

# **Sistema Informativo dei Trapianti e dei Servizi Trasfusionali**

Ambiente Hardware, Software e  
Architettura del sistema

## Indice

1	Obiettivi del documento.....	4
1.1	Definizioni.....	4
2	Component Model.....	5
2.1	Component Model.....	5
2.2	Schema Architettura Applicativa .....	10
2.3	Schema Architettura fisica e di sicurezza.....	13
2.3.1	Misure di sicurezza fisica.....	13
2.3.2	ACCESSO APPLICAZIONI SISTRA .....	15
2.3.3	ACCESSO APPLICAZIONI SIT .....	16
3	Utilizzo di Componenti Architeturali .....	20
3.1	Componenti Architeturali DBMS Oracle.....	20
3.1.1	Razionali della componente architettuale .....	20
3.1.2	Integrazione con l'ambiente SIS-N .....	20
3.1.3	Elementi di dimensionamento.....	20
3.1.4	Requisiti/Vincoli di Configurazione .....	21
3.2	Componente Architettuale Web Application Server .....	21
3.2.1	Razionali della componente architettuale .....	21
3.2.2	Integrazione con l'ambiente SIS-N .....	21
3.2.3	Elementi di dimensionamento.....	22
3.2.4	Requisiti/Vincoli di Configurazione .....	22
3.3	Componente Architettuale Reverse Gateway .....	23
3.3.1	Razionali della componente architettuale .....	23
3.3.2	Integrazione con l'ambiente SIS-N .....	23
3.3.3	Elementi di dimensionamento.....	23
3.3.5	Requisiti/Vincoli di Configurazione .....	24
3.4	Componente Batch .....	24
3.4.1	Razionali della componente architettuale .....	24
3.4.2	Integrazione con l'ambiente SIS-N .....	24
3.4.3	Elementi di dimensionamento.....	24
3.4.4	Requisiti/Vincoli di Configurazione .....	25
3.5	Componente Architettuale EDW .....	25
3.5.1	Razionali della componente architettuale .....	25
3.5.2	Integrazione con l'ambiente SIS-N .....	25
3.5.3	Elementi di dimensionamento.....	26
3.5.4	Requisiti/Vincoli di Configurazione .....	26
3.6	Componente Architettuale DW.....	26
3.6.1	Razionali della componente architettuale .....	26
3.6.2	Integrazione con l'ambiente SIS-N .....	26
3.6.3	Elementi di dimensionamento.....	26
3.6.4	Requisiti/Vincoli di Configurazione .....	27
3.7	Componente Architettuale Web Server IIS .....	28
3.7.1	Razionali della componente architettuale .....	28
3.7.2	Integrazione con l'ambiente SIS-N .....	28
3.7.3	Elementi di dimensionamento.....	28
3.7.4	Requisiti/Vincoli di Configurazione .....	28
3.8	Componente Architettuale Reverse Proxy .....	29

---

3.8.1	Razionali della componente architettuale .....	29
3.8.2	Integrazione con l'ambiente SIS-N .....	29
3.8.3	Elementi di dimensionamento .....	29
3.8.4	Requisiti/Vincoli di Configurazione .....	29
3.9	Componente Architettuale Profile Manager .....	30
3.9.1	Razionali della componente architettuale .....	30
3.9.2	Integrazione con l'ambiente SIS-N .....	30
3.9.3	Elementi di dimensionamento .....	30
3.9.4	Requisiti/Vincoli di Configurazione .....	30
3.10	Business Objects .....	31
3.10.1	Razionali della componente architettuale .....	31
3.10.2	Integrazione con l'ambiente SIS-N .....	31
3.10.3	Elementi di dimensionamento .....	31
3.10.4	Requisiti/Vincoli di Configurazione .....	31
3.11	PDD MdS (Porta Di Dominio – Ministero della Salute) .....	31
3.11.1	Razionali della componente architettuale .....	31
3.11.2	Integrazione con l'ambiente SIS-N .....	31
3.11.3	Elementi di dimensionamento .....	31
3.11.4	Requisiti/Vincoli di Configurazione .....	31
3.12	DB Profile Manager .....	33
3.12.1	Razionali della componente architettuale .....	33
3.12.2	Integrazione con l'ambiente SIS-N .....	33
3.12.3	Elementi di dimensionamento .....	33
3.12.4	Requisiti/Vincoli di Configurazione .....	33
3.13	Componente architettuale Posta Elettronica .....	34
3.13.1	Razionali della componente architettuale .....	34
3.13.2	Integrazione con l'ambiente SIS-N .....	34
3.13.3	Elementi di dimensionamento .....	34
3.13.4	Requisiti/Vincoli di Configurazione .....	34
3.14	WAS .....	35
3.14.1	Razionali della componente architettuale .....	35
3.14.2	Integrazione con l'ambiente SIS-N .....	35
3.14.3	Elementi di dimensionamento .....	35
3.14.4	Requisiti/Vincoli di Configurazione .....	35

## 1 OBIETTIVI DEL DOCUMENTO

Lo scopo di questo documento è quello di fornire tutti gli **elementi necessari per il corretto e completo dimensionamento e configurazione** dell'infrastruttura "fisica" del Sistema Informativo Trapianti e Servizi trasfusionali (SIT-SISTRA) in termini di Hardware, Software di Base, Rete.

### 1.1 Definizioni

Nella tabella riportata di seguito sono elencati tutti gli acronimi e le definizioni adottate nel presente documento.

Termini		Definizione
1	J2EE	Java 2 Enterprise Edition
2	EDW	Enterprise DataWarehouse
3	SIT	Sistema Informativo Trapianti
4	SISTRA	Sistema Informativo dei Servizi Trasfusionali
5	MVC	Model View Controller
6	DBMS	Data Base Management System
7	DB	Data Base
8	MDS	Ministero della Salute
9	HW	Hardware
10	SW	Software
11	LAN	Local Area Network

## 2 COMPONENT MODEL

### 2.1 COMPONENT MODEL

Lo schema di base che viene utilizzato per legare gli aspetti applicativi all'architettura fisica è il **Component Model** che **suddivide e relaziona** le differenti **Componenti Architetture** coinvolte o introdotte all'interno dei sistemi SIT e SISTRA e le **integrazioni** (flussi dati e/o richiami funzionali) tra i moduli stessi

Per "**Componente Architetture**" si intende un **elemento isolabile** dell'architettura che rappresenti univocamente **caratteristiche tecnologico/funzionali** proprie: in particolare l'aspetto tecnologico si riferisce ad esigenze **HW, SW di Base e Rete**; identificabile su una macchina fisica/logica indipendente dalle caratteristiche della stessa (es. Cluster = 1 macchina logica).

Nello schema del Component Model sono individuate:

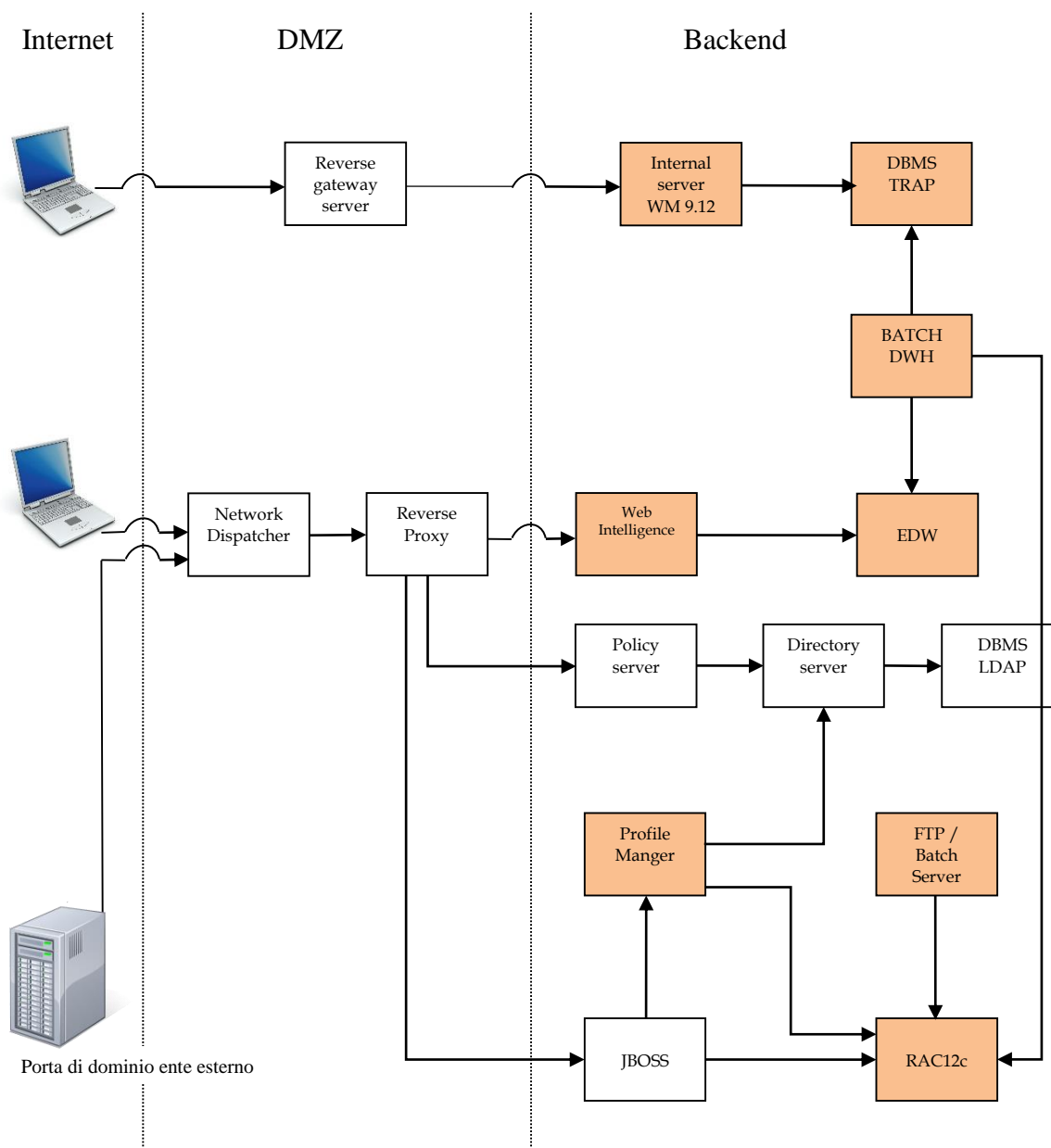
- le **componenti architetture nuove ed esistenti** coinvolte in termini di utilizzo direttamente nel processo del sistema;
- le **componenti architetture nuove introdotte**
- le **componenti architetture esistenti** che prevedono una qualche **aggiunta/variazione** in termini di configurazione/funzionalità

Nello schema seguente, **Component Model**, si individuano tutte le componenti coinvolte nelle diverse tipologie di applicazioni presenti nel SIT e nel SISTRA.

