DECRETO 19 gennaio 2012, n. 32: Nuovo regolamento di gestione dell'Indice nazionale delle anagrafi. (12G0052)

(Gazzetta Ufficiale n. 76 del 30 aprile 2012) – **In vigore dal 14 aprile 2012.**

IL MINISTRO DELL'INTERNO
di concerto con
IL MINISTRO PER LA PUBBLICA
AMMINISTRAZIONE E LA SEMPLIFICAZIONE
e
IL MINISTRO DELL'ISTRUZIONE,
DELL'UNIVERSITA' E DELLA RICERCA

Visto l'articolo 17, comma 3, della legge 23 agosto 1988, n. 400;

Visto l'articolo 50, comma 5, del decreto-legge 31 maggio 2010, n. 78, convertito in legge 30 luglio 2010, n. 122, recante «Misure urgenti in materia di stabilizzazione finanziaria e di competitivita' economica», che prevede l'emanazione di disposizioni di armonizzazione del regolamento di gestione dell'INA, emanato con decreto del Ministro dell'interno 13 ottobre 2005, n. 240;

Vista la legge 24 dicembre 1954, n. 1228, recante «Ordinamento delle anagrafi della popolazione residente», ed in particolare l'articolo 1, comma 5, come modificato dall'articolo 1-novies del decreto-legge 31 marzo 2005, n. 44, convertito con modificazioni in legge 31 maggio 2005, n. 88, e l'articolo 1, comma 6, come modificato dall'articolo 50, comma 5, del decreto-legge 31 maggio 2010, n. 78, convertito con la legge 30 luglio 2010, n. 122;

Visto il decreto del Presidente della Repubblica 30 maggio 1989, n. 223, recante l'approvazione del nuovo regolamento anagrafico della popolazione residente;

Visto il decreto legislativo 6 settembre 1989, n. 322, recante «Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica» e successive modifiche e integrazioni;

Vista la legge 7 agosto 1990, n. 241 e successive modificazioni, recante «Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi»;

Visto il decreto-legge 15 gennaio 1993, n. 6, convertito in legge 17 marzo 1993, n. 63, recante «Disposizioni urgenti per il recupero degli introiti contributivi in materia previdenziale», e, in particolare, l'articolo 2 che disciplina lo scambio dei dati nei rapporti tra le pubbliche amministrazioni e tra queste e altri soggetti pubblici o privati, sulla base del codice fiscale quale elemento identificativo di ogni soggetto;

Visto l'articolo 2, comma 5, della legge 15 maggio 1997, n. 127 e successive modificazioni, recante «Misure urgenti per lo snellimento dell'attivita' amministrativa e dei procedimenti di decisione e di controllo»;

Visto il decreto del Presidente del Consiglio dei Ministri 22 ottobre 1999, n. 437, recante «Regolamento recante caratteristiche e modalita' per il rilascio della carta d'identita' elettronica e del documento d'identita' elettronico»;

Visto il decreto del Ministro dell'interno in data 8 novembre 2007 recante «Regole tecniche della carta di identita' elettronica»;

Visto il decreto del Ministro dell'interno in data 6 ottobre 2000, recante «Specifiche tecniche per l'allineamento dei dati contenuti nelle anagrafi comunali con quelli contenuti nell'archivio

dell'Agenzia delle entrate»;

Visto il decreto del Presidente della Repubblica 3 novembre 2000, n. 396, recante «Regolamento per la revisione e la semplificazione dell'ordinamento dello stato civile, a norma dell'articolo 2, comma 12, della legge 15 maggio 1997, n. 127;

Visto l'articolo 25 della legge 24 novembre 2000, n. 340, recante «Disposizioni per la delegificazione di norme e per la semplificazione di procedimenti amministrativi - Legge di semplificazione 1999»;

Visto il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante «Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa»;

