

ARCHITETTURA TECNICA

Sottosistema di Sicurezza

Indice

1	Impianto architetturale	1-5
1.1	<i>Component Model</i>	1-5
1.2	<i>Mapping Funzionale-Architetturale (UML)</i>	1-8
1.2.1	Design view.....	1-8
1.2.2	Interaction view.....	1-14
1.2.3	Implementation view.....	1-16
1.3	<i>Mapping Architetturale-Tecnologico (TOGAF)</i>	1-16
1.3.1	Application Architecture.....	1-16
1.3.2	Data Architecture	1-17
1.3.3	Technology Architecture.....	1-18
1.3.3.1	Infrastruttura dei sistemi.....	1-18
1.3.3.2	Infrastruttura di sicurezza.....	1-20
2	Componenti Architetturali.....	2-21
2.1	<i>Componente Architetturale Novell Identity Server</i>	2-22
2.1.1	Razionali della componente architetturale	2-22
2.1.2	Elementi di dimensionamento.....	2-22
	<i>Dimensionamento Infrastruttura</i>	2-23
2.1.2.1	Capacità Elaborativa	2-23
2.1.2.2	Spazio Disco.....	Errore. Il segnalibro non è definito.
2.1.2.3	Ampiezza di Banda di Rete	Errore. Il segnalibro non è definito.
2.1.3	Requisiti/Vincoli di Configurazione	2-23
2.2	<i>Componente Architetturale Novell Access Gateway</i>	2-24
2.2.1	Razionali della componente architetturale	2-24
2.2.2	Elementi di dimensionamento.....	2-24
	<i>Dimensionamento Infrastruttura</i>	2-25
2.2.2.1	Capacità Elaborativa	2-25
2.2.2.2	Spazio Disco.....	Errore. Il segnalibro non è definito.
2.2.2.3	Ampiezza di Banda di Rete	Errore. Il segnalibro non è definito.
2.2.3	Requisiti/Vincoli di Configurazione	2-25
2.3	<i>Componente Architetturale di sincronizzazione Metadirectory Novell IDM</i>	2-25
2.3.1	Razionali della componente architetturale	2-25
2.3.2	Integrazione con l'ambiente SISN.....	2-27
2.3.3	Elementi di dimensionamento.....	2-27
2.3.3.1	Capacità Elaborativa	2-27
2.3.3.2	Spazio Disco.....	Errore. Il segnalibro non è definito.8
2.3.3.3	Ampiezza di Banda di Rete	Errore. Il segnalibro non è definito.8
2.3.4	Requisiti/Vincoli di Configurazione	2-27
2.4	<i>Componente Architetturale IDEAS Profile Manager</i>	2-28
2.4.1	Razionali della componente architetturale	2-31
2.4.2	Integrazione con l'ambiente SISN.....	2-31
2.4.3	Elementi di dimensionamento.....	2-31
	<i>Indicatori di Dimensionamento</i>	2-31
	<i>Dimensionamento Infrastruttura</i>	2-32
2.4.3.1	Capacità Elaborativa	2-32
2.4.3.2	Spazio Disco.....	Errore. Il segnalibro non è definito.

2.4.3.3	Ampiezza di Banda di Rete	Errore. Il segnalibro non è definito.
2.4.4	Requisiti/Vincoli di Configurazione	2-32
2.5	<i>Componente Architetturale di IDEAS Audit</i>	2-323
2.5.1	Razionali della componente architetturale	2-32
2.5.2	Integrazione con l'ambiente SISN	2-35
2.5.3	Elementi di dimensionamento	2-35
	<i>Indicatori di Dimensionamento</i>	2-35
	<i>Dimensionamento Infrastruttura</i>	2-35
2.5.3.1	Capacità Elaborativa	2-35
2.5.3.2	Spazio Disco	Errore. Il segnalibro non è definito.
2.5.3.3	Ampiezza di Banda di Rete	Errore. Il segnalibro non è definito.
2.5.4	Requisiti/Vincoli di Configurazione	2-35
2.6	<i>Componente Architetturale Novell eDirectory (eDir)</i>	2-36
2.6.1	Razionali della componente architetturale	2-36
2.6.2	Integrazione con l'ambiente SISN	2-37
2.6.3	Elementi di dimensionamento	2-37
	<i>Indicatori di Dimensionamento</i>	2-37
	<i>Dimensionamento Infrastruttura</i>	2-38
2.6.3.1	Capacità Elaborativa	2-38
2.6.3.2	Spazio Disco	Errore. Il segnalibro non è definito.
2.6.3.3	Ampiezza di Banda di Rete	Errore. Il segnalibro non è definito.
2.6.4	Requisiti/Vincoli di Configurazione	2-38
2.7	<i>Componente Architetturale AccessPortal</i>	2-39
2.7.1	Razionali della componente architetturale	2-39
2.7.2	Elementi di dimensionamento	2-39
	<i>Indicatori di Dimensionamento</i>	2-39
	<i>Dimensionamento Infrastruttura</i>	2-40
2.7.3	Requisiti/Vincoli di Configurazione	2-40
2.8	<i>Componente Architetturale IDEAS Profile Provisioning (SWIM)</i>	2-40
2.8.1	Razionali della componente architetturale	2-40
2.8.2	Elementi di dimensionamento	2-41
	<i>Indicatori di Dimensionamento</i>	2-41
	<i>Dimensionamento Infrastruttura</i>	2-41
2.8.3	Requisiti/Vincoli di Configurazione	2-41
2.9	<i>Componente Architetturale Crypto Server(CS)</i>	2-423
2.9.1	Razionali della componente architetturale	2-423
2.9.2	Elementi di dimensionamento	2-43
	<i>Indicatori di Dimensionamento</i>	2-43
	<i>Dimensionamento Infrastruttura</i>	2-43
2.9.3	Requisiti/Vincoli di Configurazione	2-43
2.10	<i>Componente Architetturale Sign@Web</i>	2-44
2.10.1	Razionali della componente architetturale	2-44
2.10.2	Elementi di dimensionamento	2-44
	<i>Indicatori di Dimensionamento</i>	2-44
	<i>Dimensionamento Infrastruttura</i>	2-45
2.10.3	Requisiti/Vincoli di Configurazione	2-45
2.11	<i>Componente Architetturale IDEAS Account Provisioning</i>	2-45
2.11.1	Razionali della componente architetturale	2-45
2.11.2	Elementi di dimensionamento	2-45

<i>Indicatori di Dimensionamento</i>	2-46
<i>Dimensionamento Infrastruttura</i>	2-467
2.11.3 Requisiti/Vincoli di Configurazione	2-467
2.12 <i>Componente Architetture SISN RAC 10g</i>	2-47
2.12.1 Razionali della componente architetture	2-47
2.12.2 Elementi di dimensionamento	2-47

1 Impianto architetturale

In questa sezione si riportano le specifiche architetture del sottosistema di sicurezza del Sistema Informativo Sanitario Nazionale (SISN), in particolare con riferimento alle recenti evoluzioni operate per il Sistema che fornisce i servizi di Autenticazione e Autorizzazione (SAA) degli utenti che accedono alle risorse informatiche (applicazioni, funzionalità) messe a disposizione dal Ministero della Salute.

1.1 Component Model

Il **Component Model** è uno schema di base utilizzato per correlare gli aspetti applicativi di un'infrastruttura ICT all'architettura fisica; esso consente di suddividere e relazionare le differenti componenti architetture coinvolte all'interno del SISN e di rappresentare le integrazioni (in termini di flussi di dati e/o di richiami funzionali) tra i moduli stessi.

In questo contesto per "Componente Architetturale" si intende un elemento isolabile dell'architettura del SISN che rappresenta univocamente caratteristiche tecnologico/funzionali proprie.

Nello schema del Component Model sono indicate, con riferimento alla recente evoluzione architetturale dal vecchio al nuovo sistema di sicurezza:

- le **componenti architetture nuove ed esistenti** coinvolte;
- le **componenti architetture nuove introdotte**
- le **componenti architetture esistenti** che prevedono una qualche **aggiunta/variazione** in termini di configurazione/funzionalità

Lo schema Component Model è di seguito illustrato per mezzo dei *deployment diagram* UML, che consentono di identificare le diverse componenti coinvolte.

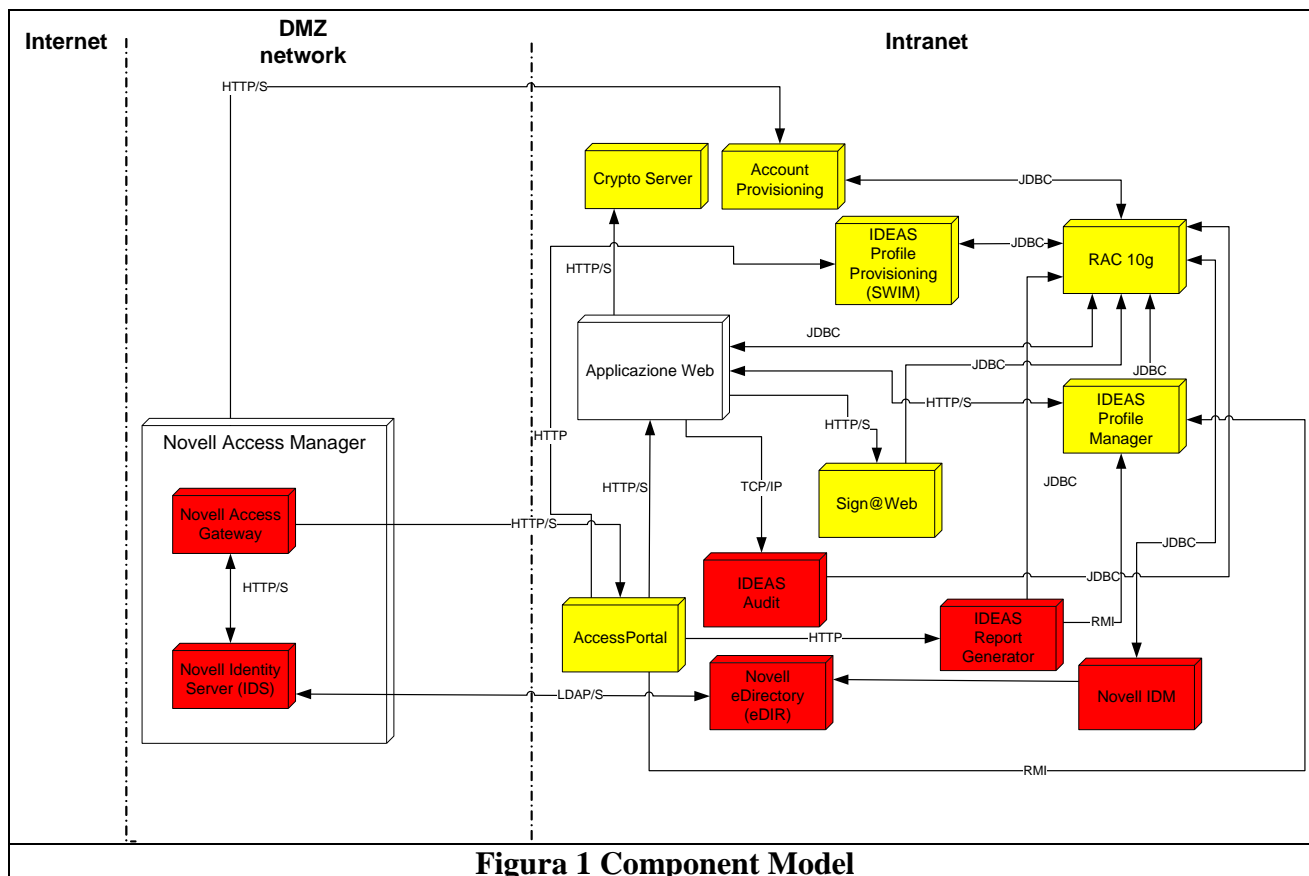
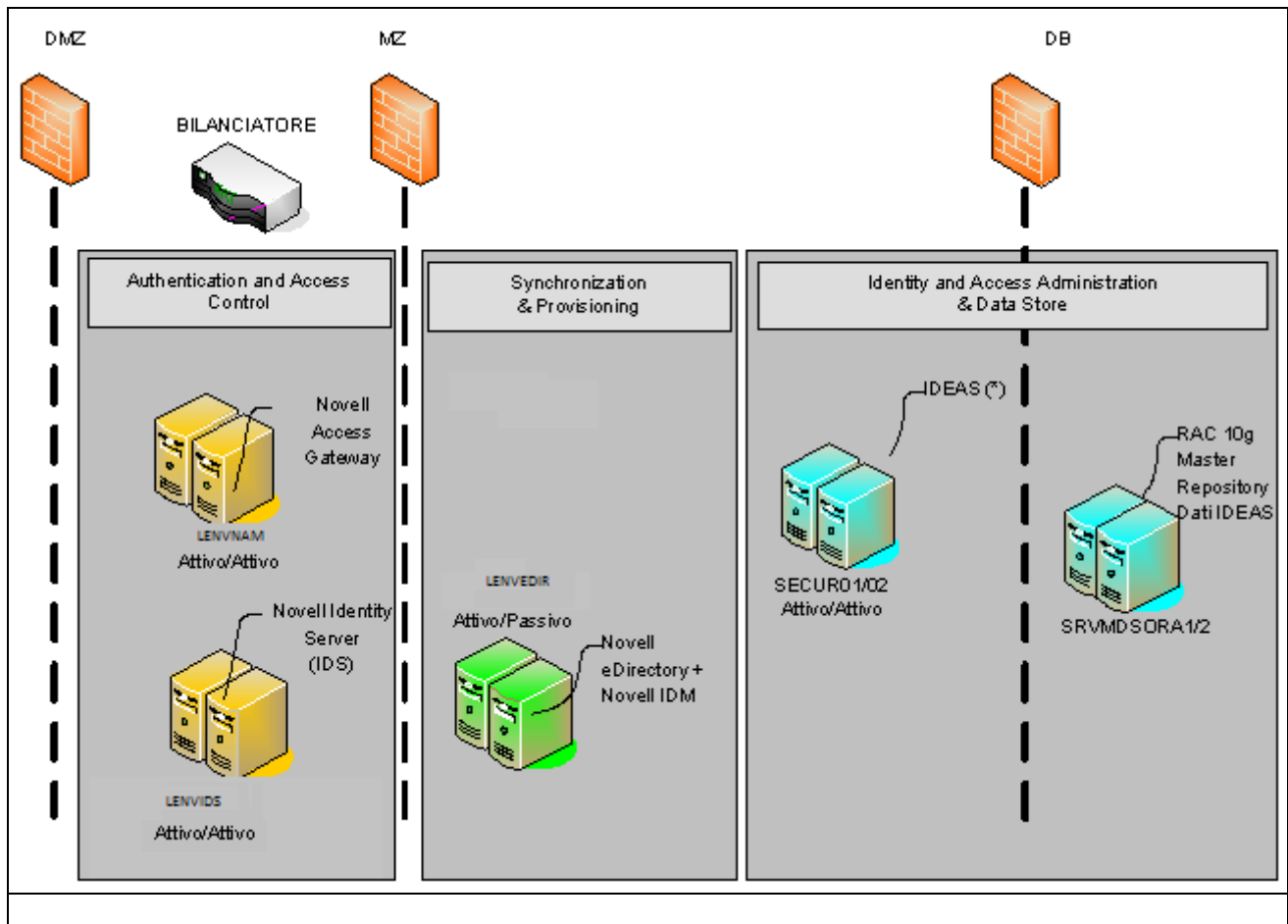


