

ARCHITETTURA TECNICA

Sottosistema Piattaforma Gestione Codice Univoco Nazionale Assistito

Indice

1	Obiettivi del documento.....	4
1.1	<i>Glossario.....</i>	4
2	Impianto architettuale	5
2.1	<i>Component Model.....</i>	5
2.2	<i>Mapping Funzionale-Architettuale (UML)</i>	9
2.2.1	Design View.....	9
2.2.2	Interaction View.....	10
2.2.3	Implementation View.....	15
2.3	<i>Mapping Architettuale-Tecnologico (TOGAF)</i>	15
2.3.1	Application Architecture.....	15
2.3.2	Regole per il backup/restore, storicizzazione, logging, orari del servizio applicativo.....	16
2.3.3	Technology Architecture.....	16
2.3.4	Capacity planning (hw, sw, rete, security, licencing).....	17
2.3.5	Requisiti/Vincoli di Configurazione per l'esercizio	18
3	Componenti Architeturali.....	19
3.1	<i>Componente Layer 2.....</i>	19
3.1.1	Razionali della componente architettuale.....	19
3.1.2	Integrazione con l'ambiente NSIS.....	19
3.1.3	Elementi di dimensionamento.....	20
3.1.4	Requisiti/Vincoli di Configurazione	21
3.1.5	Requisiti/Vincoli di Configurazione	21
3.2	<i>Componente Layer 3.....</i>	21
3.2.1	Razionali della componente architettuale.....	21
3.2.2	Integrazione con l'ambiente NSIS.....	22
3.2.3	Elementi di dimensionamento.....	22
3.2.4	Requisiti/Vincoli di Configurazione	23
3.2.5	Requisiti/Vincoli di Configurazione	23
4	Componenti Architeturali NSIS utilizzati dal sistema	24
4.1	<i>Componente Architettuale Hardware Security Module (HSM)</i>	24
4.1.1	Razionali della componente architettuale.....	24
4.1.2	Integrazione con l'ambiente NSIS.....	24
4.1.3	Elementi di dimensionamento.....	24
4.1.4	Requisiti/Vincoli di Configurazione	25
4.2	<i>Componente Architettuale Authentication Server/Reverse Proxy.....</i>	25

4.2.1	Razionali della componente architettuale	25
4.2.2	Integrazione con l'ambiente NSIS	25
4.2.3	Elementi di dimensionamento	25
4.2.4	Requisiti/Vincoli di Configurazione	25
4.3	<i>Componente Architettuale Profile Manager</i>	26
4.3.1	Razionali della componente architettuale	26
4.3.2	Integrazione con l'ambiente NSIS	26
4.3.3	Elementi di dimensionamento	26
4.3.4	Requisiti/Vincoli di Configurazione	27

1 Obiettivi del documento

Il seguente documento viene redatto al fine di descrivere il contesto architetturale e di gestione del progetto relativo alla piattaforma Gestione Codice Univoco del NSIS.

1.1 Glossario

Nella tabella riportata di seguito sono elencati tutti gli acronimi adottati nel presente documento.

Termini		Definizione
01	API	Application Programming Interface
02	BIA	Business Impact Analysis
03	CED	Centro Elaborazione Dati
04	CF	Codice Fiscale
05	CSV	Comma Separated Value
06	CUNI	Codice Univoco Non Invertibile
07	CUNA	Codice Univoco Nazionale Assistito
08	DGSISS	Direzione Generale del Sistema Informativo e Statistico Sanitario del MdS
09	DR/DRP	Disaster Recovery, Disaster Recovery Plan
10	FIFO	First In First Out
11	HMAC	keyed-Hash Message Authentication Code
12	HSM	Hardware Security Module
13	IPSEC	Internet Protocol Security
14	MdS	Ministero della Salute
15	NSIS	Nuovo Sistema Informativo Sanitario
16	NTP	Network Time Protocol
17	RBAC	Role Based Access Control
18	RPO	Recovery Point Objective
19	RTO	Recovery Time Objective
20	SoA	Service Oriented Architecture
21	SSH	Secure Shell
22	SSL	Secure Socket Layer
23	VPN	Virtual Private Network
24	WSDL	Web Services Description Language
25	WSS	Web Services Security
26	XML	eXtensible Markup Language

2 Impianto architetturale

In questa sezione sono indicate le informazioni necessarie ad una comprensione di dettaglio delle specifiche dell'architettura della soluzione.

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 del sistema NSIS e le integrazioni (flussi dati e/o richiami funzionali) tra i moduli stessi.

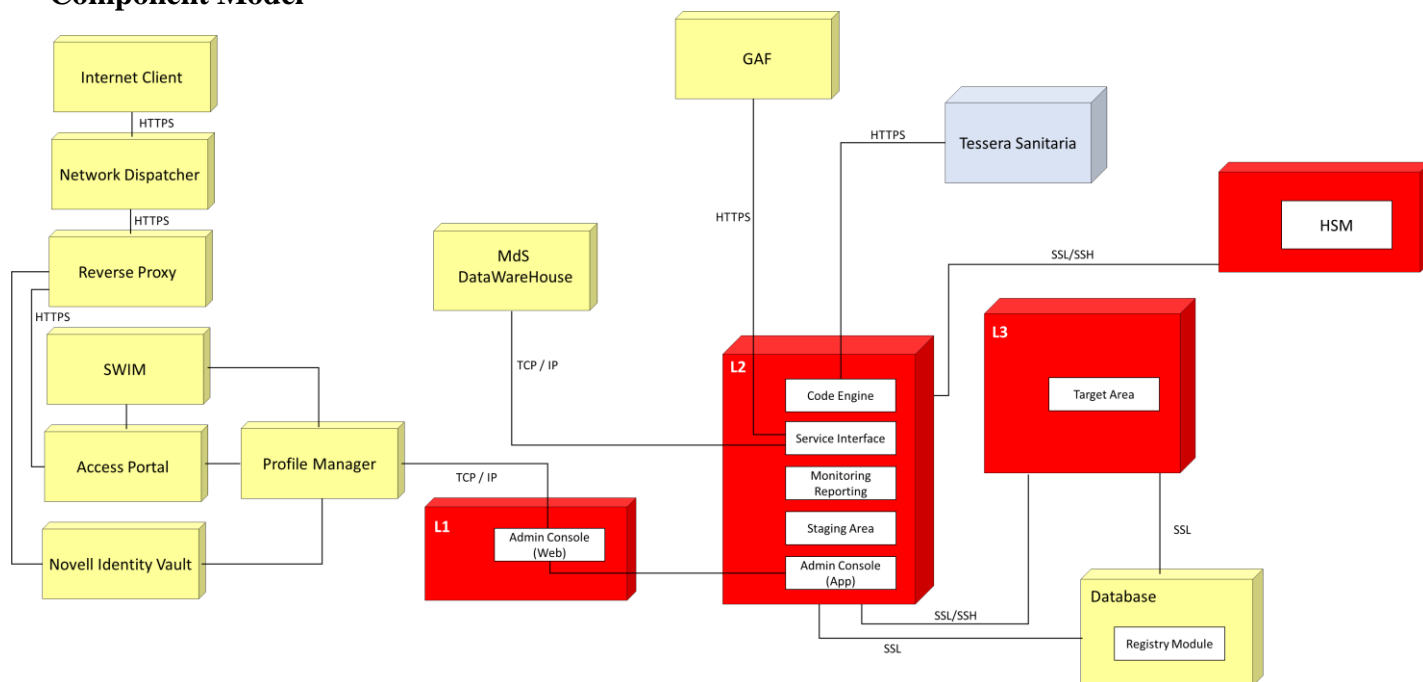
Per "**Componente Architetture**" si intende un elemento isolabile dell'architettura NSIS che rappresenti univocamente caratteristiche tecnologico/funzionali proprie: in particolare l'aspetto tecnologico si riferisce ad esigenze hardware, software di base e rete identificabili su una macchina fisica/logica, 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 esistenti che prevedono una qualche aggiunta/variazione in termini di configurazione/funzionalità.

