

ARCHITETTURA DI SICUREZZA DELL'INA

Sommario:

- 1. Scopo e campo di applicazione**
- 2. Glossario**
- 3. Premessa**
- 4. Architettura di cooperazione e sicurezza del CNSD applicata all'INA**
 - a. Infrastruttura di cooperazione e sicurezza «Backbone» 3**
 - b. Sistema di Monitoraggio dei servizi: Allarmi sicurezza e allarmi servizi**
 - Allarmi sicurezza**
 - Allarmi servizi**
- 5. Misure di sicurezza garantite dall'infrastruttura di cooperazione e sicurezza Backbone**

1. Scopo e campo di applicazione.

Il presente disciplinare tecnico allegato al nuovo regolamento di gestione dell'INA descrive l'architettura di sicurezza prevista per l'accesso ai servizi del CNSD e le relative misure di sicurezza.

2. Glossario.

Le componenti di sicurezza, descritte nello specifico capitolo, sono le seguenti:

INA: Indice Nazionale delle Anagrafi;

SAIA: Sistema di Accesso ed Interscambio Anagrafico;

CNSD: Centro Nazionale per i Servizi Demografici;

SPC: Sistema Pubblico di Connettività;

Backbone CNSD/INA.: Infrastruttura di sicurezza del CNSD e dell'Indice Nazionale delle Anagrafi, che certifica lo scambio e l'integrità del contenuto informativo tra i soggetti fornitori e/o fruitori di cui all'art. 5, comma 1, del Regolamento di gestione n. 240/2005;

Modulo Porta di Accesso-Backbone Ente (SS_BKPDD ENTE): modulo della Porta di Dominio dell'Ente; è il sistema, all'interno dell'Ente, abilitante per l'accesso in rete ai servizi applicativi del CNSD. Porta di Dominio del CNSD: Porta di Dominio del CNSD, qualificata DigitPA, comprensiva del «modulo Porta di Accesso Backbone CNSD» (SS_BKPDD CNSD), sistema di sicurezza del CNSD che abilita e gestisce l'accesso ai domini applicativi del CNSD per gli Enti che utilizzano il Sistema Pubblico di Connettività; Porta di Dominio dell'Ente: Porta di Dominio dell'Ente, qualificata DigitPA, che si interfaccia da un lato con il Modulo «Porta di Accesso-Backbone CNSD» presso l'Ente (modulo SS_BKPDD ENTE) per l'invocazione dei servizi applicativi del CNSD da parte degli applicativi interni all'Ente e dall'altro con la Porta di Dominio del CNSD per l'accesso a tali servizi;

Porta di Accesso ai Domini Applicativi del CNSD: è il sistema di sicurezza del CNSD che abilita e gestisce l'accesso ai domini applicativi del CNSD per gli Enti che non utilizzano il Sistema Pubblico di Connettività. Porta di Accesso Comunale: la «Porta di Accesso ai Domini Applicativi del CNSD» situata presso il Comune; rappresenta il solo sistema, presente presso il Comune, abilitato all'accesso in rete ai servizi applicativi del CNSD.

Porta di Accesso Ente: la «Porta di Accesso ai Domini Applicativi del CNSD» situata presso l'Ente; rappresenta il solo sistema, presente presso l'Ente, abilitato all'accesso in rete ai servizi applicativi del CNSD. Utilizzata dagli Enti che ancora non utilizzano il Sistema Pubblico di Connettività. Sistema di monitoraggio, tracciatura e allarme: sistema di vigilanza informatica del Ministero dell'Interno in grado di assicurare, per l'intera filiera di comunicazione, il controllo della sicurezza, la tutela della riservatezza, la gestione degli allarmi e la misura della qualità dei servizi del CNSD.

3. Premessa.

Presso Il CNSD, Centro nazionale per i Servizi Demografici, operano i servizi anagrafici del Dipartimento degli Affari Interni e Territoriali del Ministero dell'Interno.

I servizi anagrafici del CNSD rappresentano un sistema complesso di cooperazione a garanzia della circolarità anagrafica tra diverse Amministrazioni il cui fulcro principale è l'Indice Nazionale delle Anagrafi (INA), realizzato con strumenti informatici nel rispetto delle regole tecniche concernenti il sistema pubblico di connettività.

Il modello organizzativo del CNSD, il modello di cooperazione e di circolarità anagrafica, nonché la sicurezza e tutela della privacy si basano sui seguenti presupposti:

Da un punto di vista normativo:

Decreto legislativo n. 82/2005 e successive modificazioni e integrazioni

Circolare n. 23/2005 del 20 giugno 2005 e relativo allegato tecnico

D.M. 2 agosto 2005 sulla sicurezza: Gazzetta Ufficiale n. 218 del 19 settembre 2005 - supplemento ordinario n. 155

Piano di Sicurezza Comunale

Piano di Sicurezza del CNSD

D.M. n. 240/2005

Convenzioni con gli enti centrali per i processi di circolarità anagrafica

Schema di CONVENZIONE tra il MINISTERO DELL'INTERNO e la REGIONE ... per il collegamento all'INDICE NAZIONALE DELLE ANAGRAFI (I.N.A.) approvato dalla Conferenza Unificata nella seduta del 10 febbraio 2011

