione desktop:

- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10

Versione server:

- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Linux (Web GUI).

E' possibile generare report di sintesi e di dettaglio tramite le funzionalità della console. In particolare è possibile ottenere (sotto forma di report tabellari e/o grafici):

- Anagrafica e Report del parco macchine, rilevate all'interno della rete, organizzate secondo gruppi definiti dagli operatori che utilizzeranno la console.
- Anagrafica e Report degli Stati, per ciascuna macchina sulla quale è installato il software; gli stati di funzionamento tra attivo, allarme, errore, inattivo.
- Anagrafica e Report delle Versioni del SW e stato dell'Aggiornamento.

3.10.3. Servizio L2.S3.6 – Database security (tecnologia McAfee)

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

Il servizio di compone delle seguenti funzionalità:

- monitoraggio in tempo reale di tutte le transazioni del database
- 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 di governance IT interni;

- blocco 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) e indicazione di script correttivi.

Il servizio prevede l'installazione di un sw agent "on premise" ed è compatibile con i principali DB quali Oracle, MS SQL Server, IBM DB2, SAP Sybase, MySQL.

Architettura

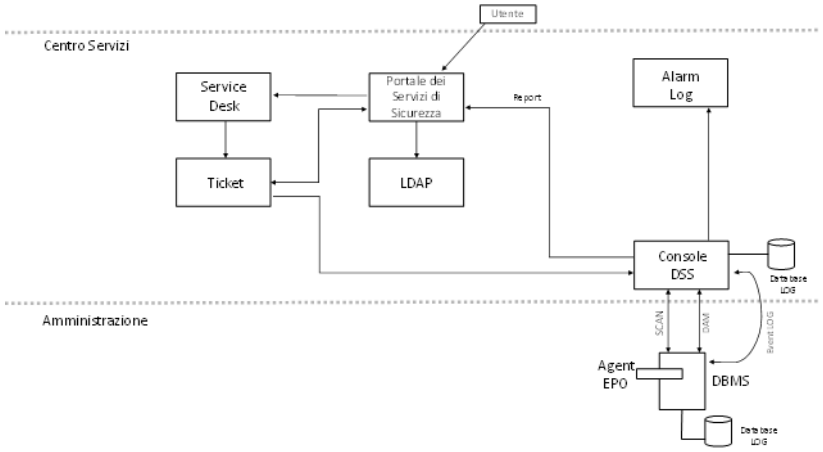


Fig 17 Architettura servizio database security

L'architettura è dislocata presso:

- Centro Servizi;
- Pubblica Amministrazione.

Presso il Centro Servizi sono dislocati:

- Portale dei Servizi di Sicurezza: per effettuare nuove richieste di servizi (es.: creazione o modifica di una policy);
- LDAP: per l'accesso ai servizi con utenza di dominio;
- Service Desk / Ticket: piattaforma di ticketing per la gestione delle richieste;
- Event Logs: per la raccolta di tutti gli eventi;

Presso la Pubblica Amministrazione:

- DBMS;
- Agent ePO.

La piattaforma tecnologica a supporto del servizio Database Security consentirà all'Amministrazione la protezione in tempo reale delle basi dati da minacce esterne o interne mediante la configurazione di policy "ad hoc" in grado di generare alerting su attività sospette fino al suo eventuale blocco.

Tale soluzione è basata sulla tecnologia leader di mercato McAfee DSS ed è in grado di impostare una vasta gamma di controlli per la protezione dei database. Individua automaticamente i database nella rete, determina se le ultime patch sono state applicate ed esegue test su password

deboli, account predefiniti e altre minacce diffuse, abilitando quindi la dimostrazione della conformità e migliorando la protezione delle risorse di dati critiche.

L'architettura prevede l'installazione di un agent "on premise" sulle macchine DB dell'Amministrazione incluse nel perimetro di monitoraggio come attuatore delle policy e la presenza di un sistema di gestione all'interno del Centro Servizi, che avrà il triplice ruolo di:

- raccogliere in maniera centralizzata e attraverso canali cifrati (SSL) i log generati dagli agent;
- gestire la soluzione nelle sue funzioni di sicurezza previste dal servizio comprese la gestione delle configurazioni di policy, le scansioni delle vulnerabilità, la definizione degli alert e report;
- rendere disponibile ad un team di specialistici per la gestione degli incidenti, un cruscotto (dashboard) per il monitoraggio.

Tecnologie e Prodotti di riferimento

Il servizio viene erogato mediante tecnologia McAfee, secondo l'architettura applicativa riportata nello schema.

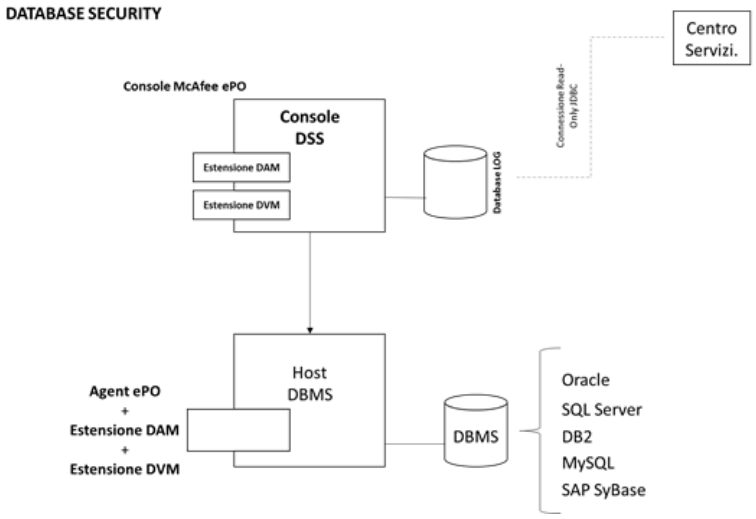


Fig 18 Architettura servizio database security

i seguito il dettaglio sui prodotti utilizzati:

- Console McAfee DSS – La console è basata su piattaforma McAfee e comprende le due estensioni DAM (Database Activity Monitoring) e DVM (Database Vulnerability Manager). La console McAfee DSS è dotata di un Database interno per lo storage dei log basato su SQL Server ePo DB. I log vengono inviati al SIEM del Centro Servizi tramite una connessione sicura read-only JDBC. La connessione JDBC è studiata per poter essere collegata a qualsiasi motore database, indipendentemente da esso e dalla piattaforma di utilizzo. La connessione JDBC è basata su tecnologia Java.
- Console McAfee ePO – Il software ePolicy Orchestrator è la componente principale della piattaforma McAfee, che consente la gestione unificata della sicurezza dei dati. Il software ePolicy Orchestrator è una piattaforma di gestione scalabile ed estendibile che consente di centralizzare la gestione e l'imposizione delle policy di sicurezza. Grazie al software ePolicy Orchestrator è possibile eseguire le seguenti attività per la sicurezza del Database:
    - Gestire e applicare la sicurezza utilizzando le assegnazioni delle policy e le attività client;

- Aggiornare i file di definizione dei rilevamenti (DAT), motori antivirus e altro contenuto di sicurezza necessario affinché il software di sicurezza utilizzato sia in grado di proteggere i sistemi gestiti;
- Creare report utilizzando la procedura guidata del sistema di query integrato, in cui sono visualizzati grafici e tabelle informativi, configurati dall'utente, contenenti i dati per la protezione della rete.

3.10.4. Servizio L2.S3.6 – Database security (tecnologia Imperva)

L'infrastruttura tecnologica è a tre livelli e si avvale delle seguenti componenti.

SecureSphere Gateway: Il Gateway è l'appliance responsabile dell'analisi del traffico SQL in tempo reale e dell'enforcement (in collaborazione con l'Agent) delle policy.

Il gateway può essere configurato per il blocco o per la sola segnalazione a seconda della funzionalità e del livello della minaccia.

Le appliance Imperva SecureSphere possono monitorare e proteggere un numero illimitato di database, limitato solo dal throughput espresso in TPS (Transactions Per Second).

SecureSphere Agent: L'Agent è la componente software che, installata sui DB server, cattura tutta l'attività del database e la inoltra al Gateway per l'elaborazione. L'Agent è in ascolto sulle interfacce di rete, loopback, SHM, BEQ, IPC e tutti i connettori che il sistema di database mette a disposizione per l'interrogazione dei dati. L'Agent ha una capacità di elaborazione limitata, per ridurre al minimo l'occupazione di risorse sul DB server; la maggior parte dell'elaborazione e del parsing dei comandi SQL avviene sul Gateway.

SecureSphere MX Management Server: L'unità MX Server è il punto focale di un'architettura di gestione a tre livelli che permette di gestire simultaneamente gateway multipli, rispondendo alle esigenze di scalabilità delle grandi organizzazioni.

Le policy di sicurezza sono gestite centralmente e distribuite ai diversi gateway con un singolo click. L'unità MX funge anche da collettore di dati provenienti dai gateway (gli alert, ad esempio).

L'MX Server riceve gli aggiornamenti automatici di signatures, report, normative, policy predefinite da parte dell'ADC (Application Defense Center, il team Imperva che si occupa di reazione ai problemi di security).

L'unità MX Server include anche le funzionalità DAS. DAS (Discovery and Assessment Server) scansiona la rete alla ricerca di database server, classifica i dati in essi contenuti in base al livello di sensibilità, esegue i vulnerability assessment al database.

La soluzione offre piena visibilità sull'utilizzo dei dati e sulle vulnerabilità che affliggono i DB, . Essa consente alle Amministrazioni di attivare se necessario, una protezione attiva dei dati contenuti nei database e si pone come strumento di ausilio al raggiungimento delle compliance rispetto alle normative ed agli standard Internazionali.

Il servizio del RTI ed il framework tecnologico offerto permette il controllo tutti gli accessi ai dati da parte di tutti gli utenti compresi quelli privilegiati (come ad esempio il database administrator).

La soluzione è in grado di rilevare in real-time gli attacchi al database, sia in termini di attacchi tecnici (sfruttamento di vulnerabilità del motore DBMS), sia in termini di attacchi logici (lettura non autorizzata di dati, inserimento/modifica/cancellazione non autorizzata di dati, inserimento/modifica/cancellazione di utenti ed oggetti). La protezione dagli attacchi tecnici è comunemente definita con il termine "virtual patching". Tale strumento di protezione (virtual patching) è continuamente aggiornato dai centri di ricerca specializzati del vendor tecnologico rendendo disponibile in breve tempo la contromisura di sicurezza più idonea. Questa funzionalità oltre a ridurre la finestra di esposizione, permette alle Amministrazioni di gestire le attività di patching e/o upgrade in maniera coerente con i propri processi di manutenzione evolutiva dei software.

A fronte della violazione di una policy di qualunque tipo, è previsto il blocco della connessione verso il DB e l'eventuale quarantena di utente/ip. Il blocco della connessione avviene, nella pratica comune, in real-time su criteri della connessione (ip, processo) o in near-real-time su criteri SQL. E' possibile, ma meno comune, abilitare il blocco in real-time per tutti i criteri, aggiungendo una latenza al processo di ispezione.

Le funzionalità offerte dalla soluzione proposta sono le seguenti:

- *Intrusion Detection & Prevention*
  Protegge in modo evidente i dati dalle minacce, monitorando localmente l'attività su ciascun server database e allertando sulla presenza di utilizzi pericolosi o bloccandoli in tempo reale, anche quando viene eseguito in ambienti virtualizzati o di cloud computing.
- *Vulnerability Assessment*
  Consente la scansione delle sottoreti dell'Amministrazione individuando tutti i DB presenti. Su tali DB e' possibile poi effettuare le scansioni di Vulnerability Assessment (VA) per individuare le vulnerabilita'. Nell'output del risultato delle scansioni viene fornita anche la procedura correttiva.
- *Data Classification*
  Permette di analizzare i dati contenuti nel database e classificarli per tipologia (carte di crediti, dati anagrafici, password, ecc.)
- *Virtual Patching*
  Patching semplificato che non richiede downtime. Applicando le patch mancanti e correggendo le configurazioni errate individuate dalla scansione delle vulnerabilità di Database Security Monitoring e' possibile migliorare immediatamente lo stato di sicurezza dei database, senza interrompere la attività in produzione grazie alla tecnologia di patching virtuale. La soluzione. protegge anche i database senza patch contro gli attacchi di tipo zero-day bloccando gli attacchi che possono sfruttare le vulnerabilità note e terminando le sessioni che violano le policy di sicurezza.
- *Auditing and Compliance*
  - Tracciatura delle operazioni effettuate sul database con altissimi livelli di scalabilità e indipendentemente dalle funzioni di native audit del database stesso.
  - Compliance con i più diffusi standard normativi (CobiT/SOX, PCI DSS, HIPAA, G.d.P Dlgs 196/2003 e DBA 2009, ISO 27001, EU Data Privacy Directive) e con le best practice organizzative
  - Reportistica con un centinaio di template customizzabili
  - Interfaccia di forensics per investigazioni mirate

La soluzione è compatibile con Oracle, DB2, Microsoft SQL Server, Informix, MySQL, Sybase, Postgres, Netezza, Teradata su sistemi operativi Linux RHEL, Suse, Oracle, Solaris, HP-UX, AIX, Windows Server.

Analisi dei DB e valutazione dei rischi – Il processo di Vulnerability Assessment individua le vulnerabilità e gli errori di configurazione dei DB server. Viene fornito un indice di rischio per ogni test effettuato. Conseguentemente a un processo di Data Classification sopra descritto, è possibile avere un indice di rischio per tipologia di dato, anzichè semplicemente per server, permettendo così lo svincolo dalla dislocazione di server e storage.

Individuazione alterazioni – Tramite le policy di security è possibile individuare tutte le operazioni DML, DDL, DCL e l'utilizzo delle Stored Procedures.

Creazione personalizzata di policy di sicurezza – Imperva SecureSphere include decine di policy predefinite. E' comunque possibile creare policy personalizzate basate su un set di oltre 30 criteri.

Arresto in tempo reale delle sessioni che violano le policy – L'arresto delle sessioni avviene in real-time o near-real-time nelle modalità sopra esposte.

Controllo degli accessi, identificazione e arresto dei comportamenti non autorizzati – Tramite le policy di sicurezza sopra descritte è possibile controllare gli accessi (connettore utilizzato, ip, porta,

username, applicazione, utenza e nome macchina a sistema operativo) e bloccare quanto non autorizzato.

Classificazione delle minacce – Il modulo di Risk Management permette non solo di ottenere un indice di rischio relativo alle singole vulnerabilità, ma di calcolarne il rischio complessivo basandosi sulla classificazione del dato.

Generazione reportistica – I report sono ampiamente customizzabili. Il prodotto viene fornito con circa 100 template modificabili, che includono best practice e report di compliance alle normative più comuni. Sono disponibili i formati PDF e CSV. I report sono schedulabili e consentono la creazione di grafici e raggruppamenti.