Qui di seguito si fornisce lo schema Component Model, che utilizza i Deployment Diagram di UML per l'identificazione delle diverse componenti, relativo all'intervento in oggetto.

Component Model

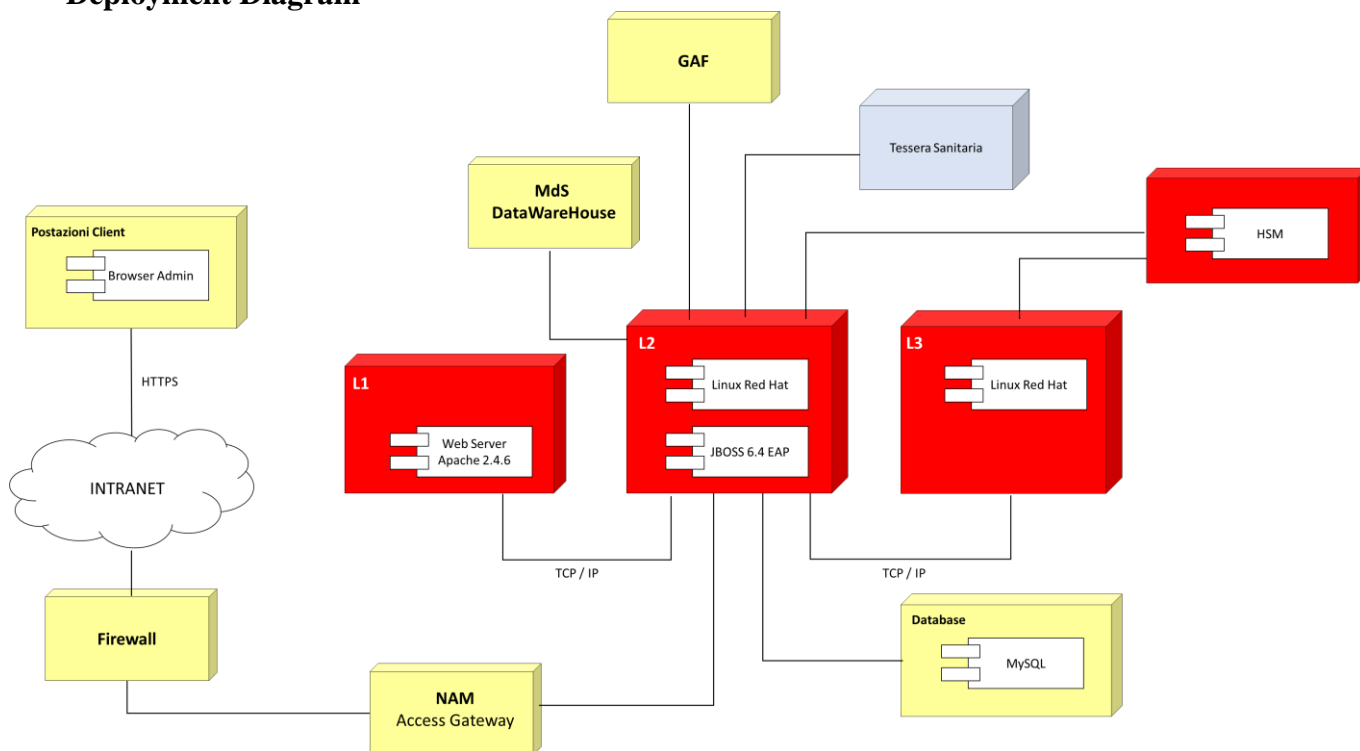


LEGENDA:



Componenti nuovi
Componenti coinvolti o modificati
Componenti esterni

Deployment Diagram



LEGENDA:



Componenti nuovi
Componenti coinvolti
Componenti esterni

A partire dai due schemi di “Component Model” e di “Deployment Diagram” sopra riportati, è possibile estendere l’architettura esistente al fine di rafforzare l’infrastruttura e supportare i nuovi componenti che sono stati adottati per la realizzazione della piattaforma Gestione Codice Univoco del NSIS.

L’estensione dell’attuale infrastruttura è avvenuta secondo le seguenti modalità:

- 1) Per la componente Layer 2 della piattaforma vengono utilizzate 2 virtual machine con FileSystem (shared) di tipo NFS. La componente di Application Server su cui sono installate le applicazioni è gestita con il prodotto JBOSS 6.4 EAP;
- 2) Per la componente Layer 3 della piattaforma vengono utilizzate 2 virtual machine con Cluster FileSystem (shared);
- 3) Per la componente responsabile della gestione del ciclo di vita di chiavi di cifratura viene utilizzato un dispositivo di tipo Hardware Security Module (HSM);
- 4) La componente di Database è composta da una istanza HA MySQL Enterprise Edition.