Figura 1 Component Model

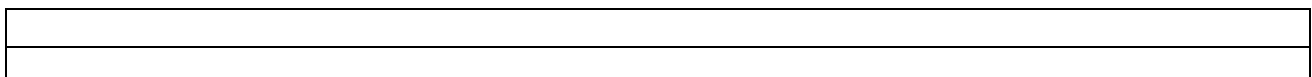
Di seguito si riporta l'architettura fisica del Sistema di Autenticazione e Autorizzazione (SAA)

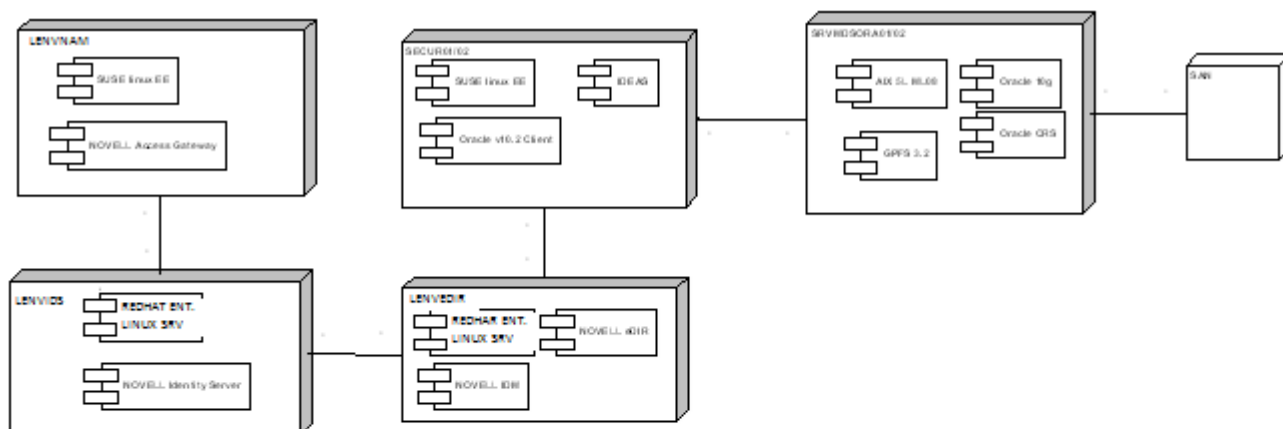


(*) La dicitura IDEAS indica i seguenti componenti software di terze parti:

- Access Portal;
- IDEAS Profile Provisioning;
- IDEAS Profile Manager;
- Crypto Server;
- IDEAS Account Provisioning;
- IDEAS Audit;
- IDEAS Report Generator;
- Sign@Web.

Di seguito si riporta il *deployment diagram* del Sistema di Autenticazione e Autorizzazione (SAA)





1.2 Mapping Funzionale-Architetturale (UML)

In questa sezione si fornisce la descrizione dell'architettura del SAA in una **logica applicativo-architetturale**, con riferimento ai seguenti aspetti:

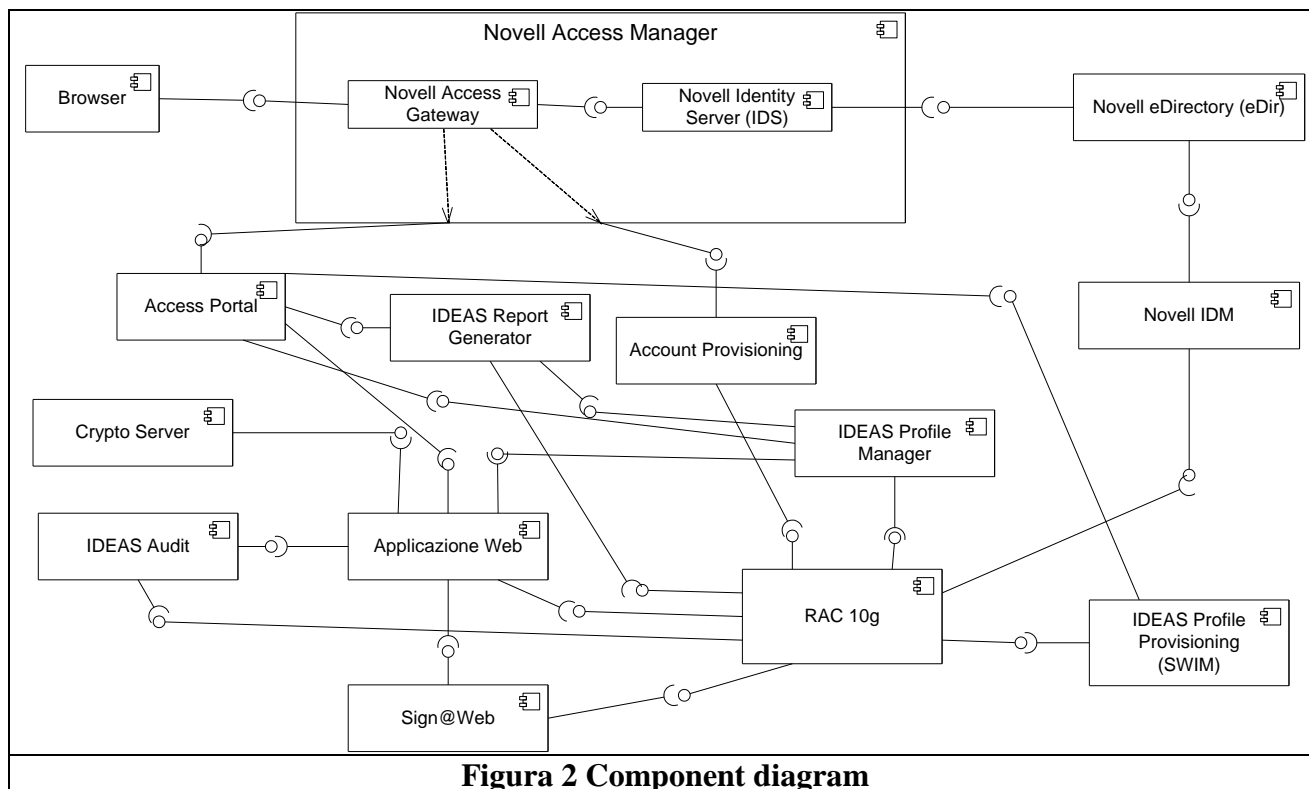
- il contesto (ambiente esterno) in cui il sistema si colloca;
- l'organizzazione interna del sistema in componenti applicative/architetturali e le modalità in cui tali componenti interagiscono tra loro per fornire le funzionalità complessive di utilizzo
- le tecnologie software utilizzate per l'implementazione delle componenti.

Per la descrizione si fa ricorso alle seguenti viste UML:

- Design view
- Implementation view
- Interaction view

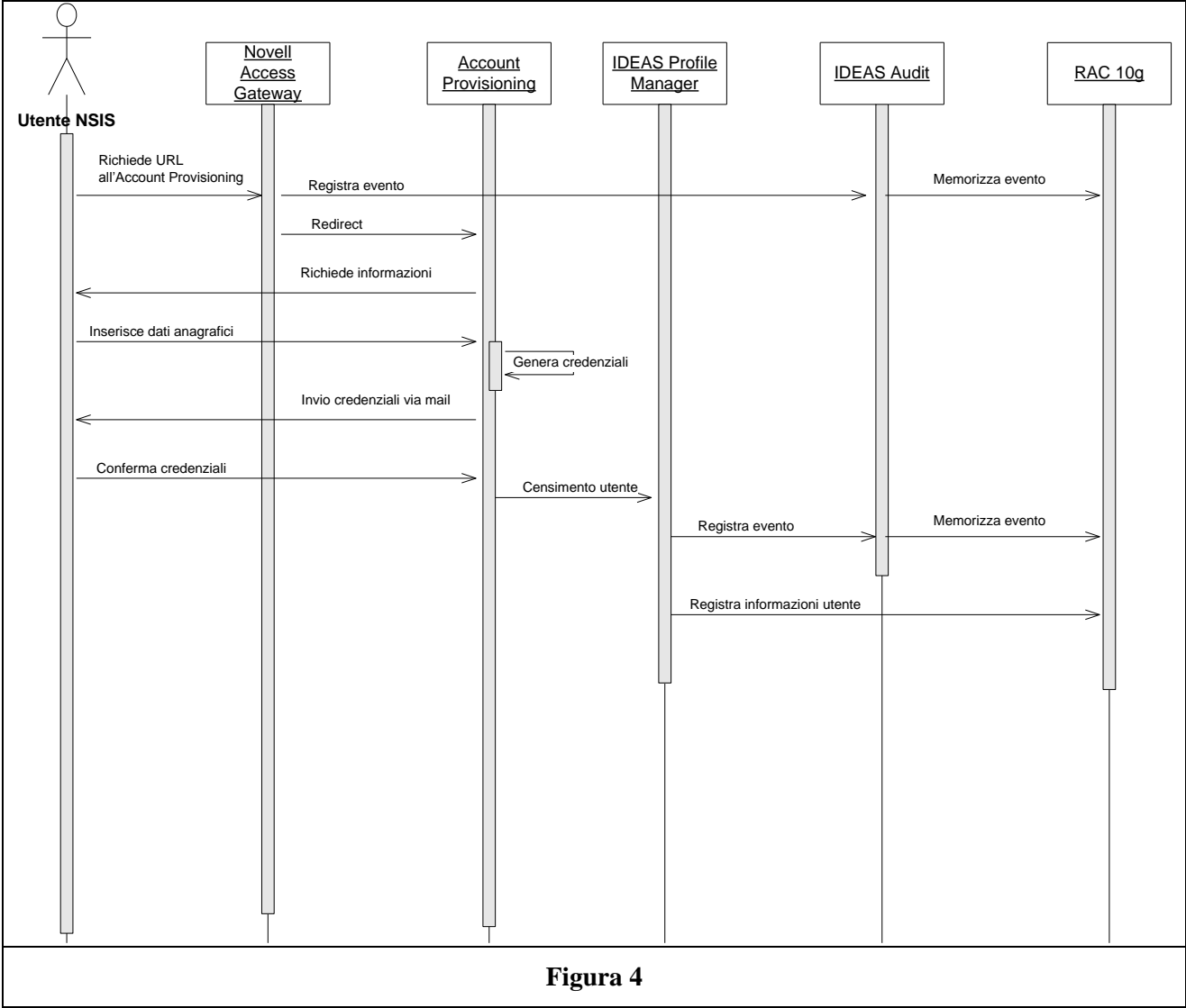
1.2.1 Design view

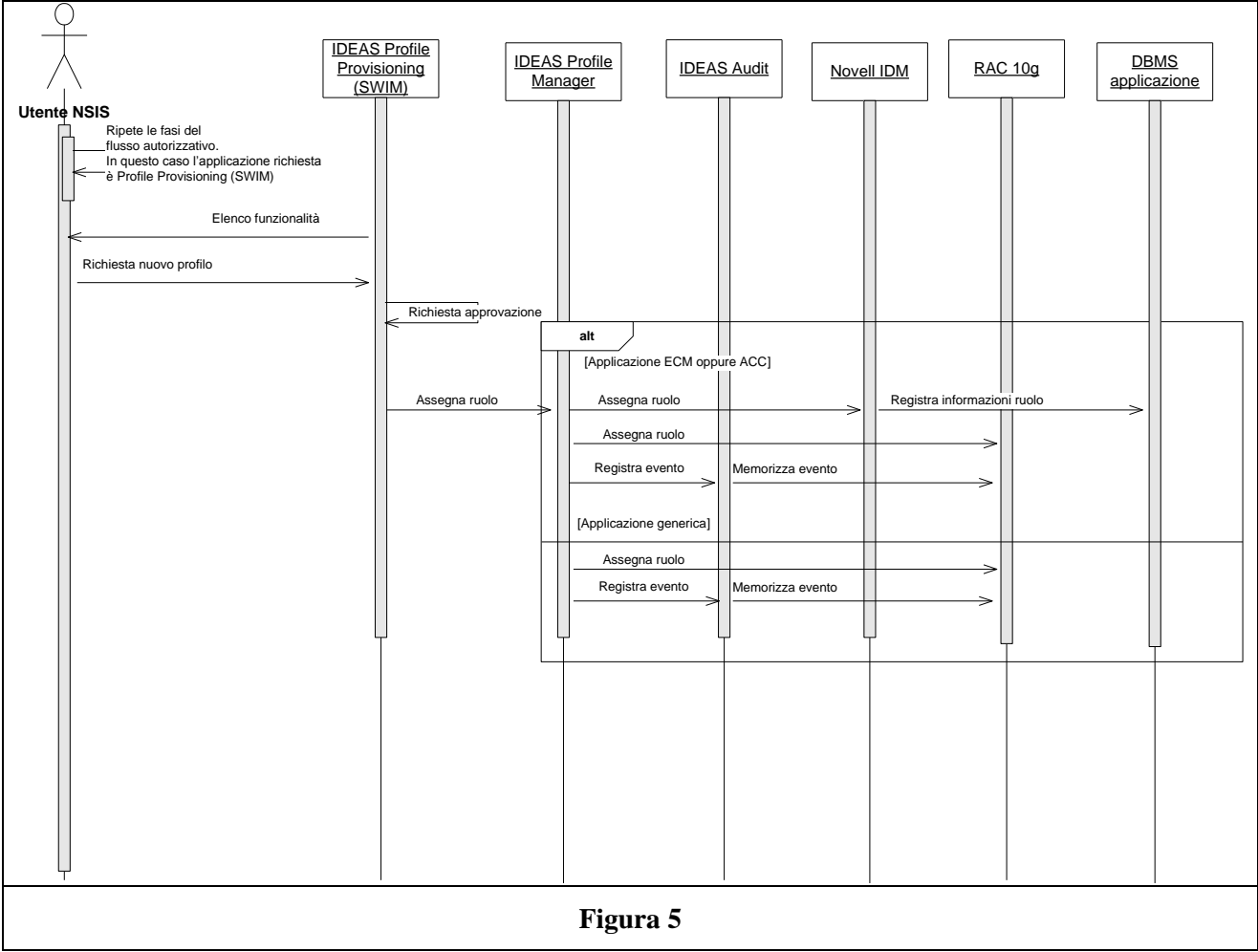
Di seguito viene riportato il *component diagram* del sistema di autenticazione ed autorizzazione.