Accordi di servizio, in aggiunta alle Convenzioni, per gli enti che adottano SPC

Da un punto di vista tecnico:

Architettura di sicurezza della Porta di Accesso e del protocollo Backbone e relativa regolamentazione tecnica

Architettura di sicurezza per l'integrazione del protocollo Backbone nelle Porte di Dominio degli enti che adottano SPC, coerentemente con il modello di sicurezza del SPC

Indicazioni tecniche per la connessione delle Regioni e Province Autonome al CNSD - allegato allo schema di CONVENZIONE tra il MINISTERO DELL'INTERNO e la REGIONE ... per il collegamento all'INDICE NAZIONALE DELLE ANAGRAFI (I.N.A.) - approvate dalla Conferenza Unificata nella seduta del 10 febbraio 2011.

Grazie ad una grande flessibilità allo stato attuale il CNSD vede, contemporaneamente, enti connessi su SPC con Porta di Dominio integrata con Modulo Porta di Accesso-Backbone, denominato «modulo SS_BKPDD», (tipicamente le Regioni e alcuni enti centrali) ed enti (tipicamente i Comuni e i primi enti centrali collegati), connessi tramite l'architettura, definita nei regolamenti tecnici richiamati, basata su «Porta di Accesso» e protocollo di sicurezza «Backbone».

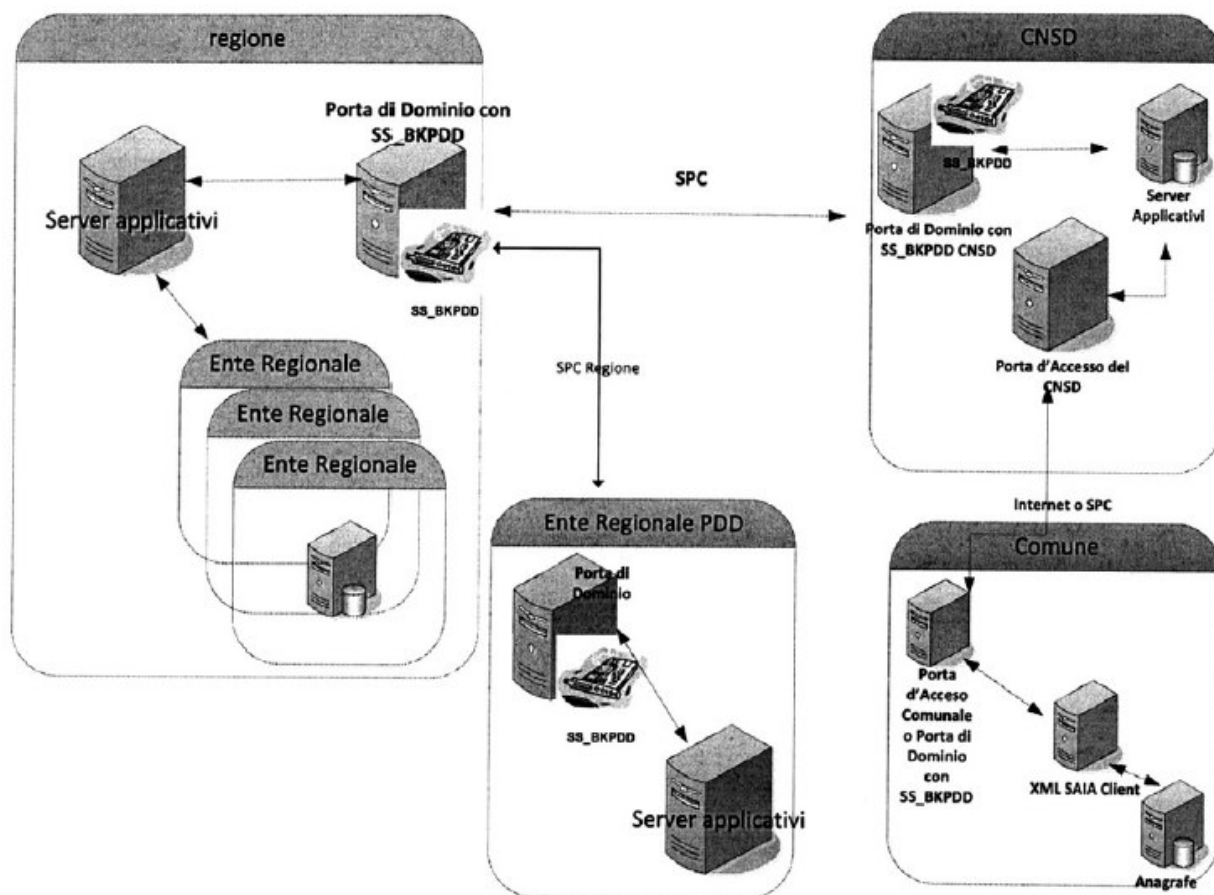
Per utilizzare il Sistema Pubblico di Connettività e nel contempo rispettare gli stringenti requisiti di sicurezza e privacy del CNSD il protocollo Backbone è stato integrato in SPC realizzando un «modulo plug-in» della Porta di Dominio denominato SS_BKPDD CNSD (per la Porta di Dominio del CNSD qualificata DigitPA) e SS_BKPDD ENTE (per la Porta di Dominio qualificata DigitPA degli enti che si connettono al CNSD per i processi di circolarità anagrafica). Il modulo SS_BKPDD ENTE viene fornito dal Ministero dell'interno a tutti gli enti dotati di Porta di Dominio che sottoscrivono la convenzione e il relativo accordo di servizio con il Ministero stesso per i processi di circolarità anagrafica. La relativa architettura è descritta nell'allegato tecnico allo schema di Convenzione tra il Ministero dell'interno e le Regioni per il collegamento all'Indice Nazionale delle Anagrafi approvato ufficialmente il 10 febbraio 2011 dalla Conferenza Unificata. A tendere, in relazione al grado di evoluzione e dispiegamento del SPC e delle relative regole tecniche e di sicurezza, l'infrastruttura INA utilizzerà pienamente tale sistema, prevedendo anche l'interfacciamento del sistema di sicurezza INA CNSD per fornire informazioni di monitoraggio al CERT-SPC.