Tale configurazione, nel suo complesso, è inserita in un ambiente accessibile attraverso il servizio GAF - Gestione Accoglienza Flussi. Il flusso di comunicazione avviene in modalità sicura tramite l'utilizzo del protocollo SSL (Secure Sockets Layer) con autenticazione mutua delle parti tramite l'utilizzo di certificati digitali. La piattaforma Gestione Codice Univoco è anche integrata con il SAA secondo le seguenti caratteristiche:

- Il modulo “Admin Console”, deployato nella componente Layer 2, espone le proprie funzionalità attraverso l’autorizzazione ed autenticazione prevista dal SAA. Gli operatori/amministratori/Addetti IT Regioni, fruitori della piattaforma, devono pertanto registrarsi e, previa autorizzazione del SAA, accedere tramite un portale di accesso web al fine di ottenere il token di autenticazione. L’applicazione, in fase di primo accesso, provvede ad accertare la presenza e la validità del token. Il passaggio da Access Portal verso il modulo è effettuato attraverso la configurazione di una junction sotto NAM che punta alla componente Admin Console presente in L2.

Le versioni dei software utilizzate sono riportate in tabella

Sistema Operativo	Linux Red Hat 6.7 64 bit Linux Red Hat 7.2 64 bit
Database	s.o. CentOS 7 e MySQL Enterprise Edition v 5.7.10
Web Server	Apache 2.4.6 o superiore *
Application Server	JBOSS 6.4

* Specifica di configurazione legata al livello L1 al momento non implementata.

Tutti i software sono da intendersi in versione 64 bit.

2.2 Mapping Funzionale-Architetturale (UML)

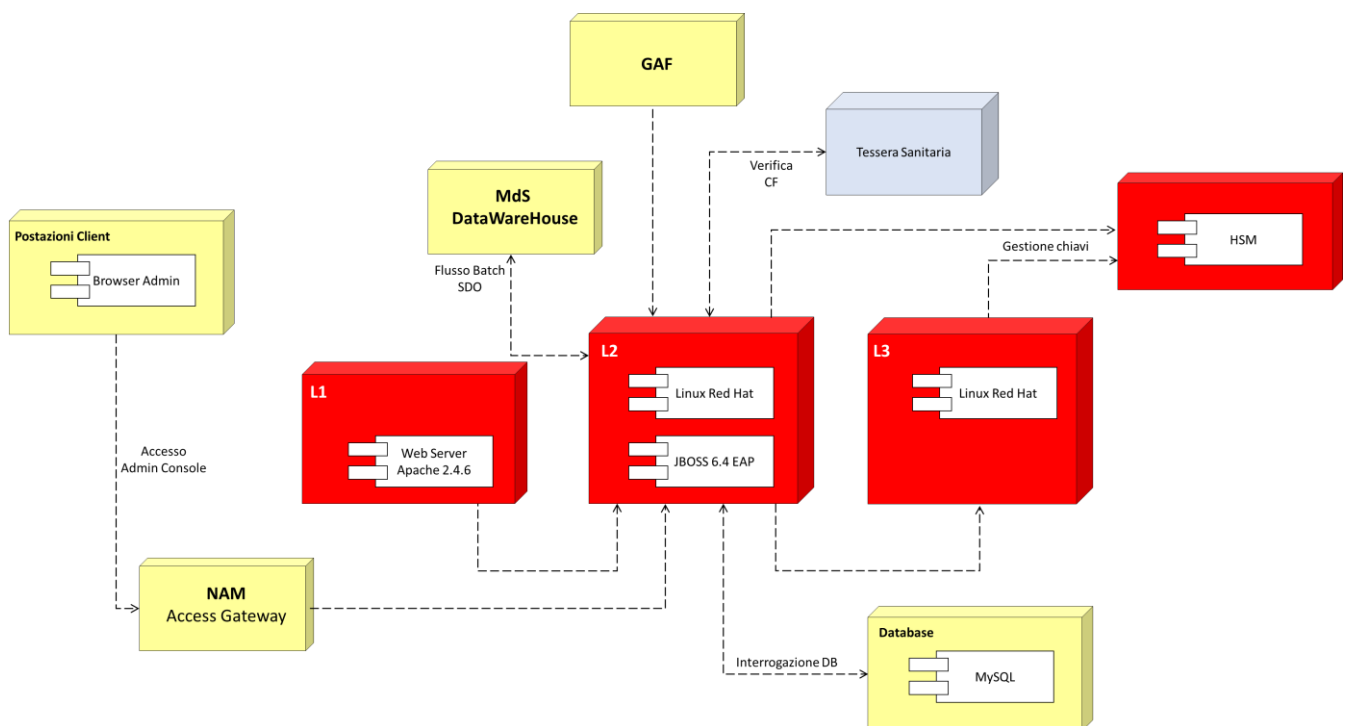
Obiettivo di tale sezione è la documentazione dell'architettura in una **logica applicativa-architetturale**. La documentazione prodotta secondo le indicazioni fornite in questa parte consentiranno di specificare:

- Il contesto in cui la piattaforma si colloca;
- L'organizzazione interna della piattaforma e le modalità in cui le "parti" interagiscono tra loro per fornire le funzionalità complessive di utilizzo.

2.2.1 Design View

Il paragrafo illustra lo schema generale dell'architettura applicativa evidenziando i principali componenti software e il loro livello di comunicazione.