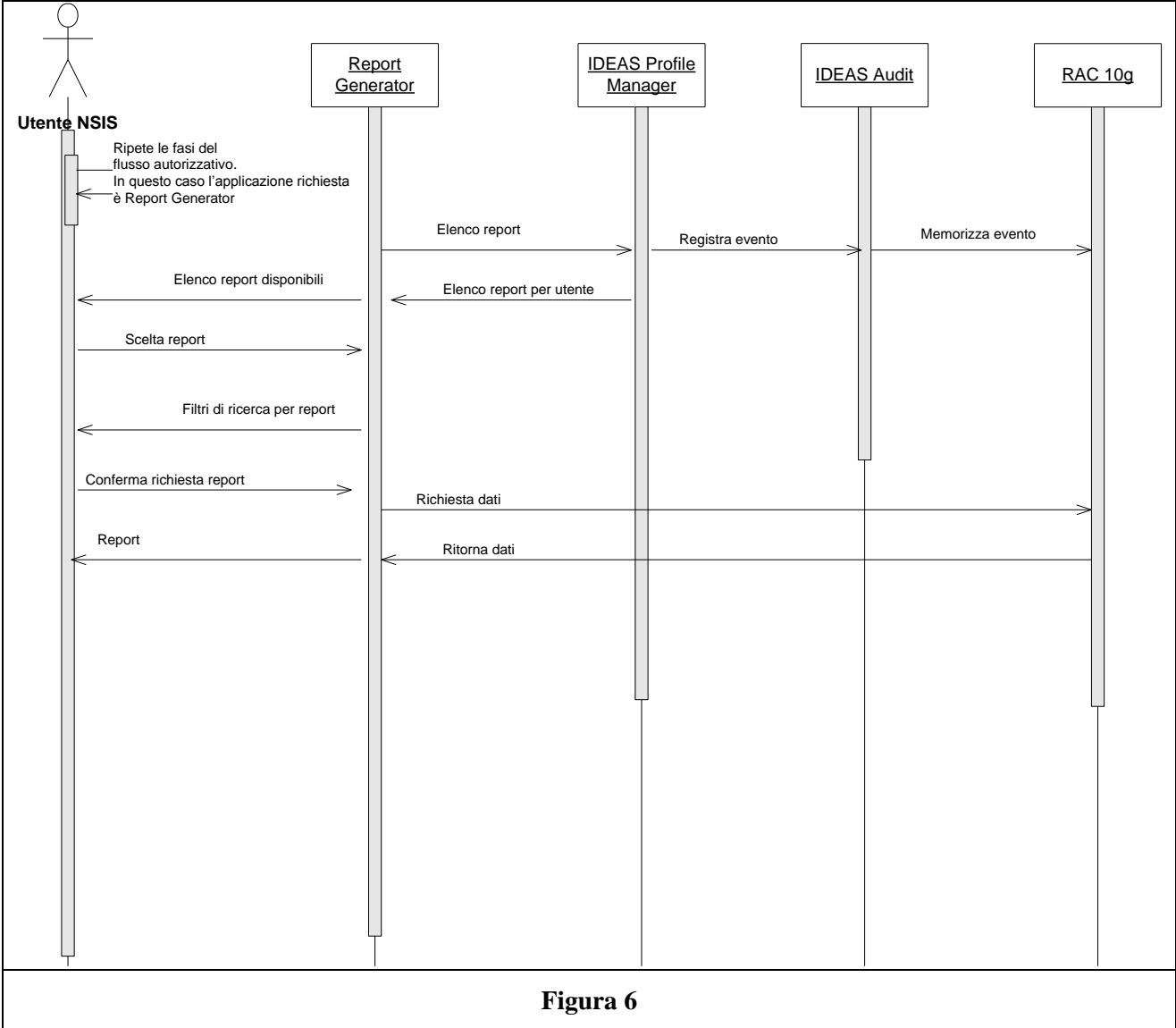


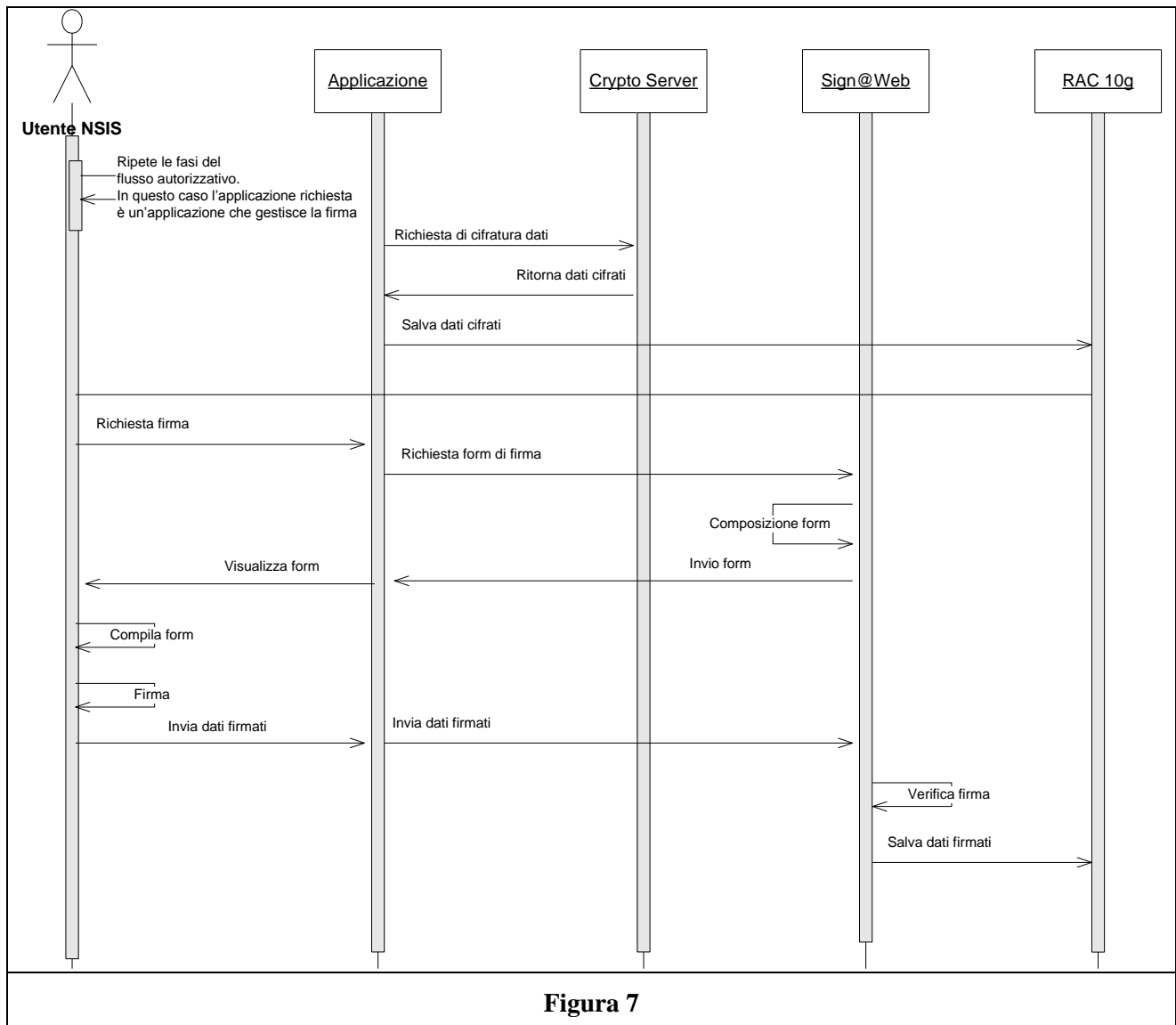
Per la descrizione degli aspetti dinamici di interazione tra le componenti del sistema, si riportano i *sequence diagram* relativi al flusso autorizzativo (Figura 3), alla registrazione di un utente (Figura 4), alla richiesta di autorizzazione (Figura 5), alla richiesta e generazione di report (Figura 6), e alla cifratura di dati e di firma digitale (Figura 7).











1.2.2 Interaction view

Tutti i colloqui tra le componenti architetturali avvengono mediante il certificato X509, ad eccezione di quelli tra le componenti Access Portal e Profile Provisioning e tra Access Portal e applicazioni SISN, che avvengono invece attraverso un token SAML firmato.

Le applicazioni, a seconda della loro tipologia, sono integrate al Sistema di Autenticazione e Autorizzazione attraverso le modalità di seguito indicate.

1. Modalità d'integrazione con il servizio di autenticazione:
 - integrazione di tipo unificato, attraverso l'uso del software Novell Access Manager (NAM)
 - integrazione di tipo custom, attraverso l'uso del software IDEAS Profile Manager
 - integrazione di tipo custom, senza l'uso del software IDEAS Profile Manager
2. Modalità d'integrazione con il servizio di Autorizzazione:
 - integrazione totale

- integrazione parziale, mediante l'uso di un repository applicativo

L'integrazione che comporta il minimo impatto sulle applicazioni è quella che prevede l'autenticazione unificata e l'autorizzazione parziale e prevede la creazione di un connettore.

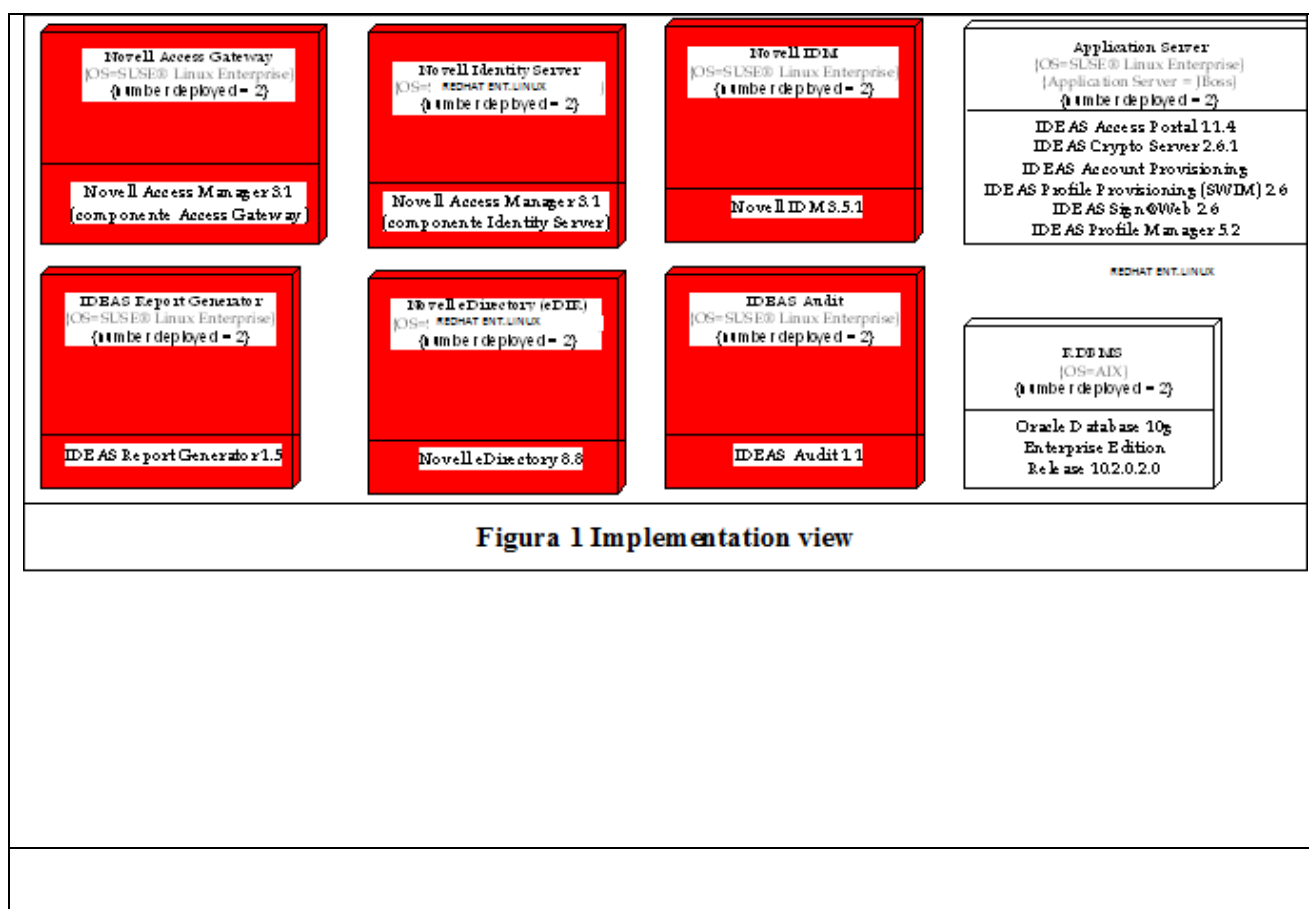
Di seguito sono riportati i flussi tra i moduli.

Modulo chiamante	INPUT	Modulo chiamato	OUTPUT
Browser	Credenziali di accesso	Novell Access Manager	Accesso all'applicazione
Novell Identity Server	Credenziali di accesso	Novell eDirectory	Esito verifica credenziali di accesso
Novell IDM	Dati per sincronizzazione utenze	Novell eDirectory	Dati utenze sincronizzati
Applicazione Web	Informazioni delle operazioni eseguite	IDEAS Audit	Salvataggio informazioni su DBMS
Access Portal	Dati utente	IDEAS Report Generator	Tipi di report
Novell Access Manager	Funzione di Proxy	Account Provisioning	Pagina di registrazione utente
Account Provisioning	Dati anagrafici utente	RAC 10g	N.A.
Applicazione Web	Dati da criptare	Cripto Server	Dati criptati
AccessPortal	Token SAML	Ideas Profile Provisioning (SWIM)	Home Page SWIM
AccessPortal	Token SAML	Applicazione Web	Home page Applicazione
Novell Access Manager	Credenziali di accesso	AccessPortal	Home page AccessPortal
AccessPortal	Token SAML	IDEAS Profile Manager	Elenco autorizzativi
Novell IDM	Eventi da e verso IDEAS Profile Manager	RAC 10g	N.A.
IDEAS Audit	Eventi da loggare	RAC 10g	N.A.
IDEAS Report Generator	Dati utente	IDEAS Profile Manager	Elenco tipi di report per utente
IDEAS Profile Manager	Modello RBAC	RAC 10g	Modello RBAC
Sign@Web	Dati firmati	RAC 10g	N.A.
Applicazione Web	Token SAML	IDEAS Profile Manager	Elenco autorizzazioni
Applicazione Web	Dati da firmare	Sign@Web	Dati firmati
Applicazione Web	Dati applicativi	RAC 10g	N.A.
IDEAS Profile Provisioning	Richieste di	RAC 10g	N.A.

