Sistema pubblico di cooperazione:

SERVIZI DI SICUREZZA

Versione 1.1

DigitPA

INDICE

1. MODIFICHE DOCUMENTO

Descrizione Modifica	Edizione	Data
Versione 1.0	1.0	14/10/2005
Adeguamento documentazione DigitPA	1.1	25/07/2011

2. OBIETTIVI E CONTESTO DI RIFERIMENTO

Il quadro tecnico di riferimento per attuare la cooperazione applicativa tra le amministrazioni pubbliche nell'ambito del Sistema Pubblico di Connettività e Cooperazione è stato definito con l'approvazione, avvenuta nell'ottobre del 2004 da parte delle associazioni dei fornitori, delle amministrazioni partecipanti alla loro stesura e del Tavolo Congiunto Permanente della Conferenza Unificata Stato Regioni Città e Autonomie Locali, dei documenti che ne delineano l'architettura, l'organizzazione e le tecnologie standard da adottare.

Tali documenti hanno definito il "giusto" livello di condivisione che consente sia la maggiore stabilità nel tempo del modello rispetto al contesto organizzativo e tecnologico di riferimento, sia i necessari gradi di libertà per la sua implementazione. Il decreto legislativo n.42 del 28 febbraio 2005 che istituisce il Sistema Pubblico di Connettività e Cooperazione, ne stabilisce i valori fondanti, la validità giuridica, nonché il modello di governo strategico ed operativo ed i ruoli del CNIPA e delle Regioni in tali ambiti.

I suddetti documenti tracciano un primo quadro di evoluzione del modello e definiscono gli ulteriori documenti di maggiore dettaglio da produrre per l'implementazione dei servizi previsti. La redazione di questi ultimi, come concordato, è stata portata avanti dal CNIPA ed ha dato luogo ai documenti di cui alla seguente tabella 1. Quest'ultimo insieme di documenti rappresenta le specifiche per la realizzazione e gestione dei servizi di cooperazione SPC e delle procedure di qualificazione, come già definito nei documenti approvati.

	Titolo Documento	Stato e Data Pubblicazione
1.	*Sistema Pubblico di Cooperazione: QUADRO TECNICO D'INSIEME*	Pubblicato V. 1.1 del 25/07/2011
2.	*Sistema Pubblico di Cooperazione: TERMINI E DEFINIZIONI*	Pubblicato V. 1.1 del 25/07/2011
3.	*Sistema Pubblico di Cooperazione: ACCORDO DI SERVIZIO*	Pubblicato V. 1.1 del 25/07/2011
4.	*Sistema Pubblico di Cooperazione: PORTA DI DOMINIO*	Pubblicato V. 1.1 del 25/07/2011
5.	*Sistema Pubblico di Cooperazione: BUSTA DI E-GOV*	Pubblicato V. 1.2 del 25/07/2011
6.	*Sistema Pubblico di Cooperazione: SERVIZI DI REGISTRO*	Pubblicato V. 1.1 del 25/07/2011
7.	*Sistema Pubblico di Cooperazione: SERVIZI DI SICUREZZA*	Pubblicato V. 1.1 del 25/07/2011
8.	*Sistema Pubblico di Cooperazione: CONVENZIONI DI NOMENCLATURA E SEMANTICA*	Pubblicato V. 1.1 del 25/07/2011
9.	*Sistema Pubblico di Cooperazione: ESERCIZIO E GESTIONE*	Pubblicato V. 1.1 del 25/07/2011

Tabella 1. Documenti di specifica del SPCoop

2.1. Scopi del documento

Il presente documento specifica i Servizi di Sicurezza del Sistema Pubblico di Cooperazione (SPCoop). Questo si fonda sull'uso di messaggi applicativi per realizzare la cooperazione dei servizi applicativi delle Pubbliche Amministrazioni e, in prospettiva, tra le Pubbliche Amministrazioni e il cittadino, le imprese, le associazioni e le istituzioni, all'interno di un quadro nel quale devono essere assicurati livelli ottimali di qualità e di sicurezza.

Gli elementi cardine del SPCoop sono le Porte di Dominio delle varie Amministrazioni, che ne sono responsabili come dei servizi esposti attraverso le stesse, ed i Servizi di Registro previsti nell'ambito dei servizi infrastrutturali SICA, il cui compito è quello di garantire a tutte le Amministrazioni la ricerca e l'accesso dei servizi disponibili tramite le Porte di Dominio.

Questo quadro d'insieme impone innanzitutto che le Porte di Dominio siano qualificate prima di esporre i servizi e che sia le Porte di Dominio che i Servizi di Registro (in particolare al livello Generale) siano adeguatamente protetti da Servizi di Sicurezza. Sono, inoltre, necessarie anche regole comuni per il trattamento dei messaggi applicativi, per assicurare requisisti di autenticità, riservatezza, integrità, non ripudio e tracciabilità degli stessi. Tali obiettivi sono conseguiti facendo uso di protocolli e standard basati sull'uso dei certificati digitali, per cui si rendono necessari anche servizi di certificazione a chiave pubblica.

Il documento si articola nei seguenti capitoli:

Capitolo 4 – Introduzione: delinea il contenuto del documento, e lo pone nel contesto di tutti gli altri documenti, al fine di identificare quali aspetti vengono qui trattati e con quale ottica.

Capitolo 5 – Il Modello della Sicurezza: fornisce le indicazioni sul contesto architetturale, sulle tecnologie e sui documenti di riferimento per delimitare l'ambito in cui sono predisposti, applicati ed aggiornati i requisiti funzionali ed organizzativi per la sicurezza de SPCoop.

Capitolo 6 – I Servizi di Sicurezza di Supporto: contiene la descrizione dei servizi di sicurezza necessari per il corretto funzionamento del SPCoop, essenzialmente di supporto al sistema, quali il rilascio dei certificati digitali, nonché i meccanismi per assicurare l'interoperabilità tra Autorità di Certificazione diverse.

Capitolo 7 – I Servizi di Sicurezza per i Servizi di Registro SICA Generale: contiene la descrizione dei servizi di sicurezza necessari per il corretto funzionamento dei Servizi di Registro SICA di livello Generale, in particolare al fine di realizzare la prevenzione degli incidenti di sicurezza ed assicurare il pronto intervento, con misure di sicurezza proattive, quali la rilevazione delle intrusioni e la protezione mediante firewall del traffico XML.

Capitolo 8 – I Servizi di Sicurezza per le Porte di Dominio: contiene la descrizione dei servizi di sicurezza che le Amministrazioni devono assicurare per il corretto funzionamento di SPCoop, che ruotano sulla qualificazione e protezione delle Porte di Dominio, sul monitoraggio, controllo e gestione della sicurezza tramite firewall del traffico XML, rilevazione delle intrusioni nonché la registrazione degli eventi al fine di rendere possibile la ricostruzione dei processi, sia per garantire la verifica della loro corretta esecuzione, sia per individuare, in caso contrario, quali siano state le anomalie.

Appendice: vengono riportati argomenti di carattere specifico per i quali è sembrato conveniente fornire indicazioni e raccomandazioni. In particolare viene descritta una proposta per la checklist ed il processo da utilizzare nell'ambito della qualificazione delle Porte di

Dominio e alcune raccomandazioni indirizzate all'implementazione operativa della Porta di Dominio di un'Amministrazione.

La redazione è stata ad opera di:

- Ubaldo Bussotti (CNIPA);
- Mario Terranova(CNIPA).

Hanno collaborato:

- Roberto Baldoni (Università di Roma "La Sapienza");
- Stefano Fuligni (CNIPA);
- Massimo Mecella (Università di Roma "La Sapienza");
- Francesco Tortorelli (CNIPA);

2.2. Note di lettura del documento

Nella definizione dei requisiti, delle specifiche e delle regole descritte nei documenti precedentemente indicati sono utilizzate le parole chiave DEVE, NON DEVE, OBBLIGATORIO, VIETATO, DOVREBBE, CONSIGLIATO, NON DOVREBBE, SCONSIGLIATO, POTREBBE, OPZIONALE che devono essere interpretate in conformità con [RFC2119]. In particolare:

- DEVE, OBBLIGATORIO significano che la definizione è un requisito assoluto, la specifica deve essere implementata, la consegna è inderogabile.
- DOVREBBE, CONSIGLIATO significano che in particolari circostanze possono esistere validi motivi per ignorare un requisito, non implementare una specifica, derogare alla consegna, ma che occorre esaminare e valutare con attenzione le implicazioni correlate alla scelta.
- PUÒ, OPZIONALE significano che un elemento della specifica è a implementazione facoltativa.
- NON DOVREBBE, SCONSIGLIATO significano che in particolari circostanze possono esistere validi di motivi per cui un elemento di specifica è accettabile o persino utile, ma, prima di implementarlo, le implicazioni correlate dovrebbero essere esaminate e valutate con attenzione.
- NON DEVE, VIETATO significano che c'e proibizione assoluta di implementazione di un determinato elemento di specifica.

2.3. Note sul Copyright

3. INTRODUZIONE ALLA SICUREZZA NEL SPCOOP

La sicurezza di un sistema complesso quale SPCoop presenta molte sfaccettature, sia di carattere architetturale che tecnologico che organizzativo, in particolare:

- **Aspetti Architetturali**: SPCoop è strutturato secondo un'architettura concettuale a due livelli: le Amministrazioni, attraverso le Porte di Dominio, espongono servizi applicativi; a livello inter-Amministrazione, mentre il SICA offre una serie di componenti/servizi infrastrutturali, che secondo un'architettura di tipo SOA sono necessari al funzionamento e gestione dei servizi applicativi delle Amministrazioni. Pertanto la sicurezza riguarda entrambi questi livelli. Deve essere definita a livello delle singole Amministrazioni, al fine di rendere sicure le Porte di Dominio ed i servizi applicativi da esse esposte, e deve essere definita per i componenti del SICA.
  Ciò porta all'introduzione di opportuni elementi architetturali:
  - *Firewall XML*, necessario alla protezione e messa in sicurezza dal punto di vista applicativo della Porta di Dominio e di tutti i messagi da/verso i servizi applicativi; questo elemento è a livello di singola Amministrazione.
  - *Autorità di Certificazione*, necessaria per la gestione di un'infrastruttura a chiave pubblica (PKI), che è il meccanismo base utilizzato per la gestione di tutti gli aspetti crittografici. L'Autorità di Certificazione, insieme ai Servizi di Registro SICA, è uno degli *elementi base del SICA*, e analogamente può essere articolato su due livelli, indicati come Generale e Secondario. Si rimanda al documento SERVIZI DI SICUREZZA per tutti gli aspetti di dettaglio.

  Va osservato che essendo i componenti infrastrutturali SICA essi stessi dei servizi, il Firewall XML viene utilizzato anche per la messa in sicurezza di questi ultimi.
- **Aspetti Tecnologici**: gli elementi architetturali precedentemente introdotti (ed approfonditi nel documento SERVIZI DI SICUREZZA) devono essere realizzati sulla base di tecnologie e standard largamente condivisi, e coerenti con le tecnologie Web Service su cui si basa l'intero SPCoop. Pertanto viene adottato il cosiddetto Web Service Security Framework, che è un insieme di standard riguardanti la sicurezza dei Web Service.
- **Aspetti Organizzativi e di Gestione della Sicurezza**: la sicurezza non è solamente questione di elementi architetturali e di standard tecnologici con cui realizzare i primi. È anche e soprattutto questione di *best practice* organizzative, di politiche di gestione di una serie di servizi accessori (qualificazione, scoperta delle intrusioni, registrazione degli eventi e delle anomalie, gestione della concessione delle autorizzazioni, ecc.) che ogni Amministrazione, nel rispetto di minime regole comuni, deve realizzare a garantire. Nel documento SERVIZI DI SICUREZZA vengono descritte appunto tali regole, il cui enforcement (attraverso la predisposizione degli opportuni servizi organizzativi) garantisce e supporta gli elementi architetturali e tecnologici precedentemente introdotti.

4. IL MODELLO DELLA SICUREZZA DEL SPCOOP

Questo capitolo fornisce le indicazioni sul modello della sicurezza per il Sistema Pubblico di Cooperazione (SPCoop), definendo il contesto di riferimento, individuando gli obiettivi di sicurezza, elencando i requisiti funzionali di sicurezza nel trattamento dei messaggi SPCoop, i servizi di sicurezza di supporto ed i servizi di sicurezza per il corretto funzionamento delle Porte di Dominio (PD) e dei Servizi di Registro SICA.

SPCoop è un insieme di standard tecnologici e di servizi infrastrutturali il cui obiettivo è di permettere l'interoperabilità e la cooperazione di sistemi informatici per la realizzazione di adempimenti amministrativi. Tali sistemi sono sotto la responsabilità di *soggetti pubblici*, costituiti da amministrazioni centrali, enti pubblici, regioni, provincie, comuni, comunità di enti locali, e *soggetti privati* (imprese e associazioni accreditate). L'insieme dei soggetti pubblici e privati operanti su SPCoop costituiscono la *comunità dei soggetti* di SPCoop.

Quando i dati ed i servizi sono distribuiti tra più organizzazioni autonome, i problemi tecnici, organizzativi ed istituzionali rendono necessaria la progettazione di un'architettura di sicurezza che deve garantire la corretta individuazione dei rispettivi ambiti di competenza e nel contempo escludere la presenza di anelli deboli.

Un sistema di servizi erogato da una pubblica amministrazione deve quindi rispettare specifici requisiti per assicurare la cooperazione e l'interscambio dei dati in modalità sicura, cioè tale da garantire il controllo completo della catena del servizio distribuita tra diverse componenti amministrative sia centrali che locali, sia pubbliche che private o miste.

Lo scenario di riferimento che viene qui analizzato è rappresentato dal modello architetturale di SPCoop, cioè l'insieme dei Servizi Applicativi, dei Registri SICA Secondari e del Registro SICA Generale, delle Porte di Dominio delle amministrazioni. Per quanto attiene lo studio delle problematiche di sicurezza, in questo documento non sono analizzate le questioni legate ai protocolli ed agli standard riferiti al livello del trasporto dei dati ed alla sicurezza fisica dei componenti del Sistema Pubblico di Connettività.

Nei documenti della Fase 2 (cfr. § 2) sono stati identificati gli obiettivi di sicurezza e quindi definiti, nelle linee generali, i requisiti funzionali di sicurezza dei componenti architetturali dell'SPCoop. Nel presente documento vengono descritti, con maggiore dettaglio ed a livello di specifiche, i requisiti funzionali e i servizi di sicurezza a livello infrastrutturale, in particolare per le Porte di Dominio ed per il Registro SICA Generale.

4.1. Analisi del contesto

4.1.1. Obiettivi di sicurezza

Nell'architettura SPCoop gli obiettivi minimi di sicurezza sono:

- *Autenticazione delle entità.*
  Deve essere verificata l'*identità* dichiarata da tutte le entità implicate direttamente o

indirettamente nello scambio di messaggi e nella erogazione e/o fruizione dei servizi. Essa riguarda i soggetti (utenti ed amministratori), i sistemi (PD, Registri, etc.) e le applicazioni che richiedono e/o erogano servizi. Le modalità di autenticazione sono dipendenti dalle operazioni effettuate. Devono essere individuate le categorie di operazioni per le quali è richiesto sempre l'uso dei certificati digitali nell'ambito di uno scenario di identità federate secondo standard generali ed a valenza normativa (Carta Nazionale dei Servizi, CIE, ecc.). Per i sistemi e le applicazioni è raccomandato l'uso dei certificati digitali emessi da PKI accreditate in ambito SPC.

- *Autorizzazione dei soggetti/applicazioni all'effettuazione delle operazioni*.
  Devono essere gestite le autorizzazioni intese come attribuzione, sospensione e revoca dei profili di accesso ai soggetti. I profili di accesso sono predisposti in relazione alle operazioni consentite, secondo i tempi previsti, relativamente ad insiemi di dati definiti, e secondo le altre modalità ritenute necessarie. Sono individuati i responsabili dell'attribuzione dei privilegi, che curano altresì le modalità di conferimento e revoca. Per il conseguimento di tale obiettivo è richiesto sempre l'uso dei certificati digitali, salvo eccezioni corrispondenti a modalità di gestione ben individuate e circoscritte.