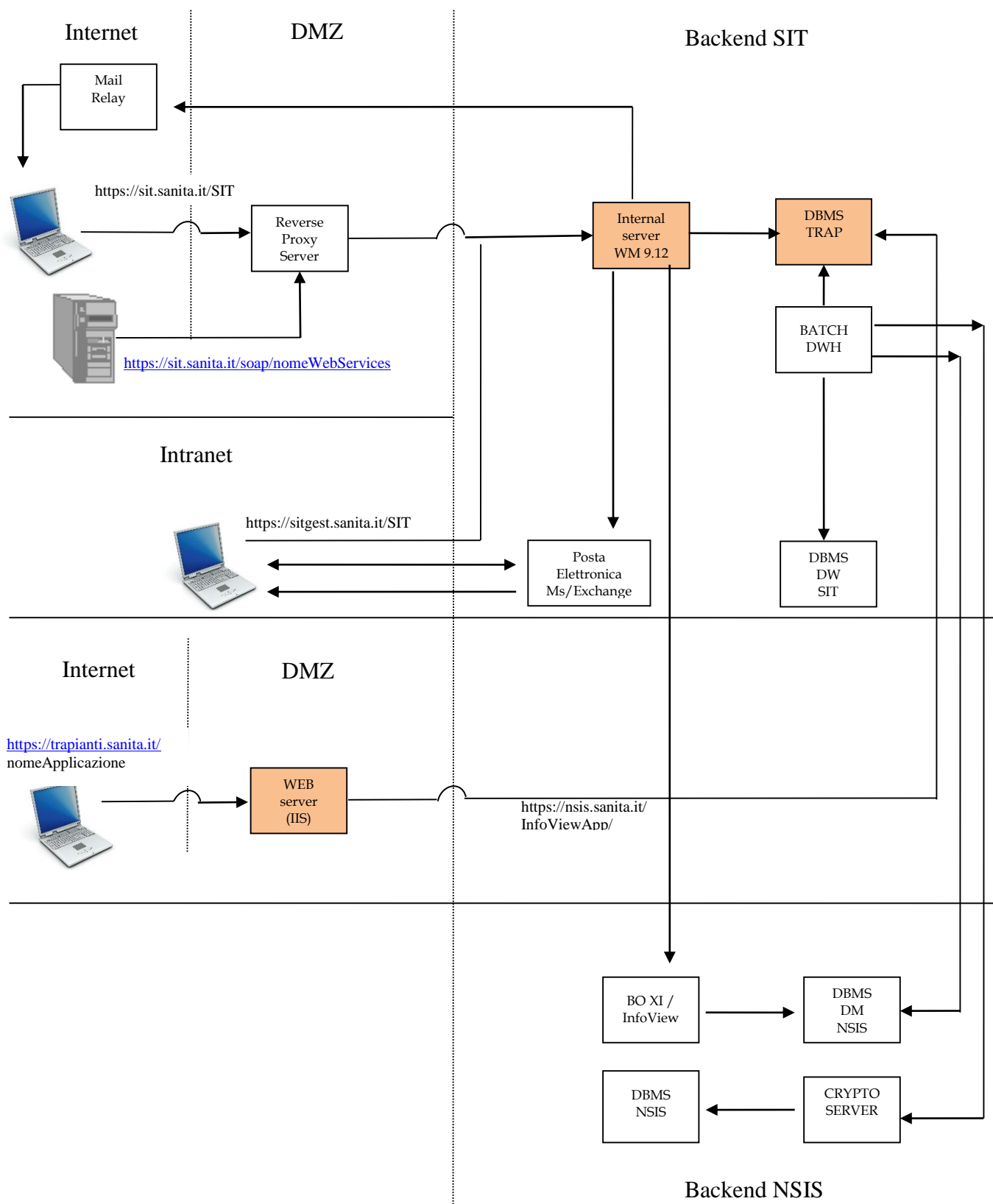
Per la componente Business Intelligence, il Sistema Informativo Trapianti e il SISTRA si vanno ad integrare nell'architettura trasversale del SIS-N.

Nella figura seguente sono state individuate tutte le componenti architetture necessarie ai sistemi e le relazioni tra esse.

## Sistema Informativo dei Servizi Trasfusionali - SISTRA



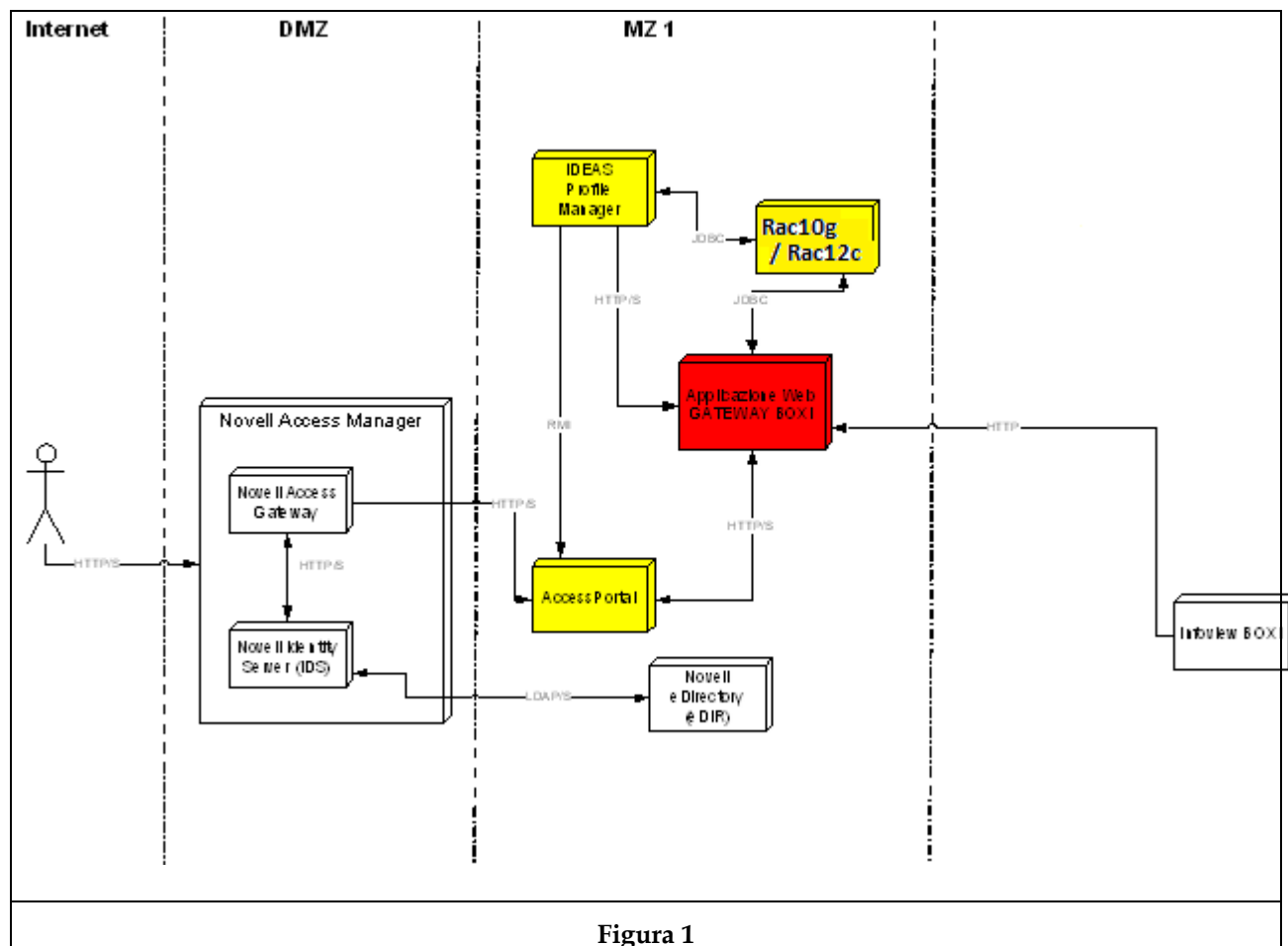
## Sistema Informativo Trapianti - SIT



Componente	Descrizione
DBMS Oracle	Il DBMS Oracle è il sistema di amministrazione della base dati necessario per contenere i dati e le procedure gestite dall'applicazione.
Internal Server WM 9.12	L'applicazione si basa su piattaforma J2EE di Web Methods 9.12 e quindi è necessario effettuarne il deploy all'interno di un Application Server J2EE compliant.
Reverse Gateway Server	L'applicazione è veicolata attraverso il Gateway dove è installata la componente base di Web Methods 9.12. In questo caso è necessario effettuarne la configurazione per il colloquio con l'Internal Server dove risiedono le applicazioni.
ETL (SISTRA)	Procedure Java per l'elaborazione dei dati verso il sistema di EDW
ETL (SIT)	Procedure Java per l'elaborazione dei dati che al termine dell'elaborazione dovranno confluire sull'ambiente DM del SIS-N dopo aver opportunamente anonimizzato i dati
Profile Manager	Per la componente Business Objects l'applicazione necessita di una fase di autenticazione (Reverse Proxy) e di una fase di autorizzazione (Profile Manager). Su tale componente è necessario definire gli utenti, le risorse, le funzionalità e i ruoli ad essa associati.
Profile Provisioning	E' necessario per le fasi di creazione ed assegnazione di risorse, di utenze e funzionalità e per la gestione delle deleghe di amministrazione degli accessi al sistema.
EDW/DM (DBMS Oracle)	Il DBMS Oracle è necessario per contenere i dati utilizzati dal sistema di reportistica BO. I dati SISTRA e SIT sono trasferiti, rispettivamente, su EDW e su DM tramite l'utilizzo di procedure Java.
DW (DBMS Oracle)	Il DBMS Oracle è necessario per contenere i dati SIT su area di staging. I dati SIT una volta trasformati ed anonimizzati sono trasferiti su DM tramite l'utilizzo di procedure Java.
BO XI (Web Intelligence) (SISTRA)	Componente necessario alla consultazione dei dati storici SISTRA contenuti nel database DW. Utilizza l'infrastruttura dell'NSIS
BO XI (Web Intelligence) (SIT)	Componente necessario alla consultazione dei dati storici di SIT anonimizzati contenuti nel database DM.
Posta Elettronica (MS Exchange)	Il componente di posta elettronica SIT è definito come un sistema di posta "chiuso" implementato ad uso esclusivo della comunicazione tra gli utenti interni al dominio TRAPDOM. Tale tipologia di utenti comprende i referenti del CNT e dei CR. Il componente è inoltre utilizzato per l'invio delle notifiche generate dall'application server Webmethods ad utenti interni alla rete SIT
Mail Relay	Il componente di Mail Relay rappresenta un'integrazione all'architettura SISTRA e SIT che consente di inviare messaggi di posta verso destinatari Internet