Architettura Applicativa



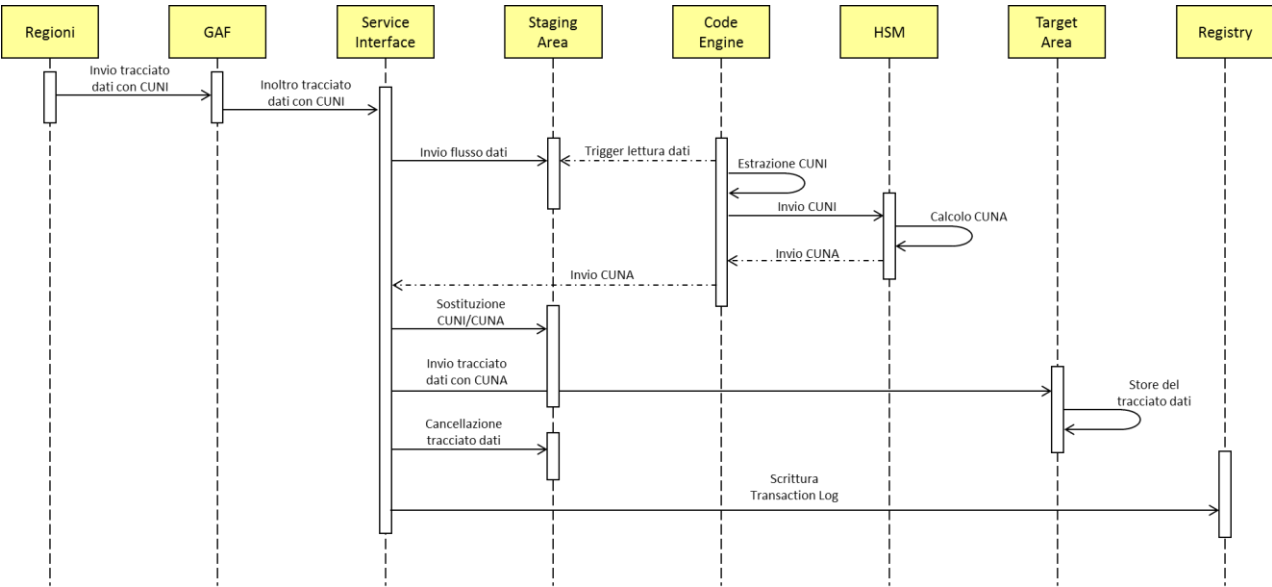
LEGENDA:

	Componenti nuovi
	Componenti coinvolti
	Componenti esterni

2.2.2 Interaction View

L’interaction view mostra il flusso di controllo ed il livello di comunicazione tra le varie componenti architetturali definite all’interno del Component Model, includendo i possibili meccanismi di concorrenza e sincronizzazione.
Si riportano, nelle tabelle di seguito riportate, i principali flussi informativi di input e di output.

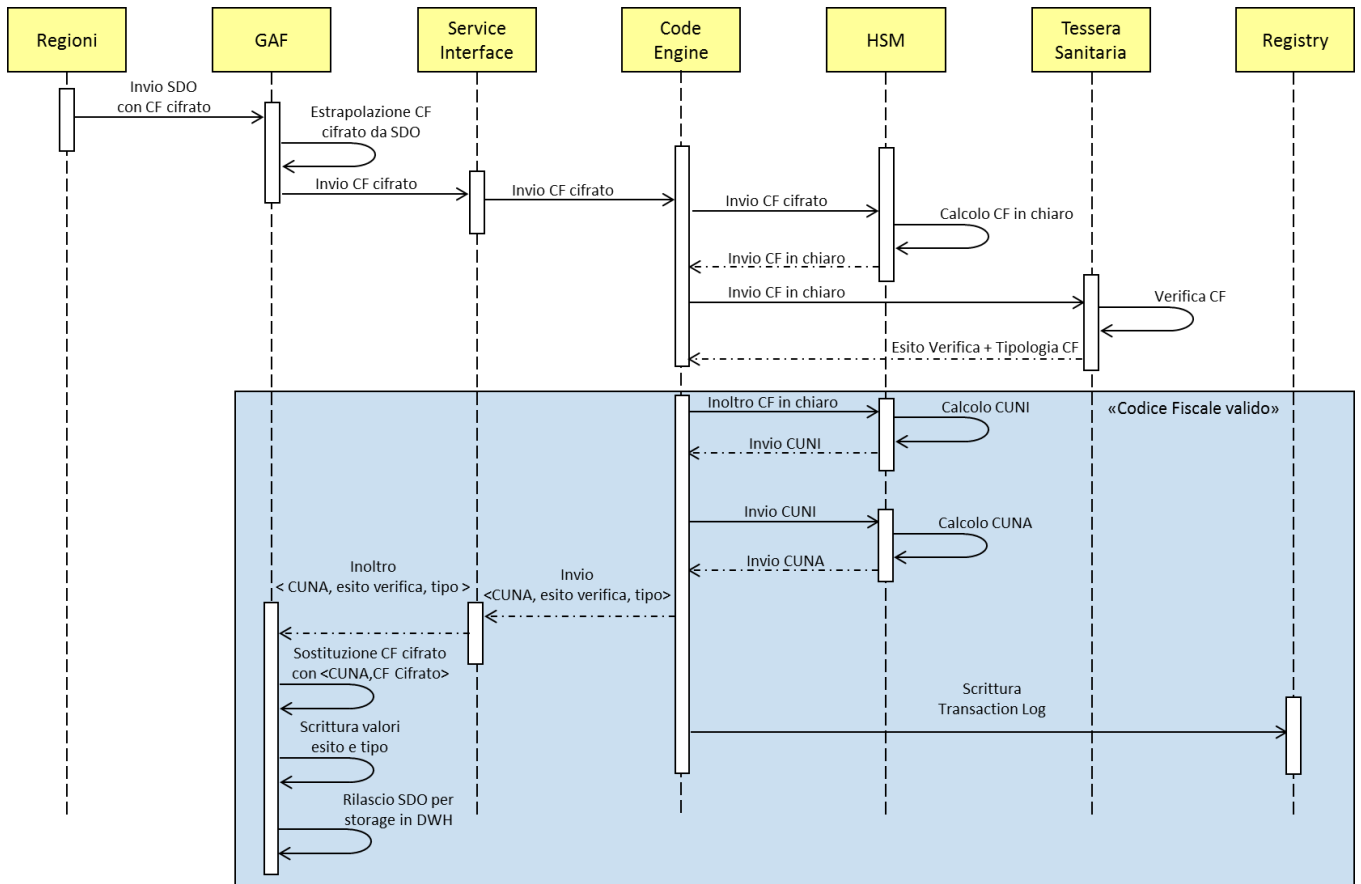
2.2.2.1 Gestione tracciato dati con assegnazione del CUNI da parte delle Regioni



Modulo chiamante	INPUT	Modulo chiamato	OUTPUT
Regioni	Tracciato dati con CUNI	GAF	-
GAF	Tracciato dati con CUNI	Service Interface	-
Service Interface	Tracciato dati con CUNI	Staging Area	-
Code Engine	Tracciato dati con CUNI	Staging Area	Presa in carico del tracciato rilasciato in Staging Area dal modulo Service Interface
Code Engine	Tracciato dati con CUNI	-	CUNI salvato in area di memoria
Code Engine	CUNI	HSM	Invio CUNI ad HSM
HSM	CUNI	-	Calcolo CUNA