- *Delega delle Autorizzazioni all'effettuazione delle operazioni*.
  Deve essere possibile da parte di un soggetto delegante a favore di un soggetto delegato il conferimento delle autorizzazioni all'effettuazione di operazioni, come previsto dalla normativa vigente (delega, procura speciale, procura generale, etc.). Il conferimento delle autorizzazioni richiede l'uso di strumenti a valenza normativa (Firma Digitale, ecc).

- *Mantenimento dell'Integrità dei dati.*
  Deve essere assicurata l'integrità dei dati tra l'originatore delle richieste e l'erogatore, nel senso che vi deve essere assoluta confidenza che i dati non vengano modificati in modo accidentale o intenzionale e, sopratutto, all'insaputa di una o entrambe le entità.

- *Assicurazione della Riservatezza dei dati.*
  Deve essere assicurata la riservatezza dei dati scambiati sia in conformità alla normativa vigente (Decreto Legislativo n. 196/2003, conosciuto come Codice per la protezione dei dati personali, e successive modificazioni e integrazioni) sia per ogni altra ragione valida (ad esempio per evitare l'intercettazione dei dati classificati dall'amministrazione come "riservati");

- *Non ripudiabilità a livello di richiesta e di risposta*.
  Ogni messaggio contenente una richiesta inoltrata ed ogni messaggio contenete una risposta erogata devono contenere la prova che sono state effettuate da determinate entità, in un determinato contesto spazio/temporale di esecuzione.

- *Registrazione degli eventi/Ispezione/Tracciabilità.*
  Deve essere sempre possibile risalire a chi ha effettuato le operazioni, dove, quali operazioni sono state effettuate e quando. L'ispezione è la capacità di acquisire dinamicamente le informazioni di registrazione.

- *Amministrazione della sicurezza*.
  Devono essere individuate ed attribuite responsabilità al personale incaricato di gestire, in particolare, le operazioni di definizione dei profili di accesso, configurazione dei sistemi, generazione degli account, ecc.

4.1.2. Tipologia dei rischi da valutare

I principali rischi di attacco a cui sono esposti i sistemi partecipanti a SPCoop sono (lista non esaustiva):

- *Intrusione attraverso impersonificazione*: un'entità cerca di raggirare il processo di autenticazione e presentarsi sotto falsa identità. Per raggiungere lo scopo vengono solitamente sfruttate delle anomalie (*exploit*) presenti nei sistemi operativi/applicazioni a livello di codice o causate da errate configurazioni.
- *Abuso di privilegi*: un'entità sfrutta le vulnerabilità dei sistemi per accedere a funzionalità con privilegi differenti da quelli attribuiti. Per limitare tale rischio occorre definire un meccanismo rigoroso di controllo degli accessi, rilevazione di intrusioni e verifiche sulle assegnazioni dei privilegi.
- *Intercettazione dei dati*: un'entità non autorizzata cerca di acquisire dati durante il transito. Per limitare tale rischio devono essere implementate tecniche di *cifratura*.
- *Manomissione dei dati*: un'entità cerca di inserire dati non autentici o alterare il contenuto dei messaggi. Per ovviare a questo attacco devono essere implementate tecniche per la "firma" dei dati.
- *Distruzione delle tracce*: un'entità all'origine di un attacco vuole evitare di essere identificata e/o che si ritrovi la traccia di talune operazioni che ha effettuato, quindi cerca di cancellare le tracce di tutte o parte delle operazioni effettuate. Per garantire l'imputabilità delle azioni devono essere attivate le registrazioni degli eventi, meccanismi di allerta e di controllo della disponibilità e corretto funzionamento dei sistemi. Devono essere custoditi secondo procedure di sicurezza gli archivi contenenti le tracce informatiche.
- *Riutilizzazione/Dirottamento dei messaggi*: un'entità intercetta i messaggi trasmessi e li riutilizza effettuando nuovi invii. Per ovviare a questo attacco occorre che i produttori dei dati e i mittenti ed i destinatari dei messaggi vengano autenticati, che i messaggi stessi siano identificati, autenticati e datati.
- *Distruzione dei messaggi/Negazione di invio/Negazione di ricezione*: un'entità vuole evitare che vengano eseguite talune operazioni oppure vuole negare che esse siano state effettivamente richieste, attraverso la distruzione dei messaggi. Per garantire l'imputabilità delle azioni devono essere attivate le registrazioni degli eventi, meccanismi di allerta e di controllo della disponibilità e corretto funzionamento dei sistemi. Devono essere custoditi secondo procedure di sicurezza gli archivi contenenti le tracce informatiche.

4.1.3. Politica di sicurezza (Security Policy)

Una corretta gestione delle problematiche di sicurezza nell'ambito di SPCoop non può prescindere dall'individuazione e dall'adozione di appropriate e specifiche politiche di sicurezza, anche in accordo con la normativa vigente (Direttiva del PCM del 16 gennaio 2002, Decreto Legislativo n. 196/2003, Decreto Legislativo n. 42/2005, ecc.).

Attraverso la politica di sicurezza si intende stabilire in modo certo, chiaro e condiviso, gli obiettivi di ordine generale che devono essere assicurati attraverso l'adozione delle misure minime di sicurezza, documentate nei piani operativi per la sicurezza delle amministrazioni.

Le linee principali sono le seguenti:

- Ogni amministrazione DEVE adottare e rispettare gli schemi architetturali, tecnici ed organizzativi riportati nei documenti SPC, e quindi gli standard ed i requisiti ivi indicati;
- Ogni amministrazione che aderisce ad SPCoop DEVE applicare, in ambito SPCoop, la politica di sicurezza generale definita ed approvata dalla Commissione di coordinamento del SPC, e le successive modificazioni per la gestione dei rischi e delle minacce di volta in volta individuate;
- Ogni amministrazione che intende pubblicare nuovi servizi DEVE preliminarmente aver superato con successo la qualificazione della propria PD, tra i requisiti richiesti figurano le misure di sicurezza fisica e la dimostrazione del possesso delle risorse necessarie per l'ordinaria amministrazione della sicurezza.

4.1.4. Gestione della sicurezza da parte delle Amministrazioni

Ogni Amministrazione coinvolta in SPCoop è tenuta alla gestione delle misure organizzative e procedurali nel rispetto della Politica di Sicurezza SPCoop, con particolare riguardo alla gestione delle PD ed i sistemi e le interfacce verso i sistemi informativi interni e quindi:

- Ogni Amministrazione DEVE individuare le risorse necessarie per lo svolgimento delle attività di amministrazione della sicurezza;
- Ogni Amministrazione DEVE applicare le procedure per la gestione ordinaria della sicurezza coerentemente con gli obiettivi di SPCoop ;
- Ogni Amministrazione DEVE provvedere all'attribuzione corretta e compiuta delle responsabilità.

4.1.5. Gestione della sicurezza da parte dei gestori dei servizi SICA Generali

I Gestori dei Servizi SICA Generali sono tenuti, nel rispetto dei vincoli contrattuali, alla applicazione delle misure organizzative e procedurali nel rispetto della Politica di Sicurezza SPCoop:

- Ogni Gestore dei Servizi SICA DEVE predisporre ed aggiornare il Documento Programmatico per la Sicurezza, contenente le indicazioni circa le misure, le attività e le procedure di sicurezza applicate per corrispondere alla Politica di Sicurezza SPCoop;
- Ogni Gestore dei Servizi SICA DEVE provvedere a far sottoporre la propria struttura dedicata all'erogazione dei servizi SICA ad approfondito *audit* con cadenza almeno annuale, da parte di

organizzazioni specializzate che abbiano il preventivo gradimento della Commissione di Coordinamento per l'SPC;

4.2. Requisiti di sicurezza

4.2.1. Regole per l'identificazione delle entità

L'erogazione e la fruizione di un servizio applicativo richiedono come condizione preliminare che siano effettuate operazioni di identificazione univoca delle *entità* (sistemi, componenti software, utenti) che partecipano, in modo diretto e indiretto (attraverso sistemi intermediari) ed impersonando ruoli diversi, allo scambio di messaggi e alla erogazione e fruizione dei servizi.

- L'identificazione delle entità coinvolte negli scambi di servizi e di messaggi DEVE seguire le regole definite in SPCoop, approvate dal Comitato di Coordinamento per l'SPC;
- Per quanto concerne gli utenti, le regole di identificazione DEVONO includere quelle previste dalla normativa relativa alla CNS ed alla CIE;
- Per quanto concerne i software (applicazioni) delle Amministrazioni, queste DEVONO essere responsabili dell'attribuzione univoca degli identificativi all'interno del loro Dominio;
- Deve valere il vincolo secondo cui la presenza e l'attività rilevata di elementi non identificati DEVE essere considerata come elemento che può arrecare pregiudizio al sistema e quindi segnalato come incidente di sicurezza;
- Gli identificativi dei servizi DEVONO essere conformi a un formato URI specificato [URI];
- Le Amministrazioni DEVONO essere tutte registrate nel Registro SICA Generale;
- Le richieste di registrazione dei soggetti, utenti, servizi, Accordi di Servizio, indirizzi dei punti di accesso sul Registro SICA Generale DEVONO essere prodotte da parte dei responsabili autorizzati e devono essere autenticate mediante documenti informatici sottoscritti con firma digitale.

4.2.2. Regole per l'autenticazione

La verifica delle identità dichiarate (autenticazione) deve essere effettuata nel momento in cui si effettua un'operazione. I meccanismi dipendono dalla tipologia delle entità operanti in SPC (utenti, applicativi, PD, servizi applicativi, messaggi applicativi, contenuto allegato ai messaggi applicativi ecc.).

- I meccanismi di autenticazione riguardanti gli utenti sono legati alla tipologia di operazioni che vengono effettuate.

- L'insieme dei meccanismi di autenticazione riguardanti gli utenti DEVE includere quelli previsti dalla normativa vigente per CNS e CIE.
- POSSONO essere utilizzati meccanismi di autenticazione riguardanti gli utenti basati sul concetto di autenticazione "forte", cioè basata sul controllo di almeno DUE fattori, mentre tutte le eventuali deroghe sono ammesse solo se approvate preventivamente dalla Commissione per l'SPC per casi ben individuati e circoscritti;
- I meccanismi di autenticazione riguardanti gli "allegati" ai messaggi applicativi DEVONO essere implementati attraverso algoritmi e protocolli di *firma digitale* e basati su chiavi crittografiche certificate a tale scopo da una o più *infrastrutture a chiave pubblica* accreditate e i cui certificati radice sono presenti nell' Elenco Pubblico dei Certificatori tenuto dal CNIPA;
- I meccanismi di autenticazione riguardanti le PD ed i servizi applicativi DOVREBBERO essere implementati attraverso i protocolli SSL v 3.0 o TLS v. 1.0. e basati su chiavi crittografiche certificate a tale scopo da una o più *infrastrutture a chiave pubblica* accreditate e i cui certificati radice sono presenti nella Trust Control List (TCL) dell'Autorità di Certificazione che svolge le funzioni di BRIDGE (BRIDGE CA);
- I meccanismi di autenticazione a livello dei messaggi applicativi DEVONO essere implementati attraverso gli standards OASIS WS-Security [WS-Security 2004], in particolare lo standard W3C XML-Signature [XML Signature] e lo standard SAML V2.0, con l'uso esclusivo del X509 Token Profile [WSS TP X509];
- Ogni certificato digitale emesso DEVE contenere gli elementi minimi previsti da WS-Security (Subject, Key Identifier, Serial Number ed Issuer) ed il profilo del certificato DEVE essere conforme al Certificate Practice Statement (CPS) previsto per lo scopo di certificazione;
- Ogni ICP operante in SPCoop DEVE essere autorizzata secondo le regole fissate dal Comitato di Coordinamento per SPC;
- I CPS delle Infrastrutture a Chiave Pubblica (ICP) operanti DEVONO essere resi pubblici;
- Ai fini di verifica dello stato di validità dei certificati utilizzati per l'autenticazione, DEVE essere usato il protocollo OCSP [OCSP];
- Per ogni messaggio da autenticare DEVE essere creato il contrassegno di sicurezza (security token), DEVE essere inserito nel messaggio e DEVE contenere informazioni relative alle credenziali dell'applicazione che richiede il servizio;
- Per l'autenticazione POSSONO essere usate le combinazioni di Username Token Profile (combinazione di userid e password) ma solo per richieste dirette (connessione HTTPS diretta tra PD senza intermediari), altrimenti DEVE essere usato il Token Profile;
- DEVE essere presente l'elemento `<wsse:SecurityTokenReference>` all'interno dell'header `<wsse:Security >`, il subject Key Identifier (elemento `<wsse:KeyIdentifier>`), il binarySecurityToken, per rappresentare il certificato in formato X.509 v3 presente in binario all'interno di un elemento `<wsse:BynarySecurityToken>`, il serial number per identificare il certificato attraverso l'emittente.

4.2.3. Regole per l' autorizzazione

Nell'ambito dell'erogazione e della fruizione di prestazioni di servizio, i requisiti di autorizzazione riguardano essenzialmente i richiedenti (utenti ed applicazioni) di un servizio e gli amministratori dello stesso.

- Per ogni Dominio di Cooperazione DEVONO essere individuati i Responsabili ai quali sono attribuite le responsabilità della individuazione e della gestione dei profili di autorizzazione;
- I profili di autorizzazione DEVONO essere predisposti in relazione alle possibili associazioni di insiemi di diritti per le operazioni effettuabili nei confronti di insiemi di dati con i vincoli temporali previsti;
- I profili di autorizzazione POSSONO prevedere meccanismi gerarchici e POSSONO essere basati sui ruoli secondo i paradigmi RBAC (Role-Based Access Control);
- Le operazioni di attribuzione, sospensione e revoca delle autorizzazioni DEVONO essere prodotte mediante l'uso della *firma digitale* e basati su chiavi crittografiche certificate a tale scopo da una o più *infrastrutture a chiave pubblica* accreditate e i cui certificati radice sono presenti nell' Elenco Pubblico dei Certificatori tenuto dal CNIPA;
- DEVE essere possibile da parte di un soggetto delegante, effettuare il conferimento di un insieme determinato di autorizzazioni a favore di un soggetto delegato, come previsto dalla normativa vigente Per il conseguimento di tale obiettivo le deleghe DOVREBBERO essere prodotte mediante l'uso della *firma digitale* e basati su chiavi crittografiche certificate a tale scopo da una o più *infrastrutture a chiave pubblica* accreditate e i cui certificati radice sono presenti nell' Elenco Pubblico dei Certificatori tenuto dal CNIPA, a meno di utilizzare altri metodi che assicurino in modo equivalente il requisito del non-ripudio delle operazioni di conferimento di delega;

A1. Lo scambio delle informazioni relative alle autorizzazioni DEVONO essere effettuate utilizzando lo standard SAML V 2.0, mediante chiavi crittografiche certificate a tale scopo da una o più *infrastrutture a chiave pubblica* accreditate e i cui certificati radice sono presenti nella TCL della Bridge CA.

4.2.4. Regole per il controllo dell'integrità

Nell'ambito dell'erogazione e della fruizione di prestazioni di servizio, il controllo dell'integrità si applica ai messaggi scambiati ed al loro contenuto.