## Component Model – Accesso a BOXI dal portale NSIS

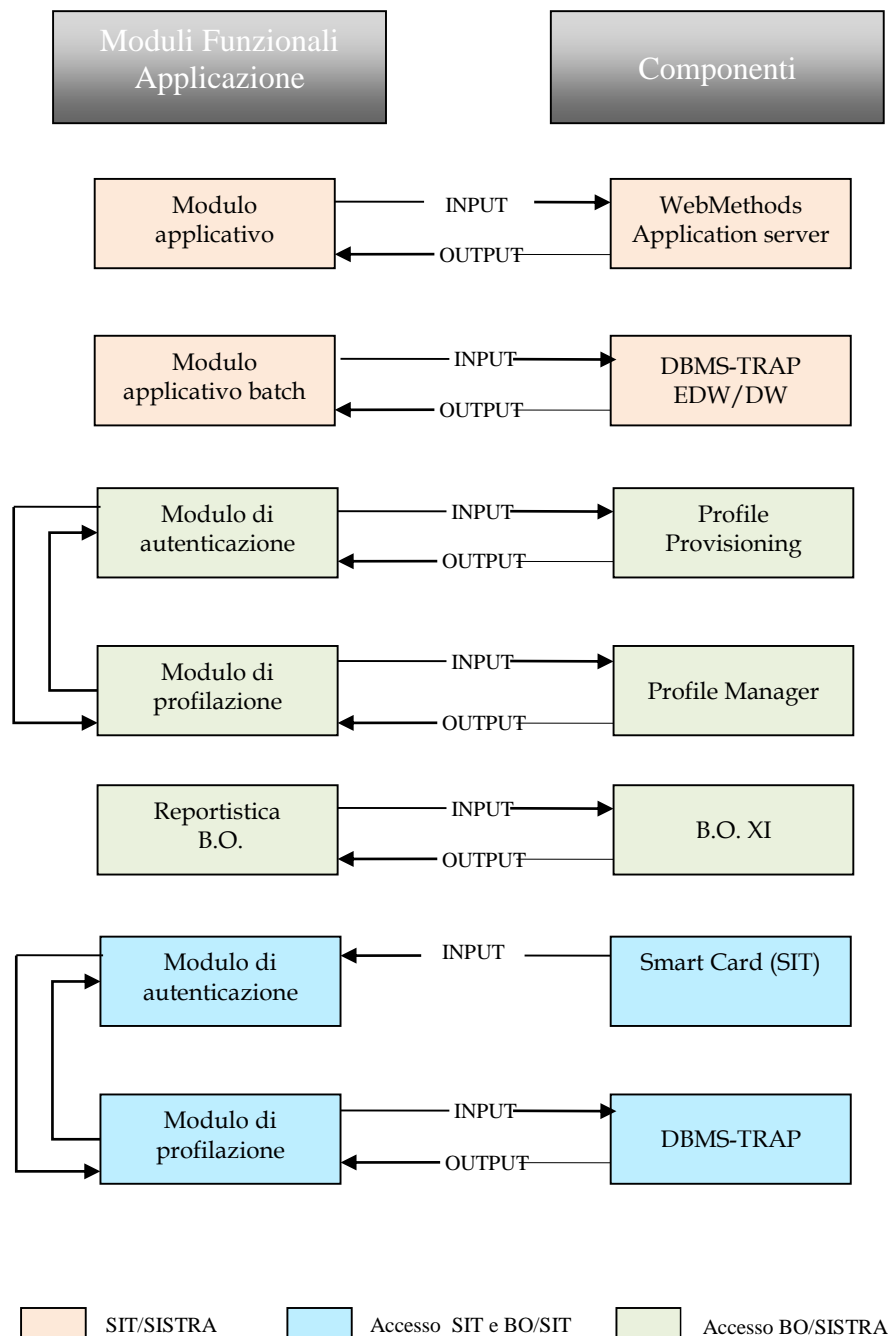


## LEGENDA:

<span style="background-color: yellow; border: 1px solid black; display: inline-block; width: 20px; height: 10px;"></span>	Componenti Esistenti e Modificate
<span style="background-color: red; border: 1px solid black; display: inline-block; width: 20px; height: 10px;"></span>	Nuove Componenti
<span style="background-color: white; border: 1px solid black; display: inline-block; width: 20px; height: 10px;"></span>	Componenti Coinvolte

## 2.2 SCHEMA ARCHITETTURA APPLICATIVA

Di seguito si mostra lo **schema generale della architettura applicativa** per inquadrare al meglio il contesto dal punto di vista dei moduli funzionali coinvolti.



Nella tabella che segue si riportano i principali flussi informativi di input e di output:

Modulo chiamante	INPUT	Modulo chiamato	OUTPUT
Modulo di autenticazione SIT	Smart Card e PIN	Firma digitale	Contesto di sicurezza con firma digitale
Modulo di autenticazione BO/SIT	User e Password dell'utente	Modulo di profilazione	Contesto di sicurezza crittografato
Modulo di autenticazione BO/SISTRA	User e Password dell'utente	Modulo di profilazione	Contesto di sicurezza crittografato
Modulo applicativo	Valori di input dei moduli applicativi	WebMethods Application Server	Valori di output applicativi
Modulo di profilazione SIT	Nome applicazione e identificativo utente	DBMS-TRAP	Funzionalità associate all'utente relativamente all'applicazione
Modulo di profilazione BO/SIT	Nome applicazione e identificativo utente (login)	Profile Manager	Funzionalità associate all'utente relativamente all'applicazione
Modulo di profilazione BO/SISTRA	Nome applicazione e identificativo utente (login)	Profile Manager	Funzionalità associate all'utente relativamente all'applicazione
Modulo applicativo batch	Valori di input da parametri in tabella	DBMS-TRAP EDW/DW	Valori di output applicativi
WebMethods Application Server SIT	Indirizzi di posta dei destinatari, oggetto e contenuto della mail	Posta Elettronica MS/Exchange	Invio mail su caselle di posta SIT agli utenti del dominio Trapdom
WebMethods Application Server SIT/SISTRA	Indirizzi di posta dei destinatari, oggetto e contenuto della mail	Mail Relay	Invio mail verso destinatari Internet

#### Schema architettura applicativa – Accesso a BOXI dal portale NSIS

Di seguito viene fornita una descrizione dell'interazione fra i componenti mostrati nel Component Model relativo.

Per la fase di autenticazione ed autorizzazione si rimanda a quanto descritto nel documento SIM\_SSW\_SINTRAS\_SAA\_ARC.

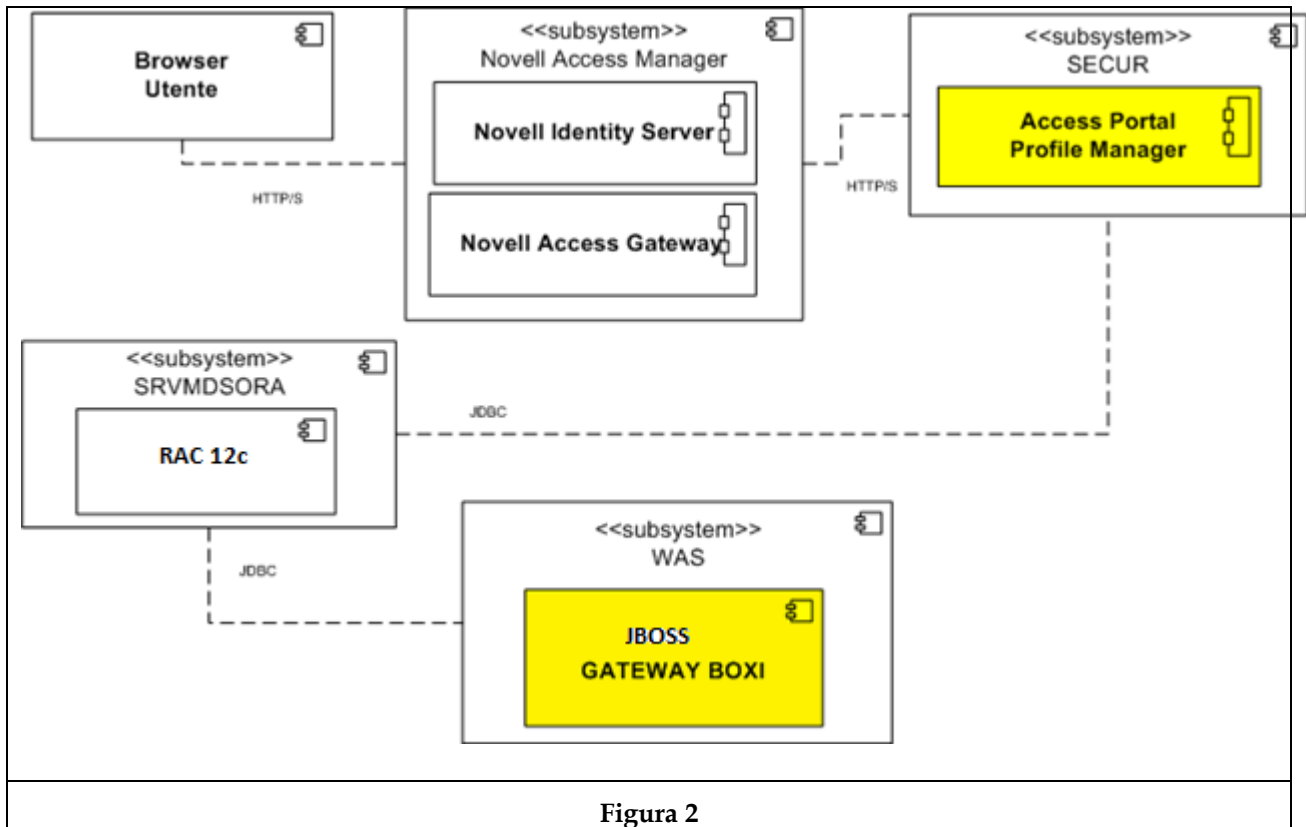
A seguito dell'autenticazione al sistema NSIS, l'utente autorizzato può accedere all'applicazione Gateway BOXI cliccando sull'apposito link.