Funzionalità migliorative principali

Policy di alert/blocco su select e su qualunque comando SQL: Riteniamo molto importante anche la protezione da accessi non autorizzati in lettura dei dati sensibili.La protezione dalle sole alterazioni richiesta dal Committente garantisce l'integrità del dato, ma non la sua riservatezza, garantita invece da policy che includano il comando "select".

Classificazione dei dati: Tramite la classificazione automatizzata dei dati è possibile taggare le tabelle dei database con la tipologia di dati in esse contenuta. Questo consentirà di creare policy a partire da criteri quali "Tabelle contenenti dati anagrafici" invece che utilizzare nomi statici di tabelle.

User chaining: Consente di individuare quando gli utenti privilegiati tentano di anonimizzarsi eseguendo "su root" o "su oracle" dopo il login a sistema con utenza nominale. Negli alert viene visualizzata tutta la catena di utenze.

Policy di audit: consentono la tracciatura delle operazioni fatte su DB

I report sono ampiamente customizzabili. Il prodotto viene fornito con circa 100 template modificabili, che includono best practice e report di compliance alle normative più comuni. Sono disponibili i formati PDF e CSV.

3.10.5. Servizio L2.S3.6 – Database security (tecnologia Guardium)

IBM Security Guardium si basa su un'architettura scalabile, multi-tier disegnata per crescere senza problemi dalla protezione di un singolo database alla protezione di migliaia di database geograficamente distribuiti.

L'architettura della soluzione supporta sia la configurazione single-tier che multi-tier e si basa su due tipologie di componenti:

- Agent, componente che viene installato sul sistema che ospita il database server e cattura real-time le attività svolte nel database;
- Appliance, di due tipi:
  - Collector che raccoglie i dati acquisiti dagli Agent
  - Aggregator che consolida i dati raccolti dai Collector e, nel caso in cui sia "promosso" a svolgere funzionalità amministrative, diventa Central Manager.

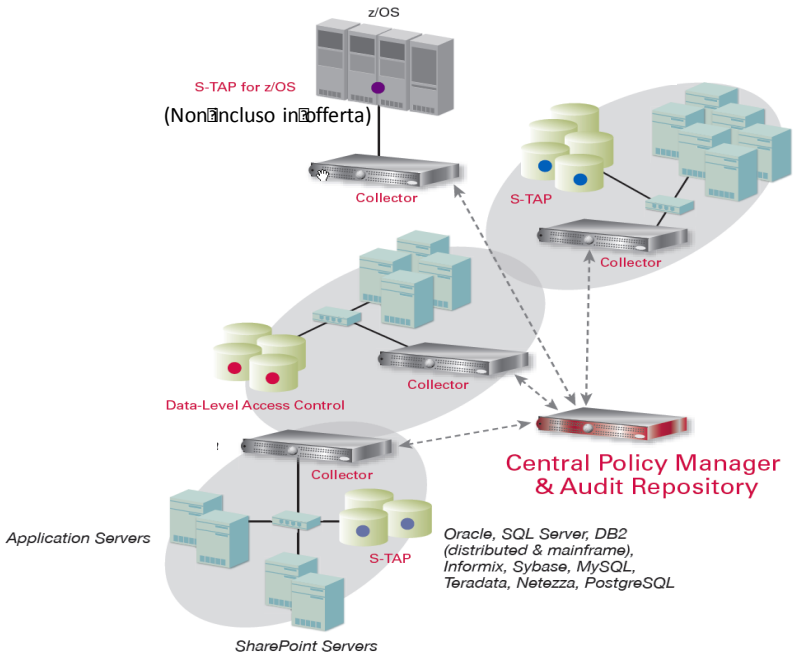
Gli appliance possono essere fisici, quindi dotati di hardware e software di base, oppure virtuali. In quest'ultimo caso essi possono essere ospitati su un'infrastruttura Intel x86-VMware-Linux.

L'Agent è la componente software che, installata sui DB server, cattura tutta l'attività del database e la inoltra al Collector per l'elaborazione In questo modo la soluzione IBM Security Guardium permette di intercettare non solo le tradizionali comunicazioni client ed application web-based ma anche ogni accesso al DB che abbia origine direttamente sul database server.

L'Agent non richiede nessun cambiamento ai database o alle applicazioni (qualora queste applicazioni non dispongano di tracciamento specifico a parte) e non presenta impatti significativi dal punto di vista prestazionale sui sistemi dove questo viene installato.

IBM Security Guardium consente di avere uno o più Aggregator/Central Manager al fine di ottenere una vista complessiva di tutti i dati monitorati e fornire un unico punto di gestione dei Collector. Questo permette di gestire regole, policy e alert sia a livello di ogni singolo appliance sia a livello enterprise che multi enterprise.

La figura successiva descrive un esempio di architettura di IBM Security Guardium.



Descrizione della soluzione:

IBMSecurity Guardium fornisce il monitoraggio dell'attività dei dati, fornisce la cognitive analytics per rilevare attività insolite attorno ai dati sensibili, impedisce gli accessi degli utenti non autorizzati, fornisce avvisi su attività sospette, automatizza i flussi di lavoro di conformità e fornisce una protezione dalle minacce interne ed esterne. L'applicazione delle policy di sicurezza in tempo reale ed un monitoraggio costante proteggono i dati aziendali, senza modifiche o impatti negativi sulle prestazioni delle fonti dei dati o delle applicazioni. IBM Security Guardium si basa su un'architettura scalabile che fornisce visibilità completa sull'attività dei dati per tutti i principali database e data warehouse.

Fornisce granularità e visibilità al 100% di tutte le transazioni del database, incluse le operazioni SQL, le eccezioni di sicurezza (come login falliti) e le attività degli utenti privilegiati.

IBM Guardium permette di definire le policy più appropriate per monitorare e proteggere i propri dati sensibili presenti su qualsiasi Database (Oracle, SQL Server, DB2, Sybase, MySQL, Informix, Netezza, PostgreSQL e altri), anche su ambienti IBM z/OS e IBM System i (AS/400) – (non in offerta), senza richiedere modifiche al Database stesso o alle applicazioni, e senza gravare sulle performance del sistema.

IBM Security Guardium è inoltre una soluzione consolidata per fornire valore significativo non solo a qualsiasi database relazionale ma anche alle tecnologie emergenti, ad esempio le architetture Big-Data (Hadoop, Cloudera, BigInsights, ...).

L'architettura di IBM Guardium inoltre:

- offre la capacità, da parte degli agent, di bufferizzare localmente le informazioni di Auditing in mancanza di collegamento di rete.
- può prevedere una configurazione distribuita, in High Availability (HA) e con bilanciamento del carico al fine di garantire l'efficacia e l'efficienza delle attività.
- consente di effettuare attività di crittografia per le comunicazioni tra Agent e Appliance per incrementare la riservatezza delle comunicazioni.

La soluzione è compatibile con Oracle,Microsoft SQL e SQL Cluster, IBM DB2 LUW,IBM DB2 Purescale, Sybase ASE,Teradata,MySQL,MariaDB,SAP HANA,PostgreSQL,IBM Informix ,Sun MySQL and MySQL Cluster ,IBM Netezza, Cloudera, Aster, Cassandra, CouchDB,Greenplum DB, Horton Works,MongoDB su sistemi operativi Linux RHEL, Suse, Ubuntu, Oracle, Solaris, HP-UX, AIX, Windows Server.

L'elenco completo delle piattaforme supportate da IBM Guardium è consultabile a questo link:

http://www-01.ibm.com/support/docview.wss?uid=swg27047801

Funzionalità richieste

Analisi dei DB e valutazione dei rischi – Il processo di Vulnerability Assessment è parte integrante della soluzione IBM Guardium e consente di fare lo scan della infrastruttura dati al fine rilevare (detect) vulnerabilità e suggerire azioni (remedial). Identifica esposizioni quali patch mancanti, weak passwords, modifiche non autorizzate, misconfigured privileges ed altre aggiuntive continuamente aggiornate in automatico. IBM Guardium segnala inoltre anche esposizioni dovute a comportamenti errati quali condivisione di accounting, eccessivo utilizzo di profili amministrativi e attività non coerenti alle finestre lavorative.

Individuazione alterazioni – Tramite le policy di security è possibile non solo individuare tutte le operazioni e l'utilizzo delle Stored Procedures ma discriminare operazioni di amministrazione dei DB rispetto a quelle di gestione dei dati o aggregare logicamente i client in base all'indirizzo IP/subnet, all' hostname ed al source program.

Creazione personalizzata di policy di sicurezza – IBM Guardium prevede la possibilità di configurare delle policy di monitoraggio personalizzate per definire le regole di tracciamento . Nelle policy è possibile utilizzare gruppi di utenti per diversificare le regole di tracciamento. I gruppi possono essere alimentati tramite connessione a LDAP esterno (quale ad esempio Active Directory), tramite inserimento manuale, oppure utilizzando specifiche API che consentono il caricamento da file.

Arresto in tempo reale delle sessioni che violano le policy – In tempo reale sono terminare le richieste di accesso ai DB prima ancora di poter accedere ai dati stessi. L'Agent S-TAP intercetta le richieste lanciate dagli utenti (anche priviledge user), verifica le policy ed in caso di violazione effettua la drop terminando così la sessione, impedendo ogni possibile modifica ai dati.

Controllo degli accessi, identificazione e arresto dei comportamenti non autorizzati – Tramite le policy di sicurezza sopra descritte è possibile controllare gli accessi (connettore utilizzato, ip, porta, username, applicazione, utenza e nome macchina a sistema operativo) e bloccare quanto non autorizzato.

Classificazione delle minacce – IBM Guardium automaticamente fa la discovery e la classificazione di oggetti e informazioni sensibili. Quando questo vengono rilevati, vengono identificati e classificati in meta-dati (tagged). La classificazione può generare alert immediati, sulla base di politiche predefinite, per aiutare ad identificare e risolvere esposizioni all'interno di processi di business.

Inoltre la funzione di Vulnerability Assessment permette di testare l'infrastruttura e la configurazione del DB rilevando vulnerabilità note sulla rete e definite dall'organismo della MITRE Corporation costantemente aggiornate al dizionario degli identificativi CVE.

Generazione reportistica –E' possibile avere un unico repository centralizzato su cui andare a svolgere attività di reportistica e compliance, ottimizzazione delle performance, investigazioni e

analisi forensi. La soluzione fornisce la possibilità di creare report completamente personalizzati, o utilizzare quelli messi già a disposizione per analizzare i dati raccolti. Tutti i report IBM Guardium possono essere esportati in formato sia CSV che PDF.

Funzionalità migliorative principali

Policy di alert/blocco su select e su qualunque comando SQL: Riteniamo molto importante anche la protezione da accessi non autorizzati in lettura dei dati sensibili.La protezione dalle sole alterazioni richiesta dal Committente garantisce l'integrità del dato, ma non la sua riservatezza, garantita invece da policy che includano il comando "select".

Classificazione dei dati: Tramite la classificazione automatizzata dei dati è possibile taggare le tabelle dei database con la tipologia di dati in esse contenuta. Questo consentirà di creare policy a partire da criteri quali "Tabelle contenenti dati anagrafici" invece che utilizzare nomi statici di tabelle.

User chaining: Consente di individuare quando gli utenti privilegiati tentano di anonimizzarsi eseguendo "su root" o "su oracle" dopo il login a sistema con utenza nominale. Negli alert viene visualizzata tutta la catena di utenze.

Policy di audit: consentono la tracciatura delle operazioni di configurazione fatte su DB.

Anomaly Detection: un meccanismo di Self Learning, crea una base di conoscenza (baseline) del comportamento delle attività sui DB per circa 30 giorni. Dopo tale fase il sistema è in grado di intercettare le operazioni anomale rispetto alla propria base di conoscenza, ed inviare alert sul comportamento anomalo intercettato.

Individuazione di frodi a livello applicativo: gli Application Server usano utenze generiche per effettuare query sui DB, IBM Guardium è in grado di integrarsi con i principali framework (Oracle EBS, PeopleSoft, SAP, Siebel, Business Objects, Cognos…) e applicazioni (WebSphere….) per individuare lo user applicativo che ha generato il particolare comando SQL di accesso sul DB.

I report sono ampiamente customizzabili. Il prodotto viene fornito con circa 100 template modificabili, che includono best practice e report di compliance alle normative più comuni. Sono disponibili i formati PDF e CSV.

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

Il servizio 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 si compone delle seguenti funzionalità:

- funzionalità standard firewall (policy enforcement, stateful 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) e compliance.

Architettura

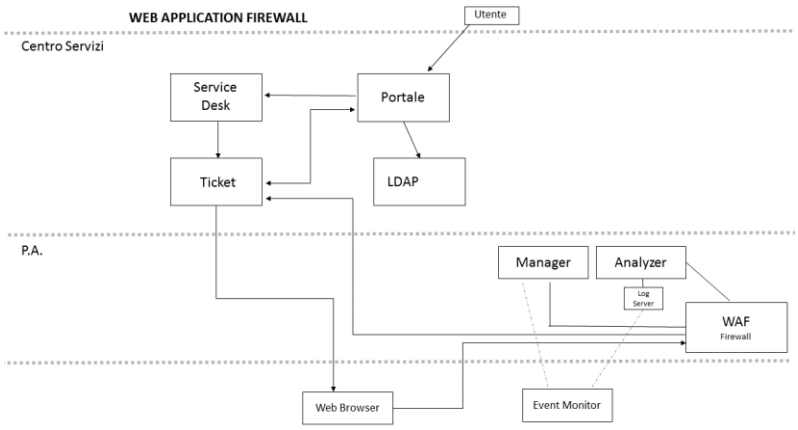


Fig 19 Architettura servizio web application firewall

L'architettura è dislocata presso:

- Centro Servizi;
- Pubblica Amministrazione (previa allocazione di spazi attrezzati, rack,..).

Presso il Centro Servizi sono dislocati:

- Portale dei Servizi di Sicurezza: per effettuare nuove richieste di servizi (es.: creazione o modifica di una policy);
- LDAP: per l'accesso ai servizi con utenza di dominio;
- Service Desk / Ticket: piattaforma di ticketing per la gestione delle richieste;
- Event Logs: per la raccolta di tutti gli eventi;

Presso la Pubblica Amministrazione:

- WAF: per l'ispezione dei contenuti e delle vulnerabilità sulla rete;
- FortiManager: per la gestione delle richieste;
- FortiAnalyzer: per l'analisi e la reportistica della rete e delle vulnerabilità;

Tecnologie e Prodotti di riferimento

Il servizio viene erogato mediante tecnologia Fortinet, secondo l'architettura applicativa riportata nello schema.