- Il controllo di integrità dei messaggi scambiati DEVE essere implementato attraverso gli standard OASIS WS-Security [WS-Security 2004], in particolare gli standard W3C XML-Signature [XML Signature];
- La scelta inerente gli algoritmi per la sottoscrizione ed i parametri specifici da utilizzare (lunghezza delle chiavi, etc.) DEVE essere approvata dalla Commissione di Coordinamento SPC;
- La firma prevista da XML-Signature DEVE essere inserita all'interno dell'header block `<wsse:security>` utilizzando l'elemento `<ds:Signature>`;

- Tutti gli elementi `<ds:Reference>` contenuti come sottoelementi di `<ds:Signature>` DEVONO contenere il riferimento ad una parte del messaggio SPCoop.
- DEVE essere seguita la procedura seguente per la "firma" ai fini dell'integrità:
  - Selezione delle parti del messaggio/parti del messaggio da firmare;
  - Effettuazione della trasformazione XML canonica;
  - Creazione dei "message digest";
  - Creazione dell'elemento di riferimento (contenente gli algoritmi di md usati, i valori, le parti cui fa riferimento la trasformazione etc.);
  - Creazione dell'elemento "*SignedInfo*", che include *SignatureMethod* e *CanonicalizationMethod*;
  - Applicazione di *CanonicalizationMethod* a *SignedInfo*;
  - Creazione della firma con gli algoritmi definiti in *SignatureMethod*
  - Creazione dell'elemento *Signature* che contiene: *SignedInfo, SignatureValue,* e opzionalmente *KeyInfo* e *Object*;
- DEVE essere seguita la procedura seguente per la "verifica della firma":
  - Effettuare la trasformazione in forma canonica del *SignedInfo* , secondo il metodo specificato in *CanonicalizationMethod;*
  - Per ogni elemento referenziato, acquisire i relativi *Object;*
  - Calcolare i rispettivi digest;
  - Verificare la corrispondenza.

4.2.5. Regole per la riservatezza

La classificazione in ambito SPCoop dei dati distingue le seguenti cinque categorie:

Livello	Declaratoria	Pubblicabilità	Accessibilità
R1	*dato pubblico*	Il dato può essere acquisito, diffuso e riprodotto ovunque senza autorizzazione	Conoscibile da chiunque indistintamente
R2	*dato interno*	Il dato è presente in atti interni di natura ordinaria al dominio dell'amministrazione, è conoscibile solo previa autorizzazione, e necessita dell'identificazione del richiedente	Riservato all'amministrazione, custodito secondo le regole del segreto d'ufficio
R3	*dato personale*	Definito ai sensi dell'art.	Accessibile secondo la normativa

Livello	Declaratoria	Pubblicabilità	Accessibilità
		4 del Decreto Legislativo n. 196/03 e succ. modd, trattati ai sensi degli artt. 11 e succ. della predetta normativa	vigente (Decreto Legislativo n. 196/03 e succ. modd. e Legge n. 241/90 e succ. modd.)
R4	*dato sensibile/dato giudiziario*	Definito ai sensi dell'art. 4 del DL 196/2003 e succ. modd, trattati ai sensi degli artt. 11, 20, 21, 22 e succ. della predetta normativa	Accessibile secondo la normativa vigente (Decreto Legislativo n. 196/03 e succ. modd. e Legge n. 241/90 e succ. modd.). Obbligo applicazione misure minime di sicurezza
R5	*dato riservato*	Dato di svariata natura sul quale è stata apposta una specifica classifica da parte dell'amministrazione, può essere acceduto solo da soggetti espressamente autorizzati	Accesso controllato con misure di sicurezza ben individuate, che devono includere l'identificazione dei richiedenti, la verifica delle autorizzazioni, il controllo degli accessi e la registrazione delle operazioni. Ogni eventuale violazione deve essere denunciata alle Autorità competenti.

Nella trattazione dei dati contenuti nei messaggi SPCoop scambiati, i Responsabili dei Sistemi informativi automatizzati ed i loro delegati DEVONO provvedere alla classificazione delle informazioni;

- I dati di livello R3, R4, R5 DEVONO essere *cifrati* ogni qualvolta sono scambiati attraverso messaggi SPCoop;
- I meccanismi di riservatezza a livello dei messaggi SPCoop DEVONO essere implementati attraverso gli standards OASIS WS-Security [WS-Security 2004], in particolare gli standards W3C XML-Encryption [XML-Encryption];
- Ogni certificato digitale emesso DEVE contenere gli elementi minimi previsti da WS-Security (Subject, Key Identifier, Serial Number ed Issuer) ed il profilo del certificato DEVE essere conforme al CPS previsto per lo scopo di certificazione.
- I meccanismi di riservatezza riguardanti lo scambio tra PD DOVREBBERO essere implementati attraverso i protocolli SSL v 3.0 o TLS v. 1.0. e basati su chiavi crittografiche certificate a tale scopo da una o più *infrastrutture a chiave pubblica* accreditate e i cui certificati radice sono presenti nella TCL della Bridge CA.
- I certificati emessi per tale finalità DEVONO essere differenti da quelli emessi per ogni altra finalità;
- La scelta inerente gli algoritmi di cifratura ed i parametri specifici da utilizzare (lunghezza delle chiavi, etc.) DEVE essere approvata dalla Commissione di Coordinamento SPC;
- La cifratura prevista da XML-ENCRYPTION DEVE essere utilizzata all'interno del blocco `<wsse:Security>` del messaggio;

- l'elemento <xenc:ReferenceList> DEVE essere utilizzato per definire quali parti di dati (identificati da elementi <xenc:EncryptedData>) sono cifrati;
- POSSONO essere utilizzate più chiavi per cifrare un messaggio e per identificare la chiave con la quale la porzione di dati è stata cifrata (<xenc:EncryptedData>) utilizzando l'elemento <ds:KeyInfo>;
- DEVE essere utilizzato un elemento <xenc:EncryptedKey> per memorizzare la chiave simmetrica all'interno del messaggio;
- DEVE essere seguita la procedura seguente per la cifratura:
  1. creazione di un <wsse:Security> header;
  2. creazione di un elemento <xenc:EncryptedKey> (in caso di utilizzo di chiave simmetrica), come sotto elemento di <wsse:Security>. L'elemento <xenc:EncryptedKey> conterrà a sua volta un sottoelemento <xenc:ReferenceList> che prevede un elemento per ogni elemento <xenc:EncryptedData> cifrato con quella chiave ;
  3. cifratura delle parti previste secondo le specifiche XML Encryption e rimpiazzare gli originali elementi con nuovi <xenc:EncryptedData>;
  4. creazione di un elemento <ds:KeyInfo> all'interno dell'elemento <xenc:EncryptedData> per referenziare una specifica chiave;
  5. creazione di un elemento <xenc:DataReference> che referenzia l'elemento <xenc:EncryptedData> generato. L'elemento <xenc:DataReference> va inserito come sottoelemento di <xenc:ReferenceList>.

4.2.6. Regole per il non-ripudio

Nell'ambito dell'erogazione e della fruizione di prestazioni di servizio, il requisito del non –ripudio riguarda il messaggio scambiato, compreso l'eventuale allegato.

- L'allegato del messaggio PUO' contenere una richiesta, in tal caso questa DEVE essere un documento informatico sottoscritto con firma digitale;
- le regole e gli standard della firma digitale fanno riferimento alla normativa seguente (DPR 29 dicembre 200 n.445 come modificato dal Decreto legislativo 29 gennaio 2002 n.10 e dal DPR 7 aprile 2003 n. 137, DPCM 13 gennaio 2004 [codice dell'amministrazione digitale][Decreto legislativo del 7 marzo 2005, n. 82 pubblicato su G.U. 16 maggio 2005, n.112 - S.O. n. 93]);
- La firma digitale PUO' essere apposta dall'utente che ha originato il processo che ha creato la busta, oppure PUO' essere apposta da altri utenti deputati a ricevere la richiesta, verificarla, e quindi apporre la propria firma;
- L'apposizione della firma sull'allegato rende possibile la memorizzazione del documento indipendentemente dal messaggio di trasporto (messaggio SPCoop), anche ai fini di dirimere possibili contenziosi;
- Gli allegati binari DEVONO essere codificati in formato BASE64 (RFC 3548);
- DEVE essere seguita la procedura seguente :

- CASO A (collegamento diretto tra PD, connessione con protocollo HTTPS). Si PUO' utilizzare lo UserName Token profile:
  - creazione di un `<wsse:Security>` header;
  - inserimento dell' elemento `<wsse:UsernameToken>`, per specificare la username del fruitore del servizio;
  - inserimento, all'interno di `<wsse:UsernameToken>`, dell'elemento `<wsse:Password>` che contiene la password del richiedente il servizio. (la password può essere inviata all'interno del messaggio in un formato chiaro (`wsse:PasswordText`) oppure in un formato "digest" (`wsse:PasswordDigest`)),
- CASO B (non esiste un collegamento diretto tra PD). Si DEVE utilizzare X.509 security token profile:
  - creazione di un `<wsse:Security>` header;
  - inserimento dell' elemento `<wsse:SecurityTokenReference>`, per specificare il riferimento al fruitore del servizio;
  - inserimento, all'interno di `<wsse:SecurityTokenReference>`, di :
    - un subject Key Identifier (elemento `<wsse:KeyIdentifier>`);
    - un binarySecurityToken, (certificato in formato X.509 v3, come elemento binario all'interno di un elemento `<wsse:BynarySecurityToken>` nel messaggio;
    - un serial number per identificare il certificato digitale.

4.2.7. Regole per la registrazione degli eventi, l'ispezione e la tracciatura

Le funzioni di registrazione e tracciatura consistono nella memorizzazione dei dati relativi alle operazioni che sono state effettuate sulle PD delle Amministrazioni.

Tali funzioni sono attivate per il conseguimento dei seguenti obiettivi:

(a) consentire la verifica delle operazioni svolte al fine di individuare eventuali problemi di natura prestazionale o di sicurezza;

(b) ricostruire le operazioni svolte da un processo cooperante per la messa a punto dei sistemi (test di funzionamento), e per il recupero di informazioni sulla mancata effettuazione delle transazioni (controllo e gestione degli errori);

(c) conservare le informazioni nel caso in cui venga attivato un procedimento diretto alla soluzione di eventuali contenziosi.

Tenendo conto della molteplicità di soluzioni per la realizzazione delle PD e della mancanza di standard cui fare riferimento per quanto attiene le tracce applicative, in questo paragrafo sono individuare le regole generali per la gestione, rimandando le scelte circa i formati ed i tracciati delle registrazioni a documenti successivi.

- Ogni PD deve farsi carico della tracciatura per ogni messaggio SOAP scambiato;

- Le tracce sono costituite da record di informazioni con in testa un identificativo univoco che include il codice della PD che genera la traccia e DEVONO contenere almeno le seguenti altre informazioni: riferimento temporale di ricezione, riferito al tempo di rete ufficiale, identificativo della PD del mittente e del destinatario (id_porta_mittente, id_porta_destinatario), identificativo univoco del messaggio SPCoop, identificativo del mittente del messaggio SPCoop, identificativo del destinatario del messaggio SPCoop, identificativo della tipologia della richiesta, identificativo della tipologia di traccia generata (spedizione, ricezione, errore, etc.);
- DEVONO essere definite le regole per l'accesso alle tracce applicative da parte dei sistemi per finalità legate al riscontro dell'esito delle operazioni di spedizione e ricezione;
- Le tracce applicative disponibili per l'accesso DEVONO essere in formato XML, ed il formato di tali registrazioni è approvato dalla Commissione di Coordinamento per l'SPC;
- I record di tracciatura prodotti in modo automatico DEVONO essere conservati con le modalità ed i tempi definiti tali da assicurare la possibilità di ricostruire senza equivoci e per periodi di tempo compatibili con la normativa vigente;
- Ai fini della correlazione tra le tracce applicative, DEVE essere rispettato il formato approvato dal Comitato di Coordinamento per l'SPC;
- Per la generazione delle tracce applicative POSSONO essere utilizzate sia informazioni presenti nelle tracce di sistema, sia le informazioni presenti nei messaggi SPCoop;
- DEVONO essere disciplinate, dai Responsabili delle PD e loro delegati, le modalità di accesso alle tracce applicative;
- Le tracce applicative generate dalle porte di dominio NON DEVONO contenere informazioni relative ai contenuti del messaggio (*body* della busta di *e-government*).

4.2.8. Regole per l' amministrazione della sicurezza

L'amministrazione della sicurezza deve essere effettuata sia a livello generale, cioè infrastrutturale, sia a cura delle amministrazioni attraverso l'applicazione dei piani per la sicurezza per SPCoop.

Nella gestione operativa dei sistemi sotto il loro controllo, i Responsabili DEVONO tenere conto di quanto previsto nei piani operativi per la sicurezza;

- DEVONO essere individuate ed attribuite responsabilità al personale incaricato di gestire le operazioni di definizione dei profili di accesso;
- DEVONO essere previste unità preposte alla configurazione dei sistemi;
- DEVONO essere previste verifiche sull'operato degli amministratori dei sistemi.

4.3.Servizi di sicurezza

L'ambito di erogazione dei servizi di sicurezza SPCoop è costituito dalle infrastrutture tecnologiche sotto il dominio amministrativo della Pubblica Amministrazione che afferisce al

SPCoop e dalle infrastrutture telematiche ad essi interconnesse, che possono ricadere sotto il dominio di amministrazione di terzi, inclusi i fornitori di connettività SPC.

Per chiarire meglio l'ambito ed il punto di applicazione di alcuni dei servizi di sicurezza disponibili in ambito SPCoop, di seguito saranno definiti alcuni concetti in riferimento al livello di sicurezza che dovrà essere garantito su SPCoop e alle relative responsabilità.

Dominio di una Pubblica Amministrazione: si definisce dominio di una Pubblica Amministrazione il complesso delle risorse informatiche ed infrastrutture che realizzano il Sistema Informativo della Pubblica Amministrazione; tale Dominio è caratterizzato da un livello di sicurezza minimo prestabilito di cui la Pubblica Amministrazione è direttamente responsabile, anche nel caso in cui la gestione dei servizi informatici sia affidati a terzi.

Dominio di Cooperazione: si definisce Dominio di Cooperazione il complesso delle risorse informatiche ed infrastrutture telematiche che differenti Amministrazioni decidono di dispiegare per supportare processi inter-amministrativi.

Porta di Dominio: si definisce Porta di Dominio la componente logica di mediazione tra il Dominio di una Pubblica Amministrazione e l'esterno. In base a tale definizione, qualora una Pubblica Amministrazione disponesse di un Sistema Informativo distribuito geograficamente ed interconnesso a SPCoop per il tramite di più di una Porta, essa verrà considerata come responsabile di differenti Domini, ognuno caratterizzato dal complesso delle risorse informatiche ed infrastrutture telematiche interconnesse al SPCoop per il tramite della particolare Porta.

A seguito di tali definizioni è possibile affermare che:

- Dato un insieme di misure di sicurezza, definite per assicurare il rispetto degli obiettivi di sicurezza (disponibilità, riservatezza, etc.), il livello minimo di sicurezza è definito come l'insieme di misure da applicarsi obbligatoriamente.
- L'elenco delle suddette misure di sicurezza è approvato dalla Commissione di Coordinamento per l'SPC.
- Il livello minimo di sicurezza del SPCoop DEVE essere garantito dalla federazione dei singoli Domini delle Pubbliche Amministrazioni e dal SICA;
- Per garantire il livello minimo di sicurezza ogni Amministrazione dovrà adottare una Politica di sicurezza interna che preveda l'implementazione di contromisure obbligatorie a livello di ciascuna Porta di Dominio; ogni Pubblica Amministrazione che intenda garantire un livello di sicurezza maggiore PUO' adottare contromisure aggiuntive, preferibilmente all'interno del proprio Sistema Informativo;
- Il rispetto dei requisiti necessari a garantire il livello minimo di sicurezza, da parte di ogni attore coinvolto nel SPCoop, DEVE essere verificato tramite *audit* con cadenza almeno annuale, da parte di organizzazioni specializzate che abbiano il preventivo gradimento della Commissione di Coordinamento per l'SPC;
- Le contromisure adottate da ogni Pubblica Amministrazione per garantire almeno il livello minimo di sicurezza imposto su SPCoop, DEVONO essere attuate per il tramite di servizi di sicurezza obbligatori per le Amministrazioni stesse.