Visto il decreto del Ministro dell'interno in data 18 dicembre 2000, recante «Modalita' di comunicazione dei dati relativi ai cittadini stranieri extracomunitari fra gli uffici anagrafici dei comuni, gli archivi dei lavoratori extracomunitari e gli archivi dei competenti organi centrali e periferici del Ministero dell'interno, nonche' le modalita' tecniche ed il termine per l'aggiornamento e la verifica delle posizioni anagrafiche dei cittadini stranieri gia' iscritti nei registri della popolazione residente;

Visto il decreto del Ministro dell'interno in data 23 aprile 2002 con il quale viene costituito presso il Dipartimento per gli Affari Interni e Territoriali - Direzione Centrale per i Servizi Demografici il Centro Nazionale per i Servizi Demografici;

Visto il decreto-legge 31 marzo 2003, n. 52, articolo 2 comma 1, convertito in legge 30 maggio 2003, n. 122, che, per il completamento dell'informatizzazione e l'aggiornamento dell'AIRE, prevede l'utilizzo dell'infrastruttura informatica di base dell'Indice Nazionale delle Anagrafi (INA);

Visto il decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali» e successive modificazioni;

Visto il decreto legislativo 7 marzo 2005, n. 82, recante «Codice dell'amministrazione digitale», e successive modificazioni;

Visto il decreto del Ministro dell'interno 2 agosto 2005, recante «Regole tecniche e di sicurezza per la redazione dei piani di sicurezza comunali per la gestione delle postazioni di emissione CIE, in attuazione del comma 2 dell'articolo 7-viciester della legge 31 marzo 2005, n. 43»;

Visto l'articolo 16-bis, del decreto-legge 29 novembre 2008, n. 185, convertito in legge 28 gennaio 2009, n. 2, recante «Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anticrisi il quadro strategico nazionale»;

Visto il decreto del Presidente della Repubblica del 7 settembre 2010, n. 166, recante il «Regolamento recante il riordino dell'Istituto nazionale di statistica»;

Visto il Regolamento (CE) 763/2008 del Parlamento europeo e del Consiglio del 9 luglio 2008 relativo ai censimenti della popolazione e delle abitazioni;

Visto il Regolamento (CE) 223/2009 del Parlamento europeo e del Consiglio dell'11 marzo 2009 relativo alle statistiche europee e che abroga il regolamento (CE, Euratom) n. 1101/2008 del Parlamento europeo e del Consiglio, relativo alla trasmissione all'Istituto statistico delle Comunita' europee di dati statistici protetti dal segreto, il regolamento (CE) n. 322/97 del Consiglio, relativo alle statistiche comunitarie, e la decisione 89/382/CEE, Euratom del Consiglio, che istituisce un comitato del programma statistico delle Comunita' europee;

Sentito l'Istituto Nazionale di Statistica, che si e' espresso con parere n. SP/559.2011 del 20 maggio 2011;

Sentito il DigitPA - Ente nazionale per la digitalizzazione della pubblica amministrazione - che si e' espresso con parere del 24 maggio 2011;

Sentito il Garante per la protezione dei dati personali, che si e' espresso con parere n. 250 del 24 giugno 2011;

Vista la nota del 20 luglio 2011 con cui il Ministero per la pubblica amministrazione e l'innovazione ha espresso il proprio concerto sullo schema di decreto;

Udito il parere n. 3703/2011 emesso dalla Sezione Consultiva per gli Atti Normativi del Consiglio di Stato nell'adunanza 27 settembre 2011;

A d o t t a
il seguente regolamento:

Art. 1
Definizioni

1. Ai fini del presente decreto verranno utilizzate le seguenti definizioni:

ISTAT: Istituto Nazionale di Statistica;

CNSD: Centro Nazionale per i Servizi Demografici;

INA: Indice Nazionale delle Anagrafi;

Backbone CNSD: Infrastruttura informatica di base dell'Indice Nazionale delle Anagrafi;

APR: Anagrafe della popolazione residente;

AIRE: Anagrafe degli Italiani Residenti all'Estero.