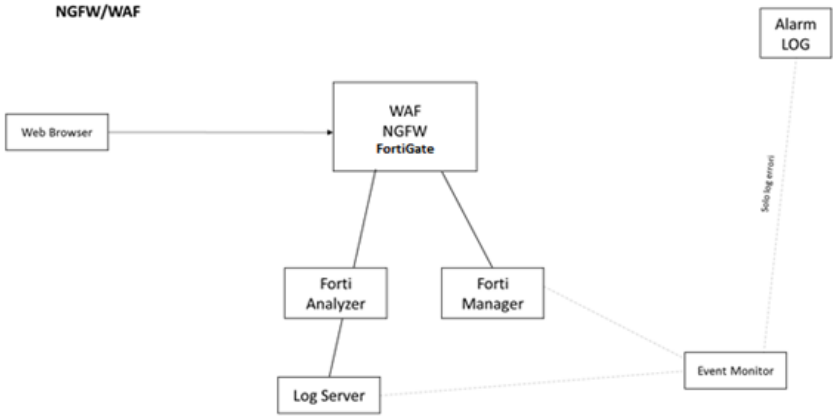


Figura 1 - Schema applicativo dei Servizi WAFM e NGFM

Fig 20 Architettura servizio WAFM/WAFl

Le componenti principali dell'architettura applicativa sono di seguito descritte.

- Gateway FortiGate - Il Firewall è alla base della soluzione di sicurezza Unified Threat Management (UTM), infatti i servizi di protezione e controllo dei flussi forniti dal firewall sono completamente integrati con le altre funzionalità di sicurezza chiave offerti dalla soluzione tra cui VPN, Antivirus, Intrusion Prevention System (IPS), Web Filtering, Antispam, Traffic Shaping e Web Application Firewall (WAF). La tecnologia di Firewalling adottata per l'erogazione del servizio introduce una serie di benefici tra cui:
    - Protezione multilivello tramite applicazione di profili di configurazione di sicurezza differenziati, attraverso l'integrazione completa con le altre tecnologie di sicurezza (Antivirus, IPS, etc.);
    - Full content inspection per i principali protocolli di rete tra cui: HTTP, FTP, SMTP, POP3, IMAP, IM e NNTP;
    - Possibilità di definire con semplicità protocolli e applicazioni custom ed elevato grado di granularità nella definizione delle politiche di protezione;
    - Diverse modalità di funzionamento (Transparent, NAT Statico e NAT Dinamico) che consentono un facile adattamento all'infrastruttura di rete e un'elevata versatilità d'implementazione;
    - Supporto dei protocolli di routing (RIP, OSPF, BGP e PIM) a garanzia di un semplice posizionamento della componente anche nelle infrastrutture di rete complesse;
    - Supporto dei protocolli H.323, SIP e SCCP con capacità di protezione per i servizi VoIP.
- FortiAnalzyer – fornisce analisi e reporting per la sicurezza di rete e aggrega in maniera sicura i log generati dalle componenti Gateway. Consente, inoltre, di analizzare e visualizzare in maniera rapida le minacce, eventuali anomalie o inefficienze e l'utilizzo della rete. L'Analyzer permette di monitorare e mantenere l'identificazione di schemi di attacco, policy d'uso accettabili e dimostrare la conformità alle policy.
- FortiManager - fornisce una capacità di configurazione differenziata e centralizzata in modo semplice tramite provisioning basato su policy, gestione degli aggiornamenti e monitoraggio della rete end-to-end. La componente Manager supporta anche le funzionalità di *multitenancy* tramite la possibilità di definire domini amministrativi geografici o funzionali.

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

Il servizio di Secure web gateway consente 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.

Il servizio di compone delle seguenti funzionalità:

- 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;
- aggiornamento automatico delle liste di siti malevoli;
- produzione di report di sintesi (executive summary) e di dettaglio (technical report)
- gestione della navigazione tramite utilizzo di categorie di siti web e protocolli.

<u>Architettura</u>

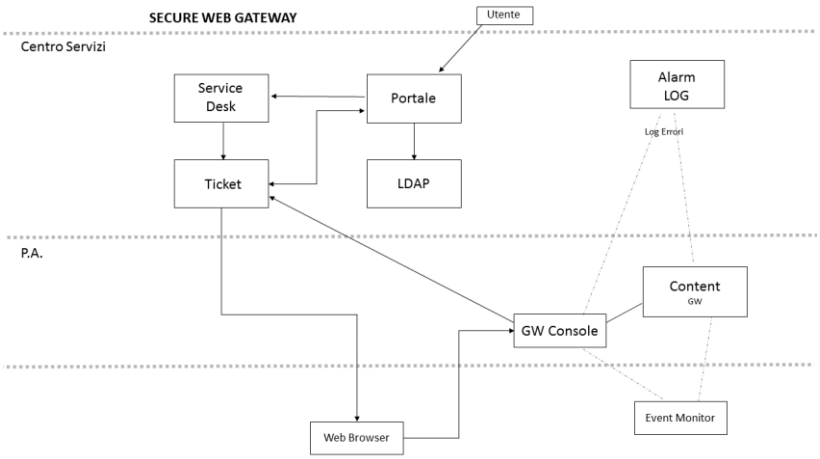


Fig 21 Architettura servizio secure web gateway

L'architettura è dislocata presso:

- Centro Servizi;
- Pubblica Amministrazione (previa allocazione di spazi attrezzati, rack,..).

Presso il Centro Servizi sono dislocati:

- Portale dei Servizi di Sicurezza: per effettuare nuove richieste di servizi (es.: creazione o modifica di una policy);
- LDAP: per l'accesso ai servizi con utenza di dominio;
- Service Desk / Ticket: piattaforma di ticketing per la gestione delle richieste;
- Alarm Logs: per la raccolta di tutti gli eventi;

Presso la Pubblica Amministrazione:

- Content GW: per l'ispezione dei contenuti HTTP/HTTPS;
- GW Console: per la gestione delle richieste.

Tecnologie e Prodotti di riferimento

La figura seguente illustra l'architettura applicativa del servizio SWG, con indicazione dei prodotti utilizzati (tecnologia FORCEPOINT)

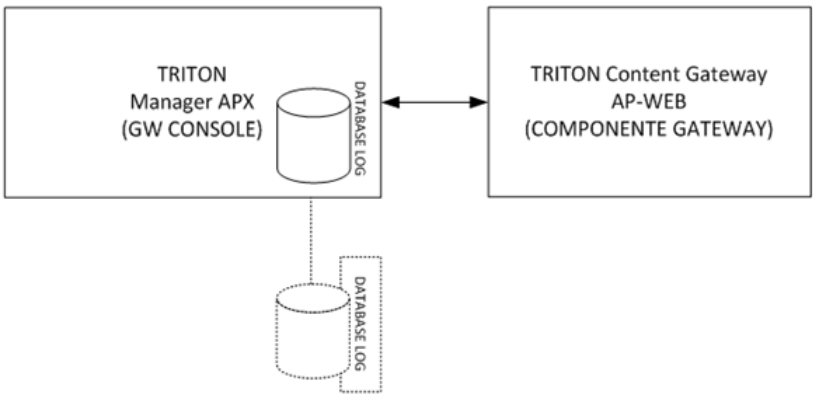


Figura 1 – Schema applicativo dei Servizi di Secure Web Gateway

Fig 22 Schema applicativo servizio secure web gateway

Di seguito il dettaglio sui prodotti che costituiscono l'architettura applicativa:

- TRITON Manager APX (GW Console) – consente di applicare le policy di sicurezza su uno o più client, identificati tramite indirizzo IP, che accedono a Internet attraverso la componente gateway. La TRITON Manager APX (GW Console) è accessibile tramite Web Browser con connessione sicura SSL e genera logs di allarmi che vengono memorizzati sul DATABASE LOG.
- TRITON Content Gateway AP-WEB (Componente GW) – si occupa della categorizzazione automatica di siti dinamici Web 2.0, categorizzazione automatica di nuovi siti non classificati, ispezione dei contenuti anche in sessioni cifrate HTTPS e blocco di siti considerati potenzialmente malevoli. Può anche fornire funzionalità di web cache, migliorando l'utilizzo della banda e le prestazioni della rete.

In merito al precedentemente citato Database Log si specifica che, allo scopo di garantire la piena efficienza del servizio (es.: adeguato supporto per la scrittura di tutti i log e per il reporting), nel caso in cui quest'ultimo si applicasse ad un numero elevato di postazioni di lavoro (oltre le 5.000 unità), è previsto l'utilizzo di un DB esterno installato presso l'Amministrazione, che sarà fornito dal RTI qualora l'Amministrazione non ne fosse già dotata. Per postazioni di lavoro inferiori a 5000 unità, sarà sufficiente il DATABASE LOG già presente nello stesso server del componente TRITON Manager APX.

3.11. 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 (Computer Emergency Response Team) 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) ;
- penetration test di tipo applicativo e infrastrutturale;
- encryption dei dati memorizzati sulle postazioni di lavoro.

Il Fornitore metterà a disposizione dell'Amministrazione servizi professionali erogati attraverso l'impiego di figure professionali di comprovata esperienza, maturata nel corso degli anni per le tematiche oggetto del servizio e con riferimento a progetti realizzati presso PA e organizzazioni private, sia nel territorio nazionale sia internazionale. Tali servizi saranno erogati esclusivamente nella modalità "on premise" con gli strumenti hardware e software presenti presso l'Amministrazione.

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.

Figure professionali

Il Fornitore ha l'obbligo di di erogare i servizi professionali secondo i profili riportati nella tabella seguente (come da richiesta del Capitolato Tecnico e caratteristiche migliorative espresse nell'Offerta Tecnica)

Qualifica Professionale	Capo Progetto
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Esperienze lavorative	• Minimo 12 anni, di cui almeno 4 nella funzione • Direzione di progetti complessi nell'area della sicurezza in contesti multidisciplinari e multi-servizi. • Redazione di documentazione di progetto • Controllo realizzazione procedure • Stima di risorse per realizzazione di progetto • Stima di tempi e pianificazione attività • Analisi e progettazione di sistemi informativi, package, procedure complesse • Uso di tecniche e prodotti software per project management e risk management • Responsabilità su gruppi di progetto
Conoscenze	• Conoscenze ed uso di tecniche e prodotti software per project management e risk management • Tecniche e metodi di quality management, norme ISO, modalità di certificazione • Tecnologie e soluzioni per servizi di sicurezza • Autorevolezza e comprovata esperienza in progetti di grandi/medie dimensioni • Progettazione e realizzazione di soluzioni di sicurezza • Conoscenza approfondita dei processi di Security Governance e Security Management

Qualifica Professionale	Capo Progetto
	• Procedure di monitoraggio e auditing di progetti • Modelli di definizione e monitoraggio di Service Level Agreement • Strumenti MS Office 2010 • Conoscenza della lingua inglese (tecnica) • Ottime capacità relazionali

Tabella 6 – Figura professionale Capo Progetto

Qualifica Professionale	Security Architect
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Esperienze lavorative	• Minimo 10 anni, di cui almeno 5 di provata esperienza nella specifica funzione. • Analisi e identificazione dei i rischi legati all'utilizzo di servizi informatici • Individuazione soluzioni per garantire livelli di sicurezza complessivi per il sistema informativo adeguato alle specifiche esigenze. • Supporto per implementazione di soluzioni di sicurezza • Definizione di procedure organizzative per la piena efficacia dei sistemi di sicurezza.
Conoscenze	Solide competenze metodologiche e tecnologiche in relazione alle architetture di sicurezza per rispondere alle minacce informatiche ed in relazione alle soluzioni dei principali *vendor*, almeno nei seguenti ambiti: • sicurezza delle reti, incluse le reti wireless • sicurezza dei sistemi operativi • sicurezza dei Data Center • sicurezza ambienti Cloud • controllo degli accessi e della gestione delle identità • sicurezza e-mail, accessi e applicazioni web

Tabella 7 – Figura professionale Security

Qualifica Professionale	Specialista di Tecnologia/Prodotto Senior
Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Esperienze lavorative	• Minimo 8 anni, di cui almeno 4 nella funzione • Analisi e progettazione di sistemi informativi, package, procedure complesse • Redazione di specifiche di progetto • Redazione di studi di fattibilità
Conoscenze	• Esperienza nell'utilizzo di metodologie di project management • Mercato e tendenze evolutive della sicurezza • Tecnologie e soluzioni per servizi di sicurezza • Progettazione e realizzazione di soluzioni di sicurezza • Conoscenza approfondita dei processi di Security Governance e Security Management • Procedure di monitoraggio e auditing di progetti. • Conoscenze approfondite dei sistemi operativi Unix e Windows per aspetti legati alla gestione della sicurezza • Buona conoscenza della lingua inglese

	• Strumenti MS Office 2010 • Conoscenza della lingua inglese (tecnica) • Ottime capacità relazionali

Tabella 8 – Figura professionale Specialista di Tecnologia/Prodotto Senior

Qualifica Professionale	Specialista di Tecnologia/Prodotto
Titolo di studio	Laurea in discipline tecniche o scientifiche
Esperienze lavorative	• Minimo 4 anni, di cui almeno 2 nella funzione • Redazione di specifiche di progetto • Partecipazione a gruppi di lavoro nell'ambito di progetti di realizzazione nell'area delle telecomunicazioni e della sicurezza
Conoscenze	• Conoscenza delle principali tendenze evolutive delle architetture tecnologiche • Architetture di soluzioni di telecomunicazioni. • Conoscenza ed esperienza nell'utilizzo di soluzioni di sicurezza • Conoscenze dei sistemi operativi Unix e Windows per aspetti legati alla gestione della sicurezza • Conoscenza delle best practice di ITIL v3 • Strumenti MS Office 2010 • Conoscenza della lingua inglese (tecnica) • Ottime capacità relazionali

Tabella 9 – Figura professionale Specialista di Tecnologia/Prodotto

In aggiunta ai requisiti sopra riportati, sono richieste ulteriori caratteristiche che dipendono dalla specifica tipologia di servizio di sicurezza e dal profilo professionale considerato, come dettagliato nella seguente tabella:

Servizi	Profilo Professionale	Caratteristiche aggiuntive
Static application security testing, **Dynamic application security testing,** **Mobile application security testing**	Capo progetto	• Conoscenza approfondita della metodologia OWASP • Profonda conoscenza delle architetture SOA
	Specialista di tecnologia/prodotto Senior	• Conoscenza approfondita della metodologia OWASP • Profonda conoscenza delle architetture SOA • Profonda conoscenza dei linguaggi di programmazione web (ASP, ASP.NET, J2EE, PHP, etc) • Conoscenza dei DBMS relazionali (Oracle, My SQL)
	Specialista di tecnologia/prodotto	• Conoscenza approfondita della metodologia OWASP • Conoscenza dei linguaggi di programmazione web (ASP, ASP.NET, J2EE, PHP, etc) • Conoscenza dei DBMS relazionali (Oracle, My SQL)
Data loss/leak prevention, **Database security**	Capo progetto	• Conoscenza ed esperienza nell'utilizzo di metodi e criteri per il controllo e la gestione del rischio in ambito IT • Esperienza nella gestione della protezione delle informazioni • Profonda Conoscenza ed esperienza dei DBMS relazionali (Oracle, My SQL)
	Specialista di tecnologia/prodotto Senior	• Conoscenza ed esperienza nell'utilizzo di metodi e criteri per il controllo e la gestione del rischio in ambito IT • Profonda Conoscenza ed esperienza dei DBMS relazionali (Oracle, My SQL)
	Specialista di	• Conoscenza dei DBMS relazionali (Oracle, My SQL)