4.4.Elenco dei servizi

La gestione ordinaria di SPCoop richiede lo svolgimento di servizi di sicurezza, tra i quali figurano l'amministrazione della sicurezza, le operazioni per la qualificazione e la protezione delle Porte di Dominio, il monitoraggio, il controllo e la gestione della sicurezza del Registro SICA Generale, la prevenzione degli incidenti di sicurezza, il pronto intervento, la certificazione delle chiavi pubbliche e la gestione dei certificati digitali e le attività di supporto connesse, tra le quali il rilascio dei certificati digitali per assicurare l'interoperabilità tra AC diverse che operano in ambito SPCoop, ecc.

Alcune attività tra quelle citate sono di natura prettamente infrastrutturale e sono suddivise in attività di supporto (Servizi di Certificazione) e attività di gestione del Registro SICA Generale, e devono essere erogate da fornitori, mentre le restanti sono sotto la responsabilità diretta delle Amministrazioni.

Sono sotto il controllo e la responsabilità dell'Amministrazione almeno le seguenti attività:

Attività
Creazione e gestione dei profili di autorizzazione per usufruire dei servizi applicativi erogati tramite le PD
Rilevazione H24 dei tentativi di intrusione alle PD
Protezione da DOS, DDOS e XDOS (XML Denial of Services) delle PD
Rilevazione H24 ed eliminazione di virus informatici eventualmente presente nelle buste SPCoop e/o nel body e/o negli attachment
Registrazione degli eventi rilevanti ai fini della sicurezza per ogni PD
Tracciamento e memorizzazione delle operazioni eseguite sulle PD
Aggiornamento delle componenti che fanno parte della PD (patch management, evolutivo e correttivo)
Gestione degli accessi alle PD

Tabella 2. Attività sotto la responsabilità della singola Amministrazione

Sono attività che possono convenientemente essere sotto il controllo e la responsabilità del CNIPA, le seguenti attività:

Attività
Rilevazione H24 dei tentativi di intrusione al Registro SICA Generale
Protezione da DOS, DDOS e XDOS del Registro SICA Generale
Gestione degli accessi al Registro SICA Generale
Registrazione degli eventi rilevanti ai fini della sicurezza sul Registro SICA Generale

Attività
Gestione delle chiavi crittografiche e dei certificati digitali
Aggiornamento delle componenti che fanno parte del Registro SICA Generale (patch management, evolutivo e correttivo)
Hardening dei sistemi che compongono il Registro SICA Generale
Effettuazione dei test di robustezza sul Registro SICA Generale
Verifica periodica delle configurazioni dei sistemi che compongono il Registro SICA Generale
Verifica periodica di integrità dei sistemi che compongono il Registro SICA Generale
Gestione incidenti di sicurezza per il Registro SICA Generale
Ripristino dei sistemi che compongono il Registro SICA Generale in caso di attacchi/guasti, ecc.

Tabella 3. Attività sotto la responsabilità del CNIPA

Le attività elencate nella tabella precedente possono essere accorpate ed inserite nei servizi integrati seguenti:

Servizio	Attività accorpate
Qualificazione delle PD	Hardening dei sistemi, verifica delle configurazioni dei sistemi
Security assessment	Effettuazione dei test di robustezza, verifica delle configurazioni dei sistemi, verifica di integrità dei sistemi, aggiornamento dei sistemi (patch management, evolutivo e/o correttivo)
XML Firewall	Protezione da DOS, DDOS e XDOS (XML Denial of Services), rilevazione H24 ed eliminazione di virus informatici eventualmente presenti nei messaggi SPCoop e/o nel body e/o negli attachment
Intrusion detection	Rilevazione H24 dei tentativi di intrusione
Registrazione degli Eventi	Registrazione degli eventi rilevanti ai fini della sicurezza, tracciamento e memorizzazione delle operazioni eseguite
Gestione emergenze	Gestione incidenti di sicurezza, ripristino dei sistemi in caso di attacchi/guasti, ecc.
Certificazione delle chiavi pubbliche	Gestione delle chiavi crittografiche e dei certificati digitali

Tabella 4. Servizi integrati

5. SERVIZI DI SICUREZZA DI SUPPORTO

5.1. Servizi di certificazione

L'implementazione delle regole per le funzionalità di autenticazione tra PD, integrità, riservatezza e non-ripudio dei messaggi SPCoop scambiati, identificazione, autenticazione ed autorizzazione dei soggetti e/o dei servizi richiedenti e/o eroganti, richiede l'uso di certificati digitali con formato diffuso (ad esempio conformi allo standard X509 v3), ed emessi per le varie tipologie di utilizzo previste. I Servizi di certificazione sono costituiti sostanzialmente dall'emissione dei certificati, dalla registrazione dei dati, l'emissione di CRL, la messa a disposizione delle informazioni su server OCSP, ecc. Per poter essere erogati nel quadro giuridico e funzionale del SPCoop, i servizi devono essere effettuati esclusivamente da Infrastrutture a Chiave Pubblica (ICP) competenti ed autorizzate.

Ad esempio i certificati per l'autenticazione contenuti nelle CNS e nelle CIE sono rilasciati da ICP costituite ed operanti secondo la normativa vigente.

Considerati i vantaggi derivanti da economie di scala e le necessità di fornire le facility per le Amministrazioni nella fase di avvio del progetto SPCoop, i servizi di certificazione possono convenientemente essere erogati da una infrastruttura a chiave pubblica (ICP) costituita a tale scopo, alla quale affidare compiti esclusivi (ad esempio la funzione di BRIDGE-CA). Tale ICP viene denominata PKI SPC e prevede supporto sia per SPCoop che per SPConn.

La gestione operativa dell'attività di certificazione segue un flusso procedurale predefinito e noto comunemente come "ciclo di vita del certificato" del quale sono riportate le fasi principali:

Fase	Attività
Fase 1. Accreditamento dei soggetti referenti	I responsabili dei sistemi informativi automatizzati individuano e trasmettono le generalità dei Responsabili delle PD e loro delegati autorizzati alla trasmissione delle richieste per la generazione dei certificati e le altre operazioni di gestione. Tali soggetti autorizzati sono denominati referenti
Fase 2. Trasmissione delle richieste	I referenti inoltrano le richieste secondo le procedure previste dalla PKI SPC e che dipendono dalla tipologia di certificato emesso
Fase 3. Registrazione dei dati	Sono acquisiti i dati necessari per le operazioni di emissione dei certificati
Fase 4. Verifica delle informazioni.	Le informazioni contenute nei dati acquisiti sono verificate secondo le procedure prefissate. In caso di riscontro di anomalie si riparte dalla fase n. 2
Fase 5. Generazione delle coppie di chiavi e memorizzazione	Il superamento della fase di verifica è la condizione per la generazione delle coppie di chiavi e la successiva memorizzazione nei dispositivi personalizzati

Fase	Attività
Fase 6. Emissione dei certificati secondo gli scopi previsti	Sono generati i certificati digitali, contenenti le chiavi pubbliche e le informazioni verificate
Fase 7. Pubblicazione dei certificati	I certificati digitali sono resi pubblici mediante memorizzazione su server pubblico e notifica al richiedente
Fase 8. Gestione (Sospensione/Revoca/Rinnovo) dei certificati	Eventi temporali successivi alla generazione possono comportare operazioni successive sui certificati quali la sospensione e la revoca, se motivate durante il periodo di validità del certificato, ed il rinnovo in prossimità della sua scadenza naturale

5.1.1. Servizi di registrazione

Questo servizio deve permettere di registrare i dati forniti dagli utilizzatori ai fini del servizio di gestione delle chiavi e dei certificati. E' opportuno l'utilizzo di una architettura tecnologica che consenta, tramite un canale sicuro, la registrazione remota dei dati degli utenti.

La registrazione dei dati deve poter avvenire anche attraverso una architettura tecnologica che consenta, tramite un canale sicuro, la ricezione remota delle richieste di certificazione delle chiavi (PKCS#10) in particolare, ma non solo, per le richieste relative ai componenti per le VPN (ad es., router di accesso).

5.1.2. Servizi di gestione delle chiavi e dei certificati

La gestione dei certificati deve prevedere tutti gli aspetti tecnici ed amministrativi inerenti l'utilizzo da parte dei sottoscrittori autorizzati ed operanti nell'ambito di SPCoop. Tale servizio deve prevedere anche le liste dei Certificati di Revoca note come CRL (Certificate Revocation List), le liste dei Certificati di Sospensione e i certificati di mutuo riconoscimento tra autorità di certificazione di infrastrutture diverse, noti come Cross Certificate, inoltre deve includere la disponibilità di un "OCSP responder" ai fini della verifica della validità dei certificati in tempo reale, per le ipologie di certificati per i quali è prevista tale modalità.

Nell'ambito della gestione dei certificati le funzionalità richieste sono:

- Emissione di nuovi certificati. Tale emissione deve avvenire in base alle informazioni di registrazione fornite alla PKI SPC. I certificati dovranno contenere le informazioni previste dalla legislazione vigente. Le informazioni contenute nel certificato dovranno essere strutturate in modalità tale da essere aderenti a quanto previsto dai documenti pubblicati dal CNIPA;
- Rinnovo dei certificati. I certificati non di chiavi di certificazione dovranno avere una validità da uno a tre anni. Alla scadenza il certificato dovrà essere rinnovato in base alle indicazioni fornite all'atto dell'emissione;
- Revoche dei certificati. Chi è autorizzato secondo i CPS (Certificate Pratice Statement) o direttamente la PKI-SPC o l'ICP che ha emesso il certificato può chiedere la revoca di un certificato secondo le procedure approvate. A fronte di tale evento, il certificato è inserito nelle liste di revoca, ed è assegnata una marca temporale all'evento. Poiché, almeno nel caso di

certificati per la firma digitale, dopo che un certificato è stato inserito su una lista di revoca, tutti i documenti firmati o cifrati con la chiave privata legata alla chiave pubblica contenuta nel certificato, successivamente alla data di revoca, perdono ogni validità, .è necessario che l'infrastruttura preveda la gestione delle CRL attraverso un directory server e un meccanismo sicuro per la convalida in tempo reale dei certificati;

- Sospensione dei certificati. Chi è autorizzato secondo i CPS (Certificate Pratice Statement) o direttamente la PKI-SPC o l'ICP che ha emesso il certificato può chiedere la sospensione di un certificato secondo le procedure approvate. A fronte di tale evento il certificatore provvede ad inserire lo stesso nelle liste di sospensione da lui gestite, e ad assegnare una marca temporale all'evento. Poiché, almeno nel caso di certificati per la firma digitale, dopo che un certificato è stato inserito su una lista di sospensione, tutti i documenti firmati o cifrati con la chiave privata legata alla chiave pubblica contenuta nel certificato, nel periodo di sospensione, perdono ogni validità, .è necessario che l'infrastruttura preveda la gestione delle CSL attraverso un directory server e un meccanismo sicuro per la convalida in tempo reale dei certificati. Contrariamente ad un certificato revocato, un certificato sospeso potrà, in un momento successivo, essere riattivato.
- Liste dei certificati revocati e sospesi. Tutti i certificati emessi, le liste di revoca (CRL) e le liste di sospensione (CSL) devono essere disponibili e consultabili in modo continuativo attraverso il protocollo LDAP oppure attraverso il protocollo HTTP o HTTPS presso un sito appositamente dedicato. Generazioni o modifiche non autorizzate di tali archivi devono essere prevenute. Le CRL e le CSL devono essere disponibili agli utenti per mantenere le informazioni a loro disposizione aggiornate.;
- Verifica in tempo reale dei certificati. Per i certificati digitali ai quali si applica, devono essere rese disponibili le informazioni sulla revoca e sospensione dei certificati anche attraverso servizi OCSP, in conformità alla specifica RFC 2560 e successive modificazioni ed in conformità alla normativa vigente, compresa quella sulle CNS e CIE. In tal caso il server che fornisce le informazioni di validità dei certificati deve essere accessibile con operatività H24, per tutti i giorni dell'anno e si deve prevedere la ridondanza di server che forniscono le informazioni (sempre riferiti al medesimo URI) per garantire la continuità del servizio;
- Archivio dei certificati scaduti. E' necessaria la gestione di un archivio permanente di certificati. Tutti i certificati emessi dalla CA, le CRL e le CSL devono essere gestiti per almeno 10 anni;
- Certificazioni incrociate. I cross certificate sono il meccanismo di mutuo riconoscimento tra i certificatori diversi. Devono quindi poter essere emessi i certificati per le coppie di Cross Certificate., indipendentemente dai fornitori di infrastrutture di certificazione;
- Logging ed auditing. Un servizio di logging ed auditing che sia in grado di registrare su dispositivo WORM gli eventi relativi a:
  - anomalie che possono modificare il funzionamento degli apparati;
  - tentativi di manomissione;
  - tutte le richieste pervenute al servizio.

5.1.3. Servizi di marcatura temporale

L'obiettivo di questo servizio è quello di realizzare un meccanismo fidato che attesti in modo certo l'esistenza di un documento informatico ad una certa data ed a una certa ora. Tale

servizio deve generare a fronte di una richiesta esplicita da parte di un utente una marca temporale, cioè un messaggio firmato digitalmente dalla autorità di validazione temporale utilizzando una chiave privata dedicata esclusivamente alla sottoscrizione delle marche temporali.

Ad un marca temporale devono essere associate almeno le seguenti informazioni:

- l'impronta del messaggio per il quale è stata richiesta la marca temporale;
- l'identificativo dell'algoritmo utilizzato per ottenere l'impronta considerata nel punto precedente;
- la data e l'ora relative alla richiesta dell'utente alla autorità di validazione temporale;
- un numero seriale progressivo che individui univocamente la marca temporale;
- il nome della autorità di validazione temporale.

Il servizio deve inoltre inviare al richiedente, tramite posta elettronica ovvero tramite il protocollo HTTP, le marche richieste ovvero eventuali messaggi di errore.

Meccanismi di logging ed auditing associati al servizio di marca temporale devono garantire:

- la rilevazione e l'archiviazione su un dispositivo non alterabile in modo malevolo degli eventi relativi a malfunzionamenti degli apparati;
- tentativi di manomissione;
- operazioni di sincronizzazione con la fonte temporale di riferimento;
- la registrazione delle richieste pervenute;
- la registrazione delle marche generate dal servizio.

Infine dovrà essere disponibile un archivio di tutte le marche temporali emesse.

5.1.4. Servizio di Bridge CA

Il servizio di Certificazione svolto dalla PKI-SPC deve includere il servizio di Bridge CA, che consiste nella emissione, pubblicazione e gestione delle TCL (Trust Certificate List) contenenti l'elenco delle AC accreditate in ambito SPC. Tale servizio assicura l'interoperabilità tra le PKI autorizzate ad operare in ambito SPC, indipendentemente dalle tipologie di certificati emessi (in particolare, ma non solo, le PKI che emettono certificati IPSEC).

5.1.5. Profilo dei certificati emessi

Le tipologie dei certificati che sono emessi dalla PKI SPC sono elencate in un apposito documento che tratta dei certificati utilizzati in tutto l'ambito SPC, quindi compreso SPCoop. In particolare la PKI SPC emette certificati per le seguenti tipologie

(1) Certificato AC radice generato dal Comitato di gestione per PKI SPC,

- Utilizzato per sottoscrivere i certificati delle AC distribuite autorizzate ad operare in ambito SPC e la CRL relativa;

(2) Certificati di certificazione delle AC distribuite,
- Utilizzati per sottoscrivere i certificati per l'autenticazione delle PD, i certificati di firma XML, i certificati per la cifratura dei messaggi, e per i servizi di OCSP Responder erogati da parte delle AC distribuite;

(3) Certificati per la firma XML del messaggio SPCoop;
- Utilizzati per garantire l'autenticità e l'integrità dei messaggi SPCoop scambiati – sono complementari a quelli di sottoscrizione;

(4) Certificati di autenticazione dei sistemi/applicazioni in modalità client e server (PD),
- Utilizzati per supportare i protocolli SSL/ TLS 1.0;

(5) Certificati di autenticazione di persone fisiche (utenti e amministratori),
- Utilizzati per il riconoscimento degli utenti nei confronti dei sistemi di accesso – sono conformi ai certificati digitali inseriti nella Carta Nazionale dei Servizi e nella Carta d'Identità Elettronica;

(6) Certificati di firma digitale,
- Utilizzati per la sottoscrizione dei documenti secondo la normativa vigente;

(7) Certificati per il servizio di OCSP Responder,
- Utilizzati per la validazione con modalità "up-to-date" dei certificati digitali;

(8) Certificati di crittografia,
- Utilizzati per la cifratura di dati e/o documenti e/o messaggi scambiati in SPC.

