

**SISTEMA INFORMATICO INTEGRATO PER LA GESTIONE DEI FLUSSI INFORMATIVI
RELATIVI AI MERCATI DELL'ENERGIA ELETTRICA E DEL GAS**

REGOLAMENTO DI FUNZIONAMENTO

ALLEGATO C: REGOLE E MISURE DI SICUREZZA

1	PREMESSA.....	3
2	MODELLO DELLA SICUREZZA DEL SII	4
2.1	POLITICA DI SICUREZZA (SECURITY POLICY).....	4
2.2	OBIETTIVI DI SICUREZZA DEL SII	5
2.3	TIPOLOGIA DEI RISCHI	6
2.4	REGOLE DI SICUREZZA.....	8
2.4.1	<i>Identificazione delle entità.....</i>	8
2.4.2	<i>Autenticazione delle entità.....</i>	8
2.4.3	<i>Autorizzazione dei soggetti/applicazioni all'effettuazione delle operazioni.....</i>	9
2.4.4	<i>Mantenimento dell'Integrità dei dati.....</i>	9
2.4.5	<i>Assicurazione della Riservatezza dei dati.....</i>	9
2.4.6	<i>Non ripudio a livello di richiesta e di risposta.....</i>	11
2.4.7	<i>Registrazione degli eventi/Ispezione/Tracciabilità.....</i>	11
2.4.8	<i>Amministrato e gestione della sicurezza.....</i>	12
3	MISURE DI SICUREZZA PER L'USO DELLE PDC.....	13
3.1	GESTIONE DELLA PDC.....	13
3.1.1	<i>Qualificazione all'uso della PdC.....</i>	14
3.1.2	<i>Verifica e mantenimento delle condizioni di qualificazione.....</i>	15
3.2	FIREWALL.....	16
3.3	INTRUSION DETECTION SYSTEM.....	17
3.4	REGISTRAZIONE DEGLI EVENTI E GENERAZIONE DI ALERT	19
4	MISURE DI SICUREZZA PER L'ACCESSO AL PORTALE WEB.....	20
5	SERVIZI DI SICUREZZA INFRASTRUTTURALI DEL SII.....	21
5.1	SERVIZI DI INFRASTRUTTURA A CHIAVE PUBBLICA (PKI)	21
5.1.1	<i>Servizi di registrazione.....</i>	22
5.1.2	<i>Servizi di gestione delle chiavi e dei certificati.....</i>	22
5.1.3	<i>Profilo dei certificati emessi.....</i>	24
5.2	SERVIZI DI IDENTIFICAZIONE, AUTENTICAZIONE E AUTORIZZAZIONE.....	24
5.3	MONITORAGGIO DEGLI EVENTI DI SICUREZZA.....	26
5.4	SECURITY ASSESSMENT	26

1 PREMESSA

Il SII assicura elevati livelli di sicurezza in conformità ai criteri indicati nell'Allegato A della Delibera AEEG del 17 novembre 2010 – ARG/com 201/10, disponibile al sito <http://www.autorita.energia.it/it/index.htm>. In particolare assicura quanto previsto all'Art. 5 del suddetto Allegato.

Il SII utilizza i messaggi applicativi per lo scambio delle informazioni tra i sistemi informativi dei Soggetti (Utenti e Gestore) del mercato energetico italiano, all'interno di un contesto in grado di assicurare elevati livelli di qualità e di sicurezza.

Gli elementi principali dell'architettura del SII sono:

- le Porte di Comunicazione (PdC) dei Soggetti ed i servizi applicativi esposti attraverso di esse;
- il Portale Web per l'interazione con gli Utenti sprovvisti di PdC e, più in generale, per l'accesso alle basi dati del SII;
- i servizi infrastrutturali per lo scambio e la certificazione dei flussi applicativi trasmessi tra i Soggetti medesimi;
- le basi dati gestite dal SII.

Gli **Utenti** sono responsabili della corretta gestione delle proprie Porte di Comunicazione e dell'erogazione dei servizi applicativi, ovvero del corretto utilizzo del Portale Web.

Il **Gestore** del SII è responsabile della corretta gestione di tutte le componenti del SII e, in particolare, delle basi dati, del Portale Web e dei servizi infrastrutturali.

Il presente documento definisce:

- il modello della sicurezza del SII, specificando la politica e gli obiettivi di sicurezza, la tipologia dei rischi e le regole di sicurezza da applicare;
- le misure di sicurezza che gli Utenti ed il Gestore sono tenuti ad implementare nei loro sistemi, in termini di gestione della PdC e di accesso al Portale Web, ma anche dei servizi di firewall, IDS, registrazione degli eventi di sicurezza e generazione dei conseguenti alert;
- i servizi infrastrutturali di sicurezza del SII relativi a:
 - servizi di infrastruttura a chiave pubblica (PKI), anche al fine di assicurare requisiti di autenticità, riservatezza, integrità, non ripudio e tracciabilità nel trattamento dei messaggi scambiati tra i Soggetti;
 - servizi specifici di identificazione, autenticazione e autorizzazione;
 - monitoraggio degli eventi di sicurezza sulle PdC degli Utenti e sulle PdC del SII;
 - security assessment: analisi delle vulnerabilità e test di penetrazione.

2 MODELLO DELLA SICUREZZA DEL SII

La sicurezza del SII, quale sistema complesso, tiene conto di molteplici aspetti:

- **Aspetti concettuali:** la sicurezza è strutturata concettualmente su due livelli di responsabilità:
 - a livello dei singoli Utenti, che attraverso le Porte di Comunicazione espongono i servizi applicativi;
 - a livello del Gestore, che oltre a gestire specifici processi applicativi e le basi dati del SII, assicura anche componenti/servizi infrastrutturali necessari al funzionamento ed alla gestione dei servizi applicativi del SII.
- **Aspetti Tecnologici:** la sicurezza è realizzata sulla base del Web Service Security Framework, che è un insieme di standard riguardanti la sicurezza dei Web Services.
- **Aspetti Organizzativi e di Gestione della Sicurezza:** sono previste best practice procedurali e opportune politiche di gestione della sicurezza con riferimento agli aspetti trattati nello standard ISO 27002.

Il modello di sicurezza del SII, descritto in questo capitolo, definisce:

- la Politica di sicurezza;
- gli Obiettivi di sicurezza;
- la tipologia dei Rischi;
- le Regole di sicurezza.

2.1 Politica di sicurezza (Security Policy)

La politica di sicurezza del SII si basa su una chiara separazione delle responsabilità dei singoli Utenti e del Gestore del SII.

Il *Dominio di competenza di un Utente SII* è il complesso delle risorse informatiche e delle infrastrutture che realizzano il Sistema Informatico che consente all'Utente medesimo l'accesso al SII.

La *Porta di Comunicazione* è la componente logica di mediazione tra il dominio di competenza dell'Utente SII ed il SII medesimo.