Servizi	Profilo Professionale	Caratteristiche aggiuntive
	tecnologia/prodotto	• Conoscenza approfondita delle problematiche di sicurezza dei dati e delle informazioni
Vulnerability assessment, **Web application firewall management e next generation firewall management,** **Security web gateway,** **Servizi di monitoraggio**	Capo progetto	• Conoscenza approfondita teorica e pratica delle problematiche di networking a livello 2 • Esperienza nell'analisi e nella valutazione delle configurazioni e delle regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere il network (Firewall, IPS/IDS, SIEM, soluzioni anti-malware, ecc.) • Esperienza nell'analisi di un'infrastruttura IT complessa volta all'individuazione di problematiche architetturali che ne potrebbero compromettere la sicurezza
	Specialista di tecnologia/prodotto Senior	• Conoscenza approfondita teorica e pratica delle problematiche di networking a livello 2 • Esperienza nell'analisi e nella valutazione delle configurazioni e delle regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere il network (Firewall, IPS/IDS, SIEM, soluzioni anti-malware, ecc.) • Esperienza nell'analisi di un'infrastruttura IT complessa volta all'individuazione di problematiche architetturali che ne potrebbero compromettere la sicurezza
	Specialista di tecnologia/prodotto	• Conoscenza teorica e pratica delle problematiche di networking a livello 2 • Esperienza comprovata nell'analisi delle vulnerabilità di sistemi e reti in esercizio senza impattare sull'operatività ed il funzionamento degli stessi • Conoscenza delle principali tecnologie di network security (firewalling e Intrusion Prevention/Detection) • Conoscenza ed esperienza di configurazione di tecnologie avanzate anti-malware

Tabella 10 – Figure professionali caratteristiche aggiuntive

Il Fornitore entro 10 giorni dalla stipula del Contratto Esecutivo dovrà presentare all'Amministrazione i curriculum vitae che svolgeranno le attività relative ai servizi professionali richiesti, utilizzando lo schema di seguito riportato. Nella redazione dei curricula il Fornitore dovrà privilegiare gli aspetti di interesse per la fornitura. Il documento non dovrà superare orientativamente le 3 pagine.

Nominativo	*(Inserire il Cognome e il Nome della risorsa)* *(Solo in sede di offerta, qualora il candidato non consentisse al trattamento dei dati, sarà possibile presentare il medesimo schema di CV correttamente compilato e allegare, in busta diversa da aprire solo successivamente all'aggiudicazione, il nominativo della risorsa)*		
Ruolo	*(Inserire il Ruolo attualmente ricoperto dalla risorsa)*		
Figura professionale	*(Indicazione del ruolo assegnato alla risorsa in funzione delle figure professionali richieste – es. Capo Progetto, Programmatore….., ecc.. - nonché eventuali specifici ruoli che il fornitore si impegna ad impiegare per la gestione degli aspetti di governo ed evoluzione dei servizi, dei rapporti con la committenza e l'utenza, ecc..)*		
Servizio/attività	*(Fornire l'indicazione del servizio/attività per cui viene proposta la risorsa in relazione agli ambiti definiti nel Capitolato o ad eventuali aspetti caratterizzanti l'Offerta tecnica)*		
Conoscenze	*(Fornire una breve descrizione del profilo professionale in termini di conoscenze/competenze e di aree chiave in cui la risorsa ha maturato esperienze significative)*		
Principali Esperienze Lavorative	*(Indicare le esperienze più significative per la gara in oggetto e comprovanti le competenze richieste nel Capitolato Tecnico, a partire dalla più recente, fornendo una breve descrizione delle attività svolte, del ruolo ricoperto, della durata del progetto. E' necessario suddividere le esperienze per anno e per settore (Es: Pubblica Amministrazione, Bancario, Telecomunicazioni)*		
	Settore	Data inizio-Data fine	Esperienze

Competenze Tecniche	*(Indicare le competenze specifiche di cui si è in possesso)*		
Specializzazioni	*(Indicare eventuali specializzazioni, master, ecc.)*		
	Anno	Titolo	Descrizione
Certificazioni	*(Indicare eventuali certificazioni)*		
	Anno	Titolo	Descrizione
Istruzione	*(indicare i titoli di studio)*		
Lingue	*Per ogni lingua straniera, indicare il grado di conoscenza, dove:* *1 -in grado di leggere* *2 - in grado di leggere e scrivere* *3 - in grado di leggere, parlare e scrivere in maniera più che comprensibile* *4 - fluente sia nello scritto che nell'orale* *5 - madrelingua - (native language)*		
	Lingue		**Grado di conoscenza**
Principali pubblicazioni	*(indicare le principali pubblicazioni)*		

3.12. Servizio L2.S3.10 – Servizi di monitoraggio

Il servizio di monitoraggio (SOC) viene erogato in modalità "*as a service*", al fine di supportare le Amministrazioni nella prevenzione e gestione degli attacchi informatici.

Il SOC è la struttura del Centro Servizi preposta alla raccolta e correlazione degli eventi provenienti dalle aree operative e tecnologiche delle Amministrazioni, al fine di garantire il corretto monitoraggio delle infrastrutture di sicurezza e la tempestiva rilevazione degli incidenti e delle attività sospette.

L'elemento tecnologico cardine costituente il SOC è la piattaforma di Security Information e Event Management (SIEM), ossia un sistema di raccolta e correlazione degli eventi di sicurezza basato sull'analisi di file di log, al fine di individuare eventuali anomalie, attacchi e/o compromissioni.

<u>Architettura SIEM</u>

L'architettura del SIEM si basa sulle seguenti componenti:

1. Console di gestione e monitoraggio;
2. Sistema di Correlazione e Log Management;
3. Collettori di eventi (log) presso le Amministrazioni per l'inoltro verso il correlatore.

Per tutte le fasce di prezzo, ad eccezione della fascia 1, si prevede la possibilità dell'installazione "on premise" presso le Amministrazioni del sistema di raccolta dei log (Collettore)". Per la fascia 1, il livello di raccolta dei log generati dai sistemi delle Amministrazioni è implementato mediante un sistema di "even collector" presente all'interno del Centro Servizi del Fornitore, che consente di mantenere la separazione logica tra i diversi domini di correlazione.

<u>Livelli di servizio</u>

Ai servizi di monitoraggio si applicano i seguenti indicatori di qualità:

- indicatori IQ01 e IQ02 in ambito "Governo della fornitura e servizi professionali";
- indicatori IQ07, IQ08 e IQ09 in ambito "Centri Servizi";

- indicatori IQ10, IQ11, IQ12 e IQ13 in ambito “Help Desk”;
- indicatori IQ14, IQ15, IQ22 e IQ23 in ambito “Qualità di erogazione dei servizi”;
- indicatori IQ24, IQ25 e IQ26 in ambito “Collaudo dei servizi”.

Il servizio di Monitoring & Alerting è garantito in modalità H24, per 365 giorni all’anno.

4. COME ORDINARE

4.1. Acquisizione dei servizi

La responsabilità del processo di acquisizione dei servizi, che include l’esecuzione di ciascuna delle fasi/attività previste dal Contratto Quadro per la stipula di ogni singolo Contratto esecutivo, è assegnata, nel modello organizzativo proposto, al Responsabile Diffusione territoriale dei Servizi del Fornitore, che ingaggia le strutture commerciali (Responsabile Commerciale) e tecniche (Responsabile Progettazione) territorialmente competenti. Il flusso del processo di acquisizione è descritto in tutte le sue fasi/attività nella seguente figura, con indicazione delle strutture coinvolte e dei ruoli responsabili dell’esecuzione di ciascuna attività.

Strutture Territoriali: È una struttura centralizzata e condivisa a livello di RTI che si articola in Funzioni Commerciali e Funzioni Tecniche di Prevendita territorialmente distribuite grazie alla capillarità del presidio delle funzioni commerciali e delle sedi operative. In queste sono concentrate le competenze tecniche da ingaggiare nella fase di supporto alla redazione dei Piani di Fabbisogno e successivamente, attraverso l’attivazione delle unità operative e/o dei Centri di Competenza delle nostre Aziende per la stesura del Progetto dei Fabbisogni.

Direzione Commerciale: È costituita dalle strutture commerciali capillarmente distribuite sul territorio nazionale presso le sedi delle aziende. Si compone di Responsabili commerciali dedicati alle Amministrazioni beneficiarie che dispongono di know how e conoscenze dei contesti presso i quali andare a posizionare i servizi oggetto del presente Contratto Quadro.

Unità Operative di Progettazione: È costituita dalle strutture tecniche e di prevendita distribuite sul territorio nazionale presenti presso le sedi delle tre aziende. Si compone di Figure di alto profilo che dispongono di know how e competenze specifiche dei contesti del presente CQ maturate grazie alle attività svolte presso le specifiche Amministrazioni.

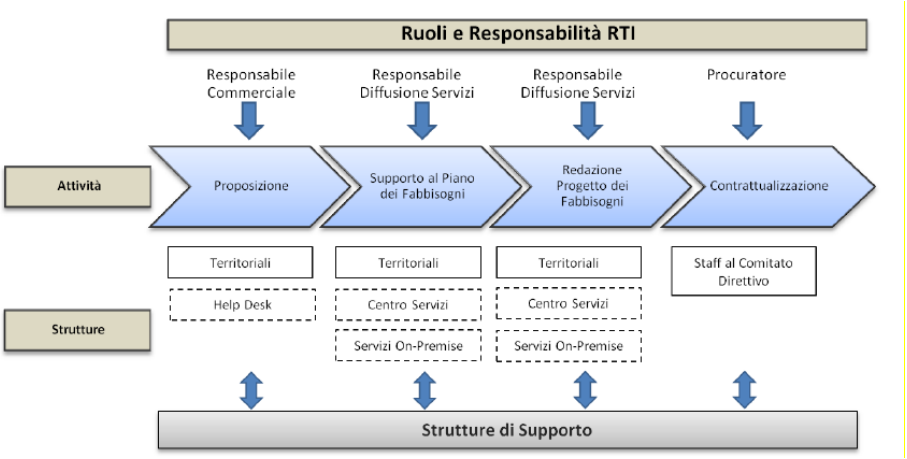


Figura 23 Flusso del Processo di proposizione e acquisizione dei servizi e adesione al CE

La matrice RACI riportata nella tabella che segue indica per ciascuna fase/attività in relazione alle figure professionali coinvolte, il tipo di relazione: Responsible (esegue l'attività), Accountable (responsabile del risultato finale), Consulted (supporta il Responsible per l'esecuzione dell'attività), Informed (informato al momento dell'esecuzione dell'attività).

ATTIVITÀ	Responsabile della Diffusione Territoriale dei servizi	Responsabile Commerciale	Responsabile Progettazione	Procuratore
Proposizione	A	R	C	I
Supporto al Piano dei Fabbisogni	A	C	R	I
Redazione Progetto dei Fabbisogni	A	C	R	I
Contrattualizzazione	A	C	I	R

Tabella 11 - Matrice RACI del Processo di Acquisizione

Responsabile della Diffusione Territoriale dei Servizi

Per meglio soddisfare le specifiche esigenze che caratterizzano i contesti tecnologici e organizzativi delle Amministrazioni, il modello organizzativo prevede la figura aggiuntiva del Responsabile Diffusione territoriale dei Servizi, che fa parte del Comitato Direttivo RTI. Il Responsabile ha il compito di individuare ed organizzare, per la specifica fase di proposizione verso le Amministrazioni il team con competenze commerciali e tecniche che meglio indirizzano l'iniziativa specifica, all'interno delle strutture territoriali. Tali strutture sono articolate in Funzioni Commerciali e Funzioni Tecniche di Prevendita, che coprono efficacemente il territorio grazie alla presenza capillare delle Aziende del RTI. Il team supporta le Amministrazioni nella fase di redazione del piano di Fabbisogni e produce successivamente il Progetto dei Fabbisogni. In accordo con il Responsabile del Contratto Quadro individua e coordina i Procuratori che hanno facoltà, se delegati dal Responsabile del Contratto Quadro, di stipulare i Contratti esecutivi con le Amministrazioni.

4.2. Amministrazioni beneficiarie dei servizi e modalità di adesione

Si descrive di seguito il percorso operativo per qualificare e dimensionare i fabbisogni ed arrivare alla stipula del Contratto Esecutivo.

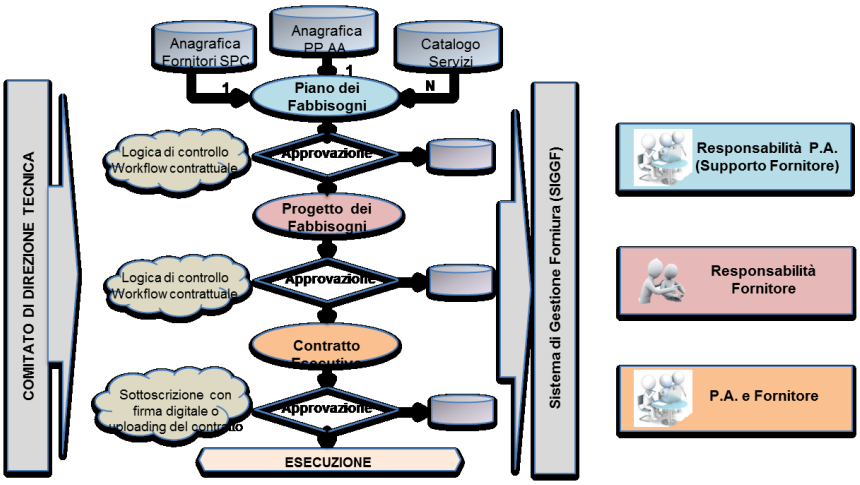


Figura 24 Flusso processo stipula Contratto Esecutivo

PIANO FABBISOGNI

L' Amministrazione, eventualmente con il supporto del Fornitore, redige ed inoltra al Fornitore il "Piano dei Fabbisogni" (vedi allegato Schema Piano Fabbisogni) che contiene la descrizione delle esigenze e indicazioni di tipo quantitativo dei servizi che la stessa intende sottoscrivere.

Il "Piano dei Fabbisogni" dovrà essere sempre mantenuto allineato con quanto richiesto dalle Amministrazioni.

PROGETTO FABBISOGNI

A fronte della ricezione del “Piano dei Fabbisogni” il Fornitore, entro il termine di 45 giorni solari formula una proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nel Contratto Quadro e nei relativi allegati.

L’Amministrazione può revisionare il Piano presentato entro ulteriori 15 gg.