6. SERVIZI DI SICUREZZA PER IL REGISTRO SICA GENERALE

6.1. Firewall XML

6.1.1. Descrizione e obiettivi del servizio

Il servizio consiste nella gestione di strumenti per il filtraggio del traffico di rete a livello applicativo secondo un insieme di regole definite, aggiornabili e verificabili. Il servizio deve consentire la possibilità di intervenire al livello 7 della pila ISO/OSI (oltre ai livelli più bassi) e porsi come obiettivo quello di consentire il transito di tutto e solo il traffico di dati non solo XML che rispetta regole determinate e, contestualmente, impedire tutto il traffico che non rispetta le regole prefissate, tenendone traccia ove ciò accada.. Le regole devono tenere conto delle esigenze di funzionalità e sicurezza descritte nei documenti PORTA DI DOMINIO e SPECIFICHE DELLA BUSTA DI E-GOVERNMENT.

Il servizio deve includere almeno a livello di funzionalità base quelle del "Network Firewall", ossia tecniche per l'analisi dei pacchetti di rete utilizzando le tecniche di "screening router" e "packet filtering", al fine di impedire lo spoofing degli indirizzi IP di origine e destinazione, di selezionare i protocolli di rete ammessi (TCP, UDP, ecc.) provenienti da determinati host/sottoreti/domini ed indirizzati a determinati host/sottoreti/domini, di selezionare le porte di rete associate al servizio (SMTP, TELNET, HTTP, HTTPS, ecc.), di analizzare il flusso della connessione ("stateful inspection") e più in generale l'"auditing" ed il "logging" del traffico. Il servizio deve essere erogato tramite elaboratori dedicati.

Tra i requisiti prestazionali del sistema FIREWALL XML devono essere previsti almeno i seguenti:

- Processore specializzato alle operazioni XSLT/XML, con rallentamento percentuale del flusso da/per gli elaboratori di max 1% e media 0,3%;
- Processore in grado di operare operazioni crittografiche derivanti da XML-Encryption, XML Signature, SSL/TLS (acceleratore SSL) ecc., con rallentamento percentuale del flusso da/per gli elaboratori di max 2% e media 0,5%;
- Gestione flusso di 10/100/1000 Gb/sec.;

Tra i requisiti funzionali del sistema FIREWALL XML devono essere previsti almeno i seguenti:

- Gestione buste SPCoop attraverso la conformità ai principali standard (XML-Schema, SOAP, Xpath, XSLT etc.);
- Funzionalità di Content Inspection;
- Funzionalità di Controllo sulla sintassi delle buste SPCoop;
- Funzionalità di controllo sui parametri della busta SPCoop (dimensioni, concatenamento etc.);

- Funzionalità di Gestione del protocollo SSL/TLS;
- Funzionalità di gestione dei certificati digitali secondo gli standard crittografici diffusi (X509v3, PKCS#7, PEM, DER, CRL, OCSP etc.);
- Compatibilità con gli standard OASIS (SAML, XML-Signature, XML-Encryption, Web Services Security etc.): deve essere possibile aggiungere/verificare firme e cifrare/decifrare i messaggi SPCoop o loro parti, allegati compresi (possibilità di definire le strutture XML e le relative regole di parsing);
- Compatibilità con sistemi per la gestione delle utenze (ad esempio RADIUS e LDAP);
- Interfaccia grafica, integrazione con i principali strumenti di creazione XML;
- Protezione da XDOS (XML Denial of Services);

Tra i requisiti del sistema FIREWALL XML attinenti ai livelli della pila ISO/OSI dal 2 al 7 devono essere previsti i seguenti (tipicamente di Network Firewall):

- Funzionalità di Network Address Translation (NAT);
- Funzionalità di Port Address Translation (PAT) ;
- Funzionalità di PROXY per i messaggi provenienti dall'interno dell'Amministrazione;
- Funzionalità di REVERSE PROXY per i messaggi provenienti dall'esterno dell'Amministrazione;
- Filtraggio basato su IP, con possibilità di abilitare sulla base degli indirizzi autorizzati, e altri criteri di content-filtering basati su orari di accesso, ecc.;
- Bloccaggio di URL inserite nei puntamenti ai servizi applicativi;
- Filtraggio in base al servizio;
- Filtraggio delle porte e dei protocolli;
- Funzionalità di Proxy per la gestione degli accessi (autenticazione ed autorizzazione) per disciplinare l'utilizzo di alcuni servizi (ad esempio FTP, TELNER, HTTP, HTTPS);
- Certificazione di sicurezza dei dispositivi utilizzati.

La fornitura del servizio è condizionata da vincoli di tipo tecnico e organizzativo, derivanti in particolare dalla particolare architettura di rete dell'amministrazione e dai sistemi e dai servizi utilizzati.

6.1.2. Modalità di erogazione del servizio

Il servizio si implementa attraverso elaboratori dedicati, che devono essere interposti tra i percorsi di rete diretti da e verso il SICA, e vengono monitorati in tempo reale presso apposite console di security management.

La fornitura del servizio, con operatività H24, prevede il riporto degli allarmi e delle reazioni, con gestione remota.

La fase di start-up deve essere svolta secondo una pianificazione concordata che preveda almeno i seguenti passi:

- Analisi dell'architettura dei sistemi componenti il Registro SICA Generale;
- Predisposizione di documenti che descrivono la soluzione per la gestione dei Firewall XML;
- Istallazione, testing e tuning del sistema di Firewall XML;

L' attività di gestione prevede:

- Gestione delle security console, elementi centralizzati di gestione delle security appliance e degli elaboratori individuati (se più di uno), utilizzate sia per l'aggiornamento delle security policies tramite un'interfaccia grafica, sia per la raccolta delle violazioni delle politiche di sicurezza, per la produzione dei report richiesti e per l'evidenziazione all'operatore degli allarmi.
- Attività di manutenzione evolutiva e correttiva;

Deve valere il principio che ogni violazione delle regole sia acquisita con la memorizzazione dei dati relativi all'evento (indirizzi IP di origine e di destinazione, riferimento temporale, protocollo, contenuti dei singoli pacchetti e sequenza concatenata ecc) e deve essere definita la reazione allo specifico allarme generato (messaggio di posta, segnalazione sonora, fino al blocco automatico delle connessioni/sistemi).

6.1.3. Reporting

La rendicontazione del servizio deve includere la stesura di rapporti sulle attività svolte, contenenti le statistiche sugli allarmi generati, i tentativi di denial of service, le reazioni attivate, le politiche di sicurezza aggiornate ecc. I report periodici sono forniti in formato cartaceo o in formato elettronico dal fornitore e contengono almeno le seguenti informazioni:

- statistiche sulle prestazioni del servizio e sui i filtraggi effettuati;
- regole di filtraggio implementate;
- regole di NAT/PAT implementate;
- log sui tentativi di infrazione della politica di sicurezza implementata;
- log sugli accessi avvenuti con successo o falliti e controllati da schemi di autenticazione abilitati sui dispositivi di firewalling;

Tutta la reportistica relativa al servizio dovrà essere archiviata e conservata a cura del fornitore. Considerando la criticità delle informazioni deve essere previsto e stipulato sia un'accordo di riservatezza, sia un sistema di gestione della documentazione riservata. Il fornitore dovrà gestire ordinatamente tutte le informazioni in modo da consentirne l'acquisizione, a richiesta e con preavviso non superiore ad un tempo predefinito, a favore dell'Autorità Giudiziaria. A tal fine il fornitore dovrà individuare e implementare, di concerto con l'amministrazione, adeguati strumenti di *information retrieval*.

6.2. Intrusion detection

6.2.1. Descrizione e obiettivi del servizio

Il servizio è mirato nella gestione del rilevamento dei tentativi di intrusione condotti con sistemi manuali/automatici indipendentemente dalla loro collocazione e diretti verso i componenti del Registro SICA Generale, allo scopo di ottenere l'accesso parziale/totale e/o di acquisire il controllo. Il servizio include le verifiche dell'integrità dei sistemi, ossia deve essere attiva la protezione dei sistemi in modo tale che nessun tentativo di intrusione possa comportare l'acquisizione, in modalità silente, di privilegi di controllo indebiti sui sistemi (forensic analysis).

La finestra di erogazione del servizio è H24.

Il servizio di intrusion detection si implementa nella sola modalità HIDS (host intrusion detection system), in quanto le altre due modalità (NIDS (network intrusion detection sysyem), per le reti "wired" e WIDS (wireless intrusion detection system), per le reti "wireless") riguardano esclusivamente le reti e non le applicazioni. E' però conveniente utilizzare il servizio NIDS per le eventuali componenti fisiche che lavorano a livello dei protocolli di rete , come ad esempio i Firewall XML ed i Proxy a cui i sistemi del Registro sono connessi.

Il servizio NIDS prevede l'uso di sonde "invisibili" istallate sui sistemi e/o collocate lungo i segmenti di rete, monitorate ed aggiornate dalle console di security management e operanti in modo da:

- acquisire informazioni sugli eventi di attacco (pattern);
- effettuare un'analisi predeterminata degli eventi rilevati;
- generare alert specifici a fronte della identificazione di un evento di attacco;
- attivare reazioni automatiche a fronte della identificazione di un evento di attacco.

I sistemi di IDS devono individuare almeno le seguenti tipologie di eventi:

- accessi non autorizzati (Password guessing);
- tentativi di intercettazione (hijacking, man-in-the-middle);
- spoofing degli indirizzi;
- port and Services scanning;
- eventi DOS (Denial of Service);
- ping Flooding, Smurf, SYN flood, IP Source routing;
- tentativi di utilizzare i Buffer Overflow

I sistemi di IDS devono consentire la configurazione di specifici profili di protezione, riferibili sia a tutte le tipologie di elaboratori, sia tipici degli applicativi usati (gestione database, gestione Web Service, ecc.), come combinazione di almeno i seguenti:

- rilevazione periodica della modifica di file di configurazione del sistema operativo, elenco utenti del sistema e privilegi loro concessi;
- rilevazione e blocco dei tentativi di esecuzione di processi con permessi differenti da quelli dell'utente originale;

- controllo di esecuzione dei processi del sistema usando tecniche quali "sandboxing", sul modello di quanto avviene per l'esecuzione di codice java sui browser;
- rilevazione periodica della modifica dei file di configurazione del database; elenco utenti del database e privilegi loro concessi;
- rilevazione periodica dell'integrità di file di configurazione dei servizi web, script ed eseguibili esposti nella radice di file system contente il codice software del servizio applicativo, elenco degli utenti del sistema e privilegi loro concessi;
- controllo delle richieste HTTP malformate (es. contenenti codice di exploit di vulnerabilità di tipo buffer overflow);
- controllo del contenuto delle transazioni client-server verso le applicazioni ospitate dal server Web, per eliminare valori non accettabili, cookie riutilizzati illecitamente, ecc.

La fornitura del servizio deve essere effettuata con gestione remotizzata.

6.2.2. *Modalità di erogazione del servizio*

La fase di start-up deve essere svolta secondo una pianificazione concordata che preveda almeno i seguenti passi:

- Analisi dell'architettura del sistema;
- Predisposizione di documenti che descrivono la posizione, il tipo ed il numero di sonde e console di management da collocare;
- Scelta delle configurazioni;
- Istallazione, testing e tuning del sistema di IDS;

L' attività di IDS (monitoraggio dei sistemi ai fini del rilevamento delle intrusioni) è effettuata tramite:

- predisposizione ed aggiornamento dei documenti di analisi del rischio, di concerto con l'amministrazione;
- istallazione e configurazione iniziale di sensori distribuiti (sonde), collocati sui segmenti di rete da controllare "wired", per la parte NIDS;
- istallazione e configurazione iniziale di moduli software specifici sugli host (server) da porre sotto controllo, per la parte HIDS;
- aggiornamento delle configurazioni in modo da assicurare i profili di protezione previsti in funzione degli elaboratori utilizzati;
- gestione degli elementi centralizzati per la raccolta degli allarmi (console di reporting e management), dai quali è possibile anche effettuare la configurazione remota dei sensori tramite un'interfaccia grafica che evidenzia all'operatore l'insorgere di situazioni anomale ed i dati necessari all'individuazione del problema. Le console di management sono aggiornabili in modalità sicura per quanto concerne il "pattern" degli attacchi noti.

- gestione delle rilevazioni degli attacchi passivi (penetrazione nelle risorse senza compromettere i sistemi) e degli attacchi attivi (accesso alle risorse per ottenerne il controllo) indipendentemente da dove sono originati.

Per ogni tentativo di intrusione è prevista l'acquisizione e memorizzazione degli indirizzi IP di origine e di destinazione dell'elaboratore origine dell'intrusione e vittima dell'intrusione, la "segnatura" dell'intrusione, riferimento temporale, protocollo, contenuti dei singoli pacchetti e sequenza concatenata ecc) e deve essere definita la reazione (messaggio di posta, segnalazione sonora, fino al blocco automatico delle connessioni/sistemi).

Il servizio deve prevedere l'aggiornamento dell'architettura dell'IDS per ogni modifica rilevante dell'architettura di rete dei sistemi informatici e/o per ogni nuovo host da porre sotto controllo.

6.2.3. *Reporting*

La rendicontazione del servizio deve includere la stesura di rapporti sulle attività svolte, contenenti

- stato corrente del database delle "segnature" presenti sulle sonde;
- elenco ed esito degli aggiornamenti del database delle "segnature";
- stato delle regole di configurazione dei sistemi IDS;
- attacchi individuati;
- trend degli attacchi individuati;
- numero dei falsi negativi e dei falsi positivi;

Tutta la reportistica relativa al servizio dovrà essere archiviata e conservata a cura del fornitore. Considerando la criticità delle informazioni deve essere previsto e stipulato sia un'accordo di riservatezza, sia un sistema di gestione della documentazione riservata.

6.3. Registrazione degli eventi

6.3.1. *Descrizione e obiettivi del servizio*

Il servizio prevede la raccolta, la verifica, la correlazione, l'analisi e la storicizzazione delle tracce applicative, comprese quelle riguardanti gli allarmi (error log) generati e delle informazioni raccolte nei file di log dalle piattaforme caratterizzanti i diversi sistemi.

Riuscendo a correlare tra loro eventi ed informazioni provenienti da sistemi/architetture differenti, il servizio di Registrazione degli Eventi permette di realizzare un cruscotto attraverso il quale monitorare il livello di sicurezza raggiunto all'interno dell'organizzazione del cliente e prevenire e/o contrastare attacchi provenienti dall'esterno.

Gli obiettivi del servizio sono quelli di fornire uno strumento utile per:

- implementare i controlli imposti per rispettare il livello minimo di sicurezza di SPCoop;
- misurare il livello di sicurezza raggiunto sul proprio Sistema Informativo;
- effettuare tutte le attività di investigazione sui sistemi in rete necessarie alla gestione degli incidenti informatici.

6.3.2. *Modalità di erogazione del servizio*

Il servizio viene erogato per il tramite di una serie di strumenti hardware/software installati presso l'ambiente operativo del cliente e che possono essere gestiti remotamente o on-site.