HSM	CUNA	Code Engine	Invio CUNA a Code Engine
Code Engine	CUNA	Service Interface	Invio CUNA a Service Interface
Service Interface	CUNA	Staging Area	Sostituzione CUNI con CUNA all'interno del tracciato dati
Service Interface	Tracciato dati con CUNA	Target Area	Invio tracciato dati a Target Area
Target Area	Tracciato dati con CUNA	-	Storage tracciato dati
Service Interface	Trigger delete tracciato dati	Staging Area	Tracciato dati rimosso da Staging Area
Service Interface	Log	Registry	Scrittura transaction log su modulo Registry

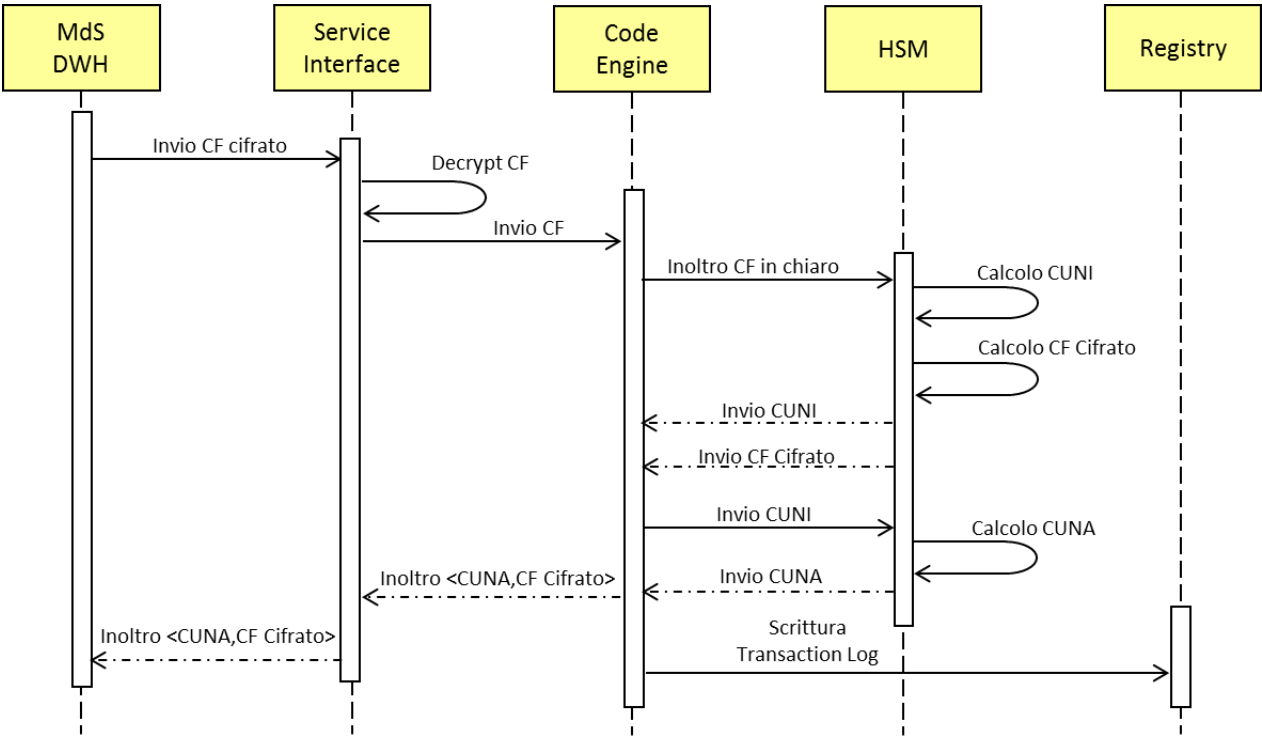
2.2.2.2 Gestione flusso SDO con assegnazione del CUNI da parte del MdS



Modulo chiamante	INPUT	Modulo chiamato	OUTPUT
Regioni	Tracciato dati con CF cifrato	GAF	-
GAF	Tracciato dati con CF cifrato	-	CF Cifrato
GAF	CF cifrato	Service Interface	Invio CF cifrato
Service Interface	CF cifrato	Code Engine	Invio CF cifrato
Code Engine	CF cifrato	HSM	Inoltro CF cifrato
HSM	CF cifrato	-	Decifratura CF
HSM	CF in chiaro	Code Engine	Invio CF in chiaro
Code Engine	CF in chiaro	Tessera Sanitaria	Invio CF in chiaro
Tessera Sanitaria	CF in chiaro	-	Verifica validità e tipo CF (Se disponibile servizio Tessera Sanitaria. In caso negativo viene sempre restituito un valore TRUE)
Tessera Sanitaria	OK / KO	Code Engine	Invio esito verifica e tipo CF (Se disponibile servizio Tessera Sanitaria. In caso negativo viene sempre restituito un valore TRUE)
Code Engine	CF in chiaro	HSM	Invio CF in chiaro
HSM	CF in chiaro	-	CUNI
HSM	CUNI	Code Engine	Invio CUNI
Code Engine	CUNI	HSM	Invio CUNI
HSM	CUNI	-	Calcolo CUNA
HSM	CUNA	Code Engine	Invio CUNA a Code Engine
Code Engine	CUNA, Esito verifica CF, Tipo CF	Service Interface	Invio CUNA, Esito verifica CF, Tipo CF
Code Engine	Log	Registry	Scrittura transaction log su modulo Registry
Service Interface	CUNA, Esito verifica CF, Tipo CF	GAF	Inoltro tupla CUNA, Esito verifica CF, Tipo CF
GAF	CUNA, Esito verifica CF, Tipo CF	-	Scrittura CUNA, Esito verifica CF, Tipo CF all'interno del campo IdentificativoPaziente,

			isIdPazienteInVerVal e tipIdPazienteInVerVal
GAF	SDO	-	Rilascio SDO a flusso verso DataWharehouse

2.2.2.3 Gestione flusso batch SDO con CF cifrato in input



Modulo chiamante	INPUT	Modulo chiamato	OUTPUT
DataWareHouse	Stringa CF cifrato	Service Interface	-
Service Interface	Stringa CF cifrato	-	CF in chiaro
Service Interface	CF in chiaro	Code Engine	Invio CF in chiaro
Code Engine	CF in chiaro	HSM	Inoltro CF in chiaro
HSM	CF in chiaro	-	CUNI
HSM	CF in chiaro	-	CF Cifrato
HSM	CUNI	Code Engine	Invio CUNI

HSM	CUNI	Code Engine	Invio CF Cifrato
Code Engine	CUNI	HSM	Invio CUNI
HSM	CUNI	-	Calcolo CUNA
HSM	CUNA	Code Engine	Invio CUNA
Code Engine	CUNA	Service Interface	Invio tupla <CUNA,CF_Cifrato>
Service Interface	CUNA	DataWareHouse	Invio tupla <CUNA,CF_Cifrato>
Code Engine	Log	Registry	Scrittura transaction log su modulo Registry

2.2.3 Implementation View

Di seguito viene fornito l'implementation view che evidenzia gli **artefatti utilizzati per assemblare e rilasciare il sistema fisico**.

