InterSail ENGINEERING

ICARO

Scheda Sicurezza
accesso ai servizi SIATEL

settembre 2011

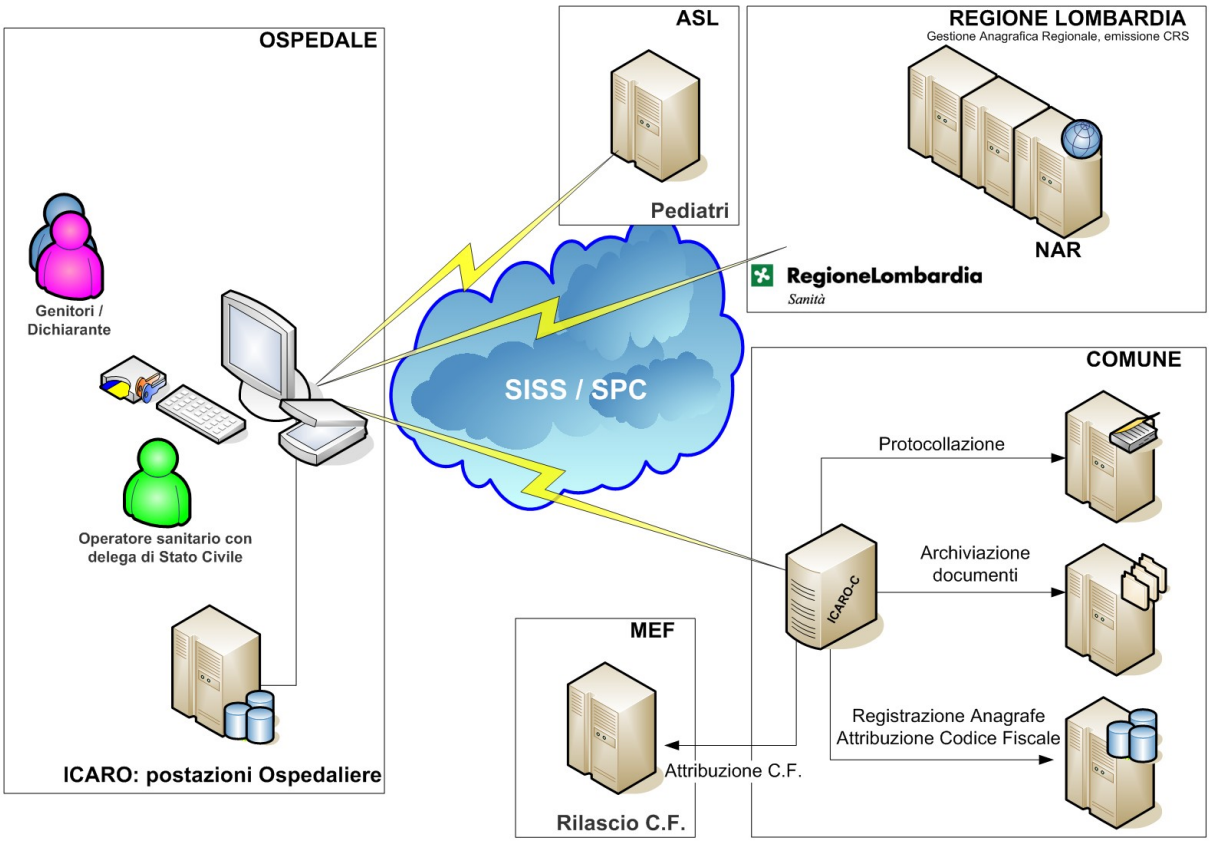
1 Abstract

La sicurezza del sistema va distinta nei diversi domini applicativi interagenti:

- Azienda Ospedaliera
- ASL / Regione Lombardia
- Comune
- Ministero delle Finanze per il rilascio del Codice Fiscale (oggi tramite SIATEL)

Nel seguito verranno analizzate gli aspetti legati ai singoli domini interni del progetto.

Lo schema di interazione base del sistema evidenzia i diversi soggetti e domini coinvolti:



2 Sicurezza a livello di Azienda Ospedaliera / ASL / Regione

La sicurezza del sistema ICARO a livello di Azienda Ospedaliera risponde ai requisiti previsti dal Sistema Informativo Socio-Sanitario (SISS) della Regione Lombardia essendo ICARO stesso parte del SISS.