L'applicazione, recupera le credenziali per l'accesso al sistema Infoview BOXI.

Tali credenziali sono rappresentate dalle risorse associate al ruolo.

Per ogni ruolo associato all'applicazione Gateway BOXI **devono** essere definite le risorse associate. Recuperate le credenziali d'accesso, l'utente sarà reindirizzato automaticamente all'applicativo Infoview BOXI senza la necessità di reinserimento delle credenziali di accesso.

Il paragrafo illustra lo schema generale dell'architettura applicativa evidenziando i principali flussi informativi di input e output tra le varie componenti.

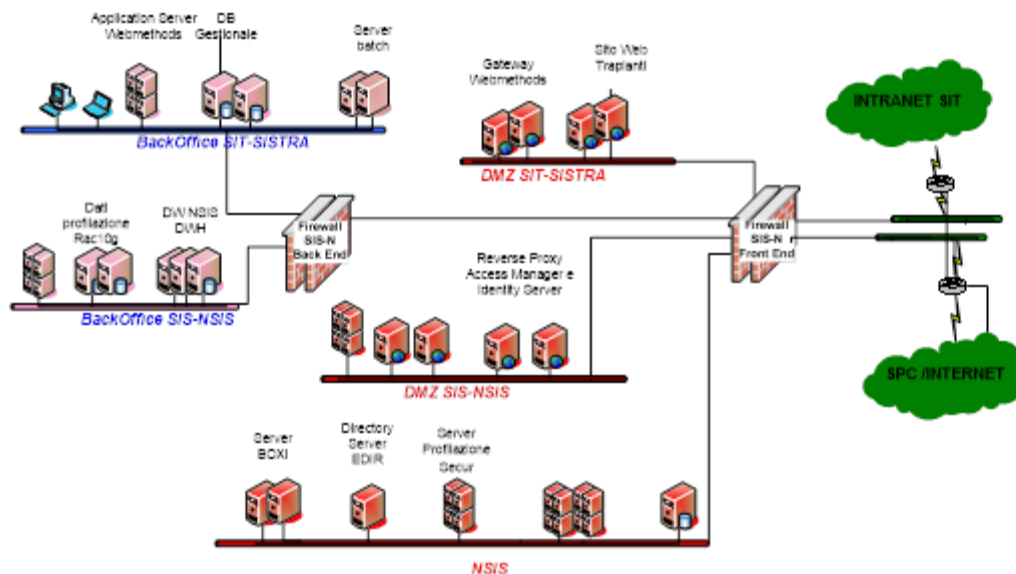


Di seguito sono riportati i flussi tra i moduli.

Modulo chiamante	INPUT	Modulo chiamato	OUTPUT
Browser		Novell Access Manager	Accesso all'applicazione
Novell Access Manager	Credenziali di accesso	AccessPortal	Home page AccessPortal
AccessPortal	Token SAML	Profile Manager	Elenco applicazioni autorizzate
AccessPortal	Token SAML	Applicazione Web GATEWAY BOXI	Accesso all'applicazione
Applicazione Web GATEWAY BOXI	Profilo utente	RAC 12c	Credenziali accesso Infoview BOXI

## 2.3 SCHEMA ARCHITETTURA FISICA E DI SICUREZZA

Nella figura seguente viene mostrata l'architettura fisica (hardware/rete) e di sicurezza su cui si articolano le applicazioni del SIT e del SISTRA



### 2.3.1 MISURE DI SICUREZZA FISICA

La sicurezza fisica dei dati è basata in primo luogo sulla ridondanza degli apparati presenti presso il CED e sul continuo monitoraggio cui sono sottoposti.

La base dati risiede su un sistema configurato in un Cluster Oracle Rac 12c a 2 Nodi attivi con le option Oracle Transparent Data Encryption (TDE) e Oracle Database Vault (ODV).

#### Oracle Transparent Data Encryption (TDE)

Il componente Oracle TDE permette di memorizzare sui suoi supporti fisici (datafiles) i dati criptati impedendo, in caso di illecito utilizzo, quali furto o semplice editing (exploiting), la possibilità di poter ricostruire i dati memorizzati.

I dati sono criptati al livello logico di database; ciò significa che possono accedere ai dati in chiaro solo gli utenti in possesso di userid e password autorizzate all'accesso allo schema Oracle; tali utenti sono:

- utenze applicative, utilizzate dalle applicazioni software;
- utenze nominative, utilizzate dai gruppi applicativi di gestione;
- utenze DBA, utilizzate dagli amministratori di sistema.

A livello sistemistico la soluzione consente di mantenere i dati criptati anche nei backup e negli export (tramite l'implementazione delle nuove funzionalità del datapump); questo comporta comunque l'adeguamento delle procedure di backup e restore.

#### Oracle Database Vault (ODV).

In relazione alle utenze DBA, a maggiore garanzia della sicurezza, è adottata la soluzione Oracle TDE con il prodotto Oracle Database Vault, che impedisce ai DBA di vedere il contenuto delle

strutture dati. La soluzione si basa sulla separazione dei ruoli tra il DBA e l'utente amministrativo degli schemi applicativi (DVA) Database Vault Administrator.

In sintesi, le funzionalità del Oracle Database Vault:

- impediscono ai DBA di accedere ai dati applicativi;
- proteggono le strutture e gli oggetti di uno schema Oracle da modifiche non autorizzate;
- forniscono un controllo sugli accessi delle utenze autorizzate.

#### Controllo degli amministratori

- Limitare gli amministratori all'accesso volontario o involontario ai dati protetti

- Separazione dei compiti

#### Controllo degli accessi in tempo reale

- Controllo degli accessi basati sull'indirizzo IP, sul metodo di autenticazione, sull'orario, ...