Ogni Utente deve adottare una Politica di sicurezza interna che preveda l'implementazione di contromisure obbligatorie a livello di Porta di Comunicazione. Più precisamente, la Porta di Comunicazione deve garantire un livello minimo di sicurezza di cui l'Utente è direttamente responsabile, anche nel caso in cui la gestione dei servizi informatici sia affidata a terzi. Ogni Utente può altresì adottare contromisure aggiuntive all'interno del proprio Dominio.

Il rispetto dei requisiti necessari a garantire quanto previsto nel presente documento da parte di ogni Utente coinvolto nel SII, è verificato tramite audit effettuate dal Gestore del SII stesso.

Il *Dominio di competenza del Gestore SII* è il complesso delle risorse informatiche e delle infrastrutture che realizzano il Centro Servizi del SII. Tale dominio deve essere caratterizzato da un elevato livello di sicurezza di cui il Gestore è direttamente responsabile.

2.2 Obiettivi di sicurezza del SII

Come evidenziato in premessa, il SII deve garantire il rispetto dei criteri di sicurezza specificati nell'Allegato A della delibera AEEG del 17 novembre 2010 – ARG/com 201/10, e, in particolare, deve garantire la sicurezza, la riservatezza delle informazioni e la loro salvaguardia nel tempo. Ogni accesso ai dati contenuti nel SII deve essere quindi tracciabile e univocamente riferibile alle entità autorizzate (siano esse utenti finali o applicazioni di sistema).

Gli obiettivi di seguito elencati sono requisiti di sicurezza di carattere generale. Essi dovranno essere contestualizzati, in fase di analisi e progettazione di dettaglio, per ciascun processo applicativo gestito tramite il SII e per i servizi e le componenti infrastrutturali, tra cui la Porta di Comunicazione.

1. *Identificazione delle entità.*
A ciascuna entità implicata direttamente o indirettamente nello scambio di messaggi, nell'erogazione e nella fruizione dei servizi, deve essere associata un'Identità univoca.
2. *Autenticazione delle entità.*
Deve essere verificata l'Identità dichiarata da tutte le entità di cui al punto precedente.
3. *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.
4. *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 confidenza che i dati non vengano modificati in modo accidentale o intenzionale e all'insaputa di una o entrambe le entità.
5. *Assicurazione della Riservatezza dei dati.*
Deve essere assicurata la riservatezza dei dati scambiati sia in conformità alla normativa vigente (Decreto Legislativo n. 196/2003 recante Codice per la protezione dei dati personali e s.m.i.) sia per ogni altra ragione valida (ad esempio per evitare l'intercettazione dei dati "riservati").

6. *Non ripudio a livello di richiesta e di risposta.*
Ogni messaggio scambiato nell'ambito del SII deve contenere la prova che è stato emesso da una determinata entità, in un determinato contesto spazio/temporale di esecuzione.
7. *Registrazione degli eventi/Ispezione/Tracciabilità.*
Deve essere sempre possibile risalire alle operazioni eseguite, a chi le ha effettuate, dove e quando. L'ispezione è la capacità di acquisire dinamicamente e analizzare le informazioni di registrazione.
8. *Amministrazione e Gestione della sicurezza.*
Devono essere individuate tutte quelle procedure che definiscono con accuratezza le attività di organizzazione della sicurezza.

2.3 Tipologia dei rischi

La seguente tabella rappresenta le principali categorie di rischi connessi al SII, con il relativo impatto sui processi gestiti:

Rischio	Impatto	Vulnerabilità sfruttabili
La base dati relativa al rapporto Cliente-Venditore viene integralmente o in larga parte trafugata e messa a disposizione di soggetti con interessi alla filiera	Altissimo	<i>Sicurezza rispetto al fornitore:</i> Personale del fornitore, o sua terza parte, deputato alla gestione dell'infrastruttura o alla gestione operativa dei dati agisce in maniera malevola sfruttando i propri privilegi di accesso fisico ai locali, o di accesso logico ai dati.
		<i>Intrusione attraverso impersonificazione:</i> un'entità cerca di raggirare il processo di autenticazione e presentarsi sotto falsa identità. Per raggiungere lo scopo vengono solitamente sfruttate delle anomalie presenti nei sistemi operativi/applicazioni a livello di codice o causate da errate configurazioni.
		<i>Abuso di privilegi:</i> 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.

Rischio	Impatto	Vulnerabilità sfruttabili
Soltanto alcuni dati relativi al rapporto cliente-Venditore vengono trafugati	Alto	<i>Intercettazione dei dati:</i> un'entità non autorizzata cerca di acquisire dati durante il transito. Per limitare tale rischio devono essere implementate tecniche di cifratura.
Una parte dei dati contenuti nel sistema (workflow dei processi/registro ufficiale) viene manomessa per fini condizionamento improprio della filiera di mercato connessa SII	Alto/Altissimo	<i>Manomissione dei dati:</i> un'entità cerca di inserire dati non autentici o alterare il contenuto dei messaggi. Per ovviare a questo tipo di attacco devono essere implementate tecniche per la "firma" dei dati.
Operazioni improprie sui sistemi informativi per fini di condizionamento improprio della filiera di mercato connessa al SII	Alto/Altissimo	<i>Riutilizzo/Dirottamento dei messaggi:</i> un'entità intercetta i messaggi trasmessi e li riutilizza effettuando nuovi invii. Per ovviare a questo attacco occorre che i produttori dei dati, i mittenti ed i destinatari dei messaggi vengano autenticati, che i messaggi stessi siano identificati, autenticati e datati.
Manomissione dei sistemi di sicurezza per rendere più efficaci minacce al sistema	Alto/Altissimo	<i>Distruzione delle tracce:</i> 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.

Rispetto a questi, ed a altri rischi di minore impatto, dovranno essere previste, attuate, verificate, e aggiornate in continuo adeguate contromisure di natura fisica, logica e organizzativa.

2.4 Regole di sicurezza

2.4.1 Identificazione delle entità

L'erogazione e la fruizione di un servizio applicativo richiede che siano effettuate operazioni di identificazione univoca delle entità (sistemi e utenti finali) che partecipano, in modo diretto o indiretto (attraverso sistemi intermediari) e con ruoli diversi, allo scambio di messaggi, alla erogazione ed alla fruizione dei servizi.

Le regole di Identificazione si basano su **UserID** per gli utenti finali e su **URI** per i Sistemi.

In particolare, gli identificativi dei servizi applicativi\operazioni esposti sulle PdC devono essere conformi al formato URI come indicato nelle specifiche di cui all'Art.14.1.2 del Regolamento.

La presenza e l'attività rilevata di elementi non identificati deve essere segnalata come incidente di sicurezza.

2.4.2 Autenticazione delle entità

Ogni operazione richiesta nell'ambito del SII implica che sia verificata preliminarmente l'identità dichiarata dall'entità.