Il reperimento dei file di log ed il collezionamento degli allarmi provenienti da sistemi/architetture impiegate nel sistema di sicurezza del cliente dipende dall'accessibilità delle informazioni prodotte dai dispositivi sotto il dominio amministrativo di fornitori terzi del cliente.

Al riguardo, quando necessario e richiesto dal cliente ed in tutti i casi in cui non sia possibile accedere alle informazioni di log e allarmi di dispositivi del sistema di sicurezza sotto il dominio amministrativo di fornitori terzi del cliente, potranno essere installati ulteriori strumenti (ad es. firewall, sonde, application proxy) per mezzo dei quali sarà possibile recuperare le informazioni e l'allarmistica utilizzati nell'ambito di erogazione del servizio.

La raccolta e la presentazione unificata di eventi/allarmi e log sarà limitata a solo quelli reperibili da strumenti hardware/software installati presso l'ambiente operativo del cliente che siano integrabili con la piattaforma impiegata dal fornitore per l'erogazione del servizio.

6.3.3. *Reporting*

Il servizio include le seguenti modalità di reportistica:

- near real time report;
- report periodici.

Il report near real time è basato sull'analisi on-line del sistema, è accessibile attraverso una interfaccia remota comunicante con il sistema attraverso un canale sicuro ed offre informazioni circa la configurazione, lo stato, le prestazioni della piattaforma e i log e gli allarmi da essa raccolti ed elaborabili.

Tutta la reportistica relativa al servizio dovrà essere archiviata e conservata a cura del fornitore. Considerando la criticità delle informazioni deve essere previsto e stipulato sia un'accordo di riservatezza, sia un sistema di gestione della documentazione riservata.

6.4.Gestione delle emergenze

6.4.1. Descrizione e obiettivi del servizio

Tale servizio consiste nella gestione di tutti i possibili incidenti di sicurezza che causano rallentamenti e difficoltà per la normale operatività, provvedendo alla identificazione del problema ed alla rimozione della causa nel minore tempo possibile. Il servizio è articolato in modo da consentire la scelta della proposta più adatta, garantendo flessibilità di utilizzo, a partire dalla semplice consulenza per la predisposizione dei piani operativi di sicurezza sino alla implementazione di piani di business continuity.

E' prevista la fornitura di personale che opera con pronto intervento locale, laddove non sia possibile risolvere il problema in remoto, ed un'attività volta alla prevenzione del verificarsi delle emergenze stesse, anche elevando la consapevolezza dei rischi ed invitando all'uso delle best practice internazionali, prevedendo a richiesta corsi di addestramento e corsi di aggiornamento periodici e bollettini informativi specifici. E' anche possibile richiedere l'attività di analisi del rischio e la predisposizione del piano operativo per la sicurezza, nel quale riportare le procedure organizzative di sicurezza e la gestione di sistemi che assicurano business continuity.

La fornitura del servizio, normalmente con operatività H24, viene effettuata a richiesta sia telefonica che per via telematica (posta elettronica) e viene subito verificato se il problema può essere risolto in remoto o se occorre il pronto intervento.

6.4.2. Modalità di erogazione del servizio

L' erogazione del servizio include quanto segue:

- dare supporto in fase iniziale per la verifica delle tecniche di difesa implementate e per la prevenzione dagli incidenti di sicurezza (sistemi ridondati, metodologie per il backup, ecc);
- raccogliere le notifiche degli incidenti di sicurezza;
- verificare il livello di criticità degli incidenti di sicurezza;
- coordinare la risposta agli incidenti e il successivo processo di ripristino;
- mantenere aggiornato un archivio relativo agli incidenti e alle contromisure intraprese;
- collaborare al processo formativo sulla sicurezza e sulla consapevolezza dei rischi tramite corsi ed incontri periodici con gli utenti dell'amministrazione.

La fase di start-up deve essere svolta secondo una pianificazione concordata che preveda almeno i seguenti passi:

- analisi dei sistemi;
- selezione degli incidenti di sicurezza da gestire (ad es., "malfunzionamento hard-disk", ecc.)
- predisposizione di documenti che descrivono modalità e tempi di ripristino.

Per ogni comunicazione inerente un possibile incidente di sicurezza deve essere attivato un "trouble-ticket" con l'acquisizione dei dati necessari (data e ora della prima rilevazione dell'evento, descrizione dell'evento, tipologia dell'evento, criticità, modalità di contenimento, modalità di rimozione dell'incidente di sicurezza, modalità di ripristino, registrazione di

avvenuta risoluzione ecc.) nonché il riporto di tale informazione in un archivio specifico e la pubblicazione periodica di report statistici.

Il servizio deve prevedere, oltre alla soluzione del problema, anche indicazioni per evitare il ripetersi dello stesso, anche attraverso l'aggiornamento dell'architettura dei sistemi con valutazione di costi-benefici.

6.4.3. Reporting

La rendicontazione del servizio deve prevedere almeno quanto segue:

- stesura di rapporti periodici sulle attività svolte;
- tabelle statistiche sugli incidenti raccolti, con correlazione degli eventi;
- azioni effettuate per la risoluzione dei problemi, con indicazione del tempo entro il quale si è giunti alla risoluzione degli inconvenienti;
- raccomandazioni prodotte in relazione agli episodi occorsi.

Tutta la reportistica relativa al servizio dovrà essere archiviata e conservata a cura del fornitore. Considerando la criticità delle informazioni deve essere previsto e stipulato sia un'accordo di riservatezza, sia un sistema di gestione della documentazione riservata.

6.5. Security assessment

6.5.1. Descrizione e obiettivi del servizio

Il servizio fa parte dell'attività di auditing e mira ad analizzare l'esposizione al rischio di attacchi informatici del Registro SICA Generale. Il servizio viene eseguito mediante l'effettuazione di una serie di test condotti sia con l'ausilio di strumenti automatici che utilizzando i comandi propri del sistema operativo di base dei dispositivi oggetto di valutazione. I test automatici prevedono:

- la scansione dei sistemi fisici, alla ricerca di configurazioni del software di base e applicativo ritenute non sicure e vulnerabili ad attacchi (vulnerability assessment);
- mediante test di penetrazione che consentono di valutare la resistenza della rete, dei sistemi e delle postazioni di lavoro a determinati attacchi informatici simulati (penetration testing).

L'esecuzione dei comandi propri del sistema operativo di base dei dispositivi oggetto di valutazione consentono di raffinare e perfezionare la valutazione, dettagliando meglio l'analisi delle configurazioni ritenute deboli.

Il servizio include la conduzione di valutazioni sugli aspetti documentali, organizzativi e procedurali concernenti le misure di sicurezza adottate, applicando metodologie riferibili a standard internazionali e best practies diffusi quali, ma non solo, le norme BS 7799/ISO17799.

L'obiettivo del servizio è quello di fornire un documento di assessment delle vulnerabilità accertate, indicante anche le possibili contromisure, che possa consentire al cliente di verificare l'adeguatezza della politica di sicurezza implementata all'interno del proprio Dominio di responsabilità e di adottare eventuali adeguamenti.

6.5.2. *Modalità di erogazione del servizio*

Il servizio di security assessment opera secondo le modalità riportate nella tabella seguente:

Modalità	Descrizione
Periodica	Le attività si svolgono secondo un piano generale pluriennale prefissato, sia per agire in termini proattivi e preventivi rispetto alle minacce informatiche, sia per tenere conto delle continue scoperte di vulnerabilità sui sistemi.
A richiesta	Le attività si svolgono con breve preavviso, qualora ne ricorrano le condizioni, ad esempio quando si presenti la necessità di aggiornare i sistemi informatici con nuove applicazioni e/o attraverso modifiche rilevanti di configurazioni e/o con l'introduzione di nuovi elementi.

Tabella 5. Modalità di erogazione del Security Assessment

Nella implementazione del servizio il fornitore dovrà adottare tutte le precauzioni volte a limitare l'ambito di test e scansioni ai soli sistemi indicati dal cliente e sotto il proprio Dominio amministrativo, scongiurando ogni possibile attività di disturbo o di allarme verso sistemi interni non oggetto della valutazione o Sistemi Informativi di soggetti terzi.

La fornitura del servizio richiede la manleva per gli esecutori da possibili interruzioni del servizio, che comportino eventualmente l'applicazione di penali contrattuali. Lo svolgimento dell'attività di security assessment avviene secondo una pianificazione preventivamente concordata, che tiene conto di eventuali attività passate e focalizza l'attenzione su elementi nuovi:

- Predisposizione di documenti che descrivono l'insieme dei sistemi da sottoporre a verifica;
- Esame della documentazione di sicurezza, incluse le procedure organizzative adottate, i registri degli utenti autorizzati, ecc;
- Scelta dei punti di accesso alla rete per i penetration test;
- Scelta dei tool automatici che effettuano le suddette operazioni;
- Scelta dei comandi da digitare direttamente sui sistemi operativi per le verifiche non automatizzabili (c.d. ethical hacking);
- Scansione dei dispositivi di rete, dei sistemi server e delle postazioni di lavoro alla ricerca di configurazioni del software di base e applicativo ritenute non sicure e vulnerabili ad attacchi (scansione ai fini dell'information retrieval);

- Penetration testing, per valutare la resistenza della rete, dei sistemi e delle postazioni di lavoro a determinati attacchi informatici simulati;
- Vulnerability assessment, per verificare la presenza di punti deboli noti del sistema, con indicazione della gravità e di come porvi rimedio;
- Produzione dei Report finali;
- Esame dei report e valutazioni sulle contromisure da adottare;
- Produzione dei piani di rientro dalle non-conformità rilevate.

L'attività si svolge per mezzo di una o più giornate durante le quali un team di esperti di sicurezza informatica eseguirà scansioni e test che potranno essere condotti dall'interno e dall'esterno della intranet del cliente. I dispositivi software e hardware utilizzati per l'erogazione del servizio potranno essere di proprietà o di uso esclusivo del fornitore o messi a disposizione dall'Amministrazione. Sulla base delle particolari esigenze dell'Amministrazione i test potranno essere condotti anche in giorni prefestivi o festivi o fuori il normale orario di lavoro.

Il servizio deve prevedere sia l'uso di tool automatici adeguatamente aggiornati in accordo con l'amministrazione, sia tecniche di ethical hacking laddove utilizzabili.

6.5.3. *Reporting*

La rendicontazione del servizio deve includere la stesura di rapporti sulle attività svolte, contenenti indicazioni sui problemi riscontrati e deve dare indicazioni per il superamento degli stessi. Tutta la reportistica relativa al servizio dovrà essere archiviata e conservata a cura del fornitore. Considerando la criticità delle informazioni deve essere previsto e stipulato sia un'accordo di riservatezza, sia un sistema di gestione della documentazione riservata.

I dati contenuti nel documento di assessment delle vulnerabilità accertate consegnato all'utente, dovranno essere sfrondati di tutte le informazioni critiche che i tool automatici riportano nei report (esempio piano di indirizzamento IP). Tutte le vulnerabilità sono catalogate secondo un metodo di valutazione quantitativo e qualitativo che permette una precisa categorizzazione dei risultati e delle contromisure suggerite.

7. SERVIZI DI SICUREZZA PER LE PORTE DI DOMINIO

7.1. Qualificazione

L'architettura SPCoop prevede che le Amministrazioni interagiscono mediante messaggi applicativi che transitano per le Porte di Dominio (PD). Tali PD sono chiamate a svolgere in sostanza una funzione cosiddetta "gateway" tra i sistemi informativi esistenti gestiti dalle amministrazioni nei confronti delle richieste. Preliminarmente alla fase di erogazione dei servizi, quindi dell'avvio in esercizio, è quindi necessario che le PD siano sottoposte a rigidi e schematici controlli, al fine di assicurare alle altre amministrazioni il soddisfacimento dei requisiti in termini funzionali, prestazionali e di sicurezza.

L'avvio in esercizio è quindi preceduto dal superamento di un insieme di test che sono svolti in due fasi: la prima è condotta direttamente dall'amministrazione, la seconda è svolta da personale qualificato e indipendente dalle amministrazioni che fornisce il servizio a livello di infrastruttura e riporta i risultati alla Commissione di Coordinamento per SPC ai fini dell'accreditamento della PD.

L'accreditamento è riferito alla PD, che sarà pertanto "qualificata" per operare in ambito SPCoop. Naturalmente, per le parti della PD costituite da istanze replicabili (ad esempio componenti software) la qualificazione viene estesa a tutte le istanze, salvo le verifiche sulle particolari specifiche di ogni PD.

Successivamente alla qualificazione della PD ed all'esercizio della stessa è previsto un ulteriore passo volto ad aumentare la fiducia nel sistema grazie al mantenimento nel tempo del livello di funzionalità delle PD, rappresentato come segue:

F1. Funzionalità di gestione della sicurezza a livello *connessione* (SSL/TLS);

F2. Funzionalità di tracciatura dei messaggi;

F3. Funzionalità di gestione dello smistamento (routing);

F4. Funzionalità di gestione della integrità dei messaggi;

F5. Funzionalità di gestione della riservatezza dei messaggi;

F6. Funzionalità di gestione del non–ripudio dei messaggi;

F7. Funzionalità di gestione degli allegati dei messaggi.

Il mantenimento della qualificazione è ottenuto mediante l'effettuazione di test periodici volti a verificare in particolare la resistenza degli elementi ad attacchi di sicurezza predefiniti (security assessment); il mancato superamento dei test comporta l'aggiornamento della PD ed una esclusione temporanea da SPCoop.

La qualificazione delle PD ha lo scopo di garantire che queste espongano i servizi applicativi mantenendo nel tempo i requisisti prefissasti di qualità e sicurezza pari al livello minimo standardizzato. Il processo di qualificazione convalida, sulla base di una dichiarazione di conformità effettuata da uno o più soggetti autorizzati dalla Commissione di Coordinamento

per SPC, l'adeguatezza di quella PD a soddisfare una serie di specifiche tecniche, funzionali e di sicurezza, al termine del processo di qualificazione se terminato con esito positivo. La qualificazione è valida solo per la specifica PD sottoposta con successo a qualificazione, nonché alle possibili repliche (nel caso le funzioni della PD siano implementate attraverso il software). L'ottenimento della qualificazione costituisce il requisito necessario per l'annuncio della PD in SPCoop.

La qualificazione non è in grado, da sola, di garantirne la corretta erogazione, infatti una cattiva amministrazione può compromettere in modo decisivo la sua efficacia, abbassando in modo inaccettabile il livello di sicurezza effettivo dell'intero sistema. È perciò necessario prevedere delle verifiche volte a confermare il mantenimento, nel tempo, delle condizioni di qualificazione. Inoltre, poiché aggiornamenti e modifiche delle modalità di erogazione possono anche comprometterne la rispondenza ai requisiti SPCoop, è prevista la sua riqualificazione a fronte di modifiche significative.

7.1.1. Il ciclo di vita della qualificazione

Stato	Descrizione
Non qualificata	La PD non è qualificata, non può operare in SPCoop
Qualificata	La PD ha superato con successo il processo di qualificazione e può esporre su SPCoop i servizi applicativi per i quali ha superato anche il processo di qualificazione dei servizi
Sospesa	La PD già qualificata non ha superato con successo il processo di verifica (security assessment) e non può operare temporaneamente in SPC
Dequalificata	La PD già qualificata non ha superato con successo il processo di verifica (security assessment) e non può operare definitivamente in SPCoop. Occorre predisporre una nuova PD, prima di potersi eventualmente sottoporre nuovamente al processo di qualificazione

Tabella 6. Stati della PD

Il diagramma di transizione riportato nella Figura 1 descrive il ciclo di vita della qualificazione della PD. In particolare i nodi di tale diagramma rappresentano vari stati nei quali una PD può trovarsi rispetto alla qualificazione. Gli archi sono invece associati ad eventi significativi che determinano la transizione da uno stato di qualificazione all'altro. Nelle Tabelle successive vengono descritti i possibili stati in cui una PD può trovarsi rispetto alla qualificazione e gli eventi associati a ciascun arco.