(SWIM)	workflow autorizzativi		
IDEAS Report Generator	Tipo di report e dati utente	RAC 10g	Dati per report

1.2.3 Implementation view

Lo schema UML *Implementation View*, di seguito illustrato, evidenzia gli artefatti utilizzati per l'implementazione e l'assemblaggio delle varie componenti dell'architettura fisica del SAA.



1.3 Mapping Architetturale-Tecnologico (TOGAF)

1.3.1 Application Architecture

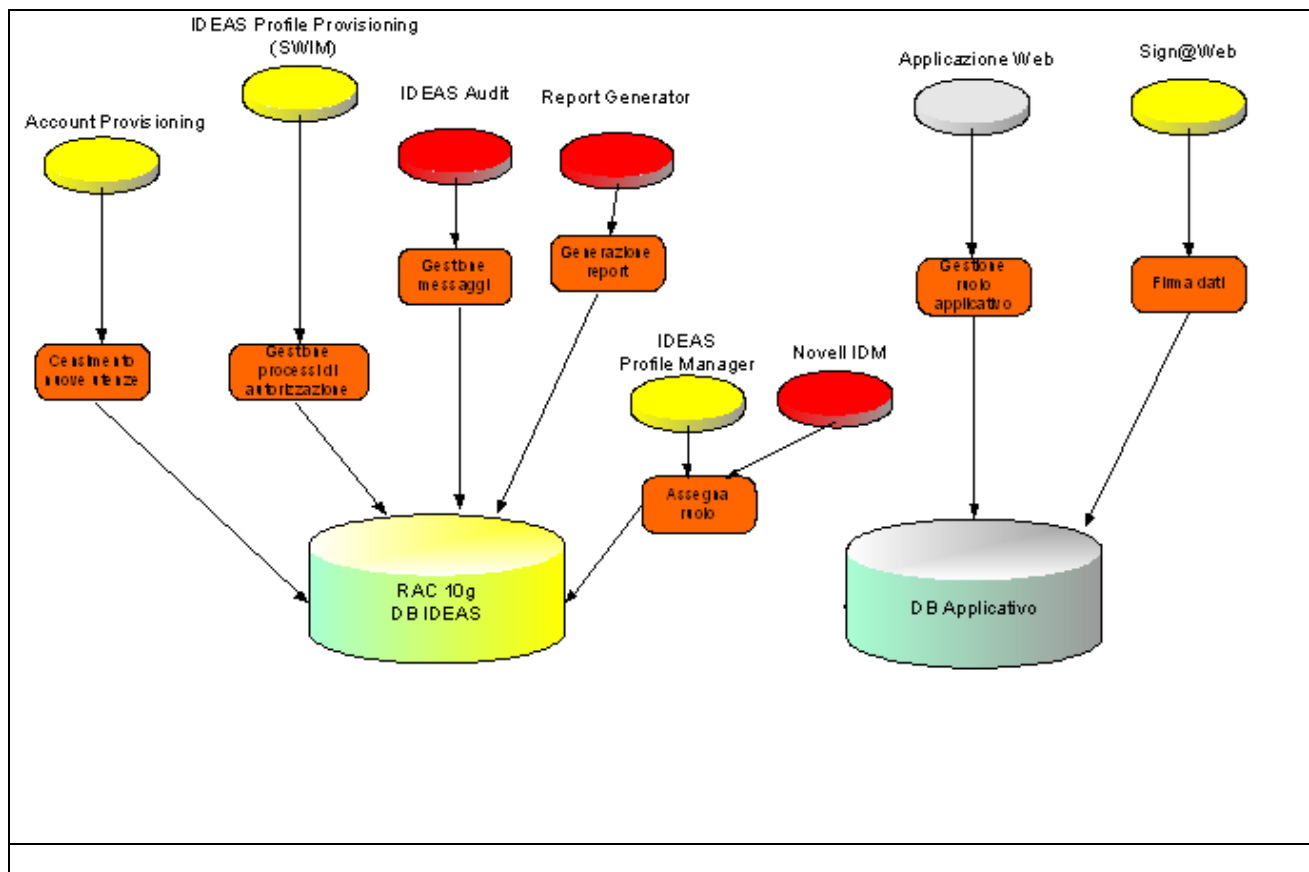
Gli artefatti riportati nella Figura 10 sono descritti nella tabella seguente in termini delle componenti applicative da cui sono costituiti.

Artefatti	Componenti applicative
Novell Access Gateway	SUSE® Linux Enterprise NetIQ Access Manager - Access Gateway Appliance 4.3 (componente Access Gateway)

Novell Identity Server	Red Hat Enterprise Linux Server release 6.7 NetIQ Access Manager - Access Gateway Appliance 4.3 (componente Identity Server)
IDEAS Audit	SUSE® Linux Enterprise IDEAS Audit 1.1
Novell eDirectory (eDir)	Red Hat Enterprise Linux Server release 6.7 NetIQ eDirectory 8.8
IDEAS Report Generator	SUSE® Linux Enterprise IDEAS Report Generator 1.5
Novell IDM	Red Hat Enterprise Linux Server release 6.7 NetIQ IDM 4.5
Application Server	SUSE® Linux Enterprise JBoss IDEAS Access Portal 1.1.4 IDEAS Crypto Server 2.6.1 IDEAS Account Provisioning IDEAS Profile Provisioning (SWIM) 2.6 IDEAS Sign@Web 2.6 IDEAS Profile Manager 5.2
RDBMS	AIX Oracle Database 10g Enterprise Edition 10.2.0.2

1.3.2 Data Architecture

Nello schema seguente è rappresentata l'integrazione dei vari moduli che concorrono all'alimentazione dei dati trattati dal SAA, con l'evidenza dei processi attraverso i quali tale integrazione ha luogo.

**LEGENDA:**

	Processi manuali
	Componenti preesistenti e modificati
	Componenti nuove
	Componenti coinvolte

1.3.3 Technology Architecture

1.3.3.1 Infrastruttura dei sistemi

L'infrastruttura hardware e software su cui è attestato il Sistema di Autenticazione e Autorizzazione, con riferimento a quanto riportato nelle figure 2 e 3, può essere considerata composta dai tre strati logico-fisici ("Authentication and Access Control", "Identity and Access Administration & Data Store", "Synchronization & Provisioning"), che sono descritti di seguito in termini dei moduli che li compongono.

*Authentication and Access Control***Novell Access Gateway Server**

La componente Novell Access Gateway, presente sui nodi NAM, implementa un reverse proxy di gestione del traffico Http tra il browser ed il server Web.

Software: NetIQ Access Manager - Access Gateway Appliance 4.3 - Componente Novell Access Gateway

Clustering: Il sistema di load balancer dispatcher (LB) provvede a rilevarne lo stato e a disabilitare logicamente l'eventuale sistema non funzionante.

Strategia Backup: Questo nodo non contiene e/o gestisce dati.

Novell Identity Server

Il Novell Identity server, presente sui nodi LENVIDS, è la componente che gestisce l'autenticazione delle utenze.

Software: NetIQ Access Manager - Access Gateway Appliance 4.3- Componente Novell Identity Server

Clustering: Il sistema provvede a rilevarne lo stato e a disabilitare logicamente l'eventuale sistema non funzionante.

Strategia Backup: Questo nodo non contiene e/o gestisce dati.

Identity and Access Administration & Data Store

Suite IDEAS

Sui nodi SECURNEW sono presenti l'application server per le applicazioni di IDEAS Profile Manager, IAM Tools e IDEAS Profile Provisioning e le componenti di Reporting.

Software: Suite IDEAS con application server JBOSS

La suite IDEAS è composta dai seguenti elementi:

- IDEAS Access Portal 1.1.4;
- IDEAS Profile Provisioning (SWIM) 2.6;
- IDEAS Profile Manager 5.2;
- IDEAS Crypto Server 2.6.1;
- IDEAS Account Provisioning;
- IDEAS Audit 1.1;
- IDEAS Report Generator 1.5;
- IDEAS Sign@Web 2.6.

Clustering: Il sistema di access gateway provvede a rilevare lo stato degli application server e a disabilitare logicamente il sistema eventualmente non funzionante. Un singolo access gateway può ridistribuire il carico su entrambi i sistemi JBoss nel caso che questa componente sia attiva.

Strategia Backup: Questo nodo non contiene e/o gestisce dati.

RAC 10g

Tale componente, presente sul nodo SRVMDSORA, è una componente architetturale SISR, esistente, che fornisce funzionalità di DataBase Management System (DBMS) relazionale.

Synchronization & Provisioning

Sui nodi EDIR sono implementate le componenti di Enterprise Directory (Novell eDirectory), Synchronization & Provisioning con i driver verso i sistemi target, Console di amministrazione iManager, Componente server del sistema di Audit.

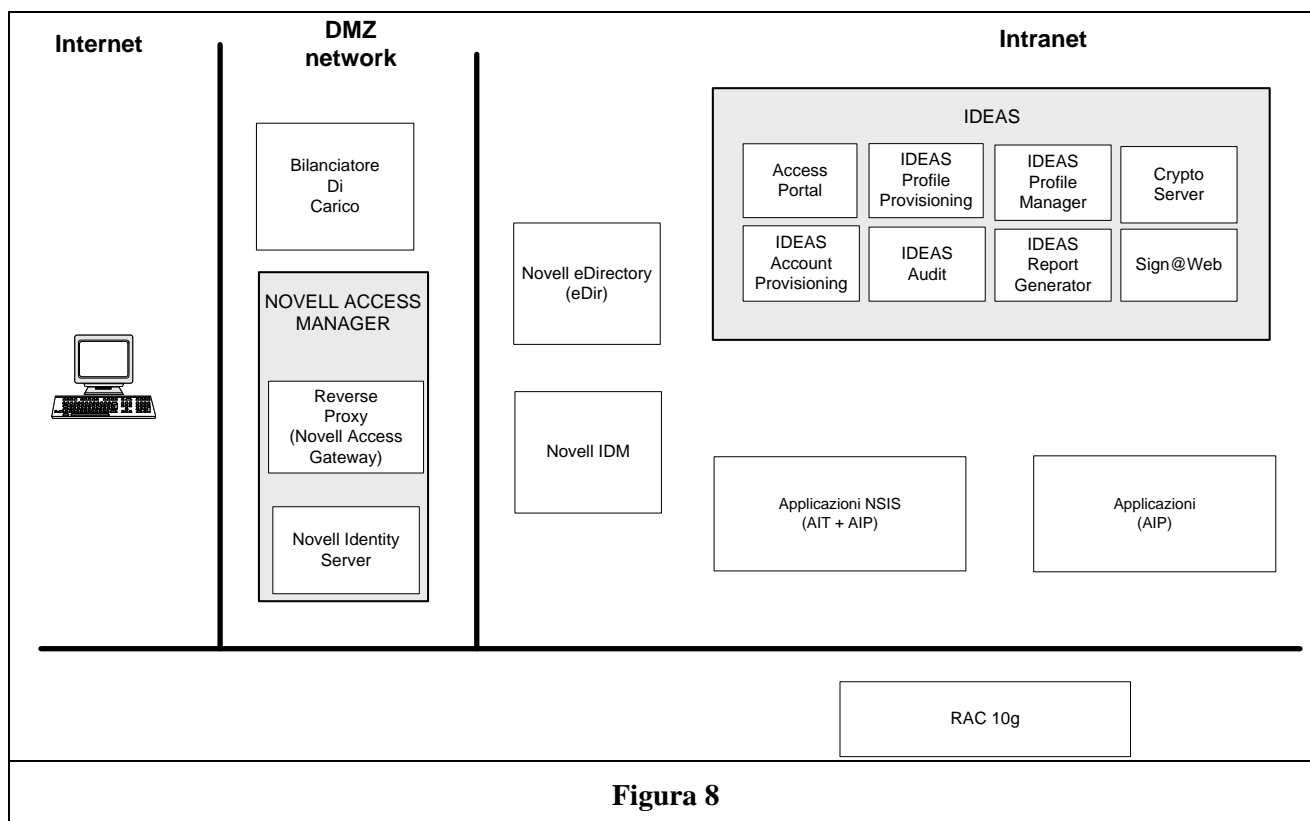
Software: Software per la gestione del cluster heartbeat per Linux; NetIQ IDM 4.5, eDirectory 8.8.

Clustering: Il sistema cluster assicura la continuità di servizio attraverso anche l'utilizzo di Storage Area Network.

Strategia Backup: Questo nodo contiene e gestisce i dati relativi agli eventi in propagazione oltre ad una replica dell'Enterprise Directory. Viene eseguito il backup periodico delle directory dell'eDirectory con i programmi installati ed i file di configurazione.

1.3.3.2 Infrastruttura di sicurezza

Nello schema seguente sono riportate le componenti, già indicate nel "Component Model", che costituiscono l'architettura di sicurezza del SISN, che risulta dalla recente evoluzione del Sistema di Autenticazione e Autorizzazione.



2 Componenti Architettureali

In questa sezione si fornisce la descrizione dei sottosistemi di cui si compone il sistema di autenticazione e autorizzazione, sia in termini di funzionalità e servizi offerti, sia con riferimento agli aspetti attinenti le modalità d'integrazione di ciascun sottosistema con le altre componenti del SISN, il dimensionamento dell'infrastruttura e la configurazione.

Lo strato di accesso alle applicazioni del SISN è rappresentato dal sottosistema Novell Access **Manager**, la cui architettura, che è illustrata nella figura seguente, si compone dei seguenti componenti principali:

- Novell Identity Server
- Novell Access Gateway

Novell Access Manager è una soluzione software di web access control e web single sign on, che fornisce un'infrastruttura di sicurezza a supporto della strong authentication e identity federation per una qualsiasi web application da qualunque web browser.

Il software supporta gli standard di riferimento SAML 2.0, Liberty Alliance e WS-Security.

Le funzionalità che il software Novell Access Manager mette a disposizione consentono di:

- garantire il Single Sign-On su applicazioni web che utilizzano form authentication o basic authentication;
- raffinare la procedura di gestione dell'autorizzazione su applicazioni J2EE, attraverso l'utilizzo di agenti specifici;
- garantire l'accesso sicuro alle applicazioni, tramite l'encryption su un canale SSL, ad applicazioni che nativamente sono erogate su canale non crittografato;
- centralizzare sia l'autenticazione standard sia l'autenticazione forte per le applicazioni web già esistenti, senza la necessità di effettuare alcuna modifica alle applicazioni stesse;
- implementare la procedura di Identity Federation secondo gli standard SAML o Liberty Alliance, nell'ottica del "Distributed Single Sign On";
- gestire i permessi di accesso ad indirizzi IP o porte di comunicazione da parte di client esterni al firewall, su canale criptato, senza alcuna necessità di installare agenti sul PC; mediante l'utilizzo di un SSL-VPN client scaricato dinamicamente via web.