4. Architettura di cooperazione e sicurezza del CNSD applicata all'INA.

L'architettura di cooperazione e sicurezza del Ministero dell'interno presso il CNSD si basa sull'infrastruttura di intermediazione, cooperazione e sicurezza «Backbone» che provvede a garantire la cooperazione applicativa, la sicurezza, la protezione dei dati e la tutela della privacy, per una molteplicità di servizi informativi utilizzati da PA centrali, PA locali ed Enti.

Tale coordinamento e composizione dei servizi erogati online dal CNSD è sostenuto, inoltre, dal Sistema di monitoraggio, tracciatura e allarme.

Il Backbone utilizza un protocollo che separa nettamente la componente applicativa da quella di autenticazione e da quella di gestione del trasporto delle informazioni associate ai servizi applicativi. La figura seguente schematizza l'architettura di cooperazione e sicurezza del CNSD.



Nella figura la Regione rappresenta un esempio tipico di ente connesso al CNSD per i processi di circolarità anagrafica. La stessa architettura viene utilizzata dagli enti centrali autorizzati ai processi di circolarità anagrafica in quanto la logica di funzionamento rimane identica.

Presso la Porta di Dominio dell'ente connesso con il CNSD è presente il modulo SS_BKPDD ENTE, mentre presso il CNSD è presente il modulo SS_BKPDD CNSD della Porta di Dominio del CNSD; tali componenti costituiscono l'infrastruttura di sicurezza Backbone per la gestione della sicurezza delle comunicazioni tra Regione e CNSD.

Presso i Comuni e alcuni enti centrali l'architettura di sicurezza per l'accesso al CNSD si può basare, invece che su Porta di Dominio integrata con modulo SS_BKPDD, anche sulla Porta di Accesso Comunale ai domini applicativi del CNSD (d'ora in avanti anche «Porta di Accesso») e sul canale sicuro Backbone per la comunicazione su rete Internet. In ogni caso la logica di funzionamento rimane identica e le funzionalità e le misure di sicurezza assicurate dall'infrastruttura di cooperazione e sicurezza «Backbone» sono uguali per cui, nel seguito, non si faranno distinzioni.

a. Infrastruttura di cooperazione e sicurezza «Backbone».

Tutti i servizi applicativi afferenti al CNSD vengono incapsulati in un canale di autenticazione e autorizzazione basato sull'infrastruttura di cooperazione e sicurezza «Backbone» che controlla i permessi di Accesso alle singole componenti applicative del soggetto che ha effettuato l'autenticazione sulla postazione dotata di Backbone. Si tratta di una autenticazione all'infrastruttura di sicurezza «Backbone» del CNSD che gestisce i profili di autorizzazione di tutti i servizi applicativi del CNSD e non di una semplice autenticazione al sistema operativo della postazione. Il Backbone consente infatti di individuare la terna «postazione-utente-servizio» tramite una gestione delle credenziali che assicura la possibilità di individuare quale utente da quale postazione è stato autenticato per usare un determinato servizio applicativo. Anche la postazione viene autenticata tramite un identificativo univocamente associato alla postazione stessa. In particolare per ogni postazione viene creato un identificativo hardware «Backbone» che consente di associare univocamente la postazione all'ente cui è assegnata. L'identificativo è costituito da una chiave hardware univoca creata nel momento della inizializzazione e abilitazione della postazione.

Utilizzando il Sistema di monitoraggio, tracciatura e allarme è possibile associare i flussi applicativi ai profili di autorizzazione nonché verificare la conformità del flusso rispetto agli schemi applicativi (ad esempio XSD)

e relativi tracciati record. I server applicativi hanno necessità di riconoscere il tipo di flusso in funzione del servizio applicativo e di un identificativo ad esso associato. A tal fine l'identificativo serve a distinguere la versione del software utilizzato sulla postazione per erogare uno specifico servizio. Ogni versione di software applicativo ha un identificativo diverso. L'identificativo viene utilizzato dal sistema di Sistema di monitoraggio, tracciatura e allarme per classificare univocamente ciascuna transazione.