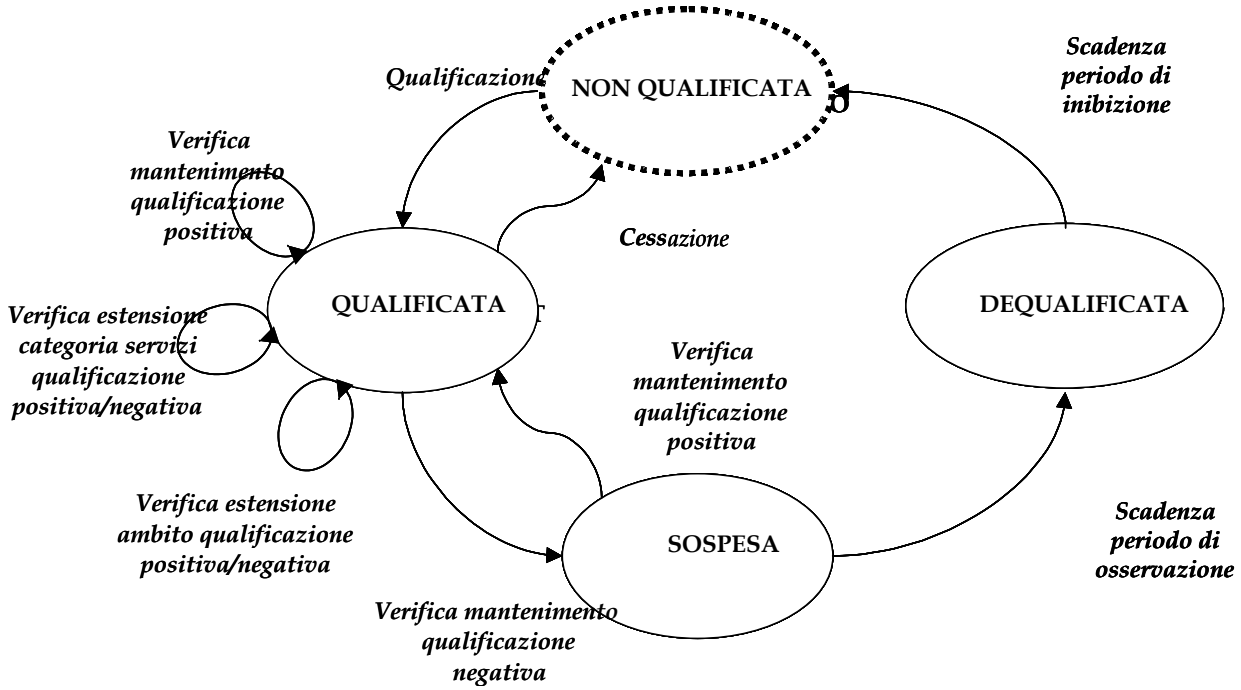

Figura 1. Digramma di transizione dello stato di qualificazione

Evento	Descrizione
Qualificazione	Superamento del processo di qualificazione
Verifica mantenimento qualificazione positiva	Superamento del processo di verifica (security assessment)
Verifica mantenimento qualificazione negativa	Mancato superamento del processo di verifica
Verifica estensione ambito qualificazione positiva/negativa	Esito del processo che accerta o meno il soddisfacimento delle condizioni per estendere ad altre PD con caratteristiche equivalenti la qualificazione già conseguita.
Verifica estensione categoria di servizi qualificazione positiva/negativa	Esito del processo che accerta o meno il soddisfacimento delle condizioni per estendere ad altre PD con caratteristiche equivalenti la qualificazione già conseguita per l'erogazione di un'altra categoria di servizi applicativi.
Scadenza periodo di osservazione	Conclusione del periodo di osservazione all'interno del quale la PD, la cui qualificazione è sospesa, può cercare, sottoponendosi ad una nuova valutazione, di riacquisire i requisiti di qualificazione
Scadenza periodo di inibizione	Conclusione del periodo obbligatorio di attesa prima che una PD a sia stata revocata la qualificazione possa richiedere di essere sottoposta nuovamente al processo di qualificazione

Evento	Descrizione
Cessazione	Scadenza del termine, preventivamente comunicato al Dominio di Cooperazione SPC, a partire dal quale la PD cessa di esporre i servizi applicativi

Tabella 7. Eventi che determinano un cambiamento di stato

Inizialmente qualsiasi PD si trova nello stato "***non qualificata***", evidenziato con il tratteggio del margine per indicare che si tratta dello stato iniziale del diagramma di transizione dello stato di qualificazione. Una PD già precedentemente qualificata torna in tale stato iniziale a seguito della dismissione volontaria ovvero al termine del "periodo di inibizione", scontato a seguito di una dequalifica (stato "***dequalificata***"). Normalmente ogni PD si trova nello stato "***qualificata***" e può erogare su SPCoop servizi con le caratteristiche specificate nell'elenco, che possono variare dinamicamente a seguito dell'accettazione di eventuali richieste di estensione ovvero della qualificazione di ulteriori servizi.

L'accertamento del mancato rispetto delle condizioni di qualificazione comporta l'applicazione, entro un periodo di osservazione, di azioni correttive adeguate, che, se non effettuate appropriatamente, portano alla revoca della qualificazione cui consegue un periodo di forzata esclusione dal SPC.

7.1.2. Processo di qualificazione

Il processo di qualificazione dei servizi viene condotto centralmente. Gli attori coinvolti nel processo sono:

- Amministrazione responsabile: ha l'onere di richiedere la qualificazione di ciascuna PD tramite la quale intende erogare servizi in ambito SPCoop, fornendo come condizione di ammissione al processo di qualificazione una dichiarazione di conformità e la documentazione necessaria a dimostrare il soddisfacimento dei requisiti relativi al servizio sottoposto a qualificazione;
- Commissione di qualificazione: ha la responsabilità di recepire la dichiarazione di conformità del servizio ricevuta dal fornitore, accreditando conseguentemente il servizio.

Tale commissione verifica la correttezza formale e la completezza della documentazione presentata dall'amministrazione, provvedendo alla qualificazione della PD.

La richiesta di qualificazione di una PD non già precedentemente qualificata deve contenere:

- la dichiarazione di conformità ai requisiti SPCoop;
- un documento, denominato "specifiche di realizzazione della PD", contenente:
  - la descrizione tecnica di come viene implementata e gestita la PD,
  - l'evidenza della conformità ai requisiti e alle specifiche tecniche, funzionali e di sicurezza SPCoop;
- un documento, denominato "specifiche di test", contenente la descrizione dei test da condurre nel corso del collaudo, da svolgere preliminarmente alla sua esposizione in SPCoop.

I documenti dovranno essere predisposti secondo le linee guida concordate in ambito SPCoop. Il processo di validazione, condotto da una apposita commissione, è inteso a verificare la coerenza tra la dichiarazione di conformità del servizio, prodotta dall'amministrazione, e il risultato dell'analisi delle specifiche di realizzazione della PD rispetto:

- al soddisfacimento delle specifiche tecniche, funzionali e di sicurezza SPC della PD;
- ai livelli di servizio minimi che devono essere garantiti.

Le specifiche funzionali e di sicurezza (checklist) sono approvate e aggiornate dalla Commissione di Coordinamento SPC, sulla base di una serie di profili di riferimento (protection profile) che saranno definiti a tale scopo.

7.1.3. Verifica e mantenimento delle condizioni di qualificazione

Durante l'esercizio del servizio di sicurezza qualificato sono previste attività di security assesment, volte a verificare il rispetto della qualificazione della PD, condotte presso le strutture dove si trovano i componenti fisici che erogano i servizi applicativi. Tale attività di auditing potrà essere condotta anche a seguito dell'accertamento, da parte della Pubblica Amministrazione che fruisce del servizio, di anomalie, del mancato rispetto dei livelli minimi garantiti sul servizio o a seguito di incidenti informatici che coinvolgano la Pubblica Amministrazione o altre Pubbliche Amministrazioni ad essa interconnesse per il tramite del SPCoop e causati dalla erogazione non adeguata del servizio. In caso di accertamento della perdita della qualificazione della PD, dovrà essere sospesa la qualificazione e la PD non potrà operare temporaneamente.

La sospensione, attribuita nel caso in cui le anomalie accertate non inficiano il livello minimo di sicurezza imposto su SPCoop, prevede che l'Amministrazione predisponga un Piano di rientro delle condizioni di qualificazione entro 5 gg dalla manifestazione dell'evento. Il Piano di rientro dovrà essere sottoposto a preventiva approvazione e, in caso di esito positivo, l'Amministrazione avrà a disposizione il tempo concordato per apportare tutti gli adeguamenti descritti nel Piano e volti a ristabilire le condizioni di qualificazione della PD. Al termine della scadenza temporale prefissata verrà svolta una nuova attività di auditing diretta ad accertare il ripristino delle conformità alle specifiche di qualificazione.

La revoca della qualificazione avverrà invece nei seguenti casi:

- le anomalie accertate durante l'audit inficiano il livello minimo di sicurezza imposto su SPCoop;
- il Piano di rientro non viene approvato;
- viene accertata la non conformità delle modifiche effettuate dall'Amministrazione sulla PD per l'attuazione del Piano di rientro.

Le Amministrazioni che avessero stipulato un contratto con un fornitore per la gestione in outsourcing della PD, nel caso in cui venisse revocata la qualificazione di una PD gestito dallo stesso, potranno rescindere il contratto, fermo restando l'obbligo per l' Amministrazione che ne ha la responsabilità di provvedere nel più breve tempo possibile alla stipula di contratti con altri fornitori qualificati al fine di ripristinare il servizio.

Nel caso in cui le attività di gestione della PD siano svolte direttamente dell'amministrazione, mediante proprio personale, dovrà essere operato il reincarico ad altro personale.

7.2. Firewall XML

7.2.1. Descrizione e obiettivi del servizio

Il servizio consiste nella gestione di strumenti per il filtraggio del traffico di rete a livello applicativo secondo un insieme di regole definite, aggiornabili e verificabili. Il servizio deve consentire la possibilità di intervenire al livello 7 della pila ISO/OSI (oltre ai livelli più bassi) e porsi come obiettivo quello di consentire il transito di tutto il traffico XML e non solo che rispetta regole determinate e, contestualmente, impedire nel modo più assoluto tutto il traffico che non rispetta le regole prefissate, tenendone traccia ove ciò accada. La scelta delle regole è sotto la responsabilità e la supervisione dell'amministrazione che deve ricevere, nel momento della definizione di ogni nuova regola da aggiungere, assistenza dal fornitore, formalizzata in un documento di sicurezza che analizzi e identifichi le minacce ed i possibili rischi derivanti dall'introduzione della nuova regola e le possibili soluzioni in termini di contromisure applicabili. Le regole devono tenere conto delle esigenze di funzionalità e sicurezza descritte nei documenti PORTA DI DOMINIO e SPECIFICHE DELLA BUSTA DI E-GOVERNMENT.

Il servizio deve includere il "Network Firewall" ossia tecniche per l'analisi dei pacchetti di rete utilizzando le tecniche di "screening router" e "packet filtering", al fine di impedire lo spoofing degli indirizzi IP di origine e destinazione, di selezionare i protocolli di rete ammessi (TCP, UDP, ecc.) provenienti da determinati host/sottoreti/domini ed indirizzati a determinati host/sottoreti/domini, di selezionare le porte di rete associate al servizio (SMTP, TELNET, HTTP, HTTPS, ecc.), di analizzare il flusso della connessione ("stateful inspection") e più in generale l'"auditing" ed il "logging" del traffico.

Il servizio deve essere erogato tramite elaboratori dedicati. Tra i requisiti prestazionali del sistema FIREWALL XML devono essere previsti almeno i seguenti:

- Processore specializzato alle operazioni XSLT/XML, con rallentamento percentuale del flusso da/per gli elaboratori di max 1% e media 0,3%;
- Processore in grado di operare operazioni crittografiche derivanti da XML-Encryption, XML Signature, SSL/TLS (acceleratore SSL) etc, con rallentamento percentuale del flusso da/per gli elaboratori di max 2% e media 0,5%;
- Gestione flusso di 10/100/1000 Gb/sec.;

Tra i requisiti funzionali del sistema FIREWALL XML devono essere previsti almeno i seguenti:

- Gestione buste SPCoop attraverso la conformità ai principali standard (XML-Schema, SOAP, Xpath, XSLT etc.);
- Funzionalità di Content Inspection;
- Funzionalità di Controllo sulla sintassi delle buste SPCoop;

- Funzionalità di controllo sui parametri della busta SPCoop (dimensioni, concatenamento, ecc.);
- Funzionalità di Gestione del protocollo SSL/TLS;
- Funzionalità di gestione dei certificati digitali secondo gli standard crittografici diffusi (esempio X509v3, PKCS#7, PEM, DER, CRL, OCSP etc.);
- Compatibilità con gli standard OASIS (SAML, XML-Signature, XML-Encryption, Web Services Security, ecc.), cioè deve essere possibile aggiungere/verificare firme e cifrare/decifrare i messaggi SPCoop o loro parti, allegati compresi;
- Compatibilità con protocolli di gestione utenze quali RADIUS e LDAP;
- Interfaccia grafica, Integrazione con i principali strumenti di creazione XML;
- Protezione da XDOS (XML Denial of Services);

Tra i requisiti del sistema FIREWALL XML attinenti ai livelli ISO/OSI dal 2 al 7 devono essere previsti i seguenti (tipici di Network firewall):

- Funzionalità di Network Address Translation (NAT);
- Funzionalità di Port Address Translation (PAT) ;
- Funzionalità di PROXY per i messaggi provenienti dall'interno dell'Amministrazione;
- Funzionalità di REVERSE PROXY per i messaggi provenienti dall'esterno dell'Amministrazione;
- Filtraggio basato su IP, con possibilità di abilitare sulla base degli indirizzi autorizzati, e altri criteri di content-filtering basati su orari di accesso etc.;
- Bloccaggio di URL inserite nei puntamenti ai servizi applicativi;
- Filtraggio in base al servizio;
- Filtraggio delle porte e dei protocolli;
- Funzionalità di Proxy per la gestione degli accessi (autenticazione ed autorizzazione) per disciplinare l'utilizzo di alcuni servizi (ad esempio FTP, TELNET, HTTP, HTTPS);
- Certificazione di sicurezza dei dispositivi utilizzati.

La fornitura del servizio è condizionata da vincoli di tipo tecnico e organizzativo, derivanti in particolare dalla particolare architettura di rete dell'amministrazione e dai sistemi e dai servizi utilizzati.

7.2.2. Modalità di erogazione del servizio

Il servizio si implementa attraverso elaboratori dedicati, che devono essere interposti tra i percorsi di rete diretti da e verso le PD, e vengono monitorati in tempo reale presso apposite console di security management. Può essere prevista, in via opzionale e comunque aggiuntiva, l'istallazione di appositi moduli software su alcuni componenti della PD, sempre gestiti in modalità centralizzata. La fornitura del servizio, con operatività H24, prevede il riporto degli allarmi e delle reazioni, con gestione remota.

Per potersi attivare, il fornitore ha la necessità di intervenire direttamente sui sistemi dell'amministrazione e quindi la fase di start-up deve essere svolta secondo una pianificazione concordata che preveda almeno i seguenti passi:

- Analisi dell'architettura del sistema per SPCoop dell'Amministrazione;
- Predisposizione di documenti che descrivono la soluzione per la gestione dei Firewall XML;
- Istallazione, testing e tuning del sistema di Firewall XML;

L' attività di gestione prevede:

- Gestione degli elaboratori firewall;
- Gestione delle security console, elementi centralizzati di gestione delle security appliance e degli elaboratori individuati, utilizzate sia per l'aggiornamento delle security policies tramite un'interfaccia grafica, sia per la raccolta delle violazioni delle politiche di sicurezza, per la produzione dei report richiesti e per l'evidenziazione all'operatore degli allarmi.
- Attività di manutenzione evolutiva e correttiva;

Deve valere il principio che ogni violazione delle regole sia acquisita con la memorizzazione dei dati relativi all'evento (indirizzi IP di origine e di destinazione, riferimento temporale, protocollo, contenuti dei singoli pacchetti e sequenza concatenata ecc) e deve essere definita la reazione allo specifico allarme generato (messaggio di posta, segnalazione sonora, fino al blocco automatico delle connessioni/sistemi).