#### Trasparenza

- Non sono necessarie variazioni alle applicazioni esistenti



Fig. 1 - ORACLE DATABASE VAULT

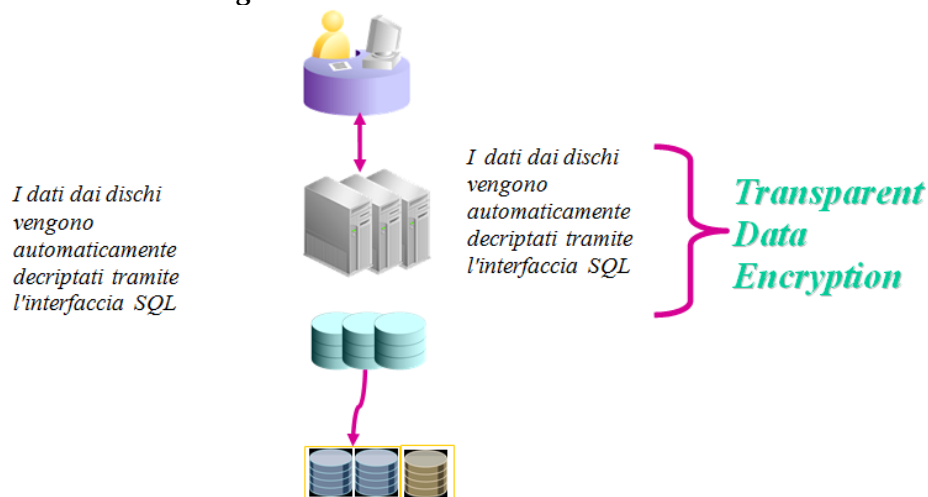


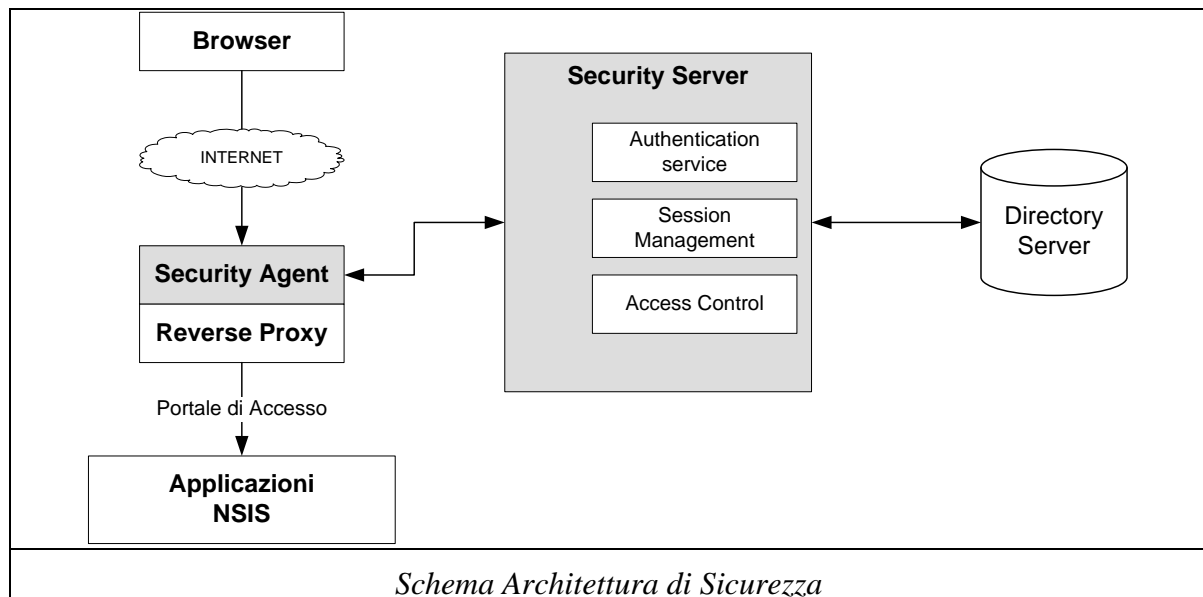
Fig. 2 - ORACLE TDE

### 2.3.2 ACCESSO APPLICAZIONI SISTRA

L'accesso alle applicazioni è possibile per mezzo di un browser web. L'utente inserisce nel browser web l'indirizzo URL del portale di accesso e all'utente viene presentato un form in cui egli ha la possibilità di inserire le proprie credenziali di accesso (la coppia username/password). Queste informazioni viaggiano sulla rete in forma cifrata. Le credenziali inviate sono intercettate dal Reverse Gateway Server che passa la richiesta all'Internal Server Web Methods alla componente di verifica delle credenziali. Questo controlla la correttezza delle credenziali, quindi invia un identificativo dell'utente all'applicazione cui l'utente vuole accedere. In questo modo l'applicazione identifica l'utente che sta tentando di accedere, per fornire la profilazione a lui riservata. Nel caso in cui le credenziali non fossero corrette, all'utente è negato l'accesso.

Una volta autenticato, l'utente può accedere alla Home-page dell'applicazione e da qui potrà decidere di entrare in una delle funzionalità abilitate.

Per la componente Business Objects l'accesso alle funzionalità è sotto il controllo dell'Architettura di Sicurezza del SIS-N. Pertanto l'utente deve essere censito nel sistema di sicurezza ed inserito negli utenti abilitati di Business Objects.



### 2.3.3 ACCESSO APPLICAZIONI SIT

L'accesso alle applicazioni del SIT è possibile solo con l'uso di certificati digitali. Gli utenti che accedono da postazioni client, attestate sulla rete SIT o da Internet devono essere dotati di smart card personali dotate di certificati digitali, mentre i sistemi informativi che effettuano la cooperazione applicativa con il SIT devono essere dotati di certificati client.

Gli utenti che accedono da postazioni client attestate sulla rete SIT, con protocollo HTTPS, vengono autenticati direttamente sull'Internal Server Web Methods, che verifica la presenza del certificato e le credenziali di accesso.

Gli utenti che accedono, con protocollo HTTPS, da postazioni client Internet o i server regionali che effettuano cooperazione applicativa vengono intercettati prima dal Reverse Gateway Server che passa la richiesta all'Internal Server Web Methods alla componente di verifica delle credenziali.

Il componente che verifica le credenziali ne controlla la correttezza, e l'applicazione in base all'utente che sta tentando di accedere fornisce la profilazione a lui riservata. Nel caso in cui le credenziali non fossero corrette, all'utente è negato l'accesso.

Una volta autenticato, l'utente può accedere alla Home-page dell'applicazione e da qui potrà decidere di entrare in una delle funzionalità abilitate.

L'accesso alla componente Business Objects XI/InfoView può essere effettuato direttamente dall'ambiente SIT, dopo che gli utenti si sono autenticati con i livelli di sicurezza descritti in precedenza. L'accesso è consentito sia dalle postazioni client attestate sulla rete SIT sia da postazioni client Internet, entrambe con protocollo HTTPS.

Per gli altri utenti, che non vogliono accedere all'applicativo SIT, l'accesso alla componente Business Objects è sotto il controllo dell'Architettura di Sicurezza del SIS-N. Pertanto l'utente deve essere censito nel sistema di sicurezza ed inserito tra gli utenti abilitati di Business Objects.

L'accesso alle funzioni del componente web server IIS avviene da postazioni internet con l'utilizzo di username e password, attraverso il protocollo HTTPS.

#### 2.3.3.1 IL SISTEMA DI CERTIFICAZIONE DELLE CHIAVI

La scelta di un sistema di autenticazione e di cifratura basato su chiavi pubbliche comporta la disponibilità di un'adeguata infrastruttura per la gestione delle stesse (Public Key Infrastructure) e di un servizio per la certificazione delle chiavi (Certification Authority).

Il sistema di sicurezza del SIT si basa su un servizio di Certification Authority affidato ad una società esterna accreditata, iscritta nell'elenco ufficiale dei certificatori.

Gli utenti del SIT sono dotati di una smart card personale che è in grado di generare al suo interno la coppia di chiavi asimmetriche.

Dopo la fase di inizializzazione della smart card l'utente, attraverso la funzione di registrazione, chiede all'autorità competente (registration authority) di certificare la propria chiave pubblica; tale autorità si accerta dell'identità dell'utente ed inoltra la richiesta di certificazione all'ente certificatore.

L'ente certificatore emette il certificato e lo distribuisce all'utente.



Le comunicazioni tra l'utente, l'autorità di registrazione e l'ente certificatore avvengono attraverso reti che offrono un sufficiente livello di protezione<sup>1</sup>.

Nelle interazioni con i server del Sistema Informativo dei Trapianti, il software presente sul client utilizza le chiavi e le funzioni crittografiche presenti nella smart card per firmare elettronicamente i messaggi XML.

Il server di applicazione, presente presso il sito ricevente, verifica l'autenticità e l'integrità del messaggio utilizzando la chiave pubblica dell'utente. Per eseguire tale verifica si avvale del certificato dell'utente, ma prima si assicura che esso non sia stato revocato accedendo ad una lista, detta CRL (Certificate Revocation List), che contiene l'elenco dei certificati revocati. Tale lista può anche essere un estratto, memorizzato localmente, della CRL gestita dall'Ente certificatore<sup>2</sup>.

Si noti che la chiave segreta dell'utente, generata nella fase iniziale all'interno della smart card, non viene mai trasmessa all'esterno di tale dispositivo e ciò è garanzia di un elevato livello di sicurezza.

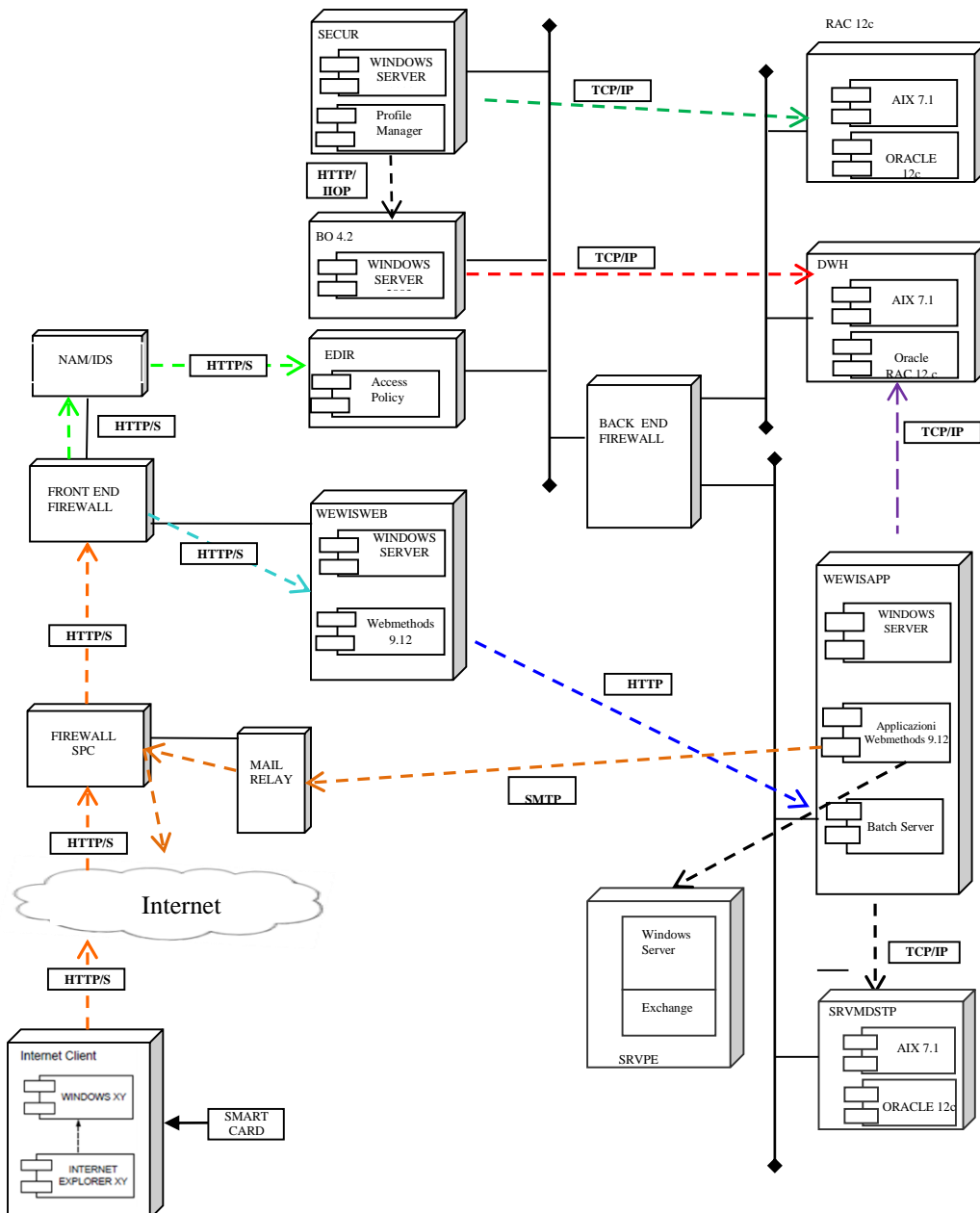
---

1 Le informazioni che viaggiano in questa fase del processo non sono riservate, non è perciò necessario utilizzare reti con particolari requisiti di sicurezza.