I servizi di autenticazione e autorizzazione dell'infrastruttura sono gestiti dal Backbone. Il Backbone incapsula i servizi applicativi nel canale di autenticazione e autorizzazione secondo il seguente paradigma di funzionamento:

La componente di Accesso del Backbone («Porta di Accesso» di front end oppure la Porta di Dominio integrata con modulo «Backbone» SS-BKPDD) verso un punto di cooperazione con un ente che accede ai servizi del CNSD viene definita sulla base di uno o più procedimenti amministrativi che determinano la necessità di cooperazione tra l'organizzazione e il Ministero dell'interno. La Porta di Accesso (o modulo SS-BKPDD della Porta di Dominio) consente quindi di assicurare la corrispondenza selettiva dei profili di autorizzazione sia degli enti, sia degli incaricati, sia dei punti di Accesso utilizzati per usufruire dei servizi applicativi relativi ai procedimenti. Infatti la Porta di Accesso (o modulo SS-BKPDD della Porta di Dominio) è definita attraverso un servizio di autenticazione che identifica l'amministrazione che coopera con il Ministero dell'interno, determina in modo univoco e certifica il punto di origine della comunicazione e associa al punto di origine le credenziali che definiscono in modo univoco il responsabile della sicurezza del dispositivo fisico presso il quale è situata la componente di front end del Backbone della Amministrazione che coopera con il Ministero dell'interno.

L'accesso al servizio applicativo esposto dal Ministero dell'interno-CNSD prevede che la richiesta venga consegnata all'agente di sicurezza Backbone presso il dispositivo (Porta di Accesso o modulo SS-BKPDD della Porta di Dominio) che risiede presso l'unità organizzativa dell'ente abilitato a cooperare con il Ministero dell'interno.

La componente Backbone verifica che il servizio applicativo appartenga ai profili di autorizzazione consentiti per quella Porta di Accesso (o modulo SS-BKPDD della Porta di Dominio). Questi profili di autorizzazione consentono di discriminare la tipologia di servizi applicativi cui l'ente è stato abilitato e le caratteristiche di utilizzo di tali servizi ad esso riservate.

Una volta consegnata alla Porta di Accesso (o modulo SS-BKPDD della Porta di Dominio), la componente di richiesta del servizio applicativo e i dati ad essa associati vengono crittografati con algoritmo a standard RSA 2048 bit e incapsulati dall'agente di sicurezza Backbone in una apposita struttura per il servizio di invio su rete. La struttura, crittografata attraverso un sistema di cifratura simmetrica con mutua autenticazione dei peer, basato sul profilo dei servizi applicativi e delle credenziali delle postazioni, viene quindi inviata al CNSD su canale di comunicazione SSL. I certificati client e server necessari per la mutua autenticazione sono emessi dalla Certification Authority del CNSD.

L'agente di sicurezza Backbone invia le comunicazioni solo dopo aver verificato la corretta corrispondenza dell'insieme di regole di sicurezza che gli sono assegnate. Tra queste regole si hanno il controllo:

dell'identificativo hardware «Backbone» della postazione di lavoro

della corrispondenza tra username e password e identificativo hardware «Backbone» della postazione di lavoro

della corretta attivazione, tramite username e password, della postazione di lavoro connessa al backbone

dello stato di abilitazione/disabilitazione della postazione di lavoro

dello stato di abilitazione/disabilitazione dell'utente

dell'abilitazione dell'utente alla transazione in rete richiesta

dell'abilitazione della postazione di lavoro alla transazione in rete richiesta

della presenza di specifici attributi nella transazione in rete richiesta.

Il servizio di invio associa alla struttura crittografata alcune informazioni necessarie a caratterizzare la richiesta come ad esempio il nome del servizio applicativo incapsulato, gli identificatori del punto di Accesso e dell'organizzazione associata.

Nel caso di un Comune abilitato all'accesso ai servizi anagrafici del CNSD con 3 postazioni riconosciute e certificate il sistema di autorizzazione prevede di identificare l'ente richiedente (il Comune), la postazione da cui è stata fatta la richiesta (una delle 3 postazioni riconosciute) oltre alle credenziali di autenticazione del richiedente. La struttura crittografata viene identificata al momento della ricezione presso la corrispondente componente Backbone del CNSD.

La componente Backbone presso il CNSD quando riceve la struttura crittografata verifica, sulla base delle credenziali, che il punto di invio e l'utente fossero autorizzati ad effettuare quella comunicazione, verifica l'integrità della struttura crittografata e quindi la decifra. In base al nome del servizio applicativo la componente Backbone consegna la struttura decifrata al servizio applicativo deputato al trattamento. Si rimanda alla Circolare del Dipartimento per gli affari interni e territoriali n. 23/2005 del 20 giugno 2005 e al D.M. 2 agosto 2005 sulla sicurezza (Gazzetta Ufficiale n. 218 del 19 settembre 2005 - Supplemento Ordinario n. 155) per i dettagli relativi alle procedure di attivazione e di gestione.