Art. 2
Finalita'

1. L'INA e' il sistema incardinato nell'infrastruttura tecnologica e di sicurezza del CNSD, istituito presso il Dipartimento per gli Affari Interni e Territoriali, che garantisce la disponibilita', in tempo reale, tramite i servizi di interscambio e di cooperazione di cui all'articolo 6, dei dati relativi alle generalita', alla cittadinanza, alla famiglia anagrafica e all'indirizzo anagrafico delle persone iscritte in APR e in AIRE, anche per un migliore esercizio della funzione di vigilanza e di gestione dei dati anagrafici e di stato civile.

2. L'INA fornisce i servizi di interscambio e di cooperazione di cui all'articolo 6, anche per assicurare l'allineamento e la coerenza degli archivi degli enti collegati all'INA con le anagrafi comunali.

3. Per le finalita' di cui ai precedenti commi 1 e 2, e' utilizzato anche il codice fiscale, che garantisce l'univocita' delle informazioni di cui al successivo articolo 3 del presente regolamento.

Art. 3
Caratteristiche

1. Nell'INA sono contenuti i dati che consentono la corretta ed univoca associazione tra cittadino e comune di residenza, nonche' l'acquisizione delle seguenti informazioni:

a) Cognome;

b) Nome;

c) Luogo e data di nascita;

d) Codice fiscale attribuito dall'Agenzia delle Entrate;

e) Codice ISTAT del Comune di ultima residenza e codice Istat della sezione di censimento;

f) Cittadinanza (denominazione dello Stato);

g) Famiglia anagrafica (componenti della famiglia, relazione di parentela o di affinita');

h) Indirizzo anagrafico (specie e denominazione del toponimo, numero civico, data di decorrenza della residenza).

Art. 4
Costituzione e aggiornamento

1. L'INA e' costituito ed aggiornato sulla base delle informazioni contenute nelle anagrafi di tutti i comuni italiani, con il codice fiscale validato dall'Agenzia delle Entrate.

2. A tal fine, i comuni inviano all'INA i dati di cui all'articolo 3, attraverso i servizi telematici e di sicurezza del CNSD, entro 24 ore dalla registrazione del dato in APR, secondo le istruzioni tecniche adottate dalla Direzione Centrale per i Servizi Demografici.

3. L'Ufficiale d'anagrafe e' responsabile del corretto e tempestivo invio delle informazioni anagrafiche all'INA.

4. L'interessato puo' esercitare il diritto di accesso ai dati personali contenuti nell'INA e gli altri diritti di cui all'articolo 7 del decreto legislativo 30 giugno 2003, n. 196, tramite il comune di residenza, che riscontra la richiesta.

5. Qualora i dati inviati all'INA siano errati o non aggiornati competente ad effettuarne la rettificazione o l'aggiornamento e' il comune di residenza del soggetto a cui i dati si riferiscono.

6. Qualora l'errore non sia imputabile al comune di residenza, quest'ultimo ne informa la Direzione Centrale per i Servizi Demografici per i conseguenti adempimenti ai sensi del decreto legislativo 30 giugno 2003, n. 196.

Art. 5
Soggetti fornitori e/o fruitori dei servizi

1. Ai servizi di cui all'articolo 6, e ai dati resi disponibili dall'INA accedono, in modalita' telematica, tramite il Centro Nazionale per i Servizi Demografici, secondo quanto previsto nell'allegato tecnico di cui al successivo articolo 8:

a) il Ministero dell'interno - Direzione Centrale per i Servizi Demografici, ai fini del migliore espletamento della vigilanza sulla tenuta delle anagrafi comunali e del rilascio della carta di identita' elettronica;

b) le Prefetture - Uffici Territoriali del Governo, le Questure e le altre strutture centrali e territoriali del Ministero dell'interno, per l'espletamento dei propri compiti istituzionali;