Il “Progetto dei fabbisogni" deve contenere i seguenti allegati:

a) “Progetto di Attuazione”: con il dettaglio, per ciascun servizio, di:

- identificativo del servizio;
- configurazione (ove applicabile);
- quantità;
- costi;
- indirizzo o indirizzi di dispiegamento (nel caso di servizi centralizzati si può riportare anche il solo indirizzo della sede centrale);
- data prevista di attivazione;
- impegno delle eventuali risorse professionali previste;
- descrizione per lo specifico servizio della struttura funzionale ed organizzativa del centro servizi, completa dei nomi e dei ruoli delle figure responsabili per ciascuno dei servizi, nonché delle relative procedure di escalation;
- specifiche di collaudo, contenenti le modalità di esecuzione dei test di collaudo, descritti tramite schede tecniche di dettaglio e le date di prevista disponibilità al collaudo;

b) “Modalità di presentazione e approvazione degli Stati di Avanzamento mensili”; su richiesta dell’Amministrazione, il Fornitore deve sottoporre all’Amministrazione medesima, con cadenza mensile a partire dalla data di approvazione del Progetto stesso ed entro il giorno 15 del mese successivo al mese di riferimento, uno “stato di avanzamento” redatto come segue, soggetto ad approvazione da parte dell’Amministrazione Beneficiaria.

Lo “stato di avanzamento” deve contenere almeno le seguenti informazioni e quant’altro ritenuto opportuno dal Fornitore:

- esito dei collaudi effettuati e collaudi previsti nel mese successivo;
- varianti e modifiche emerse nel periodo;
- ritardi verificatisi nelle attivazioni rispetto alle date previste nel Piano di Attuazione del Progetto dei Fabbisogni;
- malfunzionamenti verificatisi nel periodo.

c) “Piano di Attuazione”, articolato nei seguenti allegati:

- “Piano di lavoro”, contenente l’elenco delle attività/fasi previste con le relative date di inizio e fine,
- “Documento programmatico di gestione della sicurezza dell’Amministrazione”;
- “Piano della qualità” dello specifico servizio contenente la descrizione dettagliata degli obiettivi di qualità relativi al servizio erogato e la descrizione sintetica dei processi di controllo della qualità.

L’Amministrazione stipula il conseguente “Contratto Esecutivo”, approvando il “Progetto dei Fabbisogni”, che insieme al “Paino dei Fabbisogni” ne costituisce parte integrante.

Una volta stipulato il Contratto Esecutivo, il Fornitore nomina le figure di Responsabile del Contratto Esecutivo e di Responsabile tecnico, quali interfacce dell'Amministrazione, che dovranno essere operative entro 10 (dieci) giorni solari dalla data di stipula.

Le attività tecniche di supervisione e controllo della corretta esecuzione del Contratto Esecutivo, in relazione ai servizi richiesti, sono svolte dalla Amministrazione.

4.3. Sistema Integrato di Gestione della Fornitura

Per la gestione degli ordinativi e dei contratti è previsto a regime un sistema integrato di gestione della fornitura, che sarà disponibile successivamente. Nell'ambito della fornitura dei servizi del presente Contratto Quadro, è resa disponibile una soluzione temporanea per la gestione del transitorio.

Tale soluzione utilizza i servizi esposti dal **Sistema Integrato di Gestione e Governo della Fornitura (SIGGF)** del Lotto 2 SPC Cloud, e risulta fondamentale affinché le PA possano esprimere i propri fabbisogni di servizi e perché questi vengano analizzati da Consip / Agid.

Il sistema SIGGF supporta i seguenti servizi:

- Servizio di Gestione Automatizzata dei Contratti (SGAC) per la gestione di contratto quadro e contratti esecutivi;
- Sistema CRUD (Create, Read, Update, Delete) per la modellazione del piano dei fabbisogni (da parte delle PA) e dei progetti dei fabbisogni (da parte del RTI):
  - Piano dei fabbisogni = elenco dei servizi che la PA intende sottoscrivere, con indicazione delle quantità dei servizi richiesti;
  - Progetto dei fabbisogni = proposta tecnica ed economica del RTI che include il progetto ed il piano di attuazione e le modalità di gestione dei SAL.

Step di approvazione della documentazione:

- PA: approva piano e progetto dei fabbisogni;
- Consip / Agid: nessuna approvazione.

<u>Relazione piano / progetto / contratto</u>

I tre oggetti sono in relazione (1:1). Ad un piano dei fabbisogni corrisponde un progetto dei fabbisogni, in relazione al quale viene stipulato un Contratto Esecutivo; nuovi fabbisogni confluiscono in un nuovo piano dei fabbisogni, in un nuovo progetto e in un nuovo contratto.

<u>Reportistica</u>

La soluzione temporanea dovrà consentire l'elaborazione di statistiche di base inerenti l'andamento delle sottoscrizioni di piani, progetti e contratti (es: analisi per servizio, tipologia di PA, area geografica)

<u>Processo: consultazione documentazione</u>

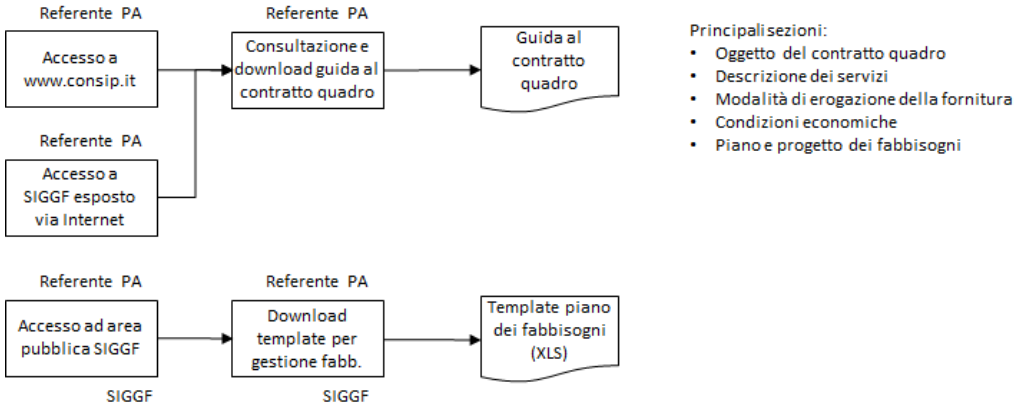


Figura 25 Flusso processo consultazione documentazione

Sull'area pubblica del SIGGF viene inserita una pagina che descrive la procedura da seguire per la redazione e consegna del Piano dei Fabbisogni e per il download del template del Piano dei Fabbisogni (che include le informazioni anagrafiche di base relative all'Amministrazione)

Processo: gestione dei fabbisogni

Oggetti applicativi

La soluzione gestisce i seguenti oggetti applicativi:

- Piano dei fabbisogni: schema strutturato ad hoc che esprime le quantità per anno per servizio ed ulteriori informazioni di caratterizzazione univocamente identificato
- Progetto dei fabbisogni: documentazione in formato Office e pdf

Le attività di upload della documentazione in SIGGF viene gestita, nell'ambito della soluzione transitoria, dal PMO RTI (nessuna operatività a carico del personale dell'Amministrazione)

La gestione del contratto viene supportata da apposita soluzione in SIGGF

Workflow approvativo

- Il processo di approvazione viene implementato all'interno del sistema documentale in SIGGF
- Via mail vengono notificate le richieste di approvazione
- L'approvazione viene effettuata dall'Amministrazione accedendo al sistema di gestione documentale all'interno del SIGGF

Tecnologie impiegate

In coerenza con gli obiettivi di reuse l'applicazione verrà realizzata in SIGGF con tecnologia IBM (prodotto Filenet per la gestione documentale)

Processo: elaborazione reporting

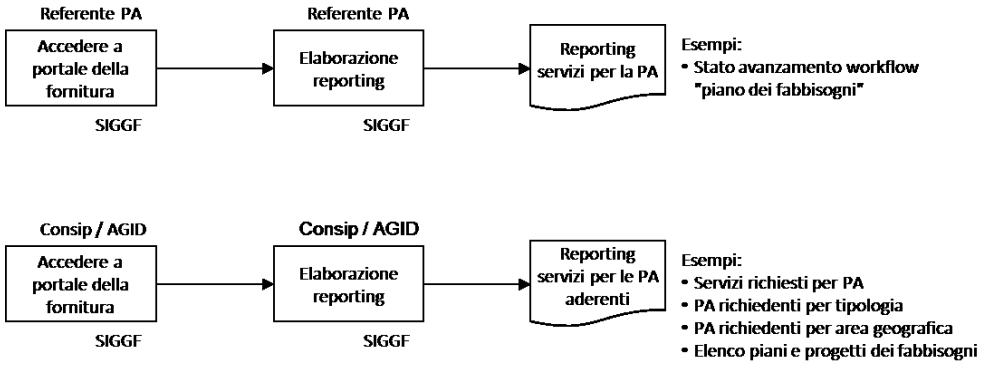


Figura 26 Flusso processo di reporting

Elementi caratterizzanti la soluzione:

In coerenza con gli obiettivi di reuse l'applicazione verrà realizzata con tecnologia IBM (prodotto COGNOS)

4.4. Variazione al Piano dei fabbisogni

Ciascun Piano dei Fabbisogni potrà essere aggiornato dall'Amministrazione nel corso del tempo in termini di tipologia di servizi e quantità degli stessi, .

Processo: variazione dei fabbisogni

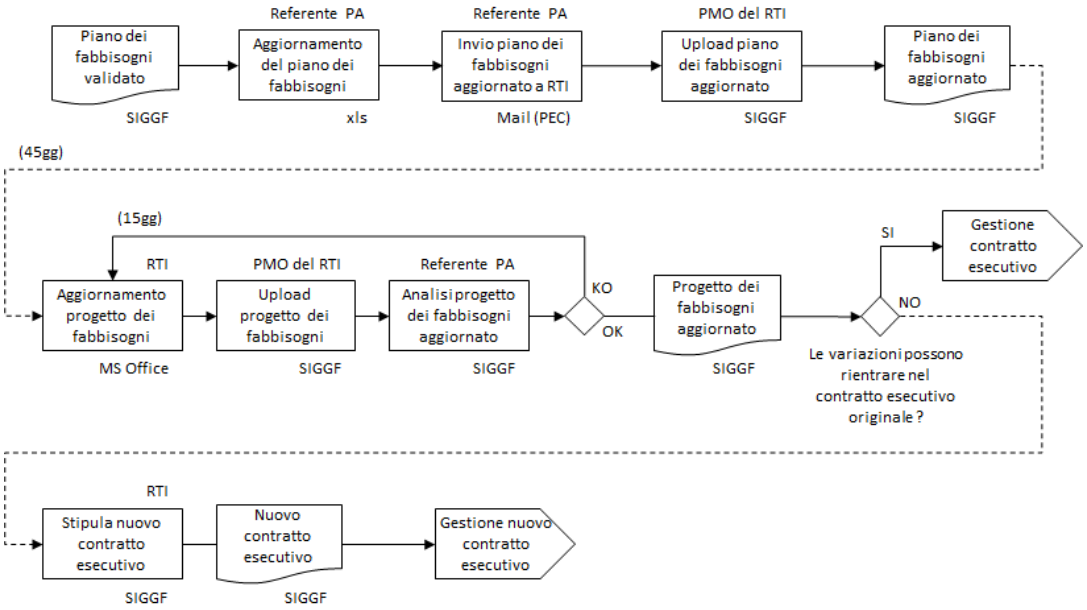


Figura 27 : variazione "Piano dei Fabbisogni"

5. MODALITA' DELLA FORNITURA

Il contesto metodologico nel quale saranno erogati tutti i servizi del Contratto Quadro, è un insieme collaudato ed utilizzato con successo dal Fornitore, di metodi e processi in grado di assicurare efficacia ed efficienza nell'esecuzione e governo delle attività, garantendo al contempo l'adattabilità al contesto e la massima flessibilità operativa.

Le aziende costituenti il RTI del Fornitore dei servizi, adottano da anni gli standard di riferimento, ITIL per la gestione e l'erogazione dei processi, CObIT per la gestione e il governo del IT interna e dei Centri Servizi, CMMI per la verifica del grado di maturità dei processi e servizi, oltreché le norme ISO 27000 (ex BS-7799) per la gestione della sicurezza delle informazioni, ISO 22301 (ex BS-25999) per la continuità operativa, MIGRA per l'analisi del Rischio.

Il Fornitore inoltre propone come modello di riferimento il Knowledge Base IBM ITUP (IBM Tivoli Unified Process) già integrato con gli strumenti adottati dalle aziende componenti il RTI del Fornitore in supporto alla gestione delle infrastrutture tecnologiche ed erogazione dei servizi. In particolare, tale asset è continuamente allineato nei contenuti con i knowledge base delle aziende e garantisce le Amministrazioni nell'adozione delle migliori best practice di mercato e di settore.

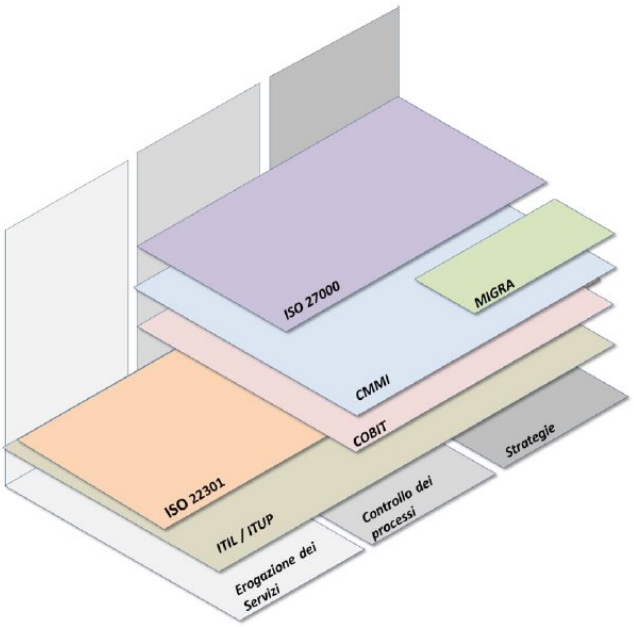


Figura 28 : framework standard e Best Practices

La Figura illustra la mappatura delle best practice all'interno del intero ciclo di gestione dei servizi IT. L'utilizzo delle best practice ITUP, in aggiunta a quelle ITIL, CObIT, CMMI e ISO 27000/22301 per la gestione del ciclo di vita dei servizi ICT consente di

► fare leva su consolidati standard e linee guida largamente utilizzati in tutte le fasi dei servizi,

► accelerare l'implementazione dei processi e ridurre i tempi di implementazione del servizio di gestione,

► migliorare la maturità dell'organizzazione ed il livello di automazione, fornendo al personale una guida dettagliata contestuale ai compiti che sono in esecuzione

► indirizzare il corretto utilizzo degli strumenti utilizzati,

► chiudere lacune di audit e/o conformità di processo, fornendo la verifica che i processi sono documentati con responsabilità chiare e definite,

► facilitare, anche con l'ausilio tecnologico di strumenti a supporto, quali GRC e DSS, le decisioni, basandosi su dati aggregati e indicatori di tendenza, con informazioni raccolte da tutte le fonti disponibili e

► supportare adeguatamente la formazione continua di tutti gli addetti al Centro Servizi. I processi di gestione e controllo della fornitura ed in particolare dei servizi/progetti integrano aspetti di Gestione della Qualità, Project Management e Gestione del Rischio, garantendo una visibilità sistematica ed organica di tutti i punti critici dei diversi Contratti Esecutivi.