L'infrastruttura di cooperazione e sicurezza «Backbone» fornisce inoltre, per tutti i servizi applicativi afferenti al CNSD, le seguenti funzioni:

Certificazione del punto di origine e destinazione delle comunicazioni tra ente e CNSD:

identificazione univoca del sistema informatico che rappresenta il punto di origine della comunicazione dell'ente verso l'INA

associazione in modo certo e sicuro del sistema informatico all'ente abilitato

Erogazione dei servizi applicativi ai soli sistemi abilitati:

Identificazione certa dei sistemi informatici dell'ente abilitati ad accedere ai servizi applicativi del CNSD

Protezione dei flussi informativi scambiati con l'ente

Riservatezza delle informazioni tramite cifratura dei flussi

Certificazione dei flussi applicativi tramite firma dei flussi con algoritmo di firma digitale che utilizza i certificati emessi dalla Certification Authority del CNSD.

L'architettura di sicurezza per l'accesso al CNSD si basa sul canale sicuro Backbone per la comunicazione su rete, sulla «Porta di Accesso», sui moduli SS_BKPDD CNSD e SS_BKPDD ENTE che si integrano rispettivamente nella Porta di Dominio del CNSD e nella Porta di Dominio dell'Ente connesso. L'architettura è stata integrata con il Sistema Pubblico di Connettività e cooperazione (SPC) definito dal Codice dell'Amministrazione Digitale e dalle Regole Tecniche (cfr. Decreto legislativo n. 235/10 del 31 dicembre 2010 e decreto del Presidente del Consiglio dei Ministri del 1° aprile 2008), e, a tendere, sarà previsto l'interfacciamento con il CERT-SPC.

La logica architettureale è basata su un sistema di agenti di natura adattiva. Ciò vuol dire che ogni agente è in grado di utilizzare regole di sicurezza diverse in funzione del servizio applicativo. L'infrastruttura di cooperazione e sicurezza Backbone si avvale di agenti di sicurezza che hanno funzionalità di configurazione e gestione dei formati di sicurezza dei dati e dei relativi flussi, per ciascun servizio applicativo, entranti/uscenti dalle postazioni protette da Backbone. Se il servizio è di consultazione allora l'agente controlla solo le credenziali di autenticazione. Se il servizio applicativo permette il trattamento di informazioni l'agente costruisce anche un hash dei flussi di comunicazione per controllare che l'hash dei dati inviati dal client corrisponda all'hash dei dati ricevuti dal server.

Se il servizio riguarda l'aggiornamento del software applicativo sulla postazione l'agente verifica anche che la versione del servizio applicativo in uso presso la postazione abbia un identificativo corrispondente a quello dell'aggiornamento ricevuto e che l'hash del software di aggiornamento corrisponda a quello di uno dei software di aggiornamento catalogati come autorizzati per accedere ai servizi del CNSD tramite infrastruttura di cooperazione e sicurezza «Backbone».

Inoltre gli agenti di sicurezza, per ogni transazione in rete verso un peer/server, si fanno carico di cifrare i dati e di inviarli verso il peer/server su un canale di comunicazione SSL secondo le modalità sopra specificate.

L'infrastruttura di cooperazione e sicurezza Backbone si avvale inoltre di agenti di cooperazione distribuiti che forniscono funzionalità di configurazione e gestione di protocolli di cooperazione specifici al fine di garantire modalità di cooperazione omogenee ed uniformi sia su SPC che su Internet.

b. Sistema di Monitoraggio dei servizi: Allarmi sicurezza e allarmi servizi

Allarmi sicurezza.

L'infrastruttura di sicurezza del CNSD include un sistema di monitoraggio e allarme che consente, relativamente alla sicurezza, di controllare le seguenti informazioni:

Monitoraggio, documentazione e certificazione delle transazioni:

Monitoraggio, tracciatura e notifica del funzionamento dei servizi applicativi del CNSD

Monitoraggio, tracciatura e notifica dei tentativi di Accesso illeciti ai servizi applicativi del CNSD

Monitoraggio, tracciatura e notifica di tentativi di intrusione e/o modifica dei flussi applicativi su rete

Controllo della disponibilità del servizio

Rilevazione e gestione di allarmi:

Verifica della connettività di rete al CNSD

Verifica della conformità dei flussi di rete

Verifica dei tentativi di Accesso illeciti

Verifica dei tentativi di intrusione e/o modifica dei flussi

Verifica e gestione della continuità di erogazione dei servizi applicativi

Allarmi servizi.

Il sistema di monitoraggio, tracciatura e allarme dell'infrastruttura di sicurezza del CNSD consente sia di monitorare e documentare la qualità dei servizi (tempi di risposta, disponibilità, errori, etc.) sia di rilevare allarmi relativamente all'utilizzo dei servizi ed agli adempimenti che questi comportano.

Tali rilevazioni possono essere effettuate dal sistema sia lato centrale (CNSD) sia periferico (Comuni, Regioni, prefetture). È inoltre prevista la produzione di report periodici.

Nell'header di trasmissione dei dati al CNSD attraverso il Backbone, viene inglobato un numero di protocollo che identifica il lotto di dati inviato. Per ogni lotto è possibile riconoscere il numero di comunicazioni per ogni singola tipologia di servizio classificata.