c) l'ISTAT per la produzione dell'informazione statistica ufficiale e per la verifica della qualita' statistica dei dati di fonte amministrativa, utile anche ai fini della vigilanza anagrafica;

d) l'Agenzia delle Entrate per l'attribuzione, l'aggiornamento e la validazione dei codici fiscali e per la corretta individuazione dei dati anagrafici e di residenza dei cittadini;

e) il Ministero degli affari esteri, per l'aggiornamento dell'AIRE e dell'elenco unico aggiornato dei cittadini italiani residenti all'estero, di cui all'articolo 5, comma 1 della legge 27 dicembre 2001, n. 459;

f) i Comuni, per il popolamento e l'aggiornamento dell'INA, per verificare la coerenza, a livello nazionale, dei cittadini iscritti nella propria anagrafe, rispetto ai cittadini iscritti nelle altre anagrafi comunali, fermo restando quanto previsto dalla lettera g);

g) ogni altra amministrazione pubblica in relazione a specifiche finalita' previste da legge o da regolamento;

h) gli organismi che esercitano attivita' di prelievo contributivo e fiscale o erogano servizi di pubblica utilita', di cui all'articolo 2, comma 3 del decreto-legge 15 gennaio 1993, n. 6, convertito nella legge 17 marzo 1993, n. 63, ai fini della corretta

individuazione della residenza anagrafica dei cittadini e della semplificazione del servizio pubblico.

2. L'autorizzazione per l'utilizzo dei servizi INA da parte dei soggetti di cui alle lettere b), c), d), e), g), h) del precedente comma 1, e' subordinata alle modalita' concordate con il Ministero dell'interno - Direzione Centrale per i Servizi Demografici ed individuate da un'apposita convenzione, nella quale sono specificati i presupposti di legge o di regolamento.

3. L'accesso ai dati contenuti nell'INA e' gratuito ai sensi di quanto previsto all'articolo 58 del decreto legislativo 7 marzo 2005, n. 82, salvo il riconoscimento dei costi derivanti da elaborazioni aggiuntive.

4. L'accesso ai servizi resi disponibili dall'INA e' assicurato, in collegamento telematico con il CNSD, tutti i giorni dell'anno e nell'arco dell'intera giornata.

Art. 6

Servizi di interscambio e di cooperazione

1. I servizi di interscambio e di cooperazione dell'INA hanno l'obiettivo di garantire una efficace realizzazione delle finalita' di cui all'articolo 2. La sicurezza, e l'integrita' delle informazioni scambiate tra i soggetti fornitori e/o fruitori di cui all'articolo 5 comma 1 sono assicurate attraverso il Backbone di sicurezza del CNSD, che certifica lo scambio e la certezza dei punti di origine e di destinazione delle comunicazioni, secondo le modalita' indicate nell'allegato tecnico di cui al successivo articolo 8.

2. I servizi di interscambio e cooperazione dell'INA riguardano:

a) i dati anagrafici trasmessi dall'INA in risposta alle richieste inoltrate, tramite l'INA, da parte dei soggetti di cui all'articolo 5, comma 1;

b) le variazioni anagrafiche trasmesse dai comuni all'INA e da quest'ultimo inviate ai soggetti di cui all'articolo 5, comma 1;

c) i dati contenuti nell'INA e quelli concernenti le variazioni anagrafiche per le rilevazioni statistiche sulla popolazione residente, notificati dai comuni all'ISTAT, secondo le modalita' stabilite d'intesa con l'ISTAT.

3. Le informazioni anagrafiche inviate dai comuni all'INA, tramite l'infrastruttura Backbone di sicurezza del CNSD, hanno valore ufficiale e sostituiscono gli altri collegamenti telematici e le altre forme di comunicazione, anche di tipo tradizionale, con i soggetti di cui al precedente articolo 5, comma 1, fatte salve le esigenze di completezza e qualita' delle informazioni statistiche derivanti dalle normative internazionali, europee e nazionali.