5.1. Predisposizione e attivazione dei servizi

Attivazione dei servizi

Il processo di attivazione dei servizi, prevede l'esecuzione di ciascuna delle fasi/attività richieste dal Contratto Esecutivo, propedeutiche alla erogazione di ciascuno dei servizi sottoscritti. Nel modello di processo proposto il Fornitore, una volta nominato il Responsabile del Contratto Esecutivo e il Responsabile Tecnico, attribuisce al primo la responsabilità dell'intero processo. Il flusso del processo di attivazione dei servizi è descritto in tutte le sue fasi/attività nella figura di seguito riportata, con indicazione delle strutture coinvolte e dei ruoli responsabili dell'esecuzione di ciascuna attività.

Mentre le prime due fasi/attività sono uniche per ciascun Contrato Esecutivo, le ultime tre si applicano a ciascun servizio sottoscritto dall'Amministrazione. È necessario sottolineare inoltre che il Responsabile del Contrato Esecutivo si occuperà degli aspetti Amministrativi. A valle del collaudo positivo da parte dell'Amministrazione, nel caso di servizi che richiedano attività una tantum il servizio si ritiene terminato, mentre nel caso di servizi che richiedano attività continuative, il modello organizzativo prevede l'esecuzione del processo di Erogazione dei Servizi descritto nel paragrafo successivo.

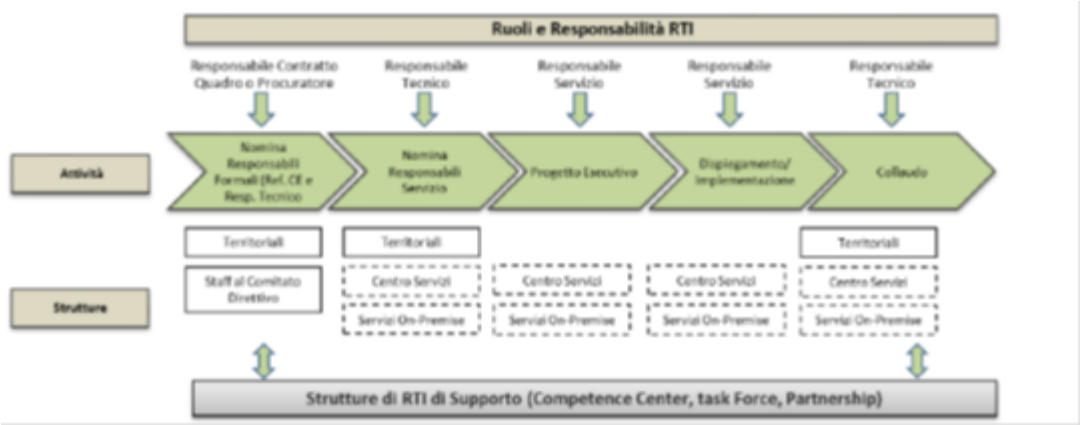


Figura 29: Processo di attivazione dei servizi

Procedura Operativa di Richiesta Servizi

Di seguito viene rappresentata nello schema, e poi descritta in dettaglio nella tabella a seguire, la procedura di attivazione per il Servizio di Sicurezza “Static Application Security Testing” che può essere preso d’esempio come procedura di attivazione per tutti gli altri Servizi di Sicurezza.

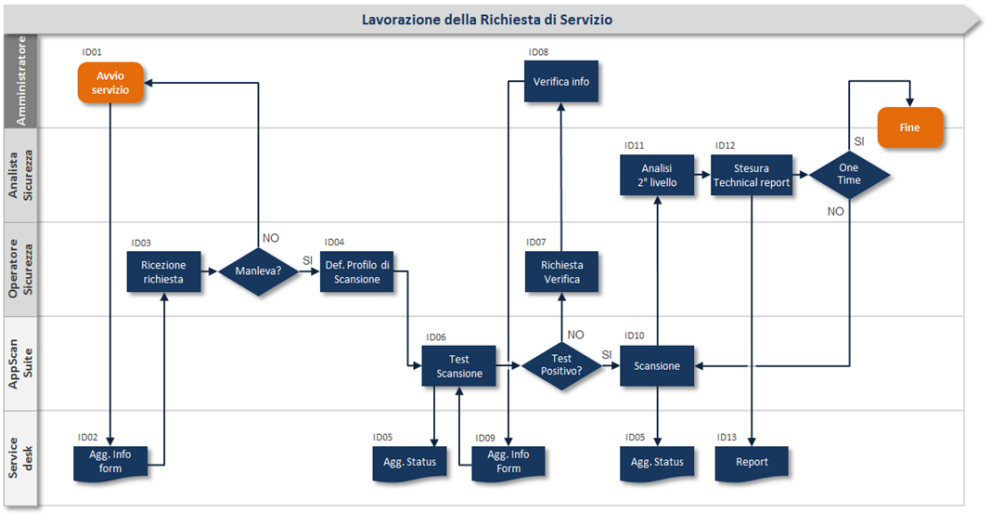


Figura 30: Procedura di attivazione dei servizi

ATTIVITÀ	INPUT	DESCRIZIONE	OUTPUT	OWNER
ID 01 Avvio Servizio	Richiesta utente	Le SR possono essere registrate dall’utente via web durante la fase di registrazione si attinge alle informazioni relative al catalogo delle SR e alle check list relative ai servizi a catalogo.	SR registrata	Utente o Service desk Agent
ID 02 Aggiornamento Info Form	ID Richiesta	Il referente dell’Amministrazione compila il Web Form con le informazioni tecniche relative alla esecuzione del servizio	Web Form Compilato	Amministrazione
ID 03 Ricezione Richiesta	Aggiornamento Info Form	L’Operatore di Sicurezza attiva il servizio, prende in carico la richiesta, attiva gli scanner necessari alla scansione. Verifica presenza dell’autorizzazione esecuzione del servizio (Malleva)	Servizio attivato	Operatore Sicurezza
ID 04 Def. profilo di scansione	Ricezione richiesta	Preparazione del profilo di scansione, attraverso utilizzo dati di Amministrazione (info Form) si effettua il caricamento codice sorgente e caricamento delle librerie, impostazione parametri di test e schedulazione.	Profilo di scansione creato	Operatore di Sicurezza
ID 05 Aggiornamento Status	Stato precedente	Ogni fase cruciale del processo è seguita da un aggiornamento dello stato sul sistema Service Desk. Gli stati possibili sono: • Richiesta sottomessa a carico Centro	Stato aggiornato sul Service Desk	Operatore di Sicurezza

		Servizi • Richiesta sospesa a carico Amministrazione • Richiesta accettata in lavorazione • Richiesta completata pubblicati i Deliverable.		

Figura 31: Fasi di attivazione dei servizi

5.2. Collaudi

In seguito alla stipula del Contratto Esecutivo, l'Amministrazione contraente potrà richiedere prove di collaudo atte a verificare la conformità di ogni singolo servizio contrattualizzato rispetto a:

- "Piano dei fabbisogni", redatto dall'Amministrazione contraente;
- **"**Progetto dei fabbisogni", redatto dal Fornitore;
- Specifiche e requisiti dei servizi, contenuti nel Capitolato Tecnico.

Il collaudo sarà effettuato in due fasi:

- Collaudo in attivazione: effettuato dal Fornitore all'atto della attivazione dei servizi, mediante test tecnici di carattere funzionale atte a verificare la corretta attivazione dei servizi. Il Fornitore darà notifica secondo le modalità concordate e definite nel Progetto dei Fabbisogni, dell'esito delle stesse;
- Collaudo in contraddittorio: secondo le modalità definite con l'Amministrazione potranno essere effettuate a campione le verifiche di Attivazione, la verifica della corretta configurazione degli stessi (in coerenza con quanto definito nei collaudi funzionali) nonché l'effettuazione di ulteriori prove concordate.

Il Fornitore consegnerà entro i tempi previsti nel Progetto dei Fabbisogni, all'Amministrazione un documento intitolato "Specifiche di dettaglio delle prove di collaudo" che descrive la tipologia delle prove di collaudo previste e la pianificazione temporale delle stesse.

Il Fornitore fornirà il supporto all'Amministrazione contraente in tutte le attività necessarie alle suddette prove di collaudo, anche interando, laddove necessario le prove proposte.

5.3. Erogazione dei servizi, stati di avanzamento, reportistica

Erogazione dei Servizi

Il processo prevede l'esecuzione delle attività cicliche necessarie per l'erogazione dei servizi di tipo continuativo. Tale processo, costruito sulla base del modello proprio della Best Practice ITILv3, garantisce il "Continual Service Improvement", ovvero il miglioramento continuo della qualità del servizio erogato non solo rispetto ai parametri di qualità previsti dal Capitolato Tecnico, ma anche relativamente agli indicatori tipici previsti da ITILv3.

L'interfaccia verso le Amministrazioni è rappresentata dal Responsabile del Contratto Esecutivo.

La matrice RACI della tabella seguente riporta il tipo di relazione, per ciascuna fase/attività in relazione alle figure professionali coinvolte.

ATTIVITÀ	Responsabile Tecnico	Quality Manager	Risk Manager	Security Mananger	Responsabile Servizio
Gestione SLA	I	R	C	C	A
Gestione Operativa	I	C	C	C	A/R
Miglioramento dei servizi	I	C	C	C	A/R

Tabella 12 Matrice RACI del Processo di erogazione

Stati d'Avanzamento e Reportistica

Durante le fasi di attivazione e durante l'erogazione dei servizi saranno fornite all'Amministrazione Reportistica atta a monitorare lo Stato d'Avanzamento delle attivazioni e la Qualità dei Servizi in erogazione o dei Deliverable Contrattuali.

La prima reportistica sarà concordata con l'Amministrazione in termini di modalità, frequenza e dettaglio di informazioni e conterrà almeno l'elenco dei servizi contrattualizzati e lo stato (in attivazione, Sospeso, Attivato, Collaudato). La responsabilità di tali attività sono demandate al Transition Manager (o Project Manager), sotto il coordinamento del Responsabile della Transizione e del Responsabile del PMO, già descritti nel paragrafo precedente.

Il secondo tipo di reportistica, fruibile attraverso il portale di Governo e Gestione della Fornitura darà contezza degli indicatori di Qualità di cui al successivo capitolo 4.5.

La responsabilità del rispetto degli indicatori per singolo Contratto Esecutivo è demandata al Quality Manager, già descritto, coordinato dal Responsabile della Qualità del Contratto Quadro.

5.4. Servizi di help desk

Il Fornitore erogherà il servizio di Help Desk attraverso un unico punto di contatto per i Referenti dell'Amministrazione; tale servizio, mediante più livelli di assistenza, svolgerà attività di accoglienza, interpretazione delle richieste, diffusione di informazioni, troubleshooting, Incident & Problem Solving, Change Management, Knowledge management.

Per garantire l'efficacia del servizio è stata studiata una soluzione fondata sui seguenti principi

► Help Desk basato su: 1° Livello, che, tramite la funzione di Service Desk, rispondendo alle domande con il Supporto Informativo e con il Supporto Tecnico tenta una prima risoluzione degli incident di minor complessità; 2° Livello altamente specializzato in funzione delle tematiche tecnico/applicative o contrattuali Contratto Quadro e Contratto Esecutivo con processi agili di escalation ed efficaci modalità di formazione iniziale e continua del personale

► utilizzo di strumenti che permettono la condivisione di un'ampia knowledge base ed il pieno accesso di tutti gli operatori ai sistemi di monitoraggio della fornitura, anche in modalità collaborativa con il Referente dell'Amministrazione.

Le figure di responsabilità rappresentate nel disegno organizzativo sono: Help Desk Manager, che governa tutte le strutture di erogazione comprese nel 1°e 2° livello di HD e si interfaccia con il Responsabile Formazione, allo scopo di selezionare le risorse e programmare gli interventi formativi specifici per ogni livello di assistenza; Responsabile della Knowledge Base per supervisionare la raccolta dei contenuti e sistematizzare il processo di popolamento della base dati; Coordinatore Operatori e Coordinatore Tecnico, che hanno invece il compito di orchestrare il lavoro delle risorse che operano rispettivamente nel Service Desk e nel Supporto di 2° livello .

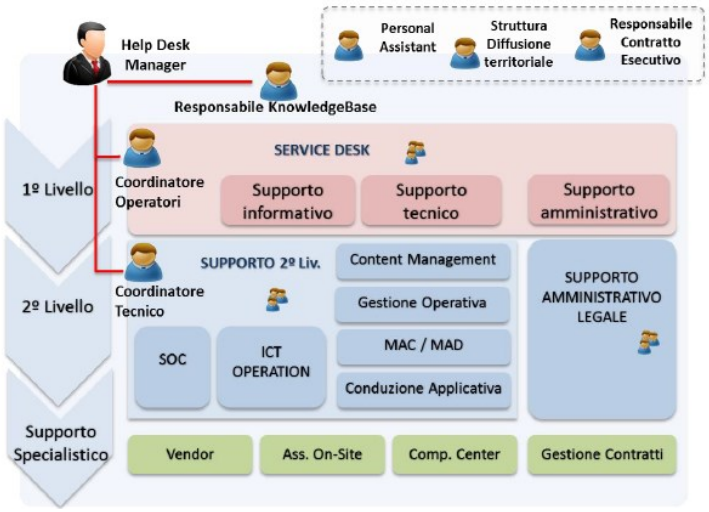


Figura 32 : Organizzazione Help Desk

Nel seguito vengono descritte le principali responsabilità dei diversi supporti:

- Service Desk di I Livello: accoglienza e primo punto di contatto coi Referenti PA; creazione Ticket e gestione del suo ciclo di vita; presa in carico delle richieste di tipo informativo, fino alla chiusura delle stesse; escalation delle richieste alle strutture di competenza; popolamento della Knowledge base; gestione proattiva dei ticket; richiesta feedback periodici all'Amministrazione; gestione reportistica dei livelli di servizio. interagisce con l'Amministrazione per tutte le richieste di informazione e incident sui servizi; governa il processo di Request Fulfillment, Incident Mngt. attiva la Struttura di Diffusione Territoriale in fase di Comprensione ed attivazione del Contratto Quadro tramite interagisce con il Team di Supporto Amm./Legale per attivare la struttura di Gestione Contratti in fase di Contratto Esecutivo
- Supporto Tecnico 1° Livello: Presa in carico degli Incident tecnici e primo tentativo di risoluzione con ausilio della knowledge base; popolamento della Knowledge base Tecnica; escalation degli incident verso il Supporto 2° Livello; effettua l'analisi e la risoluzione degli Incident di tipo tecnico a bassa complessità; interagisce con il Supporto 2° Livello per l'analisi dei problemi e la valutazione dei change;
- Supporto 2° Livello: gestione dei Ticket non risolti dal Supporto Tecnico; supporto tecnico per problematiche inerenti il servizio di Firma/Timbro; supporto tecnico per problematiche inerenti il servizio di Sicurezza; supporto per problematiche inerenti l'Identità Digitale apertura task di assistenza verso strutture di supporto specialistico interne ed esterne. Interagisce con il Supporto Tecnico del 1° Livello per arrivare alla risoluzione degli Incident; coordina e gestisce i processi di Problem e di Change Management; interviene su specifiche tematiche tecnologiche/funzionali interagisce con strutture interne di Help Desk dell'Amministrazione; interagisce con le funzioni di Supporto Specialistico (Vendor, Assistenza on-site, Competence Center).
- Supporto Amministrativo/Legale: supporto alla gestione degli aspetti amministrativi e legali relativi alla predisposizione di un nuovo Contrato Esecutivo diffusione di informazioni di dettaglio su dati amministrativi inerenti un Contrato Esecutivo in corso; guida all'utilizzo degli strumenti di collaboration, billing, document management, etc. interagisce con i team di 1° Livello o con il Referente dell'Amministrazione per approfondire e comprendere le esigenze amministrative richieste; collabora direttamente con i Responsabili Diffusione Territoriale e Contratto Esecutivo per dirimere le questioni legali e amministrative più complesse; interagisce con le strutture di governo per segnalare problematiche nella gestione degli aspetti amministrativi.