5. Misure di sicurezza garantite dall'infrastruttura di cooperazione e sicurezza Backbone.

Il presente paragrafo illustra come l'infrastruttura di cooperazione e sicurezza Backbone del CNSD, sia nella sua implementazione Porta di Accesso sia nella sua implementazione Porta di Dominio integrata con modulo Backbone SS-BKPDD, implementa le misure di sicurezza sulla base del Codice in materia di protezione dei dati personali.

Autenticazione informatica.

1. Gestione autenticazione utenti. Tutti i servizi applicativi del CNSD vengono incapsulati in un canale di autenticazione SSL basato su Backbone che controlla i permessi di Accesso alle singole componenti applicative del soggetto che ha effettuato l'autenticazione sulla postazione dotata di Backbone. Non si tratta di autenticazione al sistema operativo della postazione ma di autenticazione dell'infrastruttura di sicurezza «Backbone» del CNSD che gestisce i profili di autorizzazione di tutti i servizi applicativi del CNSD.

L'utilizzo di username e password, sul client, è direttamente sotto il controllo di un agente di sicurezza del Backbone che protegge adeguatamente la password utente cifrandola in modalità tale da evitare anche che si crei regolarità nella trasmissione di dati di autenticazione cifrati.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola «chiave» riservata conosciuta solamente dal medesimo. Sono assegnate per l'uso della postazione di accesso periferica (abilitata tramite Backbone) e permettono anche di autorizzare all'incaricato all'uso dei servizi applicativi.

3. Le credenziali per l'autenticazione della Porta di Accesso sono assegnate individualmente all'ente nella persona del responsabile della sicurezza Comunale. Il sistema Backbone consente di definire il numero massimo di utenti autorizzabili. Il responsabile può quindi richiedere l'autorizzazione per altri utenti (di norma fino a 3). È prevista un'Interfaccia per la registrazione della postazione e una interfaccia per l'abilitazione di altri utenti (da notare che l'utente può essere abilitato ai soli servizi applicativi d'interesse).

Nel caso di altro ente, diverso dal Comune, le credenziali per l'autenticazione sono consegnate al responsabile del trattamento dei dati nominato dall'ente ai sensi della convenzione stipulata tra il Ministero e l'ente stesso.

4. Il Piano di Sicurezza Comunale, verificato e approvato dagli uffici periferici (Prefettura - UTG) del Ministero definisce le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato. L'attuazione del Piano di sicurezza viene verificata nel contesto dei compiti di vigilanza del Ministero. Per gli altri enti, diversi dai Comuni, vengono adottate le specifiche cautele in uso presso gli enti stessi. È compito del responsabile del trattamento dei dati nominato dall'ente consegnare al Ministero la descrizione delle misure adottate per assicurare la segretezza della componente riservata della credenziale.

5. La parola chiave è composta da più di otto caratteri. I caratteri devono essere sia alfabetici che numerici.

6. Il Backbone consente, per alcuni servizi, l'adozione di sistemi di «autenticazione rafforzata» (password a scadenza immediata, tessere smart card dotate di Pin, credenziali digitali con scadenza prefissata o finestra temporale prefissata di validità ...) per ridurre la possibilità di usi impropri, cessione o sottrazione delle credenziali di Accesso. I servizi per cui sono stati adottati sistemi di «autenticazione rafforzata» riguardano il sistema CIE. Per altri servizi possono essere adottati a richiesta.

7. I codici per l'identificazione non vengono assegnati ad altri incaricati, neppure in tempi diversi. I codici di identificazione delle postazioni sono protetti da cifra e cambiati dinamicamente secondo un protocollo noto solo al centro (CNSD).

8. L'informazione relativa all'ultimo utilizzo della credenziale è disponibile presso il CNSD che può decidere opportune politiche di intervento (contatto con l'utente, sollecito all'uso del sistema ...) fino ad arrivare alla disattivazione della credenziale e della postazione di Accesso. La funzione di disattivazione è attivabile dal CNSD in modo centralizzato con capillarità a livello di intero ente o di singola postazione/utente.

9. Nel caso venga nominato un nuovo responsabile della sicurezza Comunale o un nuovo responsabile del trattamento dei dati per gli altri enti (quindi il precedente perde la qualità che gli consente l'accesso ai dati) le credenziali del precedente responsabile vengono disattivate e vengono create nuove credenziali. Le credenziali assegnate non possono essere ri-assegnate.

10. Il Piano di Sicurezza Comunale, verificato e approvato dagli uffici periferici (Prefettura - UTG) del Ministero definisce le necessarie cautele relativamente alle procedure adottate per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

Per gli altri enti, diversi dai Comuni, vengono adottate le specifiche cautele in uso presso gli enti stessi. Il sistema Backbone attualmente permette di tracciare dal centro la durata del fermo dell'operatività delle postazioni periferiche collegate.

11. In caso di prolungata assenza dell'incaricato le sue funzioni vengono svolte con altre credenziali create dal responsabile per altri soggetti (normalmente fino ad un massimo di 3 postazioni e 3 soggetti per ente a meno che non sia diversamente specificato in convenzione o esplicitamente richiesto e autorizzato).

12. Le misure di cui ai punti precedenti non si applicano ai dati destinati alla libera diffusione.

Autorizzazione.