I meccanismi di autenticazione dipendono dalla tipologia delle entità che operano nel SII (sistemi e utenti finali).

I meccanismi di autenticazione che riguardano gli utenti finali si basano su **UserID** e **Password**. In funzione della natura dell'operazione o del servizio applicativo, può essere richiesto di utilizzare meccanismi di autenticazione "forte", cioè basati sul controllo di almeno due fattori: **Password** (ciò che l'utente finale conosce) e **Smart Card** (ciò che l'utente finale ha).

Le credenziali associate agli utenti finali sono strettamente personali, non possono essere cedute a terzi ed il possessore si assume la responsabilità della loro custodia garantendo la confidenzialità delle stesse.

L'autenticazione dei sistemi, e in particolare dei servizi applicativi\operazioni, deve essere implementata attraverso algoritmi e protocolli basati su **certificati digitali** emessi dalla Autorità di Certificazione (CA) della Infrastruttura a Chiave Pubblica (PKI) del SII o da un Certificatore accreditato secondo la normativa vigente.

I meccanismi di autenticazione riguardanti le PdC per le funzioni di diagnostica, comandi e configurazione della porta, devono essere implementati attraverso i protocolli SSL/TLS, basati su certificati digitali emessi per tale scopo dalla CA del SII.

Il SII gestisce una propria PKI, rende pubblici i Certificate Practice Statement (CPS) e assicura il servizio di verifica della validità dei certificati¹.

¹ La verifica dello stato di validità dei certificati utilizzati per l'autenticazione, può essere effettuata con protocollo OCSP o tramite verifica sulle liste di revoca(CRL) e di sospensione (CSL).

I criteri per l'autenticazione dei messaggi e degli allegati inviati tramite le PdC devono essere conformi alle specifiche di cui all'Art.14.1.2 del Regolamento e sono gestiti dalla Porta in conformità con quanto riportato nelle specifiche medesime.

2.4.3 Autorizzazione dei soggetti/applicazioni all'effettuazione delle operazioni

I requisiti di autorizzazione riguardano i singoli fruitori di ciascun servizio applicativo (utenti finali ed applicazioni).

L'autorizzazione delle entità alla fruizione dei servizi applicativi deve seguire le regole stabilite per ciascun processo applicativo del SII, specificate e pubblicate dal Gestore del SII nel **Catalogo dei Servizi**.

I profili di autorizzazione di ciascun fruitore sono registrati dal Gestore del SII nel **Catalogo dei Profili** al momento della qualificazione dell'Utente alla fruizione dei servizi di uno specifico processo applicativo.

I profili di autorizzazione prevedono meccanismi gerarchici e sono basati sui ruoli secondo i paradigmi RBAC (Role-Based Access Control).

Le operazioni di attribuzione, sospensione e revoca delle autorizzazioni sono tracciate.

I criteri per l'autorizzazione devono essere conformi alle specifiche di cui all'Art.14.1.2 del Regolamento.

2.4.4 Mantenimento dell'Integrità dei dati

Il controllo dell'integrità si applica in modo sistematico ai messaggi scambiati attraverso il SII ed al loro contenuto.

Il controllo di integrità dei messaggi scambiati deve essere implementato attraverso gli standard OASIS WS-Security, in particolare gli standard W3C XML-Signature (basati su **certificati digitali**), in conformità alle specifiche di cui all'Art.14.1.2 del Regolamento.

Il controllo dell'integrità può essere altresì effettuato sui messaggi archiviati dal Sistema di Certificazione e Archiviazione, attraverso la verifica della consistenza delle tracce dei messaggi memorizzati.

La scelta degli algoritmi e dei parametri da utilizzare (lunghezza delle chiavi, etc.) è stabilita e pubblicata dal Gestore del SII nelle specifiche di cui all'Art.14.1.2 del Regolamento. Tali specifiche definiscono anche le modalità per assicurare e verificare l'integrità dei dati contenuti nel Registro Ufficiale.

2.4.5 Assicurazione della Riservatezza dei dati

Il Gestore provvede alla classificazione delle informazioni e dei dati contenuti nei messaggi scambiati, nel Registro ufficiale e negli altri archivi del SII nell'ambito delle Regole di Registrazione di cui all'art. 14.1.5.

Livello	Declaratoria	Pubblicabilità	Accessibilità
R1	<i>dato pubblico</i>	Il dato può essere acquisito, diffuso e riprodotto ovunque senza autorizzazione	Conoscibile da chiunque indistintamente
R2	<i>dato interno</i>	Il dato è presente in atti interni, di natura ordinaria, dell'Utente. L'atto può essere comunicato all'esterno previa autorizzazione, purché non contenga dati personali	Riservato ai soggetti autorizzati. Richiede l'identificazione del richiedente.
R3	<i>dato personale</i>	Definito ai sensi dell'art. 4 del D.Lgs n. 196/03 e s.m., trattato ai sensi degli artt. 11 e successivi; può essere comunicato ad altri soggetti pubblici o privati solo se previsto da norma di legge.	Accessibile secondo la normativa vigente sui dati personali. Obbligo misure minime di sicurezza che includono: l'identificazione del richiedente, la verifica delle autorizzazioni, il controllo degli accessi e la registrazione delle operazioni effettuate dagli Amministratori di sistema.
R4	<i>dato sensibile</i>	Definito ai sensi dell'art. 4 del D.Lgs n. 196/03 e s.m., trattato ai sensi degli artt. 11, 20, 21 e 22 può essere comunicato a soggetti pubblici o privati solo se previsto da norma di legge. I dati sensibili non possono essere diffusi.	Accessibile secondo la normativa vigente (Decreto Legislativo n. 196/03 e Legge n. 241/90). Obbligo misure minime di sicurezza vigente (Decreto Legislativo n. 196/03 e Legge n. 241/90). Obbligo misure minime di sicurezza che includono: l'identificazione del richiedente, la verifica delle autorizzazioni, il controllo degli accessi e la registrazione delle operazioni effettuate dagli Amministratori di sistema. Obbligo di cifratura e di tenuta in archivi separati (art. 22 comma 6 e 7).
R5	<i>dato riservato, soggetto al segreto d'ufficio</i>	Dato sottoposto a limitazioni di accesso per finalità diverse (brevetti, dati commerciali, dati tecnici riservati, etc).	Accessibile ai soggetti espressamente autorizzati. Accesso controllato con misure di sicurezza specifiche che includono: l'identificazione del richiedente, la verifica delle autorizzazioni, il controllo degli accessi e la registrazione delle operazioni. Ogni eventuale violazione deve essere evidenziata e può essere denunciata.