4. Il collegamento e lo scambio dei dati avviene, nel rispetto delle competenze e delle responsabilita' delle singole Amministrazioni, come regolate dalla normativa vigente e dalle Convenzioni di cui all'articolo 5, comma 2 del presente decreto.

Art. 7

Vigilanza sulla tenuta delle anagrafi

1. Ai fini della vigilanza sulla regolare ed efficiente tenuta delle anagrafi di cui al decreto del Presidente della Repubblica 30 maggio 1989, n. 223, vengono effettuati, attraverso indicatori derivati dall'INA e mediante l'utilizzo dell'informazione statistica ufficiale prodotta dall'Istat, il monitoraggio e la valutazione della qualita' dell'informazione amministrativa. I criteri e le modalita' di esercizio del monitoraggio sono definiti, d'intesa tra il Ministero dell'interno e l'ISTAT, nell'ambito di un Comitato

paritetico costituito con provvedimento del Capo del Dipartimento per gli Affari interni e territoriali del Ministero dell'interno e composto da tre rappresentanti del Ministero dell'interno - Direzione Centrale per i Servizi Demografici e da tre rappresentanti dell'ISTAT. Il Comitato si riunisce con cadenza semestrale.

Art. 8

Titolare del trattamento e misure di sicurezza

1. Titolare del trattamento dei dati contenuti nell'INA e' il Ministero dell'interno, che designa, quale responsabile del trattamento dei dati, il Direttore Centrale dei Servizi Demografici.

2. Titolare del trattamento dei dati anagrafici contenuti nell'anagrafe comunale, ivi comprese le comunicazioni all'INA e' il comune. Il Sindaco, o suo delegato, e' responsabile dell'attuazione delle misure di sicurezza.

3. La vigilanza sul tempestivo invio dei dati di cui all'articolo 4 e sull'adozione delle misure di sicurezza da parte dei Comuni nella gestione dell'anagrafe e nelle comunicazioni all'INA, rientra nella funzione generale di vigilanza sulla tenuta delle anagrafi, di competenza del Prefetto della provincia.

4. I soggetti di cui all'articolo 5, comma 1, individuano i responsabili e gli incaricati del trattamento dei dati anagrafici scambiati con l'INA, in relazione a quanto previsto dalla normativa vigente e dalle convenzioni di cui all'articolo 5 comma 2.

5. L'INA e' costituito e gestito in conformita' alle disposizioni di sicurezza dettate dall'articolo 31 e seguenti del decreto legislativo 30 giugno 2003, n. 196 e relativo allegato B. E' altresi' assicurata la conformita' alle misure di sicurezza previste dal decreto legislativo 7 marzo 2005, n. 82 e delle relative regole tecniche nonche' dalle direttive emanate dal Ministro per l'innovazione e le tecnologie, in particolare e' assicurata l'adozione della base minima di sicurezza prevista dalla direttiva del 16 gennaio 2002 del Presidente del Consiglio dei Ministri - DIT «Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali». E' inoltre realizzato un Sistema di gestione della sicurezza informativa secondo lo standard ISO 27001/27002 e BS7799, nell'ambito del quale sono progettate, mantenute ed adeguate in modo organico le misure di sicurezza, di natura tecnica, organizzative e sul personale. In tale ambito e' gestito il piano della sicurezza, con aggiornamento almeno annuale.