13. L'infrastruttura di sicurezza «Backbone» del CNSD gestisce i profili di autorizzazione per tutti i servizi applicativi del CNSD.

14. L'infrastruttura di sicurezza «Backbone» fornisce un sistema di autorizzazione che consente di identificare l'ente richiedente, la postazione da cui è stata fatta la richiesta oltre alle credenziali di autenticazione del richiedente (normalmente fino ad un massimo di 3 postazioni e 3 soggetti per ente a meno che non sia diversamente specificato in convenzione o esplicitamente richiesto e autorizzato). La configurazione delle postazioni e dei profili di autorizzazione viene effettuata preventivamente all'autorizzazione ad accedere ai servizi del CNSD. Vengono configurati i soli servizi del CNSD cui l'ente ha diritto di accedere. In tale insieme si può anche limitare l'autorizzazione di Accesso di una specifica postazione e/o utente ad un sotto-insieme di servizi.

15. Periodicamente viene rinnovata la convenzione verificando che l'ente mantenga i diritti di accedere ai servizi. La tempestiva disabilitazione all'accesso del personale adibito ad altre mansioni o non più in servizio e l'adeguamento costante dei profili di autorizzazione è attuata in funzione delle nomine dei Responsabili. Nel caso venga nominato un nuovo Responsabile (quindi il precedente perde la qualità che gli consente l'accesso ai dati) le credenziali del precedente responsabile vengono disattivate e vengono create nuove credenziali. Le credenziali assegnate non possono essere ri-assegnate.

Profilatura, monitoraggio, tracciatura e allarme.

16. Gestione profilatura utenti. Utilizzando il Sistema di monitoraggio, tracciatura e allarme è possibile associare i flussi applicativi ai profili di autorizzazione nonché verificare la conformità del flusso rispetto agli schemi applicativi (ad esempio XSD) e relativi tracciati record. I server applicativi hanno necessità di riconoscere il tipo di flusso in funzione del servizio applicativo e di un identificativo ad esso associato. A tal fine l'identificativo serve a distinguere la versione del software utilizzato sulla postazione per erogare uno specifico servizio. Ogni versione di software applicativo ha un identificativo diverso. L'identificativo viene utilizzato dal sistema di Sistema di monitoraggio, tracciatura e allarme per classificare univocamente ciascuna transazione.

17. Il Backbone rende disponibile un sistema di certificazione digitale e di censimento delle postazioni terminali dai quali si ha accesso ai dati realizzato tramite il Backbone e il modulo SS_BKPDD delle Porte di Dominio. Le postazioni vengono censite tramite l'identificativo Backbone che consente di associare univocamente la postazione all'ente cui è assegnata impedendo accessi da postazioni non dell'ente. Con modalità analoghe viene assicurata la certificazione digitale dei server del CNSD. Viene assicurata la certificazione del punto di origine e di destinazione dei flussi relativi alle transazioni (matrice origine-destinazione). La rappresentazione in tempo reale di tutti i flussi tra gli enti abilitati e il CNSD viene assicurata da un apposito «Cruscotto di tracciatura, monitoraggio e allarme» a disposizione del Ministero. In caso di necessità può essere dispiegata la funzione per disabilitare l'intera postazione oppure per disattivare un sotto-insieme di servizi applicativi selezionando il servizio o i servizi da disabilitare sulla specifica postazione.

18. Gli accessi contemporanei con medesime credenziali sono tracciati. In ogni caso è sempre conosciuto l'identificativo Backbone univoco della postazione origine e quindi è discriminata l'identità digitale delle postazioni che accedono al sistema. Se necessario è possibile dispiegare la funzione che impedisce l'accesso di una postazione se la credenziale che si sta usando è già usata da un'altra postazione.

19. Gli accessi non conformi a quanto stabilito nelle convenzioni o nei regolamenti e disposizioni del Ministero vengono tracciati e rifiutati. È possibile disabilitare, manualmente, una postazione se si rileva un eccesso di tentativi di accesso non conformi. Se necessario è possibile dispiegare la funzione che permette di disabilitare, in modo automatico, (momentaneamente o permanentemente) una postazione se i tentativi di accesso non conformi si presentano con una frequenza che supera una soglia prefissata.

20. Il Backbone e i suoi «agenti di sicurezza» consentono il tracciamento degli utenti che accedono via web, via web services e altri protocolli applicativi. Un apposito Cruscotto di monitoraggio, tracciatura e allarme consente di rappresentare sia il normale funzionamento del sistema sia le anomalie che si dovessero presentare rispetto alle normali regole di cooperazione e interscambio dei dati definite tra le parti. Se necessario è possibile dispiegare la funzione che permette di limitare quantitativamente e/o qualitativamente gli accessi e le interrogazioni.

21. Il tracciamento degli utenti che accedono ai servizi del CNSD nelle diverse modalità è assicurato dagli agenti di sicurezza del Backbone. Informazioni in merito agli orari di Accesso sono disponibili a livello di infrastruttura centrale del Backbone. Se necessario è possibile dispiegare la funzione che permette, sulla

base delle informazioni disponibili, di definire profili che prevedano limitazioni orarie per gli accessi di determinate categorie di utenti.