Nell'ottica di questo documento si considerano gli artefatti che rappresentano le nuove unità elementari utilizzate nel deployment diagram.

2.3 Mapping Architetture-Tecnologico (TOGAF)

2.3.1 Application Architecture

Si descrivono gli artefatti coinvolti che compongono il sistema.

Artefatti	s.o. e middleware
Layer 1	Linux Red Hat 6.7 64 bit
Layer 1	Apache 2.4.6
Layer 2	Linux Red Hat 6.7 64 bit
Layer 2	JBOSS 6.4 EAP
Layer 3	Linux Red Hat 7.2 64 bit e GFS2
HSM	PrivateServer HSM Enterprise-Pro Model
Database MySQL	CentOS 7
Database MySQL	Mysql Enterprise Edition v 5.7.10

2.3.2 Regole per il backup/restore, storicizzazione, logging, orari del servizio applicativo

Backup: Le regole di backup dei sistemi e dei DB sono quelle previste per gli altri sistemi e Banche Dati dell'Amministrazione, così come le procedure previste per il ripristino dei dati, ad eccezione delle procedure di backup e restore dell'HSM Private Server.

Storicizzazione: non sono previste regole di storicizzazione sui dati.

Orario del servizio: le manutenzioni programmate degli interventi GO e/o i backup dei dati, qualora non siano possibili a caldo durante l'esercizio del sistema e richiedano un'interruzione del servizio vengono concordati di volta in volta con l'Amministrazione.

2.3.3 Technology Architecture

2.3.3.1 Infrastruttura dei sistemi

I nuovi componenti sono strutturati come di seguito riportato:

- Layer 1: è costituito da due sistemi virtuali ciascuno con 4 core e 8 GB di RAM. Il sistema operativo è Linux Red Hat;
- Layer 2: è costituito da due sistemi virtuali ciascuno con 4 core e 8 GB di RAM. Il sistema operativo è Linux Red Hat e l'application server è Jboss 6.4 EAP, NFS su 200 GB di storage;
- Layer 3: è costituito da due sistemi virtuali ciascuno con 4 core e 8 GB di RAM, Clustered FS su 800 GB di storage;
- Layer 3 - DB: è costituito da una configurazione in HA a 3 nodi di MySQL Enterprise Edition.

Sempre sul livello L3, su una sottorete dedicata, è previsto i un apparato PrivateServer HSM Enterprise-Pro Model.

2.3.3.2 Infrastruttura di comunicazione:

Il protocollo di comunicazione per l'accesso da parte degli utenti è HTTPS / SSL con mutua autenticazione delle parti tramite l'utilizzo di certificati digitali. La piattaforma Gestione Codice Univoco prevede anche l'integrazione con il SAA attraverso i meccanismi di autorizzazione ed autenticazione previsti da tale infrastruttura.

2.3.3.2.1 Infrastruttura di sicurezza

Sulla base di quanto riportato nei documenti di studio del Progetto, nei quali si fa riferimento ad una architettura che prevede i 3 tier standard di sicurezza (L1 presentazione, L2 elaborazione ed orchestrazione, L3 persistenza dati), i sistemi sopra descritti sono posizionati nelle relative sotto reti.

Il componente L1 è posizionato sulla rete DMZ attraverso la quale avviene l'accesso degli utenti; sulla rete DMZ è anche posizionato il componente NAM dell'infrastruttura SAA, che veicola l'accesso al componente L2 Application Server, posizionato sulla rete degli Application Server. Infine sulla rete più interna sono posizionati il livello L3 clustered FS (Target Area) e l'istanza DB MySQL. Su una ulteriore sottorete interna dedicata è posizionato l'apparato PrivateServer HSM Enterprise-Pro Model.

Tutti i componenti previsti ad eccezione dell'apparato PrivateServer HSM Enterprise-Pro Model sono in configurazione di HA al fine di garantire la disponibilità del servizio.

I colloqui fra i vari componenti sono, così come già avviene per l'infrastruttura NSIS, governati e controllati mediante le opportune policy configurate sui firewall presenti nell'infrastruttura e che separano le sotto reti in una configurazione in HA e a doppio bastione.

2.3.4 Capacity planning (hw, sw, rete, security, licencing)

VM	N°VM	S.O.	vCPU	RAM	Network	SW
L1	1	RHEL 6.7 64 bit	4	8 GB	1000 Mbit/s	OpenSSH-Server
	1	RHEL 6.7 64 bit	4	8 GB	1000 Mbit/s	OpenSSH-Server
L2	1	RHEL 6.7 64 bit	4	8 GB	1000 Mbit/s	Jboss, OpenSSL, OpenSSH-Server
	1	RHEL 6.7 64 bit	4	8 GB	1000 Mbit/s	Jboss, OpenSSL, OpenSSH-Server
L3	1	RHEL 7.2 64 bit	4	8 GB	1000 Mbit/s	OpenSSH-Server
	1	RHEL 7.2 64 bit	4	8 GB	1000 Mbit/s	OpenSSH-Server
L3-DB	1	CentOS 7 64 bit	2	4 GB	1000 Mbit/s	MySQL EE
HSM	1	HSM PrivateServer Enterprise-Pro Model presso il sito primario (Roma Scalo Prenestino)				
Storage complessivo max: 2048 GB						

2.3.5 Requisiti/Vincoli di Configurazione per l'esercizio

Configurazione SW

Non sono previste esigenze particolari rispetto all'ambiente standard NSIS.

Infrastruttura HW

Non sono previste esigenze particolari rispetto all'ambiente standard NSIS.

Infrastruttura Rete

Non sono previste esigenze particolari rispetto all'ambiente standard NSIS.

Specifiche di Sicurezza

Sono previste le specifiche di sicurezza citate in dettaglio all'interno del capitolo 3.