6. Le misure di sicurezza dell'INA sono definite nell'allegato tecnico che forma parte integrante del presente decreto.

7. L'allegato tecnico di cui al comma precedente e' aggiornato periodicamente con decreto del Ministro dell'interno di concerto con il Ministro per la pubblica amministrazione e l'innovazione, sentito il Garante per la Protezione dei dati personali, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

8. Le misure di sicurezza sopraccitate riguardano anche i sistemi del CNSD, le connessioni con i soggetti collegati al CNSD, di cui all'articolo 5 comma 1, ed i «sistemi di frontiera» (porta applicativa Backbone del CNSD o Porta di Dominio con modulo Backbone del CNSD presso i soggetti collegati); l'adozione di misure di sicurezza relative ai sistemi interni di ciascuno dei soggetti di cui all'articolo 5 comma 1, sono di responsabilita' dello stesso, in coerenza con le prescrizioni di natura tecnica specificate nell'allegato tecnico di cui al comma 6. Prescrizioni, impegni e moduli organizzativi e gestionali sono espressamente richiamati nelle convenzioni di adesione.

Art. 9
Disposizioni finali

1. Il presente regolamento si applica nel rispetto della disciplina rilevante in materia di protezione dei dati personali, e, in particolare, delle disposizioni del Codice in materia di protezione dei dati personali, approvato con decreto legislativo 30 giugno 2003, n. 196.

2. A far data dall'entrata in vigore del presente decreto e' abrogato il decreto ministeriale 13 ottobre 2005, n. 240, recante «Regolamento di gestione dell'INA».

Il presente decreto, munito di sigillo dello Stato, sara' inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Roma, 19 gennaio 2012

Il Ministro dell'interno
Cancellieri

Il Ministro per la pubblica amministrazione e la semplificazione
Patroni Griffi

l Ministro dell'istruzione, dell'universita' e della ricerca
Profumo

Allegato
Allegato tecnico al D.M. 19 gennaio 2012 recante «Nuovo regolamento di gestione dell'Indice Nazionale delle Anagrafi»

ARCHITETTURA DI SICUREZZA DELL'INA

Sommario:

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 Connettivita'

Backbone CNSD/INA.: Infrastruttura di sicurezza del CNSD e dell'Indice Nazionale delle Anagrafi, che certifica lo scambio e l'integrita' 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; e' 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 Connettivita';

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: e' 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 Connettivita'.

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 Connettivita'.

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 qualita' 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 circolarita' anagrafica tra diverse Amministrazioni il cui fulcro principale e' l'Indice Nazionale delle Anagrafi (INA), realizzato con strumenti informatici nel rispetto delle regole tecniche concernenti il sistema pubblico di connettivita'.

Il modello organizzativo del CNSD, il modello di cooperazione e di circolarita' anagrafica, nonche' 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 circolarita' 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 flessibilita' 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 Connettivita' e nel contempo rispettare gli stringenti requisiti di sicurezza e privacy del CNSD il protocollo Backbone e' 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 circolarita' 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 circolarita' anagrafica. La relativa architettura e' 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 utilizzera' 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 molteplicita' di servizi informativi utilizzati da PA centrali, PA locali ed Enti.

Tale coordinamento e composizione dei servizi erogati online dal CNSD e' 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.

(Omissis)

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

Presso la Porta di Dominio dell'ente connesso con il CNSD e' presente il modulo SS_BKPDD ENTE, mentre presso il CNSD e' 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 puo' 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 funzionalita' 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 possibilita' di individuare quale utente da quale postazione e' 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 e' assegnata. L'identificativo e' costituito da una chiave hardware univoca creata nel momento della inizializzazione e abilitazione della postazione.

Utilizzando il Sistema di monitoraggio, tracciatura e allarme e' possibile associare i flussi applicativi ai profili di autorizzazione nonche' verificare la conformita' del flusso rispetto agli schemi applicativi (ad esempio XSD) e relativi tracciati record. I server applicativi hanno necessita' 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 piu' procedimenti amministrativi che determinano la necessita' 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) e' 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 e' 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'unita' 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 e' 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 asimmetrica 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 sevizi 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 e' 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'integrita' 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 utlizza 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 e' stata integrata con il Sistema Pubblico di Connettivita' 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, sara' previsto l'interfacciamento con il CERT-SPC.

La logica architetturale e' basata su un sistema di agenti di natura adattiva. Cio' vuol dire che ogni agente e' 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 funzionalita' 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 e' 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 modalita' sopra specificate.