22. Il Backbone e i suoi «agenti di cooperazione» consentono l'esatta associazione tra la postazione-utente e le informazioni accedute dall'utente tramite la postazione. È conservato il dettaglio delle informazioni a cui si è avuto accesso o che si sono aggiornate con una modalità che consente di ricostruire l'informazione esclusivamente su specifica richiesta dei soggetti titolari. Sono dunque conservate registrazioni (log) di tutte le operazioni effettuate, comprese le visualizzazioni con i riferimenti ai soggetti che hanno effettuato il trattamento e con l'indicazione della data, dell'orario e dei riferimenti agli interessati i cui dati sono stati trattati. Tali registrazioni sono rese accessibili solo a seguito di documentate motivazioni e solo agli incaricati del CNSD cui è associato il profilo di autorizzazione allo scopo definito. È quindi possibile associare in modo esatto l'utente, la postazione e le informazioni trattate per ciascuna transazione. In particolare è possibile tracciare quali informazioni ha trattato (inserito, aggiornato, consultato) un utente, da quale postazione, in che momento e sulla base di quale profilo autorizzativo al servizio che ha utilizzato per trattare le informazioni stesse.

23. È previsto il tracciamento delle operazioni compiute con possibilità di identificazione dell'utente (username) che accede ai dati, il timestamp, l'indirizzo IP di provenienza dell'utente e/o della postazione che rappresenta la «Porta di Accesso» o «Porta di Dominio» interconnessa, l'identificativo univoco hardware della postazione (origine della comunicazione), l'operazione effettuata e i dati trattati (tramite tecniche di hash).

24. Sono disponibili, presso il CNSD sul cruscotto di monitoraggio, tracciatura e allarme, informazioni relative all'ultima sessione effettuata con le stesse credenziali. Se necessario la funzione può essere dispiegata per renderla disponibile sulle postazioni periferiche, presentando l'informazione relativa alla data e ora dell'ultimo accesso effettuato per ciascun servizio acceduto.

25. È effettuata la ricognizione giornaliera degli enti che accedono tramite produzione del Report degli accessi effettuati da parte degli enti. Tale Report è visualizzabile tramite il Cruscotto di monitoraggio, tracciatura e allarme del CNSD anche al fine di verificare la corretta periodicità delle attività previste dalla normativa o dagli accordi tra le parti nonché il rispetto dei livelli di servizio concordati.

26. È effettuata la procedura di rilevazione e registrazione degli accessi logici (access log) ai sistemi di elaborazione e agli archivi elettronici del CNSD da parte degli amministratori di sistema come definito dal Garante per la Protezione dei dati personali.

Altre misure di sicurezza.

27. Periodicamente vengono censite le postazioni e le utenze che non accedono al sistema da un periodo troppo lungo al fine di deciderne la disabilitazione. Per le utenze di servizio presso il CNSD sono definite, nel Piano di Sicurezza del CNSD, le regole per il controllo delle liste degli incaricati per singola funzione e area del CNSD nonché le regole per il controllo del rinnovo periodico (almeno ogni 3 mesi) delle parte segreta delle credenziali.

28. I dati personali presso il centro sono adeguatamente protetti dall'infrastruttura Backbone e dalle sue tecniche di cifratura. Sono presenti anche apparati di sicurezza di rete, sia perimetrali che interni. Con cadenza almeno trimestrale ne viene effettuato il controllo e l'aggiornamento.

29. Gli aggiornamenti periodici dei programmi di elaborazione volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati con cadenza almeno trimestrale.

30. Il salvataggio dei dati avviene, in conformità con le procedure formalizzate nel Piano di Sicurezza del CNSD, con diverse modalità:

i. backup incrementale giornaliero

ii. backup completo con cadenza settimanale

iii. è prevista la procedura per la conservazione, cifrata, delle registrazioni degli accessi logici (access log) ai sistemi di elaborazione e agli archivi elettronici del CNSD da parte degli amministratori di sistema.

31. Requisiti di idoneità: Il responsabile della sicurezza Comunale è il Sindaco o un funzionario dallo stesso nominato con atto formale. Per gli altri enti il responsabile del trattamento è un dipendente nominato dall'ente stesso ai sensi della convenzione stipulata con il Ministero dell'interno per l'accesso al CNSD.

32. La gestione via web, via web services e altri protocolli applicativi dei flussi di dati avviene su canale di sicurezza Backbone che assicura un doppio livello di crittografia: del canale Backbone di comunicazione e del contenuto dei flussi che viaggiano su tale canale.

33. Sono previsti appositi accordi di servizio e stringenti requisiti di sicurezza per l'impiego di web service esposti su rete SPC al fine di impedire che i dati scambiati con il CNSD siano accessibili da altri soggetti oltre a quelli autorizzati. Per tale motivo è stato definito il modulo «Backbone» SS-BKPDD per la Porta di Dominio, modulo che implementa i protocolli di crittografia e le regole di sicurezza adottate dal Ministero dell'interno. Sono anche protette, con gli stessi protocolli di crittografia e regole di sicurezza, tutte le comunicazioni che avvengono utilizzando la rete Internet.