Deve essere garantita la riservatezza dei dati di livello R4, R5 anche durante lo scambio di messaggi effettuati attraverso il SII. La riservatezza può essere garantita a livello di messaggio (es. XML-Encryption) o di connessione (es. SSL/TLS). In entrambi i casi i meccanismi di riservatezza sono basati su **certificati digitali** emessi specificatamente per tale finalità (i certificati emessi per scopi di riservatezza i devono essere differenti da quelli emessi per ogni altra finalità).

La scelta degli algoritmi e dei parametri da utilizzare (lunghezza delle chiavi, etc.) per la cifratura è effettuata e pubblicata dal Gestore del SII nelle specifiche di cui all'Art.14.1.2 del Regolamento.

2.4.6 Non ripudio a livello di richiesta e di risposta

Nell'ambito dell'erogazione e della fruizione di servizi applicativi, il non ripudio riguarda il messaggio scambiato, compresi gli eventuali allegati.

Il non ripudio del messaggio è assicurato a diversi livelli, attraverso la firma de:

- l'intestazione del messaggio;
- il messaggio applicativo;
- gli allegati.

Le firme possono essere apposte utilizzando o l'apposito **certificato digitale** della Porta, emesso dalla CA del SII, oppure un certificato qualificato emesso da un Certificatore accreditato secondo la normativa vigente².

I criteri per le funzionalità di non ripudio devono essere conformi alle specifiche di cui all'Art.14.1.2 del Regolamento

2.4.7 Registrazione degli eventi/Ispezione/Tracciabilità

Le funzioni di registrazione degli eventi e di tracciabilità consistono nella memorizzazione dei dati relativi alle operazioni che sono state effettuate sulle PdC di tutti gli Utenti e presso il Centro Servizi del Gestore. 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.

Ogni Porta deve farsi carico della tracciatura di ogni messaggio SOAP scambiato, in conformità con le specifiche di cui all'art.14.1.2 del Regolamento. Tali specifiche descrivono il formato XML delle tracce e le modalità per l'invio periodico al Sistema Centrale, per il riscontro e la certificazione e l'archiviazione dei flussi scambiati.

Le PdC degli Utenti e il Centro Servizi presso il Gestore devono registrare gli eventi rilevanti ai fini della sicurezza e devono farsi carico della loro conservazione secondo quanto definito nell'ambito delle specifiche di cui all'art.14.1.2 del Regolamento.

Gli eventi di sicurezza e i record di tracciatura devono essere conservati presso il Gestore con modalità e tempi tali da assicurare la possibilità di ricostruire (ispezione) i messaggi scambiati, senza equivoci e per periodi di tempo compatibili con la normativa vigente.

² DPR 29 dicembre 2000 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]

2.4.8 Amministrazione e gestione della sicurezza

L'Amministrazione e la gestione della sicurezza è definita dal Gestore nel **Piano della sicurezza**.

Il Piano della sicurezza affronta ed è conforme agli argomenti trattati dallo standard ISO 27002, nel quale sono definiti:

1. l'analisi e gestione del rischio;
2. le politiche e le procedure di sicurezza;
3. l'organizzazione della sicurezza stessa;
4. la classificazione ed il controllo dei beni;
5. la sicurezza del personale;
6. la sicurezza fisica ed ambientale;
7. la gestione delle comunicazioni;
8. il controllo accessi;
9. la sicurezza del processo di sviluppo e manutenzione delle applicazioni;
10. la gestione degli incidenti;
11. la gestione della continuità operativa;
12. la conformità agli standard, regolamenti e normative vigenti.

3 MISURE DI SICUREZZA PER L'USO DELLE PdC

Ogni Soggetto (Utenti e Gestore) è tenuto alla gestione delle misure tecniche, organizzative e procedurali nel rispetto della Politica di Sicurezza del SII, con particolare riguardo alla gestione delle PdC e alle interfacce verso i sistemi informatici interni. Ciascuno deve:

- individuare le risorse necessarie per lo svolgimento delle attività di amministrazione della sicurezza;
- provvedere all'attribuzione delle responsabilità;
- applicare le procedure per la gestione ordinaria della sicurezza coerentemente con gli obiettivi del SII;
- assicurare le misure di sicurezza riportate nei paragrafi seguenti.

In particolare, sono sotto il controllo e la responsabilità di ciascun Soggetto le attività relative a:

- Installazione, richiesta di qualificazione e **gestione della PdC** (patch management evolutivo e correttivo; tracciatura dei messaggi scambiati; hardening dei sistemi che compongono la PdC; gestione degli accessi alla PdC; gestione e memorizzazione dei log delle operazioni eseguite dalla PdC, eliminazione di virus informatici, etc.).
- Installazione e gestione di un **Firewall** (protezione da DOS, DDOS; difesa da spoofing degli indirizzi, controllo dei protocolli, porte e servizi, analisi del traffico a livello applicativo, etc.).
- Installazione e gestione di un **Sistema di Intrusion Detection** e di un **Sistema di registrazione eventi di sicurezza** (rilevazione H24 dei tentativi di intrusione; registrazione e segnalazione degli eventi rilevanti ai fini della sicurezza; gestione delle emergenze e degli incidenti di sicurezza, ripristino dei sistemi in caso di attacchi/guasti, etc.).

Nello specifico, il Gestore del SII ha il controllo e la responsabilità della gestione della PdC e dei sistemi di firewalling, IDS e registrazione degli eventi di sicurezza presenti nel proprio Centro Servizi, secondo quanto previsto dal Piano della Sicurezza (vedi sezione 2.4.8).

3.1 Gestione della PdC

L'architettura SII prevede che i Soggetti interagiscono mediante messaggi applicativi che transitano attraverso le Porte di Comunicazione (PdC), che sono assimilabili ad una sorta di "gateway" tra i sistemi informativi gestiti dai singoli Soggetti.

Ciascun Utente che sceglie di aderire al SII mediante una collaborazione di tipo *Application To Application* deve dotarsi di una PdC.

Il Gestore del SII mette a disposizione un'implementazione base della PdC che l'Utente **può richiedere** al momento dell'adesione al SII. E' altresì previsto da parte del Gestore del SII il supporto tecnico per l'installazione, i test e la qualificazione della PdC.

Rimane in ogni caso responsabilità dell'Utente l'installazione, la richiesta di qualificazione e la corretta gestione della propria PdC.

La gestione comprende le ordinarie attività di conduzione degli apparati, la gestione degli aggiornamenti (patch management evolutivo e correttivo), la tracciatura dei messaggi scambiati, l'hardening dei sistemi, la profilazione e la gestione degli accessi alla PdC, la gestione e memorizzazione dei log delle operazioni eseguite dalla PdC.

Le PdC dei Soggetti devono essere dotate di Antivirus aggiornato regolarmente allo scopo di eliminare il malware eventualmente presente nei messaggi SII e/o nel body e/o negli attachment.

La PdC deve essere conforme alle specifiche di cui all'Art.14.1.2 del Regolamento.

