



**"ICT4University – WiFi SUD"**  
**Regione CAMPANIA**  
**Università degli Studi di SALERNO**  
**Progetto: UNISAIR**  
**22-lug-2008**

Sezione 1 – Dati del proponente

**Università proponente**

Denominazione	Università degli Studi di SALERNO
Sede	Salerno
Indirizzo postale	Via Ponte don Melillo
Indirizzo e-mail	ufsegret@unisa.it
Telefono	089966960
Fax	089.966116
Sito web	<a href="http://www.unisa.it/">http://www.unisa.it/</a>
Codice Fiscale	80018670655

**Rappresentante legale**

Cognome e nome	Pasquino Raimondo
Qualifica	rettore
Telefono	089966960
Fax	089966116
Indirizzo e-mail	ufsegret@unisa.it

**Referente di progetto**

Cognome e nome	De Santis Alfredo
Qualifica	Professore Ordinario
Telefono	3207406153
Fax	089 969600
Indirizzo e-mail	ads@dia.unisa.it

## Sezione 2 – Sintesi del progetto

### Identificazione e descrizione breve del progetto

Nome progetto	UNISAIR
Finalità progetto	Il progetto prevede l'estensione dell'infrastruttura di rete wireless esistente e la realizzazione di un sistema di identificazione elettronica multistandard per gli utenti. L'obiettivo è quello di garantire, la copertura della totalità delle sedi dell'Ateneo, localizzate nei due campus di Fisciano e Baronissi, per consentire la massima fruibilità dei servizi erogati on-line a tutti gli utenti, con un sistema che a regime consenta di servire in media 15.000 utenti simultanei fra studenti e personale. Un ulteriore obiettivo è la realizzazione di un sistema di sicurezza che consenta l'identificazione dell'utente per l'accesso autenticato, a diversi livelli di sicurezza, a vari tipi di applicazione. Le nuove realizzazioni saranno entrambe integrate nel sistema centralizzato di controllo degli accessi di Ateneo. L'intero di sistema sarà in grado di essere integrato, in logica federata, con altre organizzazioni a livello nazionale ed europeo.
Date inizio prevista	30/09/2008
Date fine prevista	30/09/2009

### Struttura finanziaria del progetto

Valore totale del Progetto pari a:	600.000,00
Di cui a carico:	
1. Università	300.000,00
2. Finanziamento richiesto al Dipartimento	300.000,00
3. Altri soggetti pubblici o privati	0,00
4. Altri	0,00
=====	

### Dettaglio del finanziamento richiesto al Dipartimento

Finanziamento richiesto al Dipartimento:	300.000,00
Di cui:	
1. per servizi (compresi i servizi minimi)	80.000,00
2. per infrastrutture di rete	210.000,00
3. per piano di comunicazione agli studenti	10.000,00

### Copertura della rete senza fili realizzata

Percentuale dell'area dell'Università coperta da rete senza fili prima prima del progetto	10.0
Percentuale dell'area dell'Università che si prevede sarà coperta da rete senza fili al completamento del progetto	100.0
Percentuale di studenti che si prevede saranno raggiunti dalla rete senza fili al completamento del progetto sul totale degli studenti iscritti	100.0
Numero studenti regolarmente iscritti all'ateneo	40332

## Copertura e caratteristiche dei servizi minimi

### Servizio per l'iscrizione online

Il servizio è già disponibile presso l'università?	SI
Descrizione sintetica	I servizi on-line attivati per gli studenti riguardano la gestione di tutti gli eventi di carriera (di qualunque livello: Laurea, post Laurea, Dottorati, SICSI, Scuole di Specializzazione, Esami di Stato). Essi prevedono la gestione integrata dei test di ingresso, dell'immatricolazione/iscrizione, della gestione delle tasse universitarie, della composizione via web dei piani di studio, dell'iscrizione on line agli appelli d'esame. Via web sono inoltre possibili la consultazione della carriera, della situazione pagamenti, delle registrazioni effettuate agli appelli e di ogni altro atto di carriera rilevante. Tali servizi sono accessibili da un apposita area web personale ed a disposizione di ciascuno studente.

### Servizio per la verbalizzazione elettronica degli esami

Il servizio è già disponibile presso l'università?	NO
Descrizione sintetica	La verbalizzazione elettronica degli esami è in fase di realizzazione, l'infrastruttura di sicurezza presentata in questo progetto è la base necessaria per il completamento
Qualora il servizio sia introdotto in modalità sperimentale, indicare la percentuale studenti che ne potranno usufruire (rispetto agli iscritti)	60.0

### Copertura e caratteristiche degli eventuali altri principali servizi realizzati

Denominazione del servizio	Accesso ubiquo alla rete di Ateneo
Descrizione sintetica	Possibilità di connettersi alla rete di Ateneo, da qualsiasi parte dei due campus h24 per 365 gg annui.
Percentuale studenti raggiunti dal servizio (rispetto agli iscritti)	100.0
Eventuali informazioni aggiuntive	

Denominazione del servizio	Accesso ai servizi on-line di Ateneo
Descrizione sintetica	L'Ateneo è già dotato di un sistema elettronico di gestione delle carriere degli studenti (ESSE3); i cataloghi delle biblioteche centrali e dipartimentali sono tutti accessibili on-line; diverse facoltà consentono l'accesso remoto a risorse di calcolo scientifico.
Percentuale studenti raggiunti dal servizio (rispetto agli iscritti)	100.0
Eventuali informazioni aggiuntive	

Denominazione del servizio	Unificazione dei sistemi di autenticazione
Descrizione sintetica	L'accesso alle risorse avverrà attraverso un unico strumento identificativo, con un unico punto di accesso.

Percentuale studenti raggiunti dal servizio (rispetto agli iscritti)	60.0
Eventuali informazioni aggiuntive	

### Misure di sicurezza previste

Descrizione sintetica delle procedure previste per l'autenticazione e la gestione degli accessi alla rete	L'accesso alla rete si poggia un sistema di sicurezza centralizzato e basato su standard di controllo accessi e cooperazione riconosciuti a livello internazionale, basati sul protocollo RADIUS, per la gestione delle problematiche di autenticazione, autorizzazione e accounting dei singoli utenti mobili all'atto dell'accesso alla rete è già in opera e sarà potenziato per supportare le nuove installazioni. La risultante architettura porrà in essere tutte le possibili misure di sicurezza per evitare "intrusioni", usi non autorizzati o non rispondenti alle policy stabilite, della connettività wireless, che sarà pertanto erogata in conformità a tutti gli obblighi previsti dalla legge in vigore. In dettaglio l'accesso alla rete sarà protetto e controllato attraverso meccanismi di cifratura WPA/TKIP ed autenticazione basati su captive-portal, e protocolli di AAA in grado di operare sia con credenziali "deboli" (username/password) che con certificati digitali X.509v3. Detti meccanismi saranno preposti a intercettare le richieste di accesso alla rete verificando se l'accesso è contenuto nei database locali o sia necessario un re instradamento delle stesse verso i servizi di autenticazione federata