L'infrastruttura di cooperazione e sicurezza Backbone si avvale inoltre di agenti di cooperazione distribuiti che forniscono funzionalita' di configurazione e gestione di protocolli di cooperazione specifici al fine di garantire modalita' di cooperazione omogenei 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 disponibilita' del servizio

Rilevazione e gestione di allarmi:

Verifica della connettivita' di rete al CNSD

Verifica della conformita' dei flussi di rete

Verifica dei tentativi di Accesso illeciti

Verifica dei tentativi di intrusione e/o modifica dei flussi

Verifica e gestione della continuita' 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 qualita' dei servizi (tempi di risposta, disponibilita', 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). E' 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 e' 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 all'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, e' direttamente sotto il controllo di un agente di sicurezza del Backbone che protegge adeguatamente la password utente cifrandola in modalita' tale da evitare anche che si crei regolarita' 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 puo' quindi richiedere l'autorizzazione per altri utenti (di norma fino a 3). E' prevista un'Interfaccia per la registrazione della postazione e una interfaccia per l'abilitazione di altri utenti (da notare che l'utente puo' 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. E' 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 e' composta da piu' 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 validita' ...) per ridurre la possibilita' 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 e' disponibile presso il CNSD che puo' 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 e' attivabile dal CNSD in modo centralizzato con capillarita' 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 qualita' 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'operativita' 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 e' 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 puo' 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 piu' in servizio e l'adeguamento costante dei profili di autorizzazione e' attuata in funzione delle nomine dei Responsabili. Nel caso venga nominato un nuovo Responsabile (quindi il precedente perde la qualita' 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 e' possibile associare i flussi applicativi ai profili di autorizzazione nonche' verificare la conformita' del flusso rispetto agli schemi applicativi (ad esempio XSD) e relativi tracciati record. I server applicativi hanno necessita' 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 e' assegnata impedendo accessi da postazioni non dell'ente. Con modalita' 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 necessita' puo' 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 e' sempre conosciuto l'identificativo Backbone univoco della postazione origine e quindi e' discriminata l'identita' digitale delle postazioni che accedono al sistema. Se necessario e' possibile dispiegare la funzione che impedisce l'accesso di una postazione se la credenziale che si sta usando e' gia' 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. E' possibile disabilitare, manualmente, una postazione se si rileva un eccesso di tentativi di accesso non conformi. Se necessario e' 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 e' 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 modalita' e' 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 e' 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. E' conservato il dettaglio delle informazioni a cui si e' avuto accesso o che si sono aggiornate con una modalita' che consente di ricostruire l'informazione esclusivamente su specifica richiesta dei soggetti titolati. 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 e' associato il profilo di autorizzazione allo scopo definito. E' quindi possibile associare in modo esatto l'utente, la postazione e le informazioni trattate per ciascuna transazione. In particolare e' 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. E' previsto il tracciamento delle operazioni compiute con possibilita' 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 puo' 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. E' effettuata la ricognizione giornaliera degli enti che accedono tramite produzione del Report degli accessi effettuati da parte degli enti. Tale Report e' visualizzabile tramite il Cruscotto di monitoraggio, tracciatura e allarme del CNSD anche al fine di verificare la corretta periodicita' delle attivita' previste dalla normativa o dagli accordi tra le parti nonche' il rispetto dei livelli di servizio concordati.

26. E' 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 nonche' 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 elaboratore volti a prevenire la vulnerabilita' di strumenti elettronici e a correggerne difetti sono effettuati con cadenza almeno trimestrale.

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

modalita':

i. backup incrementale giornaliero

ii. backup completo con cadenza settimanale

iii. e' 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 idoneita': Il responsabile della sicurezza Comunale e' il Sindaco o un funzionario dallo stesso nominato con atto formale. Per gli altri enti il responsabile del trattamento e' 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 e' 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.