3.1.1 Qualificazione all'uso della PdC

Preliminarmente alla fase di qualificazione degli Utenti all'uso della PdC è necessario che le PdC siano sottoposte a rigorosi controlli al fine di assicurarne la conformità rispetto ai requisiti funzionali, prestazionali e di sicurezza del SII. Le procedure per la qualificazione all'uso della PdC sono definite nell'ambito delle specifiche di cui all'Art.14.1.2 del Regolamento.

Il processo di qualificazione, se terminato con esito positivo, convalida l'adeguatezza della PdC rispetto alle specifiche tecniche, funzionali e di sicurezza del SII.

L'ottenimento della qualificazione costituisce il requisito necessario per l'inserimento dell'Utente e della sua PdC nel SII.

La qualificazione ha lo scopo di garantire che le PdC espongano i servizi applicativi mantenendo nel tempo i requisiti minimi di qualità e sicurezza stabiliti.

Successivamente alla qualificazione deve essere mantenuto costantemente il livello di funzionalità delle PdC, rappresentato come segue:

- F1. Funzionalità di gestione della sicurezza a livello connessione.
- F2. Funzionalità di tracciatura dei messaggi.
- F3. Funzionalità di gestione dello smistamento dei messaggi.
- 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 test periodici volti a verificare la resistenza degli elementi ad attacchi di sicurezza predefiniti (security assessment).

Il mancato superamento dei test comporta la necessità di un aggiornamento della PdC e può richiedere una esclusione temporanea dal SII.

A fronte di modifiche significative nelle modalità di erogazione dei servizi della Porta è altresì previsto un test di riqualificazione.

La tabella seguente riepiloga gli stati in cui può trovarsi una PdC rispetto alla sua qualificazione nel SII.

Stato	Descrizione
Non qualificata	La Porta non è qualificata, non può operare nel SII.
Qualificata	La Porta ha superato con successo il processo di qualificazione e può operare nel SII per i processi per i quali ha superato anche la qualificazione dei relativi servizi applicativi.
Sospesa	La Porta già qualificata non ha superato il processo di verifica (security assessment) e non può operare nel SII fino alla rimozione degli inconvenienti riscontrati.

Nella tabella seguente sono descritti i possibili eventi che causano la transizione da uno stato all'altro in cui una Porta può trovarsi rispetto alla qualificazione.

Evento	Stato di partenza	Stato di Arrivo
Qualificazione: superamento del processo di qualificazione.	Non qualificata	Qualificata
Mantenimento Qualificazione, verifica positiva: superamento del security assessment.	Qualificata	Qualificata
Mantenimento Qualificazione, verifica negativa: mancato superamento del security assessment.	Qualificata	Sospesa
Verifica qualificazione nuovi servizi applicativi positiva/negativa: esito del processo che accerta o meno il soddisfacimento delle condizioni per estendere la qualificazione l'adesione ad una categoria di servizi applicativi.	Qualificata	Qualificata
Scadenza periodo di osservazione: conclusione del periodo di osservazione all'interno del quale la PdC, la cui qualificazione è sospesa, può rimuovere gli inconvenienti riscontrati e sottoporsi ad una nuova valutazione.	Sospesa	Non qualificata
Riqualificazione, verifica positiva: superamento del security assessment dopo una sospensione.	Sospesa	Qualificata

3.1.2 Verifica e mantenimento delle condizioni di qualificazione

Durante l'esercizio sono previste attività di *security assessment*, finalizzate a verificare il rispetto dei requisiti di qualificazione della PdC, condotte presso le strutture dove si trovano i componenti fisici che implementano la Porta e quelli che erogano i servizi applicativi.

Tale attività di auditing può essere condotta anche a seguito dell'accertamento, da parte del Gestore del SII, di anomalie, del mancato rispetto dei livelli minimi garantiti sul servizio o a seguito di incidenti informatici che coinvolgano l'Utente o che causano una erogazione non adeguata del servizio.

La sospensione, attribuita nel caso in cui le anomalie accertate non inficiano il livello minimo di sicurezza imposto sul SII, prevede che l'Utente predisponga un piano di rientro delle condizioni di qualificazione concordato con il Gestore del SII. Al termine della scadenza concordata verrà svolta una nuova attività di auditing diretta ad accertare il ripristino delle anomalie riscontrate e la piena conformità alle specifiche di qualificazione.

La revoca della qualificazione avviene invece nei seguenti casi:

- le anomalie accertate durante l'audit inficiano il livello minimo di sicurezza del SII;
- viene accertata la non conformità delle modifiche effettuate sulla PdC per l'attuazione del piano di rientro.

Le procedure per l'esecuzione delle attività di *security assessment* sono definite nell'ambito delle specifiche di cui all'Art.14.1.2 del Regolamento.

3.2 Firewall

In conformità alle specifiche di cui all'Art.14.1.2 del Regolamento, è a cura di ciascun Soggetto:

- implementare le funzionalità di Firewall, tenuto conto che il corretto funzionamento è condizionato da vincoli di tipo tecnico e organizzativo, derivanti in particolare dalla architettura di rete del soggetto e dai sistemi e dalle applicazioni utilizzate;
- assicurare la gestione del Firewall, inclusa la notifica degli allarmi e delle reazioni al Gestore del SII.

In particolare tali specifiche stabiliscono:

- le regole da applicare, definite in base alle possibili minacce e i conseguenti rischi ed alle esigenze di funzionalità e sicurezza del SII;
- i requisiti minimi di operatività della componente, in termini di disponibilità del servizio, requisiti prestazionali, modalità di gestione;
- il contenuto minimo dei messaggi di log e di registrazioni degli eventi di violazione delle regole da gestire in locale;
- le linee guida di reazione agli eventi;
- i contenuti minimi della reportistica e dei tempi di conservazione della stessa;
- il contenuto dei messaggi di notifica, verso il Gestore del SII, degli eventi rilevanti per il SII e delle relative modalità di inoltro.

Il Firewall deve rappresentare l'end-point delle connessioni sicure basate su SSL/TLS tra le PdC degli Utenti e quella del Gestore.

Il Firewall comprende strumenti per il filtraggio del traffico di rete a livello applicativo secondo un insieme di regole definite, aggiornabili e verificabili.

Il Firewall deve poter intervenire al livello 7 della pila ISO/OSI (oltre ai livelli più bassi) con l'obiettivo di consentire il transito di tutto il traffico che rispetta le regole stabilite e,

contestualmente, di impedire tutto il traffico che non le rispetta, tenendone traccia ove ciò accada.

Il servizio deve consentire l'analisi di tutto il traffico che transita attraverso la PdC ed in particolare:

- impedire lo spoofing degli indirizzi IP di origine e destinazione;
- selezionare i protocolli di rete ammessi (TCP, UDP, ecc.) provenienti da determinati host/sottoreti/domini ed indirizzati a determinati host/sottoreti/domini;
- selezionare le porte di rete associate al servizio (SMTP, TELNET, HTTP, HTTPS, etc.);
- analizzare il flusso della connessione e la sua direzione ("stateful inspection").
- controllare i pacchetti sino al livello applicativo, ispezionando in particolare i protocolli HTTP\HTTPS e SOAP\XML.