In linea generale possiamo distinguere tra sicurezza della postazione di lavoro e sicurezza dell'infrastruttura di comunicazione tra Azienda Ospedaliera e Regione e tra Regione e Comuni.

2.1 Sicurezza a livello di postazione di lavoro

Per quanto concerne i meccanismi di sicurezza ICARO si basa sull'utilizzo delle carte di firma degli Operatori Sanitari SISS sia per l'autenticazione sia per la firma digitale degli atti creati.

L'acceso alla postazione e l'utilizzo del sistema è quindi limitato ai soli operatori SISS autorizzati. ICARO sfrutta per tali funzioni l'infrastruttura di autenticazione SISS regionale tramite le funzioni erogate dalla PdL (Postazione di Lavoro SISS).

2.2 Sicurezza a livello di comunicazione

La comunicazioni tra strutture sanitarie (Azienda Ospedaliera, anagrafe Regionale, ASL) avviene grazie all'infrastruttura SISS che prevede propri standard e modelli di interazione e sicurezza utilizzati da tutti i sistemi sanitari a livello Regione Lombardia.

Per comunicare all'esterno della rete sanitaria, in particolar modo con i Comuni (che basano i meccanismi di cooperazione sullo standard SPC[1]) è stato realizzato uno specifico nodo di conversione che funziona da router logico tra il mondo SISS ed il mondo SPC.

Solo le chiamata provenienti da postazioni autorizzate a livello SISS possono raggiungere il nodo SISS/SPC ed essere inoltrate al Comune destinatario.

Tutte le comunicazioni sono crittografate e basate su extranet dedicate.

[1] Il sistema supporta sia gli standard SPCcoop 1.1 sia gli standard ICAR

3 Sicurezza a livello di Comune

Il singolo Comune viene dotato di un appliance ICARO-C che comprende una porta di dominio standard SPCoop.

Le Aziende Ospedaliere che possono interagire con il Comune sono identificate a livello Comunale e tutte le comunicazioni da e verso sistemi terzi (AO, MEF, etc) sono tracciate e monitorate.

Il sistema ICARO-C prevede diversi livelli di utenti e solo gli utenti Amministrativi hanno accesso alla configurazione delle utenze per l'utilizzo dei servizi terzi (es: SIATEL).

3.1 Sicurezza nell'interazione con il SIATEL

Il sistema ICARO-C prevede un utenza con ruolo specifico per l'interazione con il sistema SIATEL. A tale utenza corrisponde un operatore fisico che rilascia una specifica dichiarazione con cui accetta che le proprie credenziali SIATEL siano memorizzate ed utilizzate dal sistema ICARO-C per la richiesta di codici fiscali dei nuovi nati. Le credenziali dell'utenza SIATEL vengono archiviate in ICARO-C in modo crittografato.

Ogni richiesta di codice fiscale viene prima controllata dal sistema quindi inoltrata al MEF se ritenuta idonea. Le verifiche di idoneità riguardano:

- controllo credenziali mittente
- verifica correttezza formale dei dati
- verifica univocità della richiesta
- verifica correttezza indirizzo di residenza

Per ogni codice fiscale richiesto viene inviata una mail al titolare dell'utenza SIATEL utilizzata con cui lo si informa della richiesta trasmessa al SIATEL e dell'esito della stessa.

Un sistema di monitoraggio attivo verifica costantemente il sistema e nel caso di superamento di soglie standard previste per l'utilizzo di una delle componenti (ad esempio numero di richieste al SIATEL) blocca automaticamente l'erogazione dei servizi ed allerta il personale addetto all'amministrazione.

L'utente che ha fornito le credenziali per il sistema SIATEL può verificare e modificare i propri dati o disattivare la propria utenza in qualsiasi momento. Tutte le attività compiute sia dal sistema sia dall'utente vengono tracciate.

3.2 Sicurezza nella gestione degli atti

Tutti gli atti ed i documenti ricevuti sono firmati digitalmente e archiviati secondo gli standard previsti dall'Ente. Solo gli utenti dello Stato Civile autorizzati hanno accesso a tali documenti.

Sia la trasmissione che l'archiviazione degli atti stessi avviene in modo crittografato secondo standard RSA-1024bit.