Il servizio deve prevedere l'aggiornamento delle collocazioni/dimensionamento/caratteristiche dei FIREWALL XML per ogni modifica rilevante dell'architettura di rete e/o per ogni nuova PD da proteggere e/o in base alla capacità del traffico.

7.2.3. Reporting

La rendicontazione del servizio deve includere la stesura di rapporti sulle attività svolte, contenenti le statistiche sugli allarmi generati, i tentativi di denial of service, le reazioni attivate, le politiche di sicurezza aggiornate ecc.

I report periodici sono forniti in formato cartaceo o in formato elettronico dal fornitore e contengono almeno le seguenti informazioni:

- statistiche sulle prestazioni del servizio e sui i filtraggi effettuati;
- regole di filtraggio implementate;
- regole di NAT/PAT implementate;
- log sui tentativi di infrazione della politica di sicurezza implementata;
- log sugli accessi avvenuti con successo o falliti e controllati da schemi di autenticazione abilitati sui dispositivi di firewalling;

Tutta la reportistica relativa al servizio dovrà essere archiviata e conservata a cura del fornitore. Considerando la criticità delle informazioni deve essere previsto e stipulato sia un'accordo di riservatezza, sia un sistema di gestione della documentazione riservata. Il fornitore dovrà gestire ordinatamente tutte le informazioni in modo da consentirne

l'acquisizione, a richiesta e con preavviso non superiore ad un tempo predefinito, a favore dell'Autorità Giudiziaria oppure a favore dell'Amministrazione. A tal fine il fornitore dovrà individuare e implementare, di concerto con l'amministrazione, adeguati strumenti di *information retrieval*.

7.3. Intrusion detection

7.3.1. Descrizione e obiettivi del servizio

Il servizio è mirato nella gestione del rilevamento dei tentativi di intrusione condotti con sistemi manuali/automatici indipendentemente dalla loro collocazione e diretti verso la PD, allo scopo di ottenere l'accesso parziale/totale e/o di acquisire il controllo.

Il servizio include le verifiche dell'integrità dei sistemi, ossia deve essere attiva la protezione dei sistemi in modo tale che nessun tentativo di intrusione possa comportare l'acquisizione, in modalità silente, di privilegi di controllo indebiti sui sistemi (forensic analysis).

La finestra di erogazione del servizio è H24.

Il servizio di intrusion detection si implementa, nei confronti della PD, nella sola modalità HIDS (host intrusion detection system), in quanto le altre due modalità (NIDS (network intrusion detection sysyem), per le reti "wired" e WIDS (wireless intrusion detection system), per le reti "wireless") riguardano esclusivamente le reti e non le applicazioni. E' però conveniente utilizzare il servizio NIDS per le eventuali componenti fisiche che lavorano a livello dei protocolli di rete , come ad esempio i Firewall XML ed i Proxy.

Il servizio NIDS prevede l'uso di sonde "invisibili" istallate sui sistemi e/o collocate lungo i segmenti di rete, monitorate ed aggiornate dalle console di security management e operanti in modo da:

- acquisire informazioni sugli eventi di attacco (pattern);
- effettuare un'analisi predeterminata degli eventi rilevati;
- generare allarmi specifici a fronte della identificazione di un evento di attacco;
- attivare reazioni automatiche a fronte della identificazione di un evento di attacco.

I sistemi di IDS devono individuare almeno le seguenti tipologie di eventi:

- Accessi non autorizzati (Password guessing);
- Tentativi di intercettazione (hijacking, man-in-the-middle);
- Spoofing degli indirizzi;
- Port and Services scanning;
- Eventi DOS (Denial of Service);
- Ping Flooding, Smurf, SYN flood, IP Source routing;

- Tentativi di utilizzare i Buffer Overflow

I sistemi di IDS devono consentire la configurazione di specifici profili di protezione, riferibili sia a tutte le tipologie di elaboratori, sia tipici degli applicativi usati (gestione database, gestione Web Service, ecc.), come combinazione di almeno i seguenti:

- rilevazione periodica della modifica di file di configurazione del sistema operativo, elenco utenti del sistema e privilegi loro concessi;
- rilevazione e blocco dei tentativi di esecuzione di processi con permessi differenti da quelli dell'utente originale;
- controllo di esecuzione dei processi del sistema usando tecniche quali "sandboxing", sul modello di quanto avviene per l'esecuzione di codice java sui browser;
- rilevazione periodica della modifica dei file di configurazione del database; elenco utenti del database e privilegi loro concessi;
- rilevazione periodica dell'integrità di file di configurazione dei servizi web, script ed eseguibili esposti nella radice di file system contente il codice software del servizio applicativo, elenco degli utenti del sistema e privilegi loro concessi;
- controllo delle richieste HTTP malformate (es. contenenti codice di exploit di vulnerabilità di tipo buffer overflow);
- controllo del contenuto delle transazioni client-server verso le applicazioni ospitate dal server Web, per eliminare valori non accettabili, cookie riutilizzati illecitamente, ecc.

La fornitura del servizio deve essere effettuata con gestione remotizzata.

Tutta la reportistica relativa al servizio dovrà essere archiviata e conservata a cura del fornitore. Considerando la criticità delle informazioni deve essere previsto e stipulato sia un'accordo di riservatezza, sia un sistema di gestione della documentazione riservata.

Il fornitore dovrà pubblicare su un portale tutte le informazioni, con la periodicità e nella forma che l'amministrazione ritenga necessario pubblicare (reportistica depurata da informazioni riservate, attività di monitoraggio, piani di fabbisogno, fatturazione del servizio, ecc.).

Il fornitore dovrà gestire ordinatamente tutte le informazioni in modo da consentirne l'acquisizione, a richiesta e con preavviso non superiore ad un tempo predefinito, a favore dell'Autorità Giudiziaria oppure a favore dell'Amministrazione. A tal fine il fornitore dovrà individuare e implementare, di concerto con l'amministrazione, adeguati strumenti di *information retrieval*.

7.3.2. Modalità di erogazione del servizio

Il fornitore di questo servizio ha la necessità di intervenire direttamente sui sistemi dell'amministrazione e quindi la fase di start-up deve essere svolta secondo una pianificazione concordata che preveda almeno i seguenti passi:

- Analisi dell'architettura del sistema;
- Predisposizione di documenti che descrivono la posizione, il tipo ed il numero di sonde e console di management da collocare;

- Scelta delle configurazioni;
- Istallazione, testing e tuning del sistema di IDS;

L' attività di IDS (monitoraggio dei sistemi ai fini del rilevamento delle intrusioni) è effettuata tramite:

- predisposizione ed aggiornamento dei documenti di analisi del rischio, di concerto con l'amministrazione;
- istallazione e configurazione iniziale di sensori distribuiti (sonde), collocati sui segmenti di rete da controllare "wired", per la parte NIDS;
- istallazione e configurazione iniziale di moduli software specifici sugli host (server) da porre sotto controllo, per la parte HIDS;
- aggiornamento delle configurazioni in modo da assicurare i profili di protezione previsti in funzione degli elaboratori utilizzati;
- gestione degli elementi centralizzati per la raccolta degli allarmi (console di reporting e management), dai quali è possibile anche effettuare la configurazione remota dei sensori tramite un'interfaccia grafica che evidenzia all'operatore l'insorgere di situazioni anomale ed i dati necessari all'individuazione del problema. Le console di management sono aggiornabili in modalità sicura per quanto concerne il "pattern" degli attacchi noti.
- gestione delle rilevazioni degli attacchi passivi (penetrazione nelle risorse senza compromettere i sistemi) e degli attacchi attivi (accesso alle risorse per ottenerne il controllo) indipendentemente da dove sono originati.

Per ogni tentativo di intrusione è prevista l'acquisizione e memorizzazione degli indirizzi IP di origine e di destinazione dell'elaboratore origine dell'intrusione e vittima dell'intrusione, la "segnatura" dell'intrusione, riferimento temporale, protocollo, contenuti dei singoli pacchetti e sequenza concatenata, ecc) e deve essere definita la reazione (messaggio di posta, segnalazione sonora, fino al blocco automatico delle connessioni/sistemi).

Il servizio deve prevedere l'aggiornamento dell'architettura dell'IDS per ogni modifica rilevante dell'architettura di rete dei sistemi informatici e/o per ogni nuovo host da porre sotto controllo.

7.3.3. Reporting

La rendicontazione del servizio deve includere la stesura di rapporti sulle attività svolte, contenenti

- stato corrente del database delle "segnature" presenti sulle sonde;
- elenco ed esito degli aggiornamenti del database delle "segnature";
- stato delle regole di configurazione dei sistemi IDS;
- attacchi individuati;
- trend degli attacchi individuati;
- numero dei falsi negativi e dei falsi positivi;

Tutta la reportistica relativa al servizio dovrà essere archiviata e conservata a cura del fornitore. Considerando la criticità delle informazioni deve essere previsto e stipulato sia un'accordo di riservatezza, sia un sistema di gestione della documentazione riservata.

Il fornitore dovrà gestire ordinatamente tutte le informazioni in modo da consentirne l'acquisizione, a richiesta e con preavviso non superiore ad un tempo predefinito, a favore dell'Autorità Giudiziaria oppure a favore dell'Amministrazione. A tal fine il Fornitore dovrà individuare e implementare, di concerto con l'amministrazione, adeguati strumenti di *information retrieval*.

7.4. Registrazione degli eventi

7.4.1. Descrizione e obiettivi del servizio

Il servizio prevede la raccolta, la verifica, la correlazione, l'analisi e la storicizzazione delle tracce applicative, comprese quelle riguardanti gli allarmi (error log) generati e delle informazioni raccolte nei file di log dalle piattaforme caratterizzanti i diversi sistemi.

Riuscendo a correlare tra loro eventi ed informazioni provenienti da sistemi/architetture differenti, il servizio di Registrazione degli Eventi permette di realizzare un cruscotto attraverso il quale monitorare il livello di sicurezza raggiunto all'interno dell'organizzazione del cliente e prevenire e/o contrastare attacchi provenienti dall'esterno.

Gli obiettivi del servizio sono quelli di fornire uno strumento utile per:

- implementare i controlli imposti per rispettare il livello minimo di sicurezza;
- misurare il livello di sicurezza raggiunto sul proprio Sistema Informativo;
- effettuare tutte le attività di investigazione sui sistemi in rete necessarie alla gestione degli incidenti informatici.

7.4.2. Modalità di erogazione del servizio

Il servizio viene erogato per il tramite di una serie di strumenti hardware/software installati presso l'ambiente operativo del cliente e che possono essere gestiti remotamente o on-site.

Il reperimento dei file di log ed il collezionamento degli allarmi provenienti da sistemi/architetture impiegate nel sistema di sicurezza del cliente dipende dall'accessibilità delle informazioni prodotte dai dispositivi sotto il dominio amministrativo di fornitori terzi del cliente.

Al riguardo, quando necessario e richiesto dal cliente ed in tutti i casi in cui non sia possibile accedere alle informazioni di log e allarmi di dispositivi del sistema di sicurezza sotto il dominio amministrativo di fornitori terzi del cliente, potranno essere installati ulteriori strumenti (ad es. firewall, sonde, application proxy) per mezzo dei quali sarà possibile recuperare le informazioni e l'allarmistica utilizzati nell'ambito di erogazione del servizio.

La raccolta e la presentazione unificata di eventi/allarmi e log sarà limitata a solo quelli reperibili da strumenti hardware/software installati presso l'ambiente operativo del cliente che siano integrabili con la piattaforma impiegata dal fornitore per l'erogazione del servizio.

7.4.3. Reporting

Il servizio include le seguenti modalità di reportistica:

- near real time report;
- report periodici.

Il report near real time è basato sull'analisi on-line del sistema, è accessibile attraverso una interfaccia remota comunicante con il sistema attraverso un canale sicuro ed offre informazioni circa la configurazione, lo stato, le prestazioni della piattaforma e i log e gli allarmi da essa raccolti ed elaborabili.

Tutta la reportistica relativa al servizio dovrà essere archiviata e conservata a cura del fornitore. Considerando la criticità delle informazioni deve essere previsto e stipulato sia un'accordo di riservatezza, sia un sistema di gestione della documentazione riservata.

Il fornitore dovrà gestire ordinatamente tutte le informazioni in modo da consentirne l'acquisizione, a richiesta e con preavviso non superiore ad un tempo predefinito, a favore dell'Autorità Giudiziaria oppure a favore dell'amministrazione. A tal fine il Fornitore dovrà individuare e implementare, di concerto con l'amministrazione, adeguati strumenti di *information retrieval*.

APPENDICE

A1. Checklist sui requisiti di sicurezza della PD

L'insieme dei test che devono essere compiuti sia per l'ottenimento della qualificazione, sia per l'audit periodico, sono approvati dalla Commissione di Coordinamento per l'SPC e sono formalizzati in modo da fornire risultati misurabili e confrontabili.

Tale insieme di test può essere assimilato ad una "checklist" che naturalmente deve evolvere di pari passo con l'introduzione di nuovi standard e nuove tecnologie.

E' quindi necessario prevedere un meccanismo di predisposizione ed approvazione delle "checklist". Nella seguente tabella si propone un esempio di come predisporre una checklist.

Requisito	Parametro di valutazione
L'Amministrazione deve specificare una serie di informazioni che la Commissione esaminatrice utilizzerà per la valutazione complessiva dell'adeguatezza della Porta di Dominio. In particolare dovrà specificare se è stato sviluppato un piano per la sicurezza a livello globale che preveda anche l'adozione di: – procedure e strumenti per il controllo dell'accesso fisico del personale alle sale che ospitano le PD; – procedure e strumenti per il controllo dell'accesso logico del personale alle risorse hardware e software impiegate direttamente o indirettamente per l'erogazione dei servizi offerti sulla PD; – contromisure atte a garantire la continuità dell'erogazione dei servizi anche a fronte di malfunzionamenti di parte degli elementi che costituiscono l'infrastruttura tecnologica o a fronte di eventi catastrofici o atti terroristici; – procedure per la gestione degli incidenti di sicurezza che si dovessero verificare durante l'erogazione dei servizi in ambito SPCoop alle Amministrazioni; – strumenti per l'autenticazione forte per l'accesso alle PD per operazioni di l'amministrazione quali la definizione dei profili per l'autorizzazione, ecc., il tracciamento e la storicizzazione degli accessi	**OSSERVANZA DEL REQUISITO**
Definizione della struttura di sicurezza per i servizi con un Responsabile della sicurezza e suoi delegati al quale vanno assegnate chiare responsabilità;	**OSSERVANZA DEL REQUISITO**
Impegno a condurre l'Analisi dei rischi su base sistematica, almeno con cadenza annuale. Tale analisi andrà inoltre ripetuta a seguito di attacchi o incidenti gravi di sicurezza o per variazioni significative dell'architettura	**OSSERVANZA DEL REQUISITO**
Superamento di test preliminari per accertare il rispetto delle funzionalità minime previste nel documento "Porta di Dominio"	**OSSERVANZA DEL REQUISITO**

Requisito	Parametro di valutazione
Effettuazione di sessioni di colloquio con "Richiesta-Risposta" di carattere sperimentale, tesi ad accertare l'effettiva utilizzabilità della "Porta di Dominio", secondo gli Accordi di Servizio come definiti nel documento apposito	**OSSERVANZA DEL REQUISITO**

Tabella 8. Esempio di checklist

Con riferimento alle procedure di valutazione, infine, può essere preso come riferimento lo schema nazionale per la certificazione e la valutazione della sicurezza nelle tecnologie dell'informazione di cui sono state recentemente pubblicate le linee guida provvisorie sul sito CNIPA.