Il sistema di FIREWALL deve consentire almeno i seguenti requisiti:

- Funzionalità di gestione del protocollo SSL/TLS.
- Compatibilità con protocolli di gestione utenze quali RADIUS e LDAP.
- Protezione da Ping Flooding, Smurf, SYN flood (DOS e DDOS, in generale), XDOS e IP Source routing.
- Funzionalità di Network Address Translation (NAT).
- Funzionalità di Port Address Translation (PAT).
- Funzionalità di PROXY per i messaggi provenienti dall'interno.
- Funzionalità di REVERSE PROXY per i messaggi provenienti dall'esterno.
- Filtraggio basato su IP 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).
- Funzionalità di analisi dei pacchetti a livello applicativo (nello specifico HTTP\HTTPS e SOAP\XML).

3.3 Intrusion Detection System

In conformità alle specifiche di cui all'Art.14.1.2 del Regolamento, è a cura di ciascun Soggetto:

- implementare le funzionalità di IDS, tenuto conto che il corretto funzionamento è condizionato da vincoli di tipo tecnico e organizzativo, derivanti in particolare dalla architettura di rete del soggetto e dai sistemi e dalle applicazioni utilizzate;
- assicurare la gestione del IDS, inclusa la notifica degli allarmi e delle reazioni al Gestore del SII.

In particolare tali specifiche stabiliscono:

- le regole da applicare, definite in base alle possibili minacce e i conseguenti rischi ed alle esigenze di funzionalità e sicurezza del SII;
- i requisiti minimi di operatività della componente, in termini di disponibilità del servizio, requisiti prestazionali, modalità di gestione;
- il contenuto minimo dei messaggi di log e di registrazioni degli eventi di violazione delle regole da gestire in locale;
- le linee guida per la reazione agli eventi;
- i contenuti minimi della reportistica e dei tempi di conservazione della stessa;
- il contenuto dei messaggi di notifica, verso il Gestore del SII, degli eventi rilevanti per il SII e delle relative modalità di inoltro.

La componente IDS deve rilevare i tentativi di intrusione condotti con sistemi manuali o automatici, indipendentemente dalla loro collocazione, diretti verso la PdC per ottenere l'accesso parziale/totale o di acquisirne il controllo.

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.

L'IDS si implementa, nei confronti della PdC, in modalità HIDS (Host Intrusion Detection system) e deve individuare almeno le seguenti tipologie di eventi:

- Accessi non autorizzati (Password guessing).
- Port and Services scanning.
- Eventi DOS (Denial of Service).
- Tentativi di utilizzare i Buffer Overflow.
- Attacchi noti (misuse-IDS) e anomalie (anomly-IDS).
- Tentativi di eseguire applicazioni non autorizzate.
- Tentativi di compromettere l'integrità dei file di sistema.

3.4 Registrazione degli eventi e generazione di Alert

Il servizio richiede la raccolta, la verifica, la correlazione, l'analisi e la storicizzazione delle tracce riguardanti gli allarmi generati dal Firewall, dall'IDS e dalla Porta di Comunicazione.

E' a cura del singolo Soggetto l'implementazione e la gestione del servizio in conformità alle specifiche di cui all'Art.14.1.2 del Regolamento, tenuto conto che il reperimento dei file di log e la raccolta degli allarmi provenienti da sistemi/architetture impiegate nel sistema di sicurezza del Soggetto può dipendere dall'accessibilità delle informazioni prodotte dai dispositivi sotto il dominio amministrativo di eventuali fornitori terzi. Al riguardo potrebbe essere necessaria l'installazione di ulteriori strumenti (ad es. sonde, application proxy) per mezzo dei quali recuperare le informazioni e l'allarmistica necessarie.

Le specifiche di cui all'Art.14.1.2 del Regolamento stabiliscono in particolare:

- gli eventi di sicurezza di interesse per il SII;
- i requisiti minimi di operatività della componente, in termini di disponibilità del servizio, requisiti prestazionali, modalità di gestione;
- i requisiti minimi per la raccolta, la verifica, la correlazione, l'analisi e la storicizzazione delle tracce riguardanti gli allarmi generati dal Firewall, dall'IDS e dalla Porta;
- le procedure di reazione agli allarmi di sicurezza (incluso il contenuto dei messaggi di notifica e le modalità di inoltro) da segnalare al SII;
- i contenuti minimi della reportistica e dei tempi di conservazione della stessa.

Riuscendo a correlare tra loro eventi e informazioni provenienti da sistemi/architetture differenti, la componente di Registrazione degli Eventi realizza un cruscotto con cui monitorare il livello di sicurezza raggiunto. Lo scopo è quello di prevenire e/o contrastare attacchi provenienti dall'esterno e diretti verso la PdC con l'obiettivo di compromettere l'erogazione/fruizione dei servizi applicativi del SII.

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;
- effettuare le attività di investigazione sui sistemi in rete necessarie alla gestione degli incidenti informatici.

4 MISURE DI SICUREZZA PER L'ACCESSO AL PORTALE WEB

Il Portale Web consente agli Utenti sprovvisti di Porta di Comunicazione di collaborare ai processi applicativi realizzati nel SII e costituisce l'interfaccia utente per l'accesso controllato ai contenuti delle basi dati del SII.

L'accesso al Portale Web è consentito mediante i più diffusi browser web, quali da esempio:

- Microsoft Internet Explorer versione 7 o successive;
- Mozilla Firefox 3 o versioni successive;
- Apple Safari 4.0 o versioni successive;
- Google Chrome.

Per gli utenti finali del Portale (persone fisiche) è richiesta una procedura di identificazione e autenticazione a due fattori (autenticazione forte), come definito nelle sezioni 2.4.1 e 2.4.2.

In particolare sono assegnati una username e due fattori di controllo a ciascun utente finale del Portale: il primo è una password alfanumerica, il secondo è una Smart Card contenente un certificato digitale personale (rilasciato dalla Certification Authority del SII o da un Certificatore accreditato secondo la normativa vigente). A titolo di esempio, mediante la prima password può essere possibile accedere alle funzioni di interrogazione del Portale su dati non riservati, mentre per accedere a funzionalità critiche o a dati riservati è necessario fornire entrambi i fattori di controllo.

E' cura di ciascun Utente dotarsi dei lettori di Smart Card in relazione al proprio personale abilitato ad accedere al Portale per le operazioni che richiedono l'autenticazione forte.

A ciascun Utente è associato un ruolo che descrive quali sono le funzionalità del Portale accessibili. Gli Utenti possono disporre di uno o più account di accesso, ciascuno con profili di autorizzazione uguali o gerarchicamente inferiori rispetto a quelli associati all'Utente stesso.