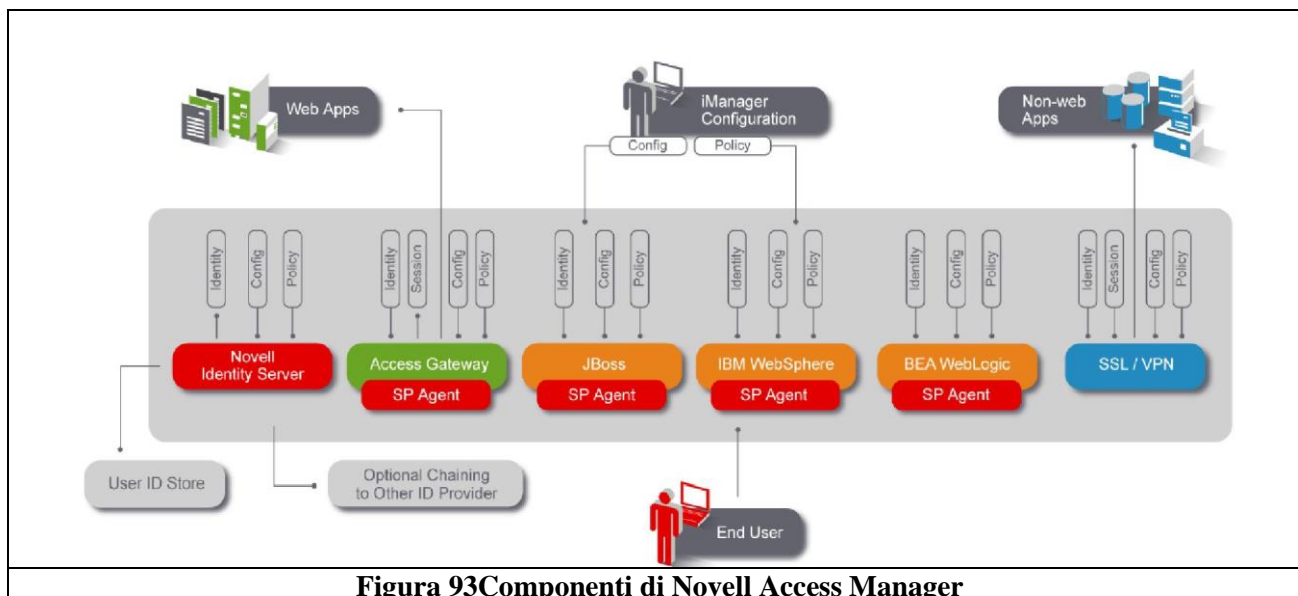


Figura 93Componenti di Novell Access Manager

2.1 Componente Architetture Novell Identity Server

2.1.1 Razionali della componente architetture

Novell Identity Server è la componente che gestisce l'autenticazione delle utenze e il supporto degli standard di federazione Liberty Alliance e SAML (versioni 1.1 e 2.0) nella comunicazione verso enti federati. Esso costituisce il punto di verifica dell'autenticazione e dei ruoli/permessi del singolo utente a garanzia dell'applicazione delle policy di accesso definite.

Novell Identity Server, supportando il paradigma del Federated Provisioning, consente implementare forme di federazione in cui l'utente può accedere sui siti federati in cui ancora non è stato censito, senza la necessità di effettuare alcuna forma di registrazione.

Novell Identity Server può avvalersi di uno o più database contenenti le informazioni sugli utenti; attualmente sono supportati i seguenti sistemi:

- Novell eDirectory™
- Sun ONE Directory Server
- Microsoft Active Directory

2.1.2 Elementi di dimensionamento

Indicatori di Dimensionamento

Si riportano di seguito gli indicatori di dimensionamento individuati per il componente di autenticazione Novell Identity Server:

Indicatore	Valore	Note
N° UTENTI COLLEGATI CONTEMPORANEAMENTE	~200	Valore stimato in base alla numerosità delle applicazioni ed al valore della popolazione utente

		delle stesse, come misurato sul sistema con gli strumenti di monitoraggio dell'infrastruttura
N° SESSIONI CONCORRENTI	~200	
SPAZIO FISICO OCCUPATO	~6 GB circa per ogni nodo coinvolto	La componente di autenticazione è distribuito su più nodi
TIPOLOGIA APPLICAZIONE ON LINE -BATCH	ON LINE	
NUMERO UTENTI ATTIVI	14.000	

Dimensionamento Infrastruttura

2.1.2.1 Capacità Elaborativa

Per i valori degli indicatori si può affermare che per il componente richiede due sistemi virtuali aventi le seguenti caratteristiche:

CPU: 4 VCPU

RAM: 4 GB

2.1.3 Requisiti/Vincoli di Configurazione

SW di Base

- Red Hat Enterprise Linux Server release 6.7
- NetIQ Access Manager - Access Gateway Appliance 4.3 (Componente Identity Server)

Infrastruttura HW

Il componente è utilizzato in configurazione ad alta affidabilità, in cluster Attivo/Attivo in modo da garantire le performance richieste e da eliminare la possibilità di avere un singolo punto di rottura (SPOF). Inoltre, per le specificità della componente Novell Identity Server e per le funzionalità di Federated Provisioning per le quali è possibile implementare forme di federazione con enti esterni si è scelto di installare questa componente software su un sistema dedicato avente le caratteristiche su riportate.

Infrastruttura Rete

Il componente non richiede configurazioni di rete particolari.

Specifiche di Sicurezza

Il componente, distribuita sulle due macchine esaminate precedentemente, si colloca nel segmento demilitarizzato della infrastruttura di rete del SISN (DMZ) ed utilizza un IP pubblico e un nome logico inserito nel DNS pubblico.

2.2 Componente Architetturale Novell Access Gateway

2.2.1 Razionali della componente architetturale

La componente Novell Access Gateway implementa il reverse proxy di gestione del traffico Http tra client browser e server Web.

Essa effettua il controllo in tempo reale dei diritti di accesso dell'utente sulla singola risorsa web ed è anche in grado di realizzare l'automazione del logon su applicazioni che implemento Form o Basic Authentication ai fini del Single Sign On.

Tale componente permette inoltre di effettuare l'encryption del traffico nella tratta tra Browser e Access Gateway in modo da rendere di tipo SSL l'accesso anche ad applicazioni che non lo consentono nativamente.

2.2.2 Elementi di dimensionamento

Indicatori di Dimensionamento

Di seguito gli indicatori di dimensionamento individuati per il componente Novell Access Gateway:

Indicatore	Valore	Note
N° UTENTI COLLEGATI CONTEMPORANEAMENTE	~200	Valore stimato in base alla numerosità delle applicazioni ed al valore della popolazione utente delle stesse, come misurato sul sistema con gli strumenti di monitoraggio dell'infrastruttura
N° SESSIONI CONCORRENTI	~200	
SPAZIO FISICO OCCUPATO	~6 GB circa per ogni nodo coinvolto	La componente di autenticazione è distribuito su più nodi
TIPOLOGIA APPLICAZIONE ON LINE -BATCH	ON LINE	
DIMENSIONE MEDIA PAGINA WEB	40 KB	
DIMENSIONE MASSIMA PAGINA WEB	80 KB	
TEMPO MEDIO DI ATTESA	5 sec.	Escludendo il tempo di rete.

Dimensionamento Infrastruttura**2.2.2.1 Capacità Elaborativa**

Per i valori degli indicatori si può affermare che per il componente richiede due sistemi virtuali con le seguenti caratteristiche:

CPU: 2 VCPU

RAM: 4 GB

2.2.3 Requisiti/Vincoli di Configurazione**SW di Base**

- SUSE® Linux Enterprise;
- NetIQ Access Manager - Access Gateway Appliance 4.3 (Componente Access Gateway)

Configurazione SW

Non sono necessarie configurazioni software particolari.

Infrastruttura HW

È garantita la continuità operativa del componente mediante la duplicazione dei sistemi, che garantisce altresì il bilanciamento del carico.

Infrastruttura Rete

Non sono necessarie particolari configurazioni di rete.

Specifiche di Sicurezza

Il componente è parte integrante della infrastruttura di sicurezza e costituisce una parte della componente di autenticazione. Esso, distribuito sulle due macchine esaminate precedentemente, si colloca nella segmento demilitarizzato della infrastruttura di rete del SISN (DMZ).

2.3 Componente Architetturale di sincronizzazione Metadirectory Novell IDM**2.3.1 Razionali della componente architetturale**

La sincronizzazione delle informazioni sulle utenze verso sistemi target esterni viene svolta dal modulo IDEAS ERC (Enterprise Repository Connector) che contiene il prodotto OEM Novell IDM 3.5.

Il componente Novell IDM (Identity Manager) è basato su un modello architetturale di tipo “hub & spoke”, in cui sono presenti:

- un motore di elaborazione centrale (Engine) che esegue le regole di trasformazione e associazione fra i dati che fluiscono da e per i vari sistemi integrati;
- più connettori (Drivers) configurabili ed estendibili specifici per i vari sistemi integrati

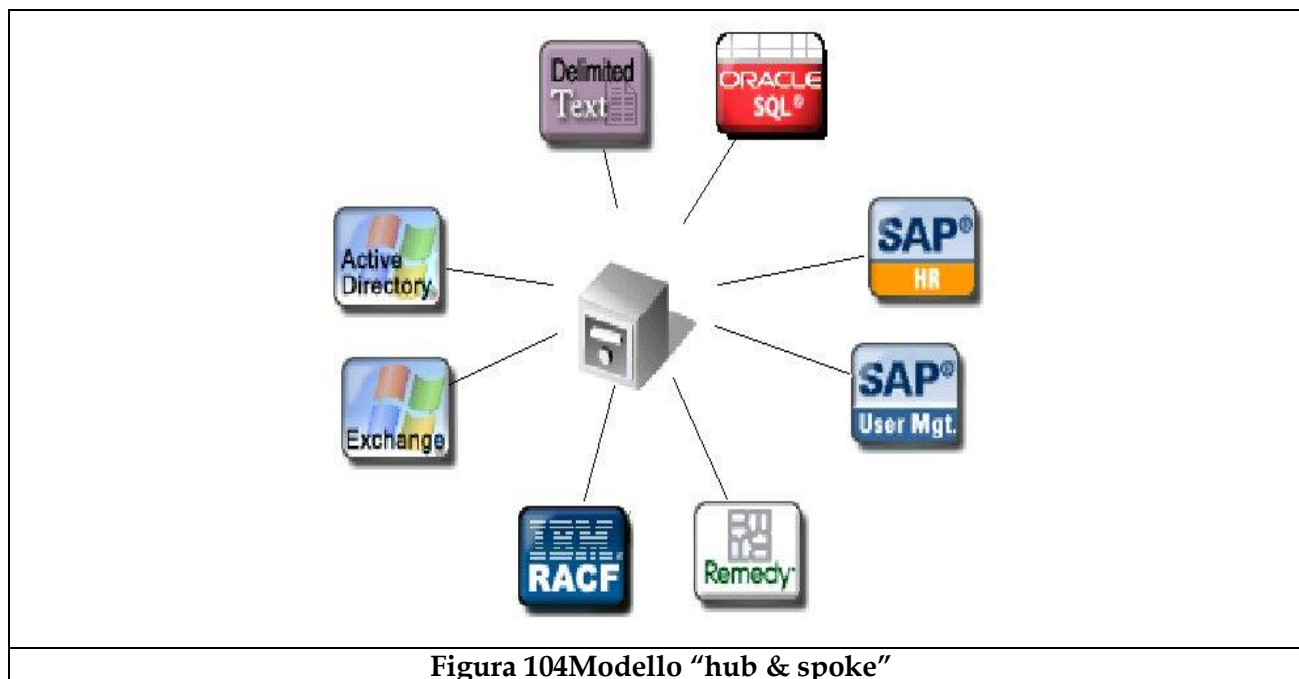


Figura 104 Modello "hub & spoke"

Ogni connessione con ciascun sistema integrato avviene tramite un driver specifico. E' inoltre disponibile un kit di sviluppo per la creazione ad hoc di driver per specifici sistemi.

In generale un driver di integrazione è un convertitore bidirezionale tra API o protocolli utilizzati da un certo sistema verso documenti XML elaborati dall'engine.

Nella lista che segue sono elencati i driver che risultano già disponibili.

Databases	Directories
IBM DB2 Informix Microsoft SQL Server MySQL Oracle Sybase JDBC	Critical Path InJoin Directory IBM Directory Server (SecureWay) iPlanet Directory Server Microsoft Active Directory Netscape Directory Server NIS NIS + Novell eDirectory Oracle Internet Directory Sun ONE Directory Server LDAP
Mainframe	E-mail systems
RACF ACF2 Top Secret	Microsoft Exchange 2000/2003/2007 Microsoft Exchange 5.5 Novell GroupWise® Lotus Notes
Midrange	PBX
i5OS (OS/400)	Avaya PBX Asterisk - (Partner Developed Driver) VoiceRD - (Partner Developed Driver)
Operating Systems	Other
SUSE® Linux Enterprise Debian Linux	Command Line Scripts Delimited Text

FreeBSD	Health Level 7 (HL7) - (Partner Developed Driver)
HP-UX	DSML
IBM AIX	Java Messaging Services (JMS) and IBM WebSphere MQ
Microsoft Windows NT Domain	Identity Manager Driver for RSA - (Partner Devel.
Red Hat AS and ES	Driver)
Red Hat Linux	Pulsen Snapshot - (3rd Party Driver)
Solaris	Remedy (for Help Desk)
UNIX Files - /etc/passwd	Schools Interoperability Framework (SIF)
	SOAP
	SPML
	EJBCA Certificate Driver-(3rd Party Driver)

Novell Identity Manager, ai fini dell'integrazione OEM con IDEAS Profile Manager, è configurato opportunamente per poter erogare solo i servizi di connettività con le risorse Target.

2.3.2 Integrazione con l'ambiente SISN

Il componente si integra con sia con il repository di utenze delle applicazioni SISN ad integrazione parziale sia con il repository unico del SISN. L'integrazione avviene mediante la realizzazione di driver specifici per ogni applicazione.