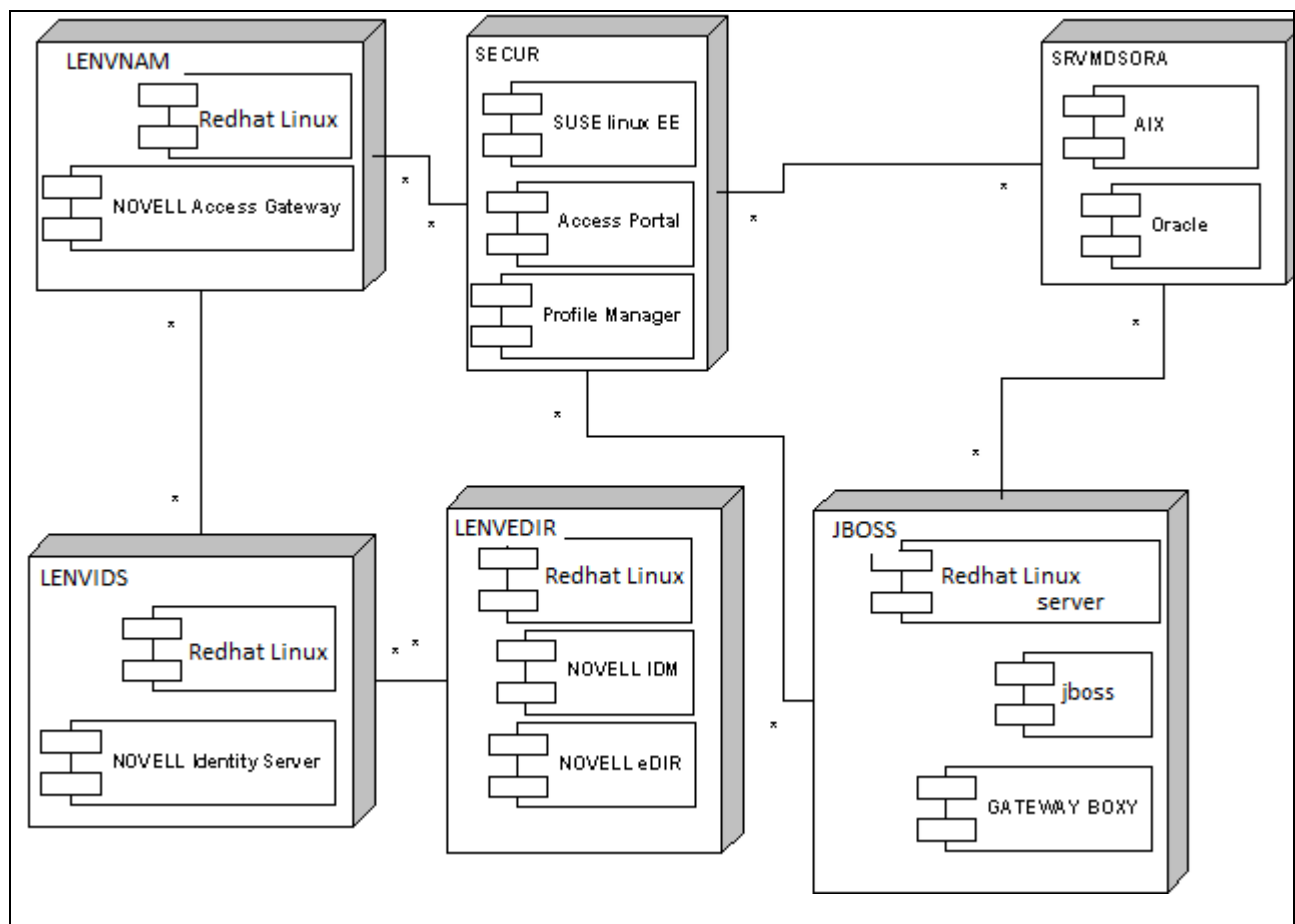
2 L'ente Certificatore detiene l'elenco di tutti i certificati revocati; presso i server di applicazione vengono invece replicati, con opportuna cadenza, i soli elementi relativi all'utenza del SIT.

---

Per descrivere schematicamente i flussi logici tra i componenti dell'architettura fisica SIT/SISTRA e SIS-N, in termini di dipendenze tra i vari sistemi, viene di seguito rappresentato il Deployment Diagram.



## Deployment Diagram – Accesso a BOXI dal portale NSIS



### 3 UTILIZZO DI COMPONENTI ARCHITETTURALI

Questa sezione descrive ogni Componente Architettuale SIS-N utilizzata dal sistema.

L'obiettivo è quello di descrivere eventuali requisiti specifici rispetto alla componente di riferimento standard SIS-N in termini di:

- *caratteristiche funzionali*
- *integrazione con l'ambiente SIS-N*
- *dimensionamento*
- *configurazione*

#### 3.1 COMPONENTI ARCHITETTURALI DBMS ORACLE

##### 3.1.1 RAZIONALI DELLA COMPONENTE ARCHITETTURALE

La componente architettuale DBMS Oracle gestisce l'archiviazione dei dati di business e di DWH (relativamente al SIT) su cui le applicazioni insistono.

Sono previste due istanze DB: TRAP e DWTRAP.

Sull'istanza TRAP sono previsti i seguenti schema:

- due schemi specifici (Sistra e Sistra\_DV) per la base dati integrata del SISTRA gestionale;
- due schemi specifici (Trapianti e Trapianti\_DV) per la base dati integrata del SIT gestionale;

Sull'istanza DWTRAP sono previsti i seguenti schema

- tre schema specifici (Trapianti, Trapianti\_DV e Dwtrap) per la base dati dei sistemi sorgenti e area di staging del DW del SIT .

##### 3.1.2 INTEGRAZIONE CON L'AMBIENTE SIS-N

Il DBMS è posizionato in un'area protetta interna separata dagli altri DBMS del SIS-N.

##### 3.1.3 ELEMENTI DI DIMENSIONAMENTO

L'obiettivo di tale paragrafo è quello di fornire tutte le informazioni riguardanti gli elementi utili al dimensionamento dell'infrastruttura del Componente Architettuale a livello di Hw, Sw, Rete (LAN/WAN). Gli indicatori considerati si basano sulle caratteristiche proprie della Componente Architettuale:

###### SIT

Indicatore	Valore	Crescita annua	Note
N° DI TRANSAZIONI CONTEMPORANEE	30	Nulla	
SPAZIO FISICO OCCUPATO	100 GB	5 GB	
N° RIGHE MASSIMA TABELLA UTILIZZATA	1200000	120000	Dimensione della tabella più grande oggetto di intervento

## SISTRA

Indicatore	Valore	Crescita annua	Note
N° DI TRANSAZIONI CONTEMPORANEE	30	Nulla	
SPAZIO FISICO OCCUPATO	100 MB	10 MB	
N° RIGHE MASSIMA TABELLA UTILIZZATA	4500	2500	Dimensione della tabella più grande oggetto di intervento

### 3.1.4 REQUISITI/VINCOLI DI CONFIGURAZIONE

**Configurazione SW**

Oracle Rac 12c con l'adozione delle option *Oracle Transparent Data Encryption (TDE)* e *Oracle Database Vault (ODV)*.

**Infrastruttura HW**

Cluster Oracle RAC 12c a 2 nodi attivi con Sistema Operativo AIX 7.1.

**Infrastruttura Rete**

I server Oracle sono attestati sulla rete chiusa SIT/SISTRA.

**Specifiche di Sicurezza**

L'accesso è consentito solo alle applicazioni SISTRA e SIT. L'utilizzo delle option *Oracle Transparent Data Encryption (TDE)* e *Oracle Database Vault (ODV)*, permettono di innalzare i livelli di sicurezza rispettivamente cifrando tutti dati del DB e rendendoli non accessibili agli amministratori del DB.

## 3.2 COMPONENTE ARCHITETTURALE WEB APPLICATION SERVER

### 3.2.1 RAZIONALI DELLA COMPONENTE ARCHITETTURALE

WebMethods Integration Server V.9.12 è la piattaforma applicativa basata sulla tecnologia J2EE (Java 2 Enterprise Edition) per servizi Web. Le nuove funzioni e opzioni di distribuzione offrono un ambiente completo per la distribuzione delle applicazioni e-business. Il server gestisce ed integra le applicazioni a livello aziendale, avvalendosi di API e di tecnologie aperte.

WebMethods Integration Server V.9.12 è disponibile con numerose opzioni di configurazione. Ciò consente di supportare una grande varietà di scenari, dalla semplice gestione di un singolo server a quella di un ambiente cluster, caratterizzato da alta disponibilità e alti volumi, con servizi di rete avanzati, tutti basati su un solo server.

### 3.2.2 INTEGRAZIONE CON L'AMBIENTE SIS-N

Non sono previste integrazioni diverse dallo standard SIS-N.

### 3.2.3 ELEMENTI DI DIMENSIONAMENTO

L'obiettivo di tale paragrafo è quello di fornire tutte le informazioni riguardanti gli elementi utili al dimensionamento dell'infrastruttura delle Componenti Architetture a livello di Hw, Sw, Rete (LAN/WAN).

Indicatore	Valore	Crescita annua	Note
N° utenti contemporanei	250 max	Nulla	
Numero/frequenza processi integrazione	5000 mese	10-20%	
Dimensione media pagina web	60 KB	N/A	
Dimensione massima pagina web	80 KB	N/A	
Tipologia applicazione on line - batch	On line / web services SOAP	N/A	
Tempo medio di attesa	2 sec.	N/A	Escludendo il tempo di rete.

### 3.2.4 REQUISITI/VINCOLI DI CONFIGURAZIONE

#### Configurazione SW

Le componenti Web Application Server risultano essere già installate e configurate in esercizio sia per supportare le applicazioni online sia per la cooperazione applicativa attraverso web services SOAP.

#### Infrastruttura HW

Non sono previste esigenze particolari rispetto all'ambiente standard.

#### Infrastruttura Rete

Non sono previste esigenze particolari rispetto all'ambiente standard.