La sicurezza della comunicazione Web con gli utenti finali è gestita mediante una connessione SSL/TLS che garantisce la riservatezza delle informazioni: si richiede che i browser web scelti per l'accesso al Portale siano in grado di supportare i protocolli SSL/TLS.

L'accesso al Portale Web deve essere consentito mediante postazioni di lavoro dotate di Antivirus aggiornato regolarmente.

La sicurezza della comunicazione tra il Portale Web ed il SII è gestita dalla PdC Portale Web, che firma e se richiesto cifra, il traffico in uscita e verifica il traffico in entrata. Il certificato utilizzato per la firma è quello assegnato alla PdC del Portale.

Per le regole di gestione si rimanda a quanto descritto nelle specifiche tecniche di cui all'Art.14.1.2.

5 SERVIZI DI SICUREZZA INFRASTRUTTURALI DEL SII

Il Gestore del SII deve assicurare, per i processi e servizi applicativi (ad esempio la gestione della banca dati centralizzata POD/PDR) e, più in generale, per i sistemi interni al proprio dominio di responsabilità, la gestione delle misure tecniche, organizzative e procedurali.

Inoltre, il Gestore del SII:

- definisce il Piano della Sicurezza e, in particolare, il Documento Programmatico per la Sicurezza del SII;
- verifica gli esiti degli audit di sicurezza sui propri sistemi e sulle PdC degli altri Utenti;
- gestisce i servizi di sicurezza infrastrutturali di propria competenza.

In particolare, il Gestore del SII assicura i servizi di sicurezza di natura infrastrutturale relativi a:

- **Servizi di certificazione** (Gestione della PKI, con gestione delle chiavi crittografiche e dei certificati digitali).
- **Servizi di Identificazione, Autenticazione e Autorizzazione** (gestione degli accessi ai diversi sistemi funzionali, alle basi dati, agli archivi ed ai cataloghi del SII e più in generale alle risorse installate presso il Centro Servizi del SII).
- **Monitoraggio degli eventi di sicurezza sulle PdC** (raccolta e registrazione degli alert e degli eventi di sicurezza generati e trasmessi dalle PdC, analisi degli eventi di sicurezza e gestione degli incidenti e delle emergenze).
- **Verifiche e audit di sicurezza** (security assessment, test di robustezza, verifica delle configurazioni dei sistemi, verifica di integrità e di aggiornamento dei sistemi).

5.1 Servizi di Infrastruttura a Chiave Pubblica (PKI)

L'implementazione delle regole per le funzionalità di autenticazione tra PdC, integrità, riservatezza e non-ripudio dei messaggi SII scambiati, l'identificazione, autenticazione e autorizzazione dei soggetti e/o dei servizi, si basa sull'uso di certificati digitali conformi allo standard X509 v3 emessi per le varie tipologie di utilizzo previste.

I Servizi di certificazione sono sostanzialmente costituiti da:

- l'emissione dei certificati,
- la registrazione dei dati,
- l'emissione di liste di revoca e di sospensione,

- la messa a disposizione dei certificati, delle chiavi private e delle liste suddette alle PdC.

Tali servizi devono essere effettuati esclusivamente o dalla Infrastruttura a Chiave Pubblica (PKI) del SII o da Certificatori accreditati ed operanti secondo la normativa vigente.

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 di ciascun Utente che richiede l'adesione al SII, individuano e trasmettono le generalità dei Responsabili delle PdC e loro degli eventuali delegati autorizzati alla trasmissione delle richieste per la generazione dei certificati e le altre operazioni di gestione (anche detti Referenti).
Fase 2	Trasmissione delle richieste I Referenti inoltrano le richieste secondo le procedure previste dalla PKI SII e che dipendono dalla tipologia di certificato emesso.
Fase 3	Verifica dei dati delle informazioni Le informazioni contenute nella richiesta sono verificate secondo le procedure prefissate. In caso di riscontro di anomalie si riparte dalla Fase 2.
Fase 4	Registrazione dei dati, generazione delle coppie di chiavi Il superamento della fase di verifica è la condizione per la registrazioni dei dati e la generazione delle coppie di chiavi e la loro comunicazione al richiedente.
Fase 5	Emissione dei certificati secondo gli scopi previsti Sono generati i certificati digitali, contenenti le chiavi pubbliche e i dati verificati e registrati.
Fase 6	Pubblicazione dei certificati I certificati digitali sono resi pubblici mediante memorizzazione su server pubblico e notifica al richiedente.
Fase 7	Gestione (Sospensione/ Revoca/Rinnovo) dei certificati Eventi temporali successivi alla generazione possono comportare operazioni 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 finali e la comunicazione delle chiavi generate.

5.1.2 Servizi di gestione delle chiavi e dei certificati

La gestione dei certificati deve comprendere tutti gli aspetti tecnici ed amministrativi inerenti l'utilizzo da parte dei sottoscrittori autorizzati ed operanti nell'ambito del SII.

La gestione dei certificati deve comprendere le seguenti funzionalità:

- **Emissione di nuovi certificati.** L'emissione deve avvenire in base alle informazioni di registrazione fornite alla PKI SII. I certificati dovranno contenere le informazioni previste e strutturate in modalità tale da essere aderenti a quanto previsto dai documenti pubblicati dal Gestore del SII.

- **Rinnovo dei certificati.** I certificati che non siano finalizzati alle chiavi di certificazione dovranno avere una validità da uno a tre anni. Alla scadenza, il certificato deve essere rinnovato in base alle indicazioni fornite all'atto dell'emissione.
- **Revoche dei certificati.** Chi è autorizzato secondo i CPS (Certificate Practice Statement) del SII 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 firmato digitalmente dalla CA del SII, utilizzando una chiave privata dedicata esclusivamente alla sottoscrizione delle liste di revoca e di sospensione dei certificati. Dopo che un certificato è stato inserito su una lista di revoca, tutti i documenti/messaggi firmati o cifrati con la chiave privata legata alla chiave pubblica contenuta nel certificato, successivamente alla data di revoca, perdono ogni validità.
- **Sospensione dei certificati.** Chi è autorizzato secondo i CPS (Certificate Practice Statement) può chiedere la sospensione di un certificato secondo le procedure approvate. A fronte di tale evento, il certificato è inserito nelle liste di sospensione ed è firmato digitalmente dalla CA del SII, utilizzando una chiave privata dedicata esclusivamente alla sottoscrizione delle liste di revoca e di sospensione dei certificati. Un certificato sospeso può, in un momento successivo, essere riattivato.
- **Liste dei certificati revocati e sospesi.** Tutti i certificati emessi dalla PKI SII, 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 finali per mantenere aggiornate le informazioni a loro disposizione.
- **Archivio dei certificati scaduti.** E' necessaria la gestione di un archivio permanente di certificati. Tutti i certificati emessi dalla CA del SII, le CRL e le CSL devono essere gestiti per almeno 5 anni.
- **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. 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.
- **Logging ed auditing.** Si deve realizzare e gestire un servizio di logging ed auditing 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 Profilo dei certificati emessi