2.3.3 Elementi di dimensionamento

Indicatori di Dimensionamento

Di seguito gli indicatori di dimensionamento individuati per il componente di Metadirectory Novell Identity Manager

Indicatore	Valore	Note
<i>N° UTENTI ATTIVI</i>	14.000	
<i>N° OPERAZIONI MEDIO GIORNALIERO SULLE UTENZE REGistrate</i>	~100	
<i>SPAZIO FISICO OCCUPATO</i>	~6 GB circa per ogni nodo coinvolto	La componente di autenticazione è distribuita su più nodi
<i>TIPOLOGIA APPLICAZIONE</i>	BACKEND	

Dimensionamento Infrastruttura

2.3.3.1 Capacità Elaborativa

Per i valori degli indicatori si può affermare che per il componente richiede due sistemi virtuali con le seguenti caratteristiche:

CPU: 4 VCPU

RAM: 4 GB

2.3.4 Requisiti/Vincoli di Configurazione

SW di Base

- Red Hat Enterprise Linux Server release 6.7;
- NetIQ IDM 4.5

Configurazione SW

Non sono necessarie configurazioni software particolari.

Infrastruttura HW

È garantita la continuità operativa del componente mediante la duplicazione dei server, che garantisce altresì il bilanciamento del carico.

Infrastruttura Rete

Non sono necessarie particolari configurazioni di rete.

Specifiche di Sicurezza

Il componente è parte integrante della infrastruttura di sicurezza e costituisce una parte della componente di autenticazione. Esso, distribuito sulle due macchine esaminate precedentemente, si colloca nella segmento demilitarizzato della infrastruttura di rete del SISN (DMZ).

2.4 Componente Architetturale IDEAS Profile Manager

Il componente IDEAS Profile Manager è costituito dai seguenti moduli:

- RBIA Manager Console
- Rule Engine (RE)
- Event Manager Console

RBIA Manager Console

RBIA Manager Console costituisce lo strumento per l'utilizzo e la configurazione di IDEAS Profile Manager. Attraverso di essa si descrive il "REAME", cioè si popola il modello dell'organizzazione in esame e si definiscono i profili degli utenti che ne fanno parte.

E' possibile accedervi previa autenticazione (via userid/password, smartcard, ecc.) eseguita da un utente Super Amministratore di IDEAS Profile Manager, ovvero da un utente Amministratore di un particolare reame.

Nel sistema è sempre presente almeno un reame, indicato come "reame di amministrazione", che contiene l'elenco di tutti gli amministratori e le relative autorizzazioni.

All'interno di ogni reame è possibile definire uno o più amministratori; ogni amministratore può avere un diverso grado di visibilità rispetto a tutto il reame o solo ad una sua parte e un diverso insieme di funzionalità da gestire.

La console mostra a ciascun amministratore le sole funzionalità a cui lo stesso è abilitato e solo la parte del reame su cui può operare.

La web console consente diprodurre report e statistiche ad hoc oltre a mettere a disposizione i seguenti report precostituiti:

- Numero di Richieste dell'ultimo mese per tipologia

- Numero di Richieste dell'ultima settimana per tipologia
- Numero di Richieste dell'ultimo anno per tipologia
- Numero di richieste per utente per risorsa
- Eventi in ingresso
- Eventi in uscita
- Eventi da sistemi target
- Numero di utenti suddivisi per tipologia
- Numero di utenti illegali
- Numero di UO suddivise per tipologia utente
- Numero totale dei ruoli
- Numero totale dei ruoli assegnati alle UO
- Numero totale dei ruoli non assegnati alle UO
- Numero totale dei ruoli non assegnati agli utenti
- Monitoring in tempo reale del sistema

Rule Engine

Il Rule Engine (RE) è un componente software che si occupa della gestione e automatizzazione delle “regole di business” dell’organizzazione, cioè di tutti quei processi che possono subire frequenti cambiamenti rispetto ai normali processi applicativi.

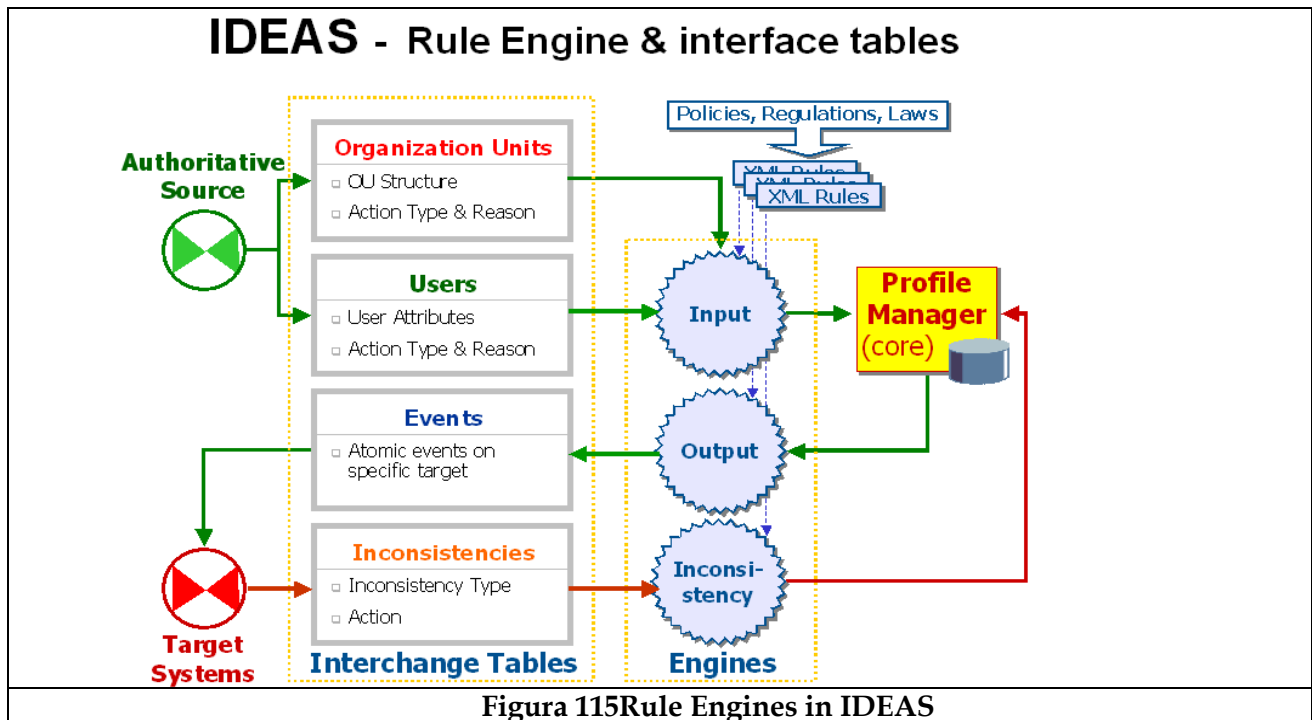
Ad esempio, quando si assegna un ruolo ad un utente, il generico processo standard prevede la registrazione dell’anagrafica dell’utente nel DB di IDEAS Profile Manager.

In aggiunta, potrebbe essere necessario prevedere la propagazione dei dati dell’utente verso un repository proprietario, dopo aver effettuato alcune trasformazioni di formato su un sottoinsieme di items dell’anagrafica.

Il RE è in grado di gestire la “personalizzazione” di questo processo; sulla base di una “regola”, il RE effettua le necessarie trasformazioni, prima di propagarle (attraverso un opportuno modulo del sottosistema Novell IDM) verso il repository proprietario.

Questo schema funzionale consente di adattare dinamicamente la gestione dei processi di un’organizzazione attraverso l’inserimento di nuove regole o la modifica/cancellazione del set di regole preesistenti, senza dover intervenire nella definizione della struttura dei processi.

Nella figura seguente viene descritta sinteticamente l’implementazione estesa del RE nell’ambito di IDEAS:



In particolare possiamo distinguere tre diversi RE:

- Input RE
- Output RE
- IncoSISNtency RE

L'Input RE considera come dominio dei dati l'Authoritative Source della generica organizzazione, che viene interfacciato da due tabelle, una inerente alla struttura organizzativa e un'altra contenente i dati degli utenti, dell'organizzazione medesima. L'Input RE agisce sul repository di riferimento di IDEAS (il DB di IDEAS Profile Manager).

L'Output RE, analogamente, considera come dominio dei dati il DB di IDEAS Profile Manager e attraverso la tabella d'interscambio Events, agisce sui sistemi target.

In tutti quei casi in cui si può verificare un'incoSISNtenza, cioè un disallineamento tra il core repository di IDEAS ed un generico sistema target, entra in azione l'IncoSISNtency RE allo scopo di porre riparo al disallineamento. L'intelligenza di questo framework risiede nelle "Regole". IDEAS dispone di una libreria di regole di default che sono il risultato di best practice sviluppate da Engiweb Security.

Event Manager (EM)

Event Manager è lo strumento che permette di tenere sotto controllo tutti gli eventi in entrata (incoming) e in uscita (outgoing) associati alle attività automatizzate del Rule Engine. Il primo scopo di EM è il monitoraggio del corretto funzionamento dei motori di regole. Durante le operazioni correnti, se ogni cosa funziona correttamente, le tabelle dati di interscambio dovrebbero essere vuote o con eventi nelle code di processing. La Web Console permette di visualizzare eventuali eventi non andati a buon fine, di correggere la causa del malfunzionamento e di rilanciare l'evento. È possibile inoltre decidere di abortire tutti gli eventi che per particolari motivi non richiedano più la loro esecuzione.

Event In Report	Reprocess (State=0)	Reprocessed (State=1)	Error (State=2)	Total
TOTALE	2080	204145	2103	208328
User ERC	2080	200035	1839	203954
CREATE USER Event (Operation=1)	0	7849	4	7853
MODIFY USER Event (Operation=2)	651	155532	1284	157467
DELETE USER Event (Operation=3)	1429	490	0	1919
MOVE EMPLOYEE Event (Operation=12)	0	36164	551	36715
OrgUnit ERC	0	4110	264	4374
CREATE OU Event (Operation=9)	0	1959	1	1960
MODIFY OU Event (Operation=10)	0	2149	263	2412
DELETE OU Event (Operation=11)	0	2	0	2

Figura 126 Console di Amministrazione dell'Event Manager: Report In-Events

In particolare gli IN events e i Target events sono eventi che, attivando specifiche regole, possono modificare dati del DB centrale di IDEAS Profile Manager.

Similmente, gli OUT events sono eventi che modificano le informazioni sui sistemi target.

Ogni operazione eseguita dal modulo IDEAS Profile Manager viene memorizzata sul sistema di audit IDEAS ALA.

2.4.1 Razionali della componente architetturale

IDEAS Profile Manager è lo strumento con il quale si modella l'organizzazione in esame, utilizzando il concetto di REAME, e si definiscono i profili degli utenti che ne fanno parte. E' sempre presente almeno un reame, il reame di amministrazione, che contiene l'elenco di tutti gli amministratori e le relative autorizzazioni. All'interno di ogni reame è possibile definire uno o più amministratori; ogni amministratore può avere un diverso grado di visibilità rispetto a tutto il reame o solo ad una sua parte e un diverso insieme di funzionalità da gestire

2.4.2 Integrazione con l'ambiente SISN

Il componente di autorizzazione si integra con le applicazioni mediante l'utilizzo di API fornite dal componente.

2.4.3 Elementi di dimensionamento

Indicatori di Dimensionamento

Di seguito gli indicatori di dimensionamento individuati per il componente IDEAS Profile Manager:

Indicatore	Valore	Note
N° UTENTI ATTIVI	14.000	
N° OPERAZIONI MEDIO GIORNALIERO SULLE UTENZE REGISTRATE	~100	
SPAZIO FISICO OCCUPATO	~3 GB circa per ogni nodo coinvolto	La componente di autorizzazione è distribuito su più nodi
TIPOLOGIA APPLICAZIONE	BACKEND	

Dimensionamento Infrastruttura

2.4.3.1 Capacità Elaborativa

Per i valori degli indicatori si può affermare che per il componente richiede due sistemi virtuali con le seguenti caratteristiche:

CPU: 8 VCPU

RAM: 16 GB

2.4.4 Requisiti/Vincoli di Configurazione

SW di Base

- SUSE® Linux Enterprise;
- Engiweb IDEAS Profile Manager.

Configurazione SW

Non sono necessarie configurazioni software particolari.

Infrastruttura HW

È garantita la continuità operativa del componente mediante la duplicazione dei server, che garantisce altresì il bilanciamento del carico.

Infrastruttura Rete

Non sono necessarie particolari configurazioni di rete.

Specifiche di Sicurezza

Il componente è parte integrante della infrastruttura di sicurezza e costituisce una parte della componente di autenticazione. Esso, distribuito sulle due macchine esaminate precedentemente, si colloca nella segmento demilitarizzato della infrastruttura di rete del SISN (DMZ).

2.5 Componente Architetturale di IDEAS Audit

2.5.1 Razionali della componente architetturale

Il modulo IDEAS Audit, attraverso una facile interfaccia di amministrazione, permette di registrare, filtrare e riorganizzare i messaggi emessi da entità (applicazioni) sia interne all'infrastruttura IAM che esterne.

Ciò allo scopo principale di tenere traccia delle operazioni e di chi le ha eseguite, in modo da mantenere un log completo ed esaustivo dei movimenti effettuati e di eventuali errori o warning rilevati.

IDEAS Audit raccoglie, mantenendole naturalmente separate, le informazioni in arrivo da qualunque numero di applicazioni: ad ogni operazione effettuata da una applicazione, la stessa

provvede a mandare un messaggio al sistema contenente una serie di informazioni (comunque configurabili).

I dati raccolti sono utilizzati per la generazione di report, statistiche, messaggi di allarme e/o di errore.

Il componente IDEAS Audit integra il prodotto "Novell Audit": la soluzione centralizzata e cross-platform di auditing e reporting di Novell, che consente di collezionare tutti gli eventi provenienti da diverse applicazioni (applicazioni, piattaforme, database etc.) registrando gli eventi stessi in un unico Data Store che offra garanzia di non-ripudiabilità.

IDEAS Audit può creare Data Store filtrati sulla base di criteri ben definiti. I dati collezionati possono essere estrapolati per generare report utili per guidare l'adozione di nuove policy di gestione/sicurezza o individuare responsabilità di eventi indesiderati. La soluzione si basa sulla cooperazione di due sottosistemi: Platform Agent e Secure Logging Server, per realizzare un sistema di log centralizzato di tutti gli eventi generati dalle applicazioni monitorate.