5.5. Indicatori Qualità, Service Level Agreement (SLA), penali

Di seguito sono sintetizzati gli indicatori di qualità e gli SLA garantiti dal Fornitore.

Definizione	Indicatore di Qualità	SLA target	Penale
IQ01 – Rispetto di una scadenza temporale	Ritardo, in gg, tra la data di consegna effettiva e la data di consegna prevista di un deliverable contrattuale, al netto delle sospensioni concordate	0 gg	0,5‰ (zerovirgolacinque per mille) dell'importo del servizio di riferimento per ogni giorno lavorativo eccedente la soglia
IQ02 – Qualità della documentazione	Numero di documenti rielaborati a seguito di richiesta da parte dell'Amministrazione	<= 1 rielaborazione nel semestre per singolo documento	emissione Rilievo
IQ03 – Rispetto tempistiche di inserimento/sostituzione di personale	Tempo trascorso tra la richiesta dell'Amministrazione e l'inserimento della risorsa, al netto delle sospensioni concordate	<= 5 gg lavorativi	0,5‰ (zerovirgolacinque per mille) dell'importo del servizio di riferimento per ogni giorno lavorativo eccedente la soglia
IQ04 – Inadeguatezza del personale proposto	Numero di sostituzioni, richieste formalmente dall'Amministrazione, che riguardano il personale della fornitura nel periodo di riferimento	0 sostituzioni nel trimestre	emissione Rilievo
IQ05 – Turn over del personale	Numero risorse impegnate nell'erogazione dei servizi sostituite su iniziativa del Fornitore nel periodo di riferimento, escluse le sostituzioni concordate e finalizzate al miglioramento dei servizi o quelle operate a fronte di dimissioni/ licenziamento	<= 1 sostituzione nel trimestre	emissione Rilievo
IQ06 – Numerosità dei rilievi sulla fornitura	Numero rilievi emessi sulla fornitura	<= 3 rilievi nel Trimestre di riferimento	0,5‰ (zerovirgolacinque per mille) dell'importo contrattuale per ogni rilievo eccedente il valore soglia
IQ07 – Rispetto dell'RTO	Tempistiche di attivazione della configurazione di emergenza/simulazione	<= 4 ore	1,0‰ (uno per mille) dell'importo del servizio di riferimento Per ogni ora solare eccedente la soglia
IQ08 – Rispetto dell'RPO	Valore di RPO (perdita dati tollerabile in termini di scostamento fra l'immagine dei dati del sito secondario rispetto ai dati del sito primario)	<=1 ora	1,0‰ (uno per mille) dell'importo del servizio di riferimento per ogni 1,0% (uno per cento) di scostamento dalla soglia definita, nonché per ogni caso di verificata inconsistenza dei dati di replica.
IQ09 – Disponibilità dei dati a fine fornitura	Ritardo, al netto delle sospensioni concordate in gg lavorativi, tra la data di consegna effettiva e la data di consegna prevista dei principali deliverable e oggetti della fornitura (es. almeno i dati memorizzati nei DB, file di configurazione, immagine server etc …) stabilita dal contratto e/o dal piano di lavoro approvato.	0 gg lavorativi	penale pari all'0,5‰ (zerovirgolacinque per mille) dell'importo del servizio di riferimento per ogni giorno lavorativo eccedente la soglia
IQ10 – Percentuale di chiamate in ingresso gestite	Tempo che intercorre tra la richiesta di contatto con l'operatore e il contatto. Per richiesta di contatto si intende l'ingresso della chiamata telefonica in coda operatore.	<= 60 secondi nel 95% dei casi nel Trimestre	emissione Rilievo
IQ11 - Tempo di presa in carico	Tempo di presa in carico della singola richiesta	<=10 minuti nel 96% dei casi nel Trimestre di riferimento	0,5‰ (zerovirgolacinque per mille) dell'importo contrattuale per ogni punto percentuale in diminuzione rispetto al valore

			soglia.
IQ12 – Tempo di risoluzione	Percentuale di richieste risolte entro i tempi massimi previsti, dipendenti dalla priorità attribuita alle richieste stesse, al netto delle sospensioni.	Priorità 1(problema di tipo bloccante): 99% delle richieste risolte entro 4 ore nel Trimestre di Riferimento Priorità 2: (problema non bloccante): 96% delle richieste risolte entro 8 ore nel Trimestre di Riferimento Priorità 3: (richiesta di informazioni/ problematiche amministrative/contrattuali): 94% delle richieste risolte entro 12 ore nel Trimestre di Riferimento	1,0‰ (uno per mille) dell'importo del servizio di riferimento per ogni punto percentuale in diminuzione rispetto al valore soglia.
IQ13 – Numerosità richieste riaperte	Numero di richieste, aventi almeno una riapertura, chiusi nel periodo di riferimento, al netto delle riaperture per cause non imputabili al fornitore	<= 5% delle richieste chiuse nel Trimestre di riferimento	emissione Rilievo
IQ14 – Tempo di attivazione degli interventi	tempo di attivazione degli interventi a partire dalla richiesta dell'Amministrazione, al netto delle sospensioni concordate	<= 5 gg lavorativi	0,5‰ (zerovirgolacinque per mille) dell'importo del servizio di riferimento per ogni giorno lavorativo eccedente la soglia
IQ15 – Uptime della singola componente di servizio e degli strumenti a supporto	Disponibilità Infrastruttura (e/o delle Risorse e/o dei servizi) virtuale(i) creata(e) ed allocata(e) dall'Amministrazione, in particolare Uptime per la disponibilità dei nodi fisici (server) che ospitano l'infrastruttura virtuale misurata come tempo di indisponibilità dell'infrastruttura rispetto al tempo totale.	>= 99,922 %	Indisponibilità delle singole componenti relative ai servizi: 1,0‰ (uno per mille) dell'importo del servizio di riferimento per ogni 0,01% (zerovirgolazerouno per cento) in diminuzione rispetto al valore soglia. Indisponibilità degli strumenti a supporto della erogazione dei servizi: emissione di un rilievo per ogni 0,01% (zerovirgolazerouno per cento) in diminuzione rispetto al valore soglia
IQ16 – Capacità di elaborazione delle richieste in parallelo del sistema di Identity Provider	Percentuale di richieste di autenticazione che il sistema di Identity Provider è in grado di elaborare in parallelo	>= 95% nel Mese di riferimento	1,0‰ (uno per mille) dell'importo del servizio di riferimento per ogni scostamento di 1,0% (uno per cento) rispetto al valore di soglia.
IQ17 - Capacità di accodamento del sistema di Identity Provider	Percentuale di richieste che il sistema di Identity Provider è in grado di mantenere in coda in attesa di elaborazione	>= 95% nel Mese di riferimento	1,0‰ (uno per mille) dell'importo del servizio di riferimento per ogni scostamento di 1,0% (uno per cento) rispetto al valore di soglia.
IQ18 – Tempo di risposta sistema di Identity Provider	il tempo di risposta che il sistema di Identity Provider deve garantire, per una percentuale indicata nei valori di soglia e nelle condizioni di dimensionamento relative al numero di utenti	>= 95% inferiore ad 1,5 sec	1,0‰ (uno per mille) dell'importo del servizio di riferimento per ogni scostamento di 1,0% (uno per cento) rispetto al valore di soglia.

	contrattualizzati e throughput minimo, per le richieste		
IQ19 – Capacità di elaborazione delle richieste in parallelo dal sistema di I&AM	Percentuale di richieste di autenticazione che il sistema di I&AM è in grado di elaborare in parallelo	>= 95% nel Mese di riferimento	1,0‰ (uno per mille) dell'importo del servizio di riferimento per ogni scostamento di 1,0% (uno per cento) rispetto al valore di soglia.
Q20 - Capacità di accodamento del sistema di I&AM	Percentuale di richieste che il sistema di I&AM è in grado di mantenere in coda in attesa di elaborazione	>= 95% nel Mese di riferimento	1,0‰ (uno per mille) dell'importo del servizio di riferimento per ogni scostamento di 1,0% (uno per cento) rispetto al valore di soglia.
IQ21 - Tempo di risposta sistema di I&AM	il tempo di risposta che il sistema di I&AM deve garantire, per una percentuale indicata nei valori di soglia e nelle condizioni di dimensionamento relative al numero di utenti contrattualizzati e throughput minimo, per le richieste	>= 95% nei target temporali definiti nel Mese di riferimento	1,0‰ (uno per mille) dell'importo del servizio di riferimento per ogni scostamento di 1,0% (uno per cento) rispetto al valore di soglia.
IQ22 – Numero di difettosità	Malfunzionamenti delle funzionalità dei servizi di Identity Provider, I&AM, Firma digitale remota e Timbro elettronico	<3 nel trimestre di riferimento	1,0‰ (uno per mille) dell'importo del servizio di riferimento per ogni unità eccedente il valore di soglia.
IQ23 –Rilevazione degli incidenti di sicurezza	Percentuale di Incident di sicurezza segnalati nei tempi previsti in base al livello di severità	Severity 1: 96% delle richieste segnalate entro 15 min nel Mese di Riferimento Severity 2: 95% delle richieste risolte entro 30 min nel Mese di Riferimento Severity 3: 94% delle richieste risolte entro 40 min nel Mese di Riferimento	1,0‰ (uno per mille) dell'importo del servizio di riferimento per ogni scostamento di 1,0% (uno per cento) rispetto al valore di soglia.
IQ24 – Casi di test negativi in collaudo	Casi di test eseguiti con successo dal Fornitore appartenenti al piano di test che, se rieseguiti durante il collaudo (funzionale o di servizio), danno esito negativo	0 casi	emissione Rilievo
IQ25 – Difettosità in collaudo	il rapporto tra il numero dei difetti nella fase di collaudo dell'obiettivo/servizio e l'effort/volume dell'obiettivo/servizio stesso, espresso in Punti Funzione/Giorni Persona/etc	<= 0,030 e valore di soglia <= 0,050	emissione Rilievo
IQ26 – Giorni di sospensione del collaudo	Numero di giorni complessivo di sospensione del collaudo (funzionale o di servizio) di un obiettivo progettuale/servizio per cause imputabili al Fornitore	0 gg	0,5‰ (zerovirgolacinque per mille) dell'importo dell'obiettivo/servizio di riferimento per ogni giorno lavorativo eccedente la soglia

6. CONDIZIONI ECONOMICHE

6.1. Corrispettivi

I corrispettivi dovuti al Fornitore per i servizi prestati in esecuzione dei singoli Contratti Esecutivi sono determinati in ragione dei prezzi unitari stabiliti nel Contratto Quadro, da intendersi validi sino ad eventuali adeguamenti e modifiche successive. Ogni aggiornamento degli stessi sostituisce ed annulla i precedenti prezzi unitari.

Con riferimento ai singoli Contratti Esecutivi, detti corrispettivi sono maturati con periodicità bimestrale in ragione dei servizi effettivamente prestati nel rispetto del Progetto dei Fabbisogni, nell'ultima versione approvata.

6.2. Procedura di applicazione delle penali

Nell'ipotesi di ritardo nell'adempimento e/o di difformità di prestazione nell'esecuzione dei servizi o, comunque, delle attività contrattuali, non imputabile rispettivamente all'Amministrazione Beneficiaria o a Consip S.p.A., ovvero a forza maggiore o caso fortuito, rispetto ai Livelli di Servizio stabiliti nel documento Indicatori di qualità della fornitura o nell'Offerta Tecnica se migliorativa, l'Amministrazione Beneficiaria applicherà al Fornitore le penali, secondo gli schemi indicati nella tabella relativa agli indicatori di qualità . Gli eventuali inadempimenti contrattuali che daranno luogo all'applicazione delle penali dovranno essere contestati al Fornitore per iscritto dalla singola Amministrazione Beneficiaria, e comunicati per conoscenza a Consip S.p.A.

In caso di contestazione dell'inadempimento da parte della singola Amministrazione Beneficiaria, il Fornitore dovrà comunicare per iscritto le proprie deduzioni, supportate da una chiara ed esauriente documentazione, all'Amministrazione medesima nel termine massimo di 5 (cinque) giorni lavorativi dalla ricezione della contestazione stessa.

Qualora le predette deduzioni non pervengano all'Amministrazione Beneficiaria nel termine indicato, ovvero, pur essendo pervenute tempestivamente, non siano idonee, a giudizio della medesima Amministrazione, a giustificare l'inadempienza, potranno essere applicate al Fornitore le penali stabilite a decorrere dall'inizio dell'inadempimento.

Per i crediti derivanti dall'applicazione delle predette penali le Amministrazioni Beneficiarie potranno compensare detti crediti di propria competenza con quanto dovuto al Fornitore a qualsiasi titolo, quindi anche con i corrispettivi maturati, ovvero, in difetto, avvalersi della cauzione, in ogni caso, senza bisogno di diffida, ulteriore accertamento o procedimento giudiziario.

Qualora l'importo complessivo delle penali applicate al Fornitore da una singola Amministrazione Beneficiaria raggiunga la somma complessiva pari al 10% del valore complessivo del Contratto Esecutivo , detta Amministrazione ha facoltà, in qualunque tempo, di risolvere di diritto il Contratto Esecutivo , con diritto al risarcimento di tutti i danni, nonché la facoltà di richiedere la prestazione dei servizi ad altro fornitore.

