diritto&diritti dal 1996
diritto.it
direttore Francesco Brugaletta

ISSN 1127-8579

Pubblicato dal 11/02/2010

All'indirizzo http://www.diritto.it/docs/28933-il-funzionamento-dell-ina-il-modello-architetturale

Autore: Guzzo Antonio

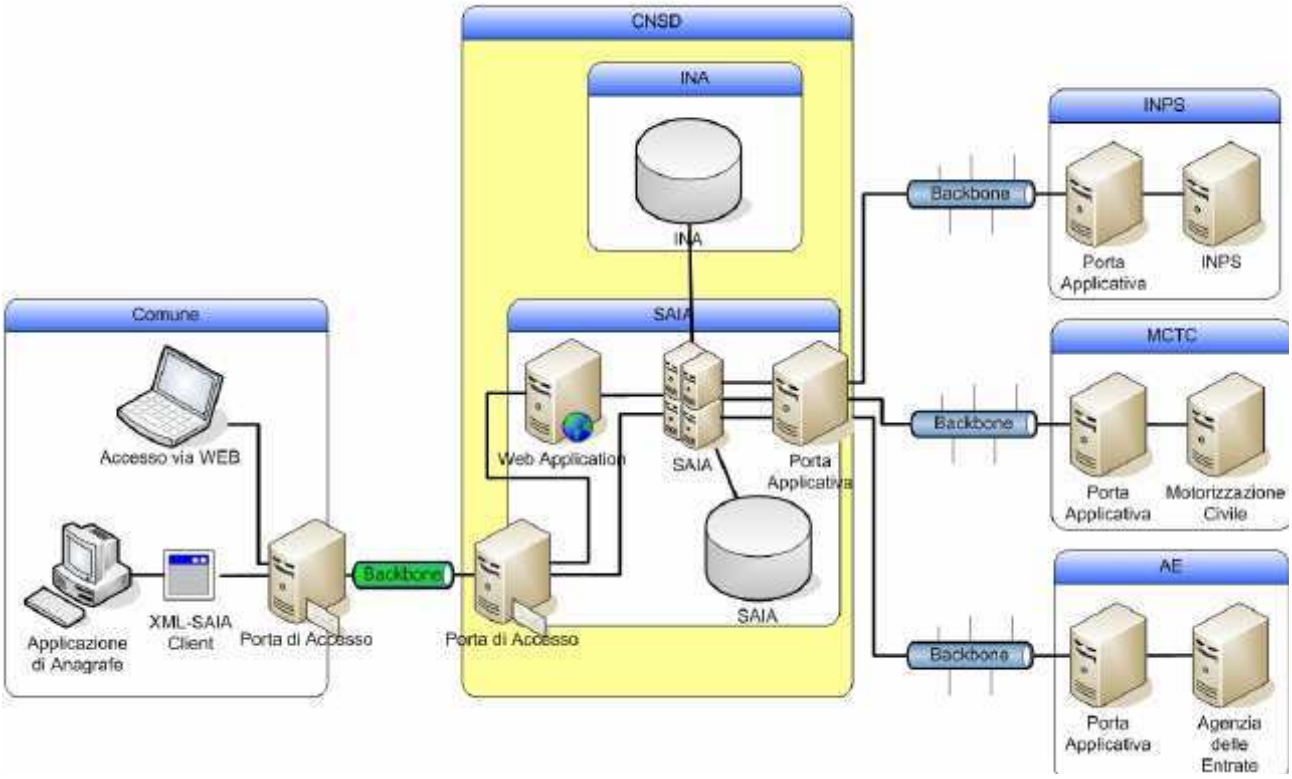
Il funzionamento dell'ina: il modello architetturale

IL FUNZIONAMENTO DELL'INA: IL MODELLO ARCHITETTURALE (a cura del Dottor Antonio Guzzo – Responsabile CED Sistemi Informativi del Comune di Praia a Mare)

L'architettura di sicurezza per l'accesso al CNSD si basa sulla Porta di Accesso Comunale ai domini applicativi del CNSD (d'ora in avanti anche "Porta di Accesso comunale") e sul canale sicuro Backbone di comunicazione su rete. Il sistema informatico adibito a Porta di Accesso comunale deve essere configurato tramite le QSAC (Quantità di Sicurezza, Attivazione e Certificazione) distribuite gratuitamente dal Ministero dell'Interno a tutti i comuni. La Porta di accesso ai domini applicativi del CNSD è il sistema di sicurezza che abilita e gestisce l'accesso ai domini applicativi del CNSD. Ogni Porta di accesso è identificata in modo univoco ed è associata in modo certo e sicuro al Comune presso cui è installata. La porta di accesso è l'unico sistema all'interno del comune abilitato all'accesso in rete ai servizi applicativi del CNSD ed in quanto tale tutte le comunicazioni applicative su rete verso il CNSD devono essere direttamente inoltrate alla Porta di Accesso comunale. Non sono consentite altre modalità di comunicazione in rete con il CNSD. Il "sistema di sicurezza" della Porta di accesso gestisce tutte le comunicazioni di rete con il CNSD offrendo servizi e funzionalità atte a salvaguardare i dati sensibili trasferiti in rete. Nel dettaglio, i servizi e le funzionalità di sicurezza gestiti dalla Porta di accesso sono così classificabili:

1 - Certificazione del punto di origine delle comunicazioni verso il CNSD:
   1 o identificazione univoca della Porta di Accesso
   2 o associazione in modo certo e sicuro della Porta di Accesso al comune di riferimento
2 - Erogazione dei servizi applicativi ai soli sistemi comunali abilitati:
   1 o Identificazione dei sistemi comunali tramite certificato SSL
   2 o Identificazione della Porta di accesso verso i sistemi comunali con certificato SSL univoco
   3 o Comunicazione con i sistemi comunali tramite canale SSL con identificazione reciproca delle parti
3 - Protezione dei flussi informativi scambiati
   1 o Riservatezza delle informazioni tramite cifratura dei flussi
   2 o Certificazione dei flussi applicativi tramite firma dei flussi
4 - Monitoraggio, documentazione e certificazione delle transazioni
   1 o Tracciatura degli accessi ai servizi applicativi del CNSD
   2 o Tracciatura dei tentativi di accesso illeciti ai servizi applicativi del CNSD
   3 o Tracciatura di tentativi di intrusione e/o modifica dei flussi applicativi su rete
2 - Rilevazione e gestione di anomalie/allarmi:
   1 o Verifica della connettività di rete al CNSD
   2 o Verifica della conformità dei flussi di rete
   3 o Verifica tentativi di accesso illeciti
   4 o Verifica tentativi di intrusione e/o modifica dei flussi

L'architettura di sicurezza per l'accesso al CNSD, così come prevista dal D.M. sulla sicurezza, è la seguente:



Una generica postazione comunale per poter accedere ai servizi applicativi del CNSD tramite Porta di Accesso deve essere prima abilitata tramite le QSAC. (Quantità di Sicurezza, Attivazione e Certificazione) distribuite gratuitamente dal Ministero dell'Interno a tutti i comuni. A seguito dell'abilitazione il sistema comunale deve inoltrare le richieste di servizio applicativo alla Porta di Accesso comunale. La porta di Accesso Comunale verifica che la postazione sia abilitata e solo in caso positivo prende in consegna la richiesta verificandone la conformità e la congruenza rispetto alle esigenze del CNSD e del servizio applicativo stesso. Le richieste sono quindi inoltrate alla Porta dei Domini applicativi del CNSD tramite busta di E-gov del CNSD e su protocollo sicuro Backbone. La porta di accesso del CNSD verifica la conformità della richiesta ed inoltra la stessa al servizio applicativo di riferimento gestendone la risposta. L'architettura di sicurezza prevede che, prima dell'inoltro ai rispettivi server applicativi, venga verificata la conformità dei flussi xml rispetto agli schemi XSD di dettaglio per i singoli servizi applicativi, schemi acquisiti in fase di attivazione di un nuovo servizio applicativo o al variare di un servizio già esistente. In base alle politiche di sicurezza del CNSD, ogniqualvolta si debba erogare un nuovo servizio del CNSD, è obbligatoria la sua registrazione al Backbone del CNSD per poterlo riconoscere e poterne consentire il transito in rete dai sistemi comunali verso il CNSD stesso. La risposta applicativa è quindi inoltrata dal CNSD alla Porta di accesso comunale sempre su canale sicuro Backbone. La porta di accesso comunale acquisisce la risposta gestendo il protocollo Backbone ed inoltra la stessa al sistema comunale. A seguire viene descritta la struttura del sistema INA-SAIA. Sono evidenziati gli attori presenti nel sistema, le varie componenti applicative e le componenti di sicurezza presenti nel sistema. In questo documento e nei vari altri a cui si rimanda si farà riferimento principalmente alla comunicazione tra il Comune ed il CNSD. Verrà trattata l'architettura del sistema, il protocollo di comunicazione applicativo, la componente di sicurezza ed i vari scenari possibili all'interno del Sistema Comunale. Dal punto di vista del protocollo applicativo l'innovazione principale riguarda l'introduzione di XML come protocollo di scambio. L'applicativo XML-SAIA Client v.1, (nascita, decesso, variazione residenza) installato nel Comune, si occupa di inoltrare al CNSD, attraverso la Porta di Accesso, i file XML predisposti dall'Anagrafe Comunale. L'applicativo è, comunque, compatibile anche con i tracciati (file testo) del PCCSA attuale. La Porta di Accesso ai domini applicativi del CNSD si fa carico di gestire la componente di sicurezza dal Comune al CNSD.