#### Specifiche di Sicurezza

Non sono previste esigenze particolari rispetto all'ambiente standard.

### **3.3 COMPONENTE ARCHITETTURALE REVERSE GATEWAY**

#### **3.3.1 RAZIONALI DELLA COMPONENTE ARCHITETTURALE**

Il Reverse Gateway Server è un server che si interpone tra l'utente e il reale web-server/application server cui l'utente vuole accedere. Esso risulta trasparente rispetto all'utente e rispetto al web-server/application server, che quindi si comportano come se stessero gestendo una comunicazione senza intermediari. Sebbene questo componente sia totalmente trasparente dal punto di vista dell'interazione e dell'utilizzabilità, esso è molto importante per la sicurezza, in quanto permette di stabilire un unico punto di accesso a tutte le applicazioni, e di cifrare il traffico tra l'utente e l'application server. In questo modo è possibile rendere sicure applicazioni che sono state sviluppate senza considerare problemi di cifratura e sicurezza, mantenendo inalterata l'esperienza dell'utente. Il Reverse Gateway Server è anche detto Reverse Proxy Server dove è installata la componente base di Webmethods.

#### **3.3.2 INTEGRAZIONE CON L'AMBIENTE SIS-N**

Non sono previste integrazioni con il SIS-N.

#### **3.3.3 ELEMENTI DI DIMENSIONAMENTO**

Non sono previste variazioni degli elementi di dimensionamento.

### 3.3.5 REQUISITI/VINCOLI DI CONFIGURAZIONE

#### Configurazione SW

Per mantenere separate le chiamate di SISTRA (con protocollo HTTPS e autenticazione User/Password)) da quelle del SIT (protocollo HTTPS e autenticazione con certificato smart card), è richiesta una installazione della piattaforma WebMethods ad un indirizzo IP dedicato per ciascuna applicazione.

#### Infrastruttura HW

Non sono previste esigenze particolari rispetto all'ambiente esistente.

#### Infrastruttura Rete

Non sono previste esigenze particolari rispetto all'ambiente esistente.

#### Specifiche di Sicurezza

Non sono previste esigenze particolari rispetto all'ambiente esistente.

## 3.4 COMPONENTE BATCH

### 3.4.1 RAZIONALI DELLA COMPONENTE ARCHITETTURALE

Tale componente è utilizzato per effettuare le attività giornaliere riconosciute come requisito per l'aggiornamento della base informativa secondo criteri e modalità stabiliti in fase di analisi. Si riportano di seguito le componenti batch e breve descrizione dell'attività svolta:

- Aggiornamento dell'ambiente EDW a partire dal gestionale SISTRA;
- Aggiornamento del gestionale SISTRA a partire dai file provenienti dalla porta di dominio;
- Aggiornamento dell'ambiente DM a partire dal gestionale SIT

### 3.4.2 INTEGRAZIONE CON L'AMBIENTE SIS-N

NA

### 3.4.3 ELEMENTI DI DIMENSIONAMENTO

L'obiettivo di tale paragrafo è quello di fornire le informazioni riguardanti gli elementi utili al dimensionamento dell'infrastruttura del Componente Architetture a livello di HW, SW, Rete (LAN/WAN).

- Aggiornamento dell'ambiente EDW a partire dal gestionale SISTRA

Indicatore	Valore	Crescita annua	Note
Frequenza di esecuzione	Giornaliera	N/A	
Numero occorrenze movimentate	5.000	nulla	

- Aggiornamento del gestionale SISTRA a partire dai file provenienti dalla porta di dominio;



Indicatore	Valore	Crescita annua	Note
Frequenza di esecuzione	Giornaliera	N/A	
Numero occorrenze movimentate	300	nulla	

- Aggiornamento dell'ambiente DM del SIT

Indicatore	Valore	Crescita annua	Note
Frequenza di esecuzione	Giornaliera	N/A	
Numero occorrenze movimentate	3.000.000	nulla	

### 3.4.4 REQUISITI/VINCOLI DI CONFIGURAZIONE

#### Configurazione SW

L'applicazione non richiede configurazioni particolari della componente rispetto agli standard SIS-N.

#### Infrastruttura HW

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

#### Infrastruttura Rete

Per consentire l'alimentazione del DBMS DM, utilizzato dalla componente Business Objects 4.2, è necessario abilitare la porta Oracle (unidirezionale) dal DBMS DWTRAP verso DBMS DM.

Inoltre per consentire l'utilizzo del modulo Cryptoserver nel batch del SIT, per procedere all'anonimizzazione dei codici fiscali, è necessario abilitare la porte di connessione al DB NSIS e le porte di connessione al Cryptoserver.

#### Specifiche di Sicurezza

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

## 3.5 COMPONENTE ARCHITETTURALE EDW

### 3.5.1 RAZIONALI DELLA COMPONENTE ARCHITETTURALE

I dati dell'applicazione sono mantenuti in DWH e DM (Data Mart) di consultazione su cluster Oracle 12c.

### 3.5.2 INTEGRAZIONE CON L'AMBIENTE SIS-N

L'integrazione tra il database e la componente applicativa avviene secondo le modalità standard SIS-N.

### 3.5.3 ELEMENTI DI DIMENSIONAMENTO

L'obiettivo di tale paragrafo è quello di fornire le informazioni riguardanti gli elementi utili al dimensionamento dell'infrastruttura del Componente Architettuale a livello di HW, SW, Rete (LAN/WAN).

Indicatore	Valore	Crescita annua	Note
N° DI TRANSAZIONI CONTEMPORANEE	2	Nulla	
SPAZIO FISICO OCCUPATO	50 GB	5 GB	
N° RIGHE MASSIMA TABELLA UTILIZZATA	300.000	30.000	Dimensione della tabella più grande oggetto di intervento

### 3.5.4 REQUISITI/VINCOLI DI CONFIGURAZIONE

#### Configurazione SW

L'applicazione non richiede configurazioni particolari della componente rispetto agli standard SIS-N.

#### Infrastruttura HW

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

#### Infrastruttura Rete

E' stata abilitata la porta Oracle (unidirezionale) che dalla rete SIT consente di alimentare il DM del SIS-N.

#### Specifiche di Sicurezza

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

## 3.6 COMPONENTE ARCHITETTURALE DW

### 3.6.1 RAZIONALI DELLA COMPONENTE ARCHITETTURALE

I dati dell'applicazione SIT sono mantenuti sull'area di staging dell'istanza Oracle Dwtrap di ORACLE 12c.

### 3.6.2 INTEGRAZIONE CON L'AMBIENTE SIS-N

L'ambiente DW del SIT non ha elementi di integrazione con l'ambiente SIS-N.

### 3.6.3 ELEMENTI DI DIMENSIONAMENTO

L'obiettivo di tale paragrafo è quello di fornire le informazioni riguardanti gli elementi utili al dimensionamento dell'infrastruttura del Componente Architettuale a livello di HW, SW, Rete (LAN/WAN).

Indicatore	Valore	Crescita annua	Note
N° DI TRANSAZIONI CONTEMPORANEE	5	Nulla	

---

Indicatore	Valore	Crescita annua	Note
SPAZIO FISICO OCCUPATO	100 GB	5 GB	
N° RIGHE MASSIMA TABELLA UTILIZZATA	1200000	120000	Dimensione della tabella più grande oggetto di intervento

### 3.6.4 REQUISITI/VINCOLI DI CONFIGURAZIONE

#### Configurazione SW

L'applicazione non richiede configurazioni particolari della componente rispetto agli standard SIS-N.

#### Infrastruttura HW

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

#### Infrastruttura Rete

L'ambiente DW è posizionato all'interno della rete SIT e non è accessibile dall'esterno.

#### Specifiche di Sicurezza

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

### 3.7 COMPONENTE ARCHITETTURALE WEB SERVER IIS

#### 3.7.1 RAZIONALI DELLA COMPONENTE ARCHITETTURALE

Questa componente, utilizzata per il SIT, è descritta in quanto utilizzata dalle applicazioni esposte su internet che trattano dati che necessitano di un livello di sicurezza inferiore e che sono accedute da classi di utenza che non fanno parte della rete trapianti del SIT e per i quali non sono disponibili postazioni client attestata sulla rete SIT.

Le applicazioni sviluppate su tale componente sono:

- Dichiarazioni di volontà
- Schede OLT

L'accesso alle applicazioni avviene tramite protocollo HTTPS con l'impostazione di Utente e Password.

#### 3.7.2 INTEGRAZIONE CON L'AMBIENTE SIS-N

Non sono previste integrazioni con l'ambiente SIS-N.

#### 3.7.3 ELEMENTI DI DIMENSIONAMENTO

L'obiettivo di tale paragrafo è quello di fornire tutte le informazioni riguardanti gli elementi utili al dimensionamento dell'infrastruttura delle Componenti Architetture a livello di Hw, Sw, Rete (LAN/WAN).

Indicatore	Valore	Crescita annua	Note
N° utenti contemporanei	20 max	Nulla	
Numero/frequenza processi integrazione	1000 mese	10-20%	
Dimensione media pagina web	60 KB	N/A	
Dimensione massima pagina web	80 KB	N/A	
Tipologia applicazione on line - batch	On line	N/A	
Tempo medio di attesa	2 sec.	N/A	Escludendo il tempo di rete.

#### 3.7.4 REQUISITI/VINCOLI DI CONFIGURAZIONE

##### Configurazione SW

Non sono previste esigenze particolari rispetto all'ambiente standard.

##### Infrastruttura HW

Non sono previste esigenze particolari rispetto all'ambiente standard.

##### Infrastruttura Rete

Non sono previste esigenze particolari rispetto all'ambiente standard.

##### Specifiche di Sicurezza

Non sono previste esigenze particolari rispetto all'ambiente standard.

### **3.8 COMPONENTE ARCHITETTURALE REVERSE PROXY**

#### **3.8.1 RAZIONALI DELLA COMPONENTE ARCHITETTURALE**

Questa componente è descritta in quanto utilizzata nel prodotto di Business Intelligence.