La PKI SII deve emettere certificati per le seguenti tipologie:

- (1) Certificato AC radice generato dal Gestore del SII per la PKI SII: utilizzato per sottoscrivere i certificati per l'autenticazione delle PdC, i certificati di firma XML, i certificati per la cifratura dei messaggi.
- (2) Certificati per la firma XML dei messaggi SII: utilizzati per garantire l'autenticità e l'integrità dei messaggi SII scambiati e per la completezza ed integrità dei messaggi applicativi archiviati.
- (3) Certificati di autenticazione dei sistemi/applicazioni in modalità client e server (PdC): utilizzati per supportare i protocolli SSL/TLS.
- (4) Certificati di autenticazione di persone fisiche (utenti finali e amministratori): utilizzati per il riconoscimento degli utenti nei confronti dei sistemi di accesso.
- (5) Certificati di crittografia: utilizzati per la cifratura di dati e/o documenti e/o messaggi scambiati nel SII.

I Certificati di firma digitale eventualmente utilizzati per la sottoscrizione dei documenti secondo la normativa vigente non sono emessi dalla PKI del SII ma devono essere certificati di firma digitale qualificati conformi alla Direttiva europea 1999/93/CE e alla normativa nazionale in materia.

5.2 Servizi di Identificazione, autenticazione e autorizzazione

Il Sistema di Identificazione, autenticazione e autorizzazione è installato e gestito nel Centro Servizi del SII e assicura i seguenti requisiti:

- essere conforme ai requisiti di sicurezza richiesti dalle normative vigenti, ivi comprese le norme sul trattamento dei dati personali di cui al Decreto Legislativo 196/2003 e successive modificazioni (sistemi di autenticazione, sistemi di autorizzazione, ecc.);
- essere indipendente dai sistemi operativi ed applicativi utilizzati e dalle architetture di rete, e deve prevedere diversi profili, a seconda degli strumenti ritenuti più idonei dal Gestore del SII rispetto alle specifiche esigenze;
- essere realizzato attraverso l'adozione di sistemi che garantiscano la conformità con lo standard SAML 2.0;
- assicurare un sistema di autenticazione univoca (operatività in modalità Single Sign-ON);
- consentire la gestione (attribuzione, sospensione, modificazione, revoca e cancellazione) dei privilegi di accesso ai sistemi secondo le direttive e sotto la supervisione del Responsabile del Gestore del SII;

- consentire di ricondurre a soggetti correttamente identificati, autenticati ed autorizzati ogni operazione effettuata sui sistemi;
- prevedere la gestione delle infrastrutture hardware e software necessarie ai fini del riconoscimento degli elementi di identificazione ed autenticazione dell'entità (credenziali). Per gli utenti finali devono essere gestite almeno le credenziali basate su:
 1. UserID-Password.
 2. Smart card nominative contenenti certificati digitali associate ad un PIN.

Per i l'identificazione e autenticazione dei Sistemi devono essere gestite almeno le credenziali basate su:

1. URI e certificati digitali.

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

Il servizio include tutte le attività che consentano al Gestore del SII di gestire l'intero ciclo di vita della richiesta, quali, ad esempio, la registrazione della richiesta, la profilazione delle utenze con riferimento alle autorizzazioni, la distribuzione dei dispositivi di accesso, l'assistenza agli utenti finali, la revoca/sostituzione dei dispositivi, l'applicazione di policy di gestione degli strumenti di accesso, delle password, nonché il rilascio di materiale informativo periodico.

L'erogazione del servizio comprende le seguenti attività:

- attivazione e gestione della infrastruttura hardware e software dedicata alla erogazione del servizio;
- attività di registrazione e gestione delle richieste di accesso (log);
- attività di generazione, ossia procedure per definire le categorie degli utenti finali, assegnare gli utenti finali alle categorie, attribuire acronimi identificativi univoci ai soggetti indicati dal Gestore, etc.;
- attività di produzione e distribuzione controllata degli strumenti per consentire il riconoscimento degli utenti finali (credenziali utente riportate in buste sigillate, gestione primo accesso ai sistemi, cambio delle credenziali, generazione certificati digitali, distribuzione smart card e lettori, etc.);
- attività per la definizione dei profili di accesso ai sistemi e per l'attribuzione di privilegi complessivi (autorizzazioni) e loro revoca parziale/totale;
- attività di gestione delle utenze, ossia procedure e criteri per il mantenimento dei registri di accesso ai sistemi (imputabilità);

- manutenzione ordinaria ed evolutiva;
- help desk di secondo livello e supporto tecnico agli utenti finali.

5.3 Monitoraggio degli eventi di sicurezza

Il servizio consiste nella gestione degli incidenti di sicurezza che causano rallentamenti e difficoltà per la normale operatività, provvedendo all'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 la massima flessibilità di utilizzo.

Il servizio si basa sul presidio, mediante un cruscotto di monitoraggio e controllo, del corretto funzionamento del SII e fornisce supporto per la risoluzione degli incidenti, con operatività H24.

Il cruscotto provvede alla raccolta ed all'analisi dei messaggi diagnostici e degli Alert su eventi di sicurezza provenienti dalle PdC degli Utenti e dal Centro Servizi presso il Gestore.

Il servizio può essere anche attivato con una richiesta diretta dei responsabili della sicurezza degli Utenti, effettuata su richiesta telefonica o via mail, verificando nell'immediato se il problema può essere risolto in remoto.

Il servizio include:

- il 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);
- la raccolta delle notifiche degli incidenti di sicurezza;
- la verifica del livello di criticità degli incidenti di sicurezza;
- il coordinamento della risposta agli incidenti e del successivo processo di ripristino;
- il mantenimento di un archivio relativo agli incidenti e alle contromisure intraprese;
- la collaborazione nel processo formativo sulla sicurezza e sulla consapevolezza dei rischi tramite seminari ed incontri periodici con i Soggetti.

5.4 Security assessment

Obiettivo del servizio è predisporre un documento di assessment delle vulnerabilità accertate, che indichi anche le possibili contromisure, che possa consentire all'Utente di verificare l'adeguatezza della politica di sicurezza implementata.

Il servizio fa parte dell'attività di auditing e mira ad analizzare l'esposizione al rischio di attacchi alla sicurezza delle PdC.

Il servizio comprende 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 dei sistemi della PdC a determinati attacchi informatici simulati (penetration testing).

Il servizio, più in generale, comprende anche la verifica degli aspetti architetturali, logici e fisici che possono influenzare il corretto funzionamento della PdC.