3 Componenti Architettureali

Questa sezione descrive i componenti architettureali del sistema. Ogni componente è descritto in termini di:

- *caratteristiche funzionali*
- *integrazione con l'ambiente NSIS*
- *dimensionamento*
- *configurazione*

3.1 Componente Layer 2

3.1.1 Razionali della componente architettureale

La componente architettureale L2 utilizza JBOSS 6.4 come Application Server e consente di mettere a disposizione dell'utente le funzionalità contenute nelle seguenti applicazioni:

- Admin Console
- Service Interface
- Code Engine

La componente interagisce con DWH e MySQL per l'archiviazione e la consultazione dei dati.

Il sistema operativo è Linux Red Hat.

3.1.2 Integrazione con l'ambiente NSIS

Tale configurazione, nel suo complesso, è inserita in un ambiente accessibile attraverso il servizio GAF - Gestione Accoglienza Flussi. Il flusso di comunicazione avviene in modalità sicura tramite l'utilizzo del protocollo SSL (Secure Sockets Layer) con autenticazione mutua delle parti tramite l'utilizzo di certificati digitali. La piattaforma Gestione Codice Univoco è anche integrata con il SAA secondo le seguenti caratteristiche:

- Il modulo "Admin Console", deployato nella componente Layer 2, espone le proprie funzionalità attraverso l'autorizzazione ed autenticazione prevista dal SAA. Gli operatori/amministratori/Addetti IT Regioni, fruitori della piattaforma, devono pertanto registrarsi e, previa autorizzazione del SAA, accedere tramite un portale di accesso web al fine di ottenere il token di autenticazione. L'applicazione, in fase di primo accesso, provvede ad accertare la presenza e la validità del token. Il passaggio da Access Portal verso il modulo è effettuato attraverso la configurazione di una junction sotto NAM che punta alla componente Admin Console presente in L2.

3.1.3 Elementi di dimensionamento

Indicatore	Valore	Crescita annua	Note
N° di transazioni Admin Console	5-10	Nulla	Essendo una console di amministrazione si prevede un numero basso di accessi contemporanei.
N° di transazioni Service Interface	1.000.000 / mese	Dipendente dal numero di flussi integrati nella nuova piattaforma	Il valore indicato si basa sul numero di SDO che alla data di rilascio del presente documento le Regioni inviano all'Amministrazione attraverso la piattaforma GAF.
N° di transazioni Code Engine	1.000.000 / mese	Dipendente dal numero di flussi integrati nella nuova piattaforma	Il valore indicato si basa sul numero di SDO che alla data di rilascio del presente documento le Regioni inviano all'Amministrazione attraverso la piattaforma GAF.

Dimensionamento Infrastruttura

3.1.3.1 Capacità Elaborativa

Il componente Layer 2 è ospitato su due sistemi virtuali dell'infrastruttura virtualizzata del Ministero della Salute.

Ciascuno dei sistemi è dotato di 4 core e 8 GB di RAM.

Si aggiungono a questi componenti due sistemi Layer 1 di front-end con funzioni di Web Server, ciascuno dotato di 4 core e 8 GB di RAM

3.1.3.2 Spazio Disco

Per i valori relativi all'occupazione dello storage (sistemi virtuali e filesystem condiviso) è utilizzato il seguente spazio:

- Per ciascuna VM L1 l'occupazione storage è pari a 60 GB,
- Per ciascuna VM L2 l'occupazione storage è pari a 150 GB
- Per il File System condiviso gestito dal L2 l'occupazione di storage è pari a 200 GB.

3.1.3.3 Ampiezza di Banda di Rete

Non sono richiesti incrementi di banda rispetto al dimensionamento attuale della rete su cui sono attestati i sistemi.

3.1.4 Requisiti/Vincoli di Configurazione

Software di base

- S.O. Linux Red Hat 6.7
- Application Server JBOSS 6.4 EAP

Configurazione SW

È installato e configurato un certificato https sul componente Layer 1 Web Server.
L'alta affidabilità dell'Application Server è garantita dalla configurazione in cluster di JBOSS.

Infrastruttura HW

I sistemi virtuali sono definiti nell'infrastruttura virtualizzata del Ministero della Salute costituita da Blade Cisco B200 M3.

Infrastruttura Rete

Il livello Layer 2 è posizionato sulla sottorete degli Application Server. Non sono necessarie particolari configurazioni di rete.

Specifiche di Sicurezza

Si veda il paragrafo "3.4.3.2.1 Infrastruttura di sicurezza" in riferimento a questo componente.

3.1.5 Requisiti/Vincoli di Configurazione

Nessun requisito

3.2 Componente Layer 3

3.2.1 Razionali della componente architetturale

La componente architetturale Layer 3 utilizza Linux Red Hat 7.2 come s.o. ed il modulo GFS2 per il Clustered FileSystem e consente di mettere a disposizione le seguenti funzionalità:

- Target Area
- Registry Module

3.2.2 Integrazione con l'ambiente NSIS

Tale configurazione, nel suo complesso, è inserita in un ambiente accessibile solo attraverso l'Application Layer. Il flusso di comunicazione avviene in modalità sicura tramite l'utilizzo del protocollo SSL (Secure Sockets Layer) con autenticazione mutua delle parti tramite l'utilizzo di certificati digitali.

3.2.3 Elementi di dimensionamento

Indicatore	Valore	Crescita annua	Note
N° di transazioni Target Area	100 / mese	Dipendente dal numero di flussi integrati nella nuova piattaforma	Il valore indicato si basa sull'assunzione che alla data di rilascio del presente documento l'integrazione del flusso SDO non prevede l'utilizzo del componente Target Area.
N° di transazioni Registry	3.000.000 / mese	Dipendente dal numero di flussi integrati nella nuova piattaforma	Il valore indicato si basa sul numero di SDO che alla data di rilascio del presente documento le Regioni inviano all'Amministrazione attraverso la piattaforma GAF.

Dimensionamento Infrastruttura

3.2.3.1 Capacità Elaborativa

Il componente Layer 3 è ospitato su due sistemi virtuali dell'infrastruttura virtualizzata del Ministero della Salute.

Ciascuno dei sistemi è dotato di 4 core e 8 GB di RAM.

Sul livello L3 è presente inoltre il componente Data Base costituito da MySQL Enterprise Edition. In particolare è stata prevista l'aggiunta di un terzo nodo MySQL Enterprise Edition agli attuali due già presenti, per una ottimizzazione dei meccanismi di alta affidabilità previsti dall'architettura del prodotto. Il dimensionamento per questo terzo nodo prevede 2 core e 4GB di RAM.

3.2.3.2 Storage

Per i valori relativi all'occupazione dello storage (per i sistemi virtuali e per il filesystem condiviso) è utilizzato il seguente spazio:

- Per ciascuna VM L3 l'occupazione storage è pari a 90 GB;
- Per il File System condiviso gestito dal L3 l'occupazione di storage è pari a 800 GB;
- Per il DB la necessità massima di spazio pari a circa 450 GB.

3.2.3.3 Ampiezza di Banda di Rete

Non sono richiesti incrementi di banda rispetto al dimensionamento attuale della rete su cui sono attestati i sistemi.

3.2.4 Requisiti/Vincoli di Configurazione

Software di base

- S.O. Linux Red Hat 7.2 con GFS2
- S.O. CentOS 7 e MySQL Enterprise Edition v 5.7.10 per il DB

Configurazione SW

La funzionalità di Clustered File System avviene attraverso il modulo GFS2 e cluster Suite Linux per la gestione della risorsa cluster di tipo active-active.

Infrastruttura HW

I sistemi virtuali sono definiti nell'infrastruttura virtualizzata del Ministero della Salute costituita da Blade Cisco B200 M3.

Infrastruttura Rete

Il livello Layer 3 è posizionato su una sottorete protetta del firewall di BE.
Non sono necessarie ulteriori particolari configurazioni di rete

Specifiche di Sicurezza

Si veda il paragrafo "3.4.3.2.1 Infrastruttura di sicurezza" in riferimento a questo componente.

3.2.5 Requisiti/Vincoli di Configurazione

Nessun requisito

4 Componenti Architetturel NSIS utilizzati dal sistema

Questa sezione descrive ogni componente architetturel NSIS utilizzata dal sistema.

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

- *caratteristiche funzionali*
- *integrazione con l'ambiente NSIS*
- *dimensionamento*
- *configurazione*

4.1 Componente Architetturel Hardware Security Module (HSM)

4.1.1 Razionali della componente architetturel

Componente responsabile della gestione del ciclo di vita di chiavi di cifratura costituita da una coppia di dispositivi di tipo Hardware Security Module (HSM).

Il modello individuato come HSM è il prodotto ARX PrivateServer.

Tale modulo è interfacciato mediante funzioni primitive di tipo API (Application Programming Interface). Le API supportate sono:

- PKCS#11
- Microsoft-Cryptographic API (CAPI/CNG)
- Java (JCA/JCE)

Le macchine HSM sono fisicamente separate dall'infrastruttura che ospita i restanti moduli dello stesso Layer 3.

L'unico modulo con cui è interfacciato direttamente è il "Code Engine".

4.1.2 Integrazione con l'ambiente NSIS

Non sono previste esigenze particolari rispetto all'ambiente standard NSIS.

4.1.3 Elementi di dimensionamento

Attualmente è previsto un unico apparato installato presso il CED sito in Via dello Scalo Prenestino (Roma);

È in programma la configurazione di altri due apparati al fine di garantire l'alta affidabilità e il Disaster Recovery del componente. I due apparati fisici verranno installati:

- 1 presso il CED sito in Via di Casal Boccone (Roma);
- 1 presso il CED di Disaster Recovery (Milano).

4.1.4 Requisiti/Vincoli di Configurazione

Configurazione SW

Non sono previste esigenze particolari rispetto all'ambiente standard NSIS.

Infrastruttura HW

Non sono previste esigenze particolari rispetto all'ambiente standard NSIS.

Infrastruttura Rete

Definita VLAN dedicata su Layer 3 per delimitare i flussi di comunicazione (logici e fisici) dell'apparato.

Specifiche di Sicurezza

Si raccomanda la conservazione dell'apparato in area protetta, rappresentando l'HSM la piattaforma per la gestione dei codici.

4.2 *Componente Architetturale Authentication Server/Reverse Proxy*

4.2.1 Razionali della componente architetturale

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. Il componente in oggetto viene gestito e implementato dal prodotto NetIQ Access Manager (NAM).

4.2.2 Integrazione con l'ambiente NSIS

Non sono previste variazioni degli elementi di integrazione.

4.2.3 Elementi di dimensionamento

Non sono previste variazioni degli elementi di dimensionamento.

4.2.4 Requisiti/Vincoli di Configurazione

Configurazione SW

Non sono previste esigenze particolari rispetto all'ambiente standard NSIS.

Infrastruttura HW

Non sono previste esigenze particolari rispetto all'ambiente standard NSIS.

Infrastruttura Rete

Non sono previste esigenze particolari rispetto all'ambiente standard NSIS.

Specifiche di Sicurezza

Non sono previste esigenze particolari rispetto all'ambiente standard NSIS.

4.3 Componente Architetturale Profile Manager**4.3.1 Razionali della componente architetturale**

Il modulo Admin Console necessita di una fase di autenticazione (Reverse Proxy) e di una fase di autorizzazione gestita tramite il prodotto *Profile Manager*.

4.3.2 Integrazione con l'ambiente NSIS

Non sono previste integrazioni diverse dallo standard NSIS.

4.3.3 Elementi di dimensionamento

È prevista la configurazione di tre ruoli al fine di autorizzare gli utenti ad accedere al modulo:

- Profilo Operatore

Indicatore	Valore	Crescita annua	Note
N° utenti registrati	10 circa	N/A	
Tipologia applicazione on line - batch	N/A	N/A	-

- Profilo Amministratore

Indicatore	Valore	Crescita annua	Note
N° utenti registrati	3 circa	N/A	
Tipologia applicazione on line - batch	N/A	N/A	-

- Profilo Operatore Regione

Indicatore	Valore	Crescita annua	Note
N° utenti registrati	40 circa	N/A	

Indicatore	Valore	Crescita annua	Note
Tipologia applicazione on line - batch	N/A	N/A	-

Non sono previste variazioni degli elementi di dimensionamento.

4.3.4 Requisiti/Vincoli di Configurazione

Configurazione SW

Non sono previste esigenze particolari rispetto all'ambiente standard NSIS.

Infrastruttura HW

Non sono previste esigenze particolari rispetto all'ambiente standard NSIS.

Infrastruttura Rete

Non sono previste esigenze particolari rispetto all'ambiente standard NSIS.

Specifiche di Sicurezza

Non sono previste esigenze particolari rispetto all'ambiente standard NSIS.