La richiesta e/o il pagamento delle penali di cui sopra non esonera in nessun caso il Fornitore dall'adempimento dell'obbligazione per la quale si è reso inadempiente e che ha fatto sorgere l'obbligo di pagamento della medesima penale.

7. FATTURAZIONE E PAGAMENTI

La fattura relativa ai corrispettivi maturati viene emessa ed inviata dal Fornitore – con le modalità stabilite dalla legge - al termine del periodo di riferimento e, comunque, all'esito delle verifica di conformità, tra le quali l'allineamento tra il Piano dei Fabbisogni ed il Progetto dei Fabbisogni. I corrispettivi saranno corrisposti dall'Amministrazioni Beneficiaria secondo la normativa vigente in materia di contabilità delle Amministrazioni e previo accertamento della prestazione effettuate.

Ciascuna fattura, inviata via fax o PEC, verrà corrisposta nel termine di pagamento di 30 (trenta) giorni, secondo le modalità di cui alla normativa vigente (D.Lgs. n. 231/2002).

In caso di ritardo nei pagamenti, il tasso di mora viene stabilito in una misura pari al tasso BCE stabilito semestralmente e pubblicato con comunicazione del Ministero dell'Economia e delle Finanze sulla G.U.R.I., maggiorato di 8 punti, secondo quanto previsto nell'art. 5 del D.Lgs. n. 231/2002.

Detti corrispettivi si riferiscono ai servizi prestati a perfetta regola d'arte, nell'osservanza di leggi e regolamenti, nonché dalle disposizioni emanate o che venissero emanate dalle competenti autorità e nel pieno adempimento delle modalità e delle prescrizioni contrattuali.

Ciascuna fattura dovrà contenere il riferimento al Contratto Quadro ed al singolo Contratto Esecutivo cui si riferisce nonché dovrà essere intestata e spedita alla Amministrazione Beneficiaria. Si evidenzia che il CIG (Codice Identificativo Gara) "derivato" rispetto a quello del Contratto Quadro , comunicato dalle Amministrazioni Beneficiarie, sarà inserito a cura del Fornitore nelle fatture ovvero comunque riportato unitamente alle medesime e dovrà essere indicato dalle medesime Amministrazioni Beneficiarie nei rispettivi pagamenti ai fini dell'ottemperanza agli obblighi scaturenti dalla normativa in tema di tracciabilità dei flussi finanziari. Nel caso in cui l'aggiudicatario sia un R.T.I., ferma l'obbligatorietà del pagamento da effettuarsi esclusivamente in favore della società mandataria del raggruppamento, gli obblighi di cui sopra dovranno essere tutti puntualmente assolti sia nelle fatture emesse dalla mandataria, sia dalle mandanti nello specifico caso di esercizio della facoltà di ricorrere alla fatturazione "pro quota", nel rispetto delle condizioni e delle modalità oltre disciplinate.

Ai fini del pagamento di corrispettivi, l'Amministrazione Beneficiaria procederà:

- per gli importi superiori ad Euro 10.000,00, all'ottemperanza alle disposizioni previste dall'art. 48-bis del D.P.R. 602 del 29 settembre 1973, con le modalità di cui al Decreto del Ministero dell'Economia e delle Finanze del 18 gennaio 2008 n. 40;

- ad acquisire d'ufficio il documento unico di regolarità contributiva (D.U.R.C.) - attestante la regolarità del Fornitore in ordine al versamento dei contributi previdenziali e dei contributi assicurativi obbligatori per gli infortuni sul lavoro e le malattie professionali dei dipendenti.

Le Amministrazioni Beneficiarie opereranno sull'importo netto progressivo delle prestazioni una ritenuta dello 0,5% (zero virgola cinque per cento) che verrà liquidata dalle stesse solo al termine del Contratto Esecutivo e previa acquisizione del documento unico di regolarità contributiva.

Resta tuttavia espressamente inteso che in nessun caso il Fornitore potrà sospendere la prestazione dei servizi e, comunque, delle attività previste nei singoli Contratti Esecutivi. Qualora il Fornitore si rendesse inadempiente a tale obbligo, i singoli Contratti Esecutivi potranno essere risolti di diritto mediante semplice ed unilaterale dichiarazione da comunicarsi con lettera raccomandata A/R dall' Amministrazione Beneficiaria

Ogni singola fattura dovrà contenere la descrizione di ciascuno dei servizi cui si riferisce.

8. REFERENTI E CONTATTI DEL FORNITORE

Organizzazione a Supporto dell'erogazione dei Servizi

L'organizzazione proposta dal RTI riflette le specificità della fornitura e le richieste della Committente, assicurando efficacia e flessibilità sia nella gestione complessiva del Contratto Quadro (nel seguito CQ), sia nell'erogazione dei singoli Contratti Esecutivi (nel seguito CE). Particolare attenzione è stata posta nella definizione dei ruoli del RTI che avranno un rapporto diretto con i Referenti Consip e AgID e delle Amministrazioni beneficiarie, al fine di individuare rapidamente responsabilità e competenze e rendere efficaci i processi di erogazione dei servizi oggetto dei Contratti. È opportuno sottolineare che tale organizzazione, nonché le metodologie e gli strumenti a supporto della fornitura, saranno oggetto di condivisione con Consip, AgID in fase di avvio delle attività, al fine di garantire il massimo allineamento con le esigenze dell'Amministrazione stessa.

Dato il perimetro e l'estensione temporale del CQ il RTI ha ritenuto opportuno impostare l'organizzazione a supporto della Fornitura secondo un modello di un'unica azienda strutturata in:

- un Comitato Direttivo di RTI a livello di Governo sia per il CQ sia per i CE;
- unità/strutture operative, deputate all'erogazione dei servizi, flessibili e territorialmente distribuite;
- strutture e funzioni di supporto all'erogazione degli stessi.

La figura seguente riporta il modello organizzativo proposto.

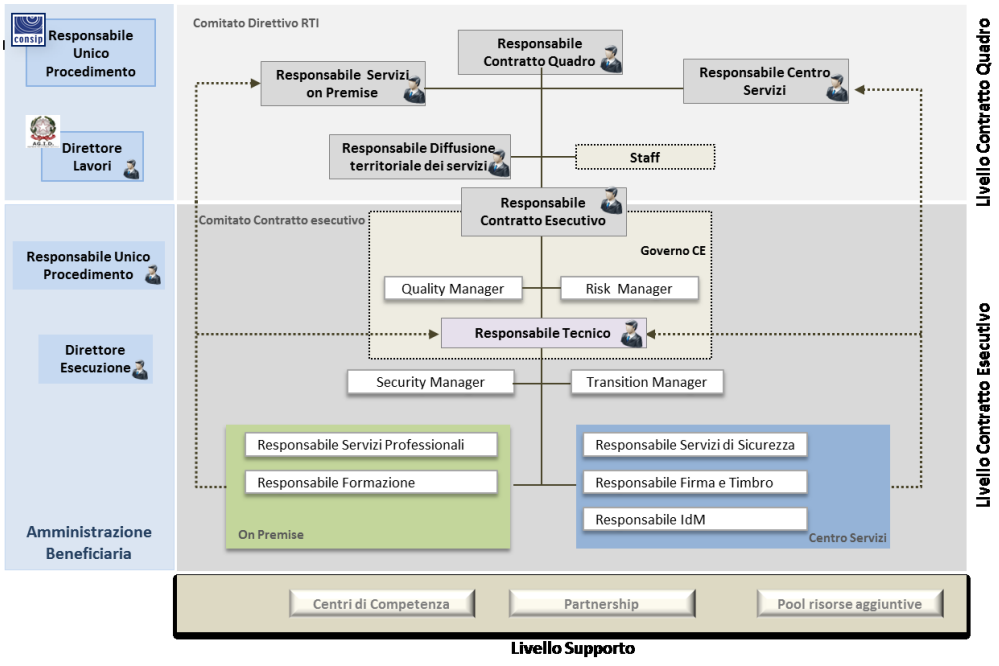


Figura 33 : Modello organizzativo RTI

Il modello proposto per rispondere a tutti i requisiti previsti dalla Gara lungo l'intero ciclo di vita del CQ e per adattarsi efficacemente alle diverse tipologie di Amministrazioni ed ai vari CE.
Il modello si articola su tre livelli:

- Livello di governo del Contratto Quadro, che rappresenta il livello di organizzazione più elevato per la gestione e il coordinamento dell'intera Fornitura. È costituito dal Comitato Direttivo del RTI che rappresenta una struttura centralizzata affidata al Responsabile del CQ che svolge un'azione di indirizzo e controllo strategico in un'ottica di gestione unitaria dei CE

stipulati con il RTI. Il Comitato Direttivo è responsabile sia della conduzione della fornitura nel suo complesso sia dell'intera struttura organizzativa; ha una visione unica ed integrata dell'andamento della Fornitura ed assicura la qualità complessiva dei CE erogati per conseguire la piena soddisfazione delle Amministrazioni;

- Livello del Contratto Esecutivo, che coordina ed eroga i servizi previsti per ogni CE attraverso il Responsabile del CE. Questa figura, le cui responsabilità sono dettagliate nel successivo paragrafo, svolge anche compiti di raccordo tra i due livelli. Il livello comprende tutte le risorse (Figure Apicali del RTI e risorse costituenti i team), le strutture operative e le strutture di supporto impiegate nell'esecuzione dei servizi. È progettato per adattarsi alle diverse tipologie di Amministrazioni che aderiranno, garantendo la qualità e fornendo la maggiore flessibilità possibile per l'erogazione dei servizi.
- Livello di Supporto all'erogazione dei Servizi: comprende, oltre ai Centri di Competenza delle aziende del RTI, Partnership aziendali, Community Practice, Collaborazioni con ambienti Universitari e scientifici di cui ciascuna azienda dispone su tematiche tecnologiche, funzionali e di processo. Tali relazioni consentono al RTI di supportare AgID, Consip e le Amministrazioni Beneficiarie nelle attività di definizione e gestione di soluzioni particolarmente innovative, coadiuvando, ove opportuno, anche il RTI durante la fase di erogazione.

Ruoli e Responsabilità del Contratto Esecutivo

Il RTI applicherà per il governo del singolo Contratto Esecutivo e per l'erogazione operativa dei relativi servizi il modello organizzativo, rappresentato di lato, ottimizzandolo in funzione delle dimensioni, del contesto e del perimetro funzionale e tecnologico dell'Amministrazione. Nel seguito ne sono descritte le figure e i ruoli.

Ruolo	Caratteristiche e Responsabilità
Responsabile Contratto Esecutivo	Costituisce l'interfaccia unica verso il Responsabile del Procedimento dell'Amministrazione Beneficiaria. L'insieme dei Responsabili di ciascun CE, nel caso di più di un'aggiudicazione, si riunisce periodicamente nel Comitato Direttivo presente a livello di CQ per condividere informazioni e situazioni generali e per allinearsi con il Responsabile del CQ e le funzioni di staff. I Comitati Direttivi saranno convocati in funzione delle specifiche esigenze dei CE oppure per tipologia di servizi oggetto di allineamento o approfondimento.
Quality manager (aggiuntivo)	Supporta il Responsabile del CE nella gestione degli aspetti di qualità relativi agli specifici servizi oggetto del Contratto stesso. Interagisce e si allinea con il Responsabile della Qualità a livello di CQ per le attività afferenti il proprio contratto. Produce i Piani della Qualità e le successive revisioni. La figura proposta ha una certificazione di "Valutatore Sistemi di Gestione per la Qualità (corso qualificato CEPAS e AICQ-SICEV)".
Risk Manager (aggiuntivo)	Costituisce la figura del RTI che supporta il Responsabile del CE nell'identificare e gestire i potenziali rischi associati alla fornitura dei servizi oggetto del proprio contratto per prevenirli e, nel caso non fosse possibile, mitigarli e monitorarli. Interagisce e si allinea con il Responsabile Gestione del Rischio a livello di CQ per le attività afferenti il proprio contratto. Viene annualmente formata, internamente all'azienda, su metodologie sulla Gestione del rischio delle forniture.
Responsabile Tecnico	È il Responsabile unico delle attività tecniche e del raggiungimento degli obiettivi dei servizi oggetto del Contratto. Costituisce l'interfaccia unica verso il Direttore Esecuzione nominato dall'Amministrazione. Ha la visione complessiva e integrata di tutte le attività tecniche legate all'attivazione, all'erogazione e al rilascio dei servizi della fornitura e ne garantisce la qualità. Ottiene dalle aziende del RTI le risorse e i contributi necessari per conseguire gli obiettivi della fornitura. Si coordina in fase di attivazione di un CE con il Responsabile del Centro Servizi e con il Responsabile dei Servizi on Premise, attivando il Responsabile della linea di servizio oggetto di fornitura. A lui riportano tutti i Responsabili dei Servizi o gruppi di servizi. Possiede certificazione PMI.
Security Manager	È il riferimento unico del Responsabile Tecnico per tutti gli aspetti legati alla sicurezza del singolo CE. Riferisce e riporta a livello di CQ al Responsabile della Sicurezza. Possiede certificazioni specifiche di sicurezza quali CISA, CISM, CISSP.
Transition Manager (aggiuntivo)	Governa e controlla lo svolgimento delle singole attività in cui si articola il processo di Phase-in e di Phase-out del proprio CE. Coordina le attività di affiancamento monitorando il rispetto del

Ruolo	Caratteristiche e Responsabilità
	piano di subentro. Verifica lo stato di avanzamento del processo e analizza i KPI col supporto del Quality Manager del proprio CE. In caso di scostamento dalla pianificazione propone ai Responsabili di Servizio, col supporto del Risk Manager, azioni preventive e/o correttive in grado di ripristinare la situazione (Risk Management). Riporta e allinea il Responsabile Transition a livello di CQ.

Responsabili del servizio

Responsabili Servizio: IdM, Firma / Timbro, Servizi di Sicurezza e Professionali	Il responsabile di ciascun servizio o gruppo di servizi coordina dal punto di vista operativo tutte le attività legate ai servizi di competenza e costituisce il punto di riferimento per l'attivazione di nuovi servizi. Produce i resoconti periodici, da presentare per discussione durante i SAL. Ciascun Responsabile di servizio riporta al Responsabile Tecnico. Avranno oltre 15 anni di anzianità lavorativa, esperienza pluriennale nella gestione e coordinamento di risorse umane, di progetti complessi e di gruppi di lavoro di grandi dimensioni, capacità relazionali, certificazioni PMI e/o ITIL, conoscenze consolidate nell'ambito del servizio in termini di processi, metodi e strumenti.

9. ALLEGATI

Allegato 1 – Listino prezzi

Allegato 2 – Schema Piano dei fabbisogni

Allegato 3 – Schema Progetto dei fabbisogni

Allegato 4 – Schema lettera di contestazione delle penali

Allegato 5 – Schema lettera di applicazione delle penali