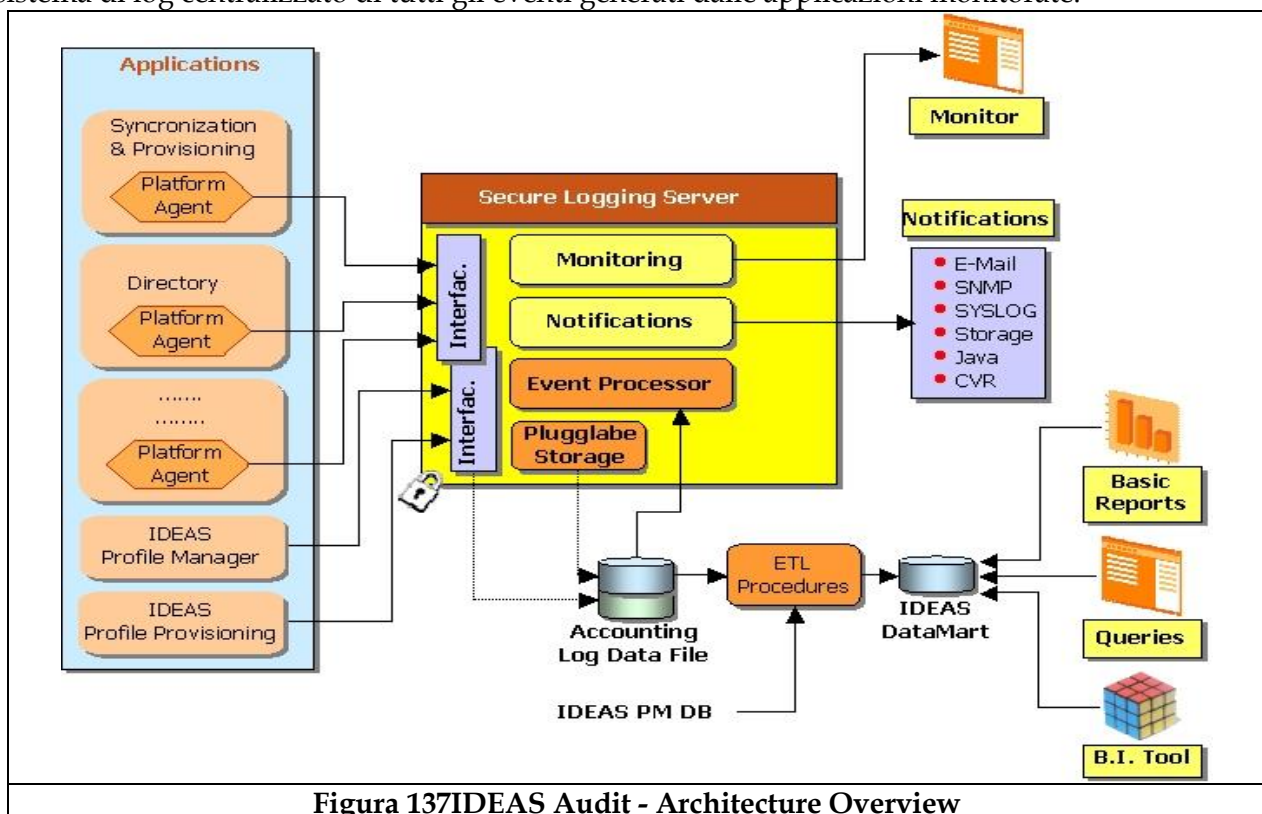


Figura 137 IDEAS Audit - Architecture Overview

Facendo riferimento all'architettura base, si distinguono le seguenti componenti chiave:

- Applicazione: applicazione monitorata da IDEAS Audit
- Acquisizione eventi
 - Platform Agent: componente "client" di Novell Audit
 - Interfaccia Generalizzata
- Secure Logging Server: componente "server" di Novell Audit che svolge le seguenti tre funzioni principali:
 - Logging
 - Notifiche
 - Monitoring
- Accounting Log Data File: DB dove vengono memorizzati gli eventi (i dati operazionali);
- IDEAS DataMart: DB dove vengono memorizzati gli eventi (i dati che rappresentano la "osservazione" dei dati operazionali).

IDEAS Audit permette di fornire notifiche di eventi ed eseguire il log di eventi attraverso i seguenti canali:

- CVR (Critical Value Reset);
- File;
- Java;
- JDBC (Java DataBase Connectivity);
- Microsoft SQL Server;
- MYSQL;
- Oracle;
- SMTP;
- SNMP;
- Syslog.

Report Generator

Il modulo di reportistica IDEAS Report Generator, è una componente della suite IDEAS finalizzata alla produzione di report.

Questo modulo si basa sui dati consolidati provenienti dai diversi moduli componenti di IDEAS. L'applicazione sfrutta i principi di profilazione ed autenticazione propri di IDEAS Profile Manager.

IDEAS Report Generator si compone:

- di un'interfaccia web (Report Manager Console) per la generazione di richieste di report e la loro consultazione;
- di una struttura dati, Data Report Manager (DRM), volta a contenere i dati necessari alla corretta creazione dei report;
- di un modulo Message Driven Bean (MDB), dedicato alla gestione delle code con cui le richieste di report debbano essere eseguite;
- di uno o più moduli Java, Java Module Report Implement (JMRI), che attraverso un'interfaccia comune, vengono istruiti dall'DBE per l'effettiva elaborazione dei report richiesti;
- di un Java Reporting Engine open source, JasperReport, che presiede al salvataggio dei report prodotti in formato .PDF o .XLS.

Come detto, il modulo IDEAS Report Generator provvede alla produzione di Report attingendo ai dati dei repository principali della suite IDEAS:

- il DB di IDEAS Profile Manager, per informazioni riguardanti i dati relativi alle entità fondamentali che modellano la struttura di un'organizzazione presenti su IDEAS Profile Manager (Unità Organizzative, Utenti, Ruoli, Risorse, ...)
- il DB di IDEAS Profile Provisioning, per informazioni relative ai flussi autorizzativi in essere nell'organizzazione richieste o a dati ad esse riguardanti.
- i DATAMART, che contengono informazioni opportunamente strutturate ed ottimizzate per specifiche attività finalizzate (Audit, analisi storicizzata, ...)

Lo schema concettuale sopra descritto può inoltre essere integrato con prodotti di Business Intelligence come, ad esempio, Spago BI o Business Object.

2.5.2 Integrazione con l'ambiente SISN

Il componente di audit si integra con le applicazioni che si avvalgono del servizio di logging ed auditing. L'integrazione avviene mediante l'utilizzo di API.

2.5.3 Elementi di dimensionamento

Indicatori di Dimensionamento

Di seguito gli indicatori di dimensionamento individuati per il componente di auditing:

Indicatore	Valore	Note
<i>N° LOG GESTITI AL SECONDO</i>	~200	
<i>SPAZIO FISICO OCCUPATO</i>	~8 GB circa per ogni nodo coinvolto	La componente di auditing e logging è distribuito su più nodi
<i>TIPOLOGIA APPLICAZIONE</i>	BACKEND	

Dimensionamento Infrastruttura

2.5.3.1 Capacità Elaborativa

Per i valori degli indicatori si può affermare che per il componente richiede due sistemi virtuali con le seguenti caratteristiche:

CPU: 8 VCPU

RAM: 16 GB

2.5.4 Requisiti/Vincoli di Configurazione

SW di Base

- SUSE® Linux Enterprise;
- IDEAS Audit 1.1

Configurazione SW

È necessario configurare i sistemi in cluster per implementare un sistema di fail over.

Infrastruttura HW

È garantita la continuità operativa del componente mediante la duplicazione dei server, che garantisce altresì il bilanciamento del carico.

Infrastruttura Rete

Non sono necessarie particolari configurazioni di rete.

Specifiche di Sicurezza

Il componente è parte integrante della infrastruttura di sicurezza e costituisce una parte della componente di autenticazione. Esso, distribuito sulle due macchine esaminate

precedentemente, si colloca nel segmento demilitarizzato della infrastruttura di rete del SISN (DMZ).

2.6 Componente Architetturale Novell eDirectory (eDir)

2.6.1 Razionali della componente architetturale

Novell eDirectory é un servizio di Directory Services multiplatforma per gestire le informazioni relative ad utenti, ruoli, licenze e risorse che compongono l'ambiente informativo in un unico repository centralizzato.

Oltre ad essere un directory server utilizzabile a supporto dello sviluppo applicativo, eDirectory è utilizzato all'interno delle principali componenti della suite di Identity and Access Management Novell.

Si riepilogano nel seguito le principali caratteristiche di Novell eDirectory.

Caratteristica	Descrizione
Multiplatforma	<ul style="list-style-type: none">• Novell NetWare• Microsoft Windows Server 2003• Sun Solaris• Red Hat / Red Hat Advanced Server• SuSE* Linux Enterprise Server• IBM AIX• HP-UX
Protocolli Supportati	<ul style="list-style-type: none">• LDAP v3 (Open Group® LDAP 2000 Certification™)• Microsoft Active Directory™ Services Interface (ADSI)• Java Naming and Directory Interface (JNDI)• Open Database Connectivity (ODBC)• Java Database Connectivity (JDBC)• Novell Directory Access Protocol (NDAP)• eXtensible Markup Language (XML) via HTTP/SOAP
Standard Supportati	Novell eDirectory è conforme a numerosi standard tra cui LDAP (v2 and v3 RFC features), LDAP search filters, LDAP referral, DSML v2, SSL, DNS, LDIF, HTTP ed altri tra cui in particolare le RFC 2459, 1777, 1778, 1779, 2222, 2248, 2251, 2252, 2253, 2254, 2255, 2256, 2279, 2459, 2559, 2589, 2596, 2696, 2798, 2820, 2829, 2830, 2849, 2891, 3377 and PKIC #10 and #7.
Security Service	<ul style="list-style-type: none">• Modular Authentication (NMAST™) - Più di 50 metodi.• Supporto per SHA-1 e MD-5 (per password hashing)• Certificate Management• Integrazione con i principali prodotti di CA sul mercato• Industry Leading Crypto via Novell NICI• Supporto SSL e TLS• Disponibilità di un Secure Data Vault per la gestione di dati altamente "sensibili"• Patented Novell Secret Store® technology• Supporto di Attributi crittografati nella memorizzazione su disco
Storage Service	<ul style="list-style-type: none">• Super-scalable relational database management system• Testato con più di 1 miliardo di oggetti

	<ul style="list-style-type: none"> • Laser quick replication protocol • Multi-threaded replication • Servizi di backup e restore ad altissime prestazioni • Backup e restore on the fly
Developer Services	<ul style="list-style-type: none"> • C/C++ • Visual Basic • Java – JavaBens – Enterprise Java Beans • Perl Javascript
Web Services	<ul style="list-style-type: none"> • Web Services Ready • Supporto XML • Universal Description, Discovery, and Integration (UDDI) • Simple Object Access Protocol (SOAP) • Directory Service Markup Language (DSML)

Caratteristiche funzionali e aspetti distintivi

Novell eDirectory è uno strumento personalizzabile le cui principali funzionalità sono di seguito illustrate.

- Console di amministrazione totalmente Web-based (Novell iManager), personalizzabile sia in termini grafici sia in termini funzionali grazie all'architettura a plug-in e all'ambiente grafico di sviluppo di nuovi plug-in;
- Funzioni di amministrazione con gestione granulare dei diritti e delle deleghe basate sul ruolo dell'utente;
- Gruppi Dinamici in cui l'appartenenza è derivata in maniera automatica a fronte del valore di attributi e non per esplicita assegnazione;
- Mappature di organizzazioni complesse tramite la possibilità di creare più alberi (territoriali, organizzativi, ...) e stabilire i legami tra di essi;
- Interrogabilità secondo standard LDAP – possibilità di interrogare e/o inserire informazioni su eDirectory sfruttando le caratteristiche di ereditarietà e integrità di Novell eDirectory;
- LDAP persistent search – possibilità di mantenere attiva una ricerca all'interno del Directory effettuando una notifica agli utenti interessati a fronte di particolari risultati;
- Auditing granulare e Event based management per potere effettuare controlli dettagliati sulle attività effettuate all'interno di eDirectory ed automatizzare operazioni sulla base di particolari eventi.

2.6.2 Integrazione con l'ambiente SISN

Il componente è integrato con la componente di autenticazione Novell e con l'attuale sistema di gestione utenze dei server applicativi Websphere di cui costituisce il repository di utenze.

2.6.3 Elementi di dimensionamento

Indicatori di Dimensionamento

Di seguito gli indicatori di dimensionamento individuati per il componente eDir:

Indicatore	Valore	Note
------------	--------	------

<i>N° UTENTI ATTIVI</i>	14.000	
<i>N° OPERAZIONI MEDIO GIORNALIERO SULLE UTENZE REGISTRATE</i>	~100	
<i>SPAZIO FISICO OCCUPATO</i>	~5 GB circa per ogni nodo coinvolto	La componente di autorizzazione è distribuito su più nodi
<i>TIPOLOGIA APPLICAZIONE</i>	BACKEND	

Dimensionamento Infrastruttura

2.6.3.1 Capacità Elaborativa

Per i valori degli indicatori si può affermare che per il componente richiede due sistemi virtuali con le seguenti caratteristiche:

CPU: 4 VCPU

RAM: 4 GB

2.6.4 Requisiti/Vincoli di Configurazione

SW di Base

- Red Hat Enterprise Linux Server release 6.7;
- NetIQ eDirectory 8.8

Configurazione SW

È necessario configurare i sistemi in cluster per implementare un sistema di fail over.

Infrastruttura HW

È garantita la continuità operativa del componente mediante la duplicazione dei server, che garantisce altresì il bilanciamento del carico.

Infrastruttura Rete

Non sono necessarie particolari configurazioni di rete.

Specifiche di Sicurezza

Il componente è parte integrante della infrastruttura di sicurezza e costituisce una parte della componente di autenticazione. Esso, distribuito sulle due macchine esaminate precedentemente, si colloca nel segmento militarizzato della infrastruttura di rete del SISN (MZ).

2.7 Componente Architetturale AccessPortal

2.7.1 Razionali della componente architetturale

AccessPortal(AP) è un componente che svolge essenzialmente tre funzioni fondamentali:

1. riceve le credenziali utente, precedentemente registrato nel Reame tramite IDEAS Profile Manager (PM);
2. li invia al PM, al fine di verificarne la correttezza, o, nel caso venga utilizzato un servizio esterno, prima del loro invio si racchiudono in un token SAML (fase di autenticazione);
3. in base al profilo di autorizzazione restituito dal PM, si crea un front-end, adeguatamente personalizzato, di applicazioni Web e le funzioni che si possono utilizzare (fase di autorizzazione).

La fase di autenticazione, punto 2, mette in evidenza una stretta sinergia che intercorre tra l'AP e il PM. Entrambi usano lo standard SAML per creare un token, che in modo sicuro "trasporti" le credenziali presentate dall'utente. Tali credenziali sono utilizzate in diversi principali passaggi del ciclo autenticazione / autorizzazione. Un secondo collegamento è fatto nel momento della verifica di queste credenziali, una operazione che viene effettuata grazie ai dati memorizzati nel DB del PM.

La fase di autorizzazione, punto 3, stabilisce la naturale conseguenza di un successo della fase di autenticazione, dopo di che l'AP consente all'utente di effettuare tutte le operazioni che i suoi profili di autorizzazione gli permettono di fare.