Il Reverse HTTP Proxy Server è un server che si interpone tra l'utente e il reale web server/application server sul quale è installata l'applicazione cui l'utente vuole accedere. Esso risulta trasparente all'utente rispetto al web server/application server, i quali si comportano come se stessero gestendo una comunicazione senza intermediari. Il Reverse Proxy consente, alla macchina su cui è installato, di dirottare richieste di particolari URI ad altre macchine server su cui sono installate le componenti architetturali e su cui risiedono fisicamente i servizi richiesti. Dopo aver dirottato le richieste, il Reverse Proxy è in grado di ricevere la risposta e di riproporla al client remoto come se fosse stata servita direttamente dal server a cui la richiesta è originariamente pervenuta.

#### **3.8.2 INTEGRAZIONE CON L'AMBIENTE SIS-N**

Non sono previste integrazioni diverse dallo standard SIS-N.

#### **3.8.3 ELEMENTI DI DIMENSIONAMENTO**

Non sono previste variazioni degli elementi di dimensionamento.

#### **3.8.4 REQUISITI/VINCOLI DI CONFIGURAZIONE**

##### **Configurazione SW**

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

##### **Infrastruttura HW**

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

##### **Infrastruttura Rete**

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

##### **Specifiche di Sicurezza**

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

### 3.9 COMPONENTE ARCHITETTURALE PROFILE MANAGER

#### 3.9.1 RAZIONALI DELLA COMPONENTE ARCHITETTURALE

Questa componente è descritta in quanto utilizzata nel prodotto di Business Intelligence. L'applicazione necessita di una fase di autenticazione (Reverse Proxy) e di una fase di autorizzazione gestita tramite il prodotto Profile Manager. Su tale componente è necessario definire utenti, unità organizzative, ruoli e funzionalità ad essi associati.

#### 3.9.2 INTEGRAZIONE CON L'AMBIENTE SIS-N

Non sono previste integrazioni diverse dallo standard SIS-N.

#### 3.9.3 ELEMENTI DI DIMENSIONAMENTO

Le utenze previste per l'applicativo sono quelle necessarie all'accesso al prodotto Business Objects:

##### Utente generico ISS

Indicatore	Valore	Crescita annua	Note
N° utenti registrati	1	0	Utente del Centro Nazionale sangue.
Numero/frequenza processi integrazione	N/A	N/A	L'integrazione con Profile Manager si ha per ogni creazione di un'utenza.
Tipologia applicazione on line - batch	On line	N/A	-

#### 3.9.4 REQUISITI/VINCOLI DI CONFIGURAZIONE

##### Configurazione SW

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

##### Infrastruttura HW

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

##### Infrastruttura Rete

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

##### Specifiche di Sicurezza

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

### **3.10 BUSINESS OBJECTS**

#### **3.10.1 RAZIONALI DELLA COMPONENTE ARCHITETTURALE**

BusinessObjects 4.2 SP3 è uno degli strumenti di Business Intelligence attualmente integrati nell'architettura SIS-N ed è la componente architetture che garantisce la fruizione della reportistica aziendale e personale agli utenti abilitati.

#### **3.10.2 INTEGRAZIONE CON L'AMBIENTE SIS-N**

E' prevista l'integrazione con il sistema di sicurezza SIS-N (autenticazione e profilazione utente), l'integrazione è realizzata secondo quanto previsto dagli standard SIS-N.

#### **3.10.3 ELEMENTI DI DIMENSIONAMENTO**

Non sono previste variazioni degli elementi di dimensionamento.

#### **3.10.4 REQUISITI/VINCOLI DI CONFIGURAZIONE**

##### **Configurazione SW**

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

##### **Infrastruttura HW**

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

##### **Infrastruttura Rete**

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

##### **Specifiche di Sicurezza**

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

### **3.11 PDD MdS (PORTA DI DOMINIO – MINISTERO DELLA SALUTE)**

#### **3.11.1 RAZIONALI DELLA COMPONENTE ARCHITETTURALE**

Il componente PDD MdS è stato soggetto a modifiche che riguardano la configurazione dei servizi.

#### **3.11.2 INTEGRAZIONE CON L'AMBIENTE SIS-N**

Non sono previste variazioni.

#### **3.11.3 ELEMENTI DI DIMENSIONAMENTO**

Non sono previste variazioni.

#### **3.11.4 REQUISITI/VINCOLI DI CONFIGURAZIONE**

##### **Configurazione SW**

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

##### **Infrastruttura HW**

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

### **Infrastruttura Rete**

Non sono previste variazioni degli elementi di dimensionamento.

### **Specifiche di Sicurezza**

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.



### 3.12 DB PROFILE MANAGER

#### 3.12.1 RAZIONALI DELLA COMPONENTE ARCHITETTURALE

Questa componente è descritta in quanto utilizzata dal componente PDD MdS.  
L'applicazione necessita di una fase di autenticazione ed autorizzazione gestita tramite il prodotto Profile Manager. Su tale componente è necessario definire utenti, unità organizzative, ruoli e funzionalità ad essi associati.

#### 3.12.2 INTEGRAZIONE CON L'AMBIENTE SIS-N

L'integrazione tra il componente PDD MdS e la DB Profile Manager avviene secondo le modalità standard SIS-N.

#### 3.12.3 ELEMENTI DI DIMENSIONAMENTO

L'obiettivo di tale paragrafo è quello di fornire le informazioni riguardanti gli elementi utili al dimensionamento dell'infrastruttura del Componente Architetture a livello di HW, SW, Rete (LAN/WAN). Gli indicatori individuati a tal fine sono:

Indicatore	Valore	Crescita annua	Note
N° utenti registrati	3	N/A	Utenti dei Centro regionale sangue.
Numero/frequenza processi integrazione	N/A	N/A	L'integrazione con Profile Manager si ha per ogni creazione di un'utenza.

#### 3.12.4 REQUISITI/VINCOLI DI CONFIGURAZIONE

##### Configurazione SW

L'applicazione non richiede configurazioni particolari della componente rispetto agli standard SIS-N.

##### Infrastruttura HW

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

##### Infrastruttura Rete

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

##### Specifiche di Sicurezza

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

### **3.13 COMPONENTE ARCHITETTURALE POSTA ELETTRONICA**

#### **3.13.1 RAZIONALI DELLA COMPONENTE ARCHITETTURALE**

Il sistema di posta SIT è stato definito inizialmente come un sistema di posta “chiuso” implementato ad uso esclusivo della comunicazione tra gli utenti interni al dominio TRAPDOM. Tale tipologia di utenti comprende i referenti del CNT, dei CIR e dei CR.

Il sistema è inoltre utilizzato per l’invio delle notifiche generate dall’application server Webmethods ad utenti interni.

L’architettura è basata su una configurazione cluster a 2 nodi (server), con software di posta MS Exchange Server, in modalità active/passive.

Il sistema di posta elettronica utilizza come base dati utenti l’ambiente Microsoft Active Directory 2003. Il dominio attualmente utilizzato è definito con il nome logico TRAPDOM ed ospita le utenze interne del sistema informativo Trapianti con rispettive caselle di posta elettronica definite sul dominio @trapdom.it.

L’implementazione del cluster di Posta Microsoft (SRVPE) garantisce la fault tolerance in modo tale che il servizio, normalmente attivo sul nodo primario, se un nodo fallisce, viene automaticamente spostato sull’altro nodo disponibile.

Il componente di posta elettronica è stato integrato con la definizione di un nuovo dominio di posta al fine di consentire l’invio tramite mail di notifica, di tipo no-replay, verso destinatari internet. Tale integrazione si realizza definendo un canale di collegamento su protocollo SMTP (tcpip port 25) tra gli application server Webmethods ed il mail relay server predisposto sulla zona perimetrale.

Il nuovo dominio di posta è definito e registrato sui DNS pubblici per garantire il corretto instradamento del flusso mail verso utenti destinatari internet.

Per l’implementazione delle funzionalità aggiuntive descritte è inoltre prevista la definizione e configurazione di un servizio di tipo mail relay in sinergia con il provider dei servizi perimetrali di connettività SPC-WIND.

#### **3.13.2 INTEGRAZIONE CON L'AMBIENTE SIS-N**

Non è prevista l’integrazione con il sistema di sicurezza SIS-N. A garanzia della sicurezza dell’ambiente SIT il nuovo dominio sarà dedicato esclusivamente alle notifiche verso internet senza interazioni con i sistemi interni di posta del SIT.

#### **3.13.3 ELEMENTI DI DIMENSIONAMENTO**

Non sono previste variazioni degli elementi di dimensionamento.

#### **3.13.4 REQUISITI/VINCOLI DI CONFIGURAZIONE**

##### **Configurazione SW**

Non sono previste componenti software aggiuntive, ma verranno effettuate esclusivamente modifiche sulla base della configurazione esistente.

##### **Infrastruttura HW**

---

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N. Ci si avvale del servizio di mail relay fornito dal provider SPC.

**Infrastruttura Rete**

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

**Specifiche di Sicurezza**

In merito alla implementazione del sistema di notifiche no-replay verso utenti internet, sono abilitate le comunicazioni su porta tcpip 25 (SMTP) per consentire l'instradamento del flusso mail verso l'esterno. Tale tipologia di abilitazione non è in contrasto con le policy di sicurezza dell'Amministrazione.

**3.14 WAS****3.14.1 RAZIONALI DELLA COMPONENTE ARCHITETTURALE**

Componente architetturale utilizzata come web container dell'applicazione Gateway BOXI. Tale componente ospita il software che realizza la business logic e la presentation logic dell'applicazione.

L'applicazione e i suoi componenti vengono sottoposti a deploy in una istanza websphere ND secondo le modalità standard NSIS.

**3.14.2 INTEGRAZIONE CON L'AMBIENTE SIS-N**

L'integrazione dei componenti è realizzata secondo quanto previsto dagli standard NSIS.

**3.14.3 ELEMENTI DI DIMENSIONAMENTO**

Non sono previste variazioni degli elementi di dimensionamento.

**3.14.4 REQUISITI/VINCOLI DI CONFIGURAZIONE****Configurazione SW**

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

**Infrastruttura HW**

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

**Infrastruttura Rete**

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.

**Specifiche di Sicurezza**

Non sono previste esigenze particolari rispetto all'ambiente standard SIS-N.