2.7.2 Elementi di dimensionamento

Indicatori di Dimensionamento

Di seguito gli indicatori di dimensionamento individuati per il componente AccessPortal:

Indicatore	Valore	Note
N° UTENTI COLLEGATI CONTEMPORANEAMENTE	~200	Valore stimato in base alla numerosità delle applicazioni ed al valore della popolazione utente delle stesse, come misurato sul sistema con gli strumenti di monitoraggio dell'infrastruttura
N° SESSIONI CONCORRENTI	~200	
SPAZIO FISICO OCCUPATO	~50 MB circa per ogni nodo coinvolto	L'Access Portal è distribuito su più nodi
TIPOLOGIA APPLICAZIONE ON LINE -BATCH	ON LINE	
DIMENSIONE MEDIA PAGINA WEB	40 KB	
DIMENSIONE MASSIMA PAGINA WEB	80 KB	
TEMPO MEDIO DI ATTESA	5 sec.	Escludendo il tempo di rete.

Dimensionamento Infrastruttura

Il componente può condividere capacità elaborative dei sistemi individuati per il componente Profile Manager.

2.7.3 Requisiti/Vincoli di Configurazione

I requisiti e vincoli di configurazione del componente in esame sono gli stessi del componente Profile Manager a meno del software di base.

SW di Base

- Ideas Access Portal

Configurazione SW

Non sono necessarie configurazioni software particolari.

Infrastruttura HW

È garantita la continuità operativa del componente mediante la duplicazione dei server, che garantisce altresì il bilanciamento del carico.

Infrastruttura Rete

Non sono necessarie particolari configurazioni di rete.

Specifiche di Sicurezza

Il componente è parte integrante della infrastruttura di sicurezza e costituisce una parte della componente di autenticazione. Esso, distribuito sulle due macchine esaminate precedentemente, si colloca nel segmento militarizzato della infrastruttura di rete del SISN (MZ).

2.8 Componente Architetturale IDEAS Profile Provisioning (SWIM)**2.8.1 Razionali della componente architetturale**

IDEAS Secure Web Identity Management (SWIM) è il modulo di IDEAS delegato per l'attuazione del progetto e la definizione dei processi di autorizzazione.

IDEAS SWIM Workflow Management è l'interfaccia a disposizione degli utenti amministrativi per gestire velocemente le richieste di accesso e le approvazioni. Il modulo gestisce l'implementazione di workflow autorizzativi personalizzati per richiesta di ruolo, richiesta di account, password reset, delega, ecc.

SWIM consente agli utenti amministrativi di modellare il workflow in tutti i suoi aspetti senza alcuna necessità di conoscenze di sviluppo utilizzando un'interfaccia centralizzata (Business Level Web-based Workflow Designer). Richieste e funzioni di approvazione sono basate sui ruoli ed anche la delega amministrativa è completamente gestita. Tutte le

richieste di rafforzamento delle policy (SoD conflicts) durante i processi sono preventivamente controllate attraverso il modulo di SoD Engine.

Inoltre SWIM consente agli utenti di eseguire un range completo di servizi in autonomia, incluso Password reset, gestione delle informazioni personali, ecc.

SWIM implementa inoltre la gestione delle attestazioni che permette di controllare il processo di approvazione scadenzata delle autorizzazioni.

2.8.2 Elementi di dimensionamento

Indicatori di Dimensionamento

Di seguito gli indicatori di dimensionamento individuati per il componente IDEAS Profile Provisioning (SWIM):

Indicatore	Valore	Note
<i>N° UTENTI COLLEGATI CONTEMPORANEAMENTE</i>	~200	Valore stimato in base alla numerosità delle applicazioni ed al valore della popolazione utente delle stesse, come misurato sul sistema con gli strumenti di monitoraggio dell'infrastruttura
<i>N° SESSIONI CONCORRENTI</i>	~200	
<i>SPAZIO FISICO OCCUPATO</i>	~50 MB circa per ogni nodo coinvolto	Il componente IDEAS Profile Provisioning (SWIM) è distribuito su più nodi
<i>TIPOLOGIA APPLICAZIONE ON LINE -BATCH</i>	ON LINE	
<i>DIMENSIONE MEDIA PAGINA WEB</i>	40 KB	
<i>DIMENSIONE MASSIMA PAGINA WEB</i>	80 KB	
<i>TEMPO MEDIO DI ATTESA</i>	5 sec.	Escludendo il tempo di rete.

Dimensionamento Infrastruttura

Il componente può condividere capacità elaborativa dei sistemi individuati per il componente Profile Manager.

2.8.3 Requisiti/Vincoli di Configurazione

I requisiti e vincoli di configurazione del componente in esame sono gli stessi del componente Profile Manager a meno del software di base

SW di Base

- IDEAS Profile Provisioning (SWIM)

Configurazione SW

Non sono necessarie configurazioni software particolari.

Infrastruttura HW

È garantita la continuità operativa del componente mediante la duplicazione dei server, che garantisce altresì il bilanciamento del carico.

Infrastruttura Rete

Non sono necessarie particolari configurazioni di rete.

Specifiche di Sicurezza

Il componente è parte integrante della infrastruttura di sicurezza e costituisce una parte della componente di autenticazione. Esso, distribuito sulle due macchine esaminate precedentemente, si colloca nel segmento militarizzato della infrastruttura di rete del SISN (MZ).

2.9 Componente Architetturale Crypto Server(CS)

2.9.1 Razionali della componente architetturale

Crypto Server è un sistema formato da un insieme di componenti EJB, una consolle web ed un insieme di tools che permettono l'utilizzo di funzioni crittografiche e consentono una semplice integrazione con le applicazioni di firma digitale.

Attraverso questo insieme di componenti EJB sono implementate una serie di funzionalità crittografiche basate sugli standard RSA (PKCS#nn) che sono adottati dalle normative emesse da DigitPA, quali:

- Firma secondo lo standard DigitPA (creazione di una busta PKCS#7)
- Verifica di una firma secondo lo standard DigitPA
- Verifica di integrità
- Verifica di integrità e di credibilità
- Verifica di integrità, di credibilità e di validità (accesso alle CRL)
- Apposizione di una Marca Temporale (richiesta ad una autorità di certificazione) secondo lo standard DigitPA
- Cifratura secondo lo standard DigitPA
- Decifratura secondo lo standard DigitPA

Le operazioni crittografiche (Firma, Verifica, Cifratura, Decifratura, richiesta di Marca Temporale) utilizzano le tecniche di crittografia a chiave pubblica e consentono la gestione di oggetti/dispositivi aderenti agli standard PKCS#11 e PKCS#12; il sistema consente anche la firma di un documento XML mediante la chiave privata estratta da un file PKCS#12, nonché la verifica d'integrità di un documento XML firmato.

Fa parte dell'architettura anche il **CRL Management System** (CRLMS), un modulo dedicato al download delle Certificate Revocation List (CRL) emesse dai diversi certificatori.

Tutte le funzionalità disponibili nel CS possono essere opportunamente amministrate attraverso l'**Admin CryptoServer** (ADMCS), un modulo web che si avvale delle funzionalità esposte da beans dedicati.

2.9.2 Elementi di dimensionamento

Indicatori di Dimensionamento

Di seguito gli indicatori di dimensionamento individuati per il componente Crypto Server:

Indicatore	Valore	Note
<i>N° UTENTI COLLEGATI CONTEMPORANEAMENTE</i>	~200	Valore stimato in base alla numerosità delle applicazioni ed al valore della popolazione utente delle stesse, come misurato sul sistema con gli strumenti di monitoraggio dell'infrastruttura
<i>N° SESSIONI CONCORRENTI</i>	~200	
<i>SPAZIO FISICO OCCUPATO</i>	~50 MB circa per ogni nodo coinvolto	Il componente Crypto Server è distribuito su più nodi
<i>TIPOLOGIA APPLICAZIONE ON LINE -BATCH</i>	ON LINE	
<i>DIMENSIONE MEDIA PAGINA WEB</i>	40 KB	

Dimensionamento Infrastruttura

Il componente può condividere capacità elaborativa dei sistemi individuati per il componente Profile Manager.

2.9.3 Requisiti/Vincoli di Configurazione

I requisiti e vincoli di configurazione del componente in esame sono gli stessi del componente IDEAS Profile Manager a meno del software di base.

SW di Base

- Crypto Server

Configurazione SW

Non sono necessarie configurazioni software particolari.

Infrastruttura HW

È garantita la continuità operativa del componente mediante la duplicazione dei server, che garantisce altresì il bilanciamento del carico.

Infrastruttura Rete

Non sono necessarie particolari configurazioni di rete.

Specifiche di Sicurezza

Il componente in esame si colloca nella segmento militarizzato della infrastruttura di rete del SISN (MZ).

Non sono necessarie particolari configurazioni dell'infrastruttura di sicurezza.

2.10 Componente Architetturale Sign@Web

2.10.1 Razionali della componente architetturale

Sign@Web è un applicativo che permette di firmare un documento da browser. Esso è composto di un applet Java che si interfaccia con i dispositivi locali di Smart card, legge il certificato e firma il documento.

Esegue in autonomia tutti i controlli necessari a garantire la validità legale della firma, attraverso le seguenti funzionalità:

- firma di un testo statico e/o dinamico secondo lo standard AgID (ex-CNIPA, ex-AIPA)(creazione di una busta PKCS#7);
- firma di file rtf e in formato mime;
- verifica di una firma secondo lo standard AgID (ex-CNIPA, ex-AIPA) tramite servlet;
- verifica di integrità.
- verifica di integrità e di credibilità.
- verifica di integrità, di credibilità e di validità (accesso alle CRL).
- firma di ricevute secondo standard AgID (ex-CNIPA, ex-AIPA);
- apposizione di una Marca Temporale (richiesta ad una autorità di certificazione) secondo lo standard AgID (ex-CNIPA, ex-AIPA);
- gestione dei log per il tracciamento di tutte le sue funzionalità;
- interfaccia grafica semplice per la generazione delle politiche che vengono applicate alla transazione;
- archivio delle politiche integrato;
- interfacce API che implementano il protocollo di comunicazione (standard XML).

2.10.2 Elementi di dimensionamento

Indicatori di Dimensionamento

Di seguito gli indicatori di dimensionamento individuati per il componente Sign@Web:

Indicatore	Valore	Note
N° UTENTI COLLEGATI CONTEMPORANEAMENTE	~2	Valore stimato in base alla numerosità delle applicazioni ed al valore della popolazione utente delle stesse, come misurato sul sistema con gli strumenti di monitoraggio dell'infrastruttura
N° SESSIONI CONCORRENTI	~2	
SPAZIO FISICO OCCUPATO	~20 MB circa per ogni nodo coinvolto	Il componente Sign@Web è distribuito su più nodi

TIPOLOGIA APPLICAZIONE ON LINE -BATCH	ON LINE	
DIMENSIONE MEDIA PAGINA WEB	20 KB	

Dimensionamento Infrastruttura

Il componente può condividere capacità elaborativa dei sistemi individuati per il componente Profile Manager.

2.10.3 Requisiti/Vincoli di Configurazione

I requisiti e vincoli di configurazione del componente in esame sono gli stessi del componente IDEAS Profile Manager a meno del software di base.

SW di Base

- Sign@Web

Configurazione SW

Non sono necessarie configurazioni software particolari.

Infrastruttura HW

È garantita la continuità operativa del componente mediante la duplicazione dei server, che garantisce altresì il bilanciamento del carico.

Infrastruttura Rete

Non sono necessarie particolari configurazioni di rete.

Specifiche di Sicurezza

Il componente in esame si colloca nella segmento militarizzato della infrastruttura di rete del SISN (MZ).

Non sono necessarie particolari configurazioni dell'infrastruttura di sicurezza.

2.11 Componente Architetturale IDEAS Account Provisioning

2.11.1 Razionali della componente architetturale

Il componente IDEAS Account Provisioning è un applicativo di sicurezza responsabile del processo di censimento di un nuovo utente all'interno del sistema SISN.

La sua configurazione è in modalità "SelfProvisioning" ovvero un utente si registra in modalità Self Service e riceve una coppia USER_ID e PASSWORD.

Al termine del processo di censimento, il nuovo utente risulta censito all'interno di IDEAS Profile Manager con un ruolo di default che permette unicamente il collegamento alla applicazione di IDEAS Profile Provisioning.

2.11.2 Elementi di dimensionamento

Indicatori di Dimensionamento

Di seguito gli indicatori di dimensionamento individuati per il componente IDEAS Account Provisioning:

Indicatore	Valore	Note
<i>N° UTENTI COLLEGATI CONTEMPORANEAMENTE</i>	~2	Valore stimato in base alla numerosità delle applicazioni ed al valore della popolazione utente delle stesse, come misurato sul sistema con gli strumenti di monitoraggio dell'infrastruttura
<i>N° SESSIONI CONCORRENTI</i>	~2	
<i>SPAZIO FISICO OCCUPATO</i>	~5 MB circa per ogni nodo coinvolto	Il componente IDEAS Account Provisioning è distribuito su più nodi
<i>TIPOLOGIA APPLICAZIONE ON LINE -BATCH</i>	ON LINE	
<i>DIMENSIONE MEDIA PAGINA WEB</i>	60 KB	

Dimensionamento Infrastruttura

Il componente può condividere capacità elaborativa dei sistemi individuati per il componente Profile Manager.

2.11.3 Requisiti/Vincoli di Configurazione

I requisiti e vincoli di configurazione del componente in esame sono gli stessi del componente IDEAS Profile Manager a meno del software di base.

SW di Base

- IDEAS Account Provisioning

Configurazione SW

Non sono necessarie configurazioni software particolari.

Infrastruttura HW

È garantita la continuità operativa del componente mediante la duplicazione dei server, che garantisce altresì il bilanciamento del carico.

Infrastruttura Rete

Non sono necessarie particolari configurazioni di rete.

Specifiche di Sicurezza

Il componente è parte integrante della infrastruttura di sicurezza e costituisce una parte della componente di autenticazione. Esso, distribuito sulle due macchine esaminate precedentemente, si colloca nel segmento militarizzato della infrastruttura di rete del SISN (MZ).

2.12 Componente Architettuale SISNRAC 10g

2.12.1 Razionali della componente architettuale

Componente architettuale utilizzata dall'architettura transazionale come DB dell'applicazione.

2.12.2 Elementi di dimensionamento

Di seguito gli indicatori di dimensionamento individuati per il componente DB

Indicatore	Valore	Crescita annua	Note
<i>N° MEDIO DI TRANSAZIONI CONTEMPORANEE</i>	5 circa	N.A.	
<i>SPAZIO FISICO OCCUPATO</i>	2 GB	50 MB circa	
<i>N° MEDIO DI RICHIESTE INTERROGAZIONI/ SQL</i>	60 circa	N.A.	
<i>N° MEDIO COMMITT DBMS</i>	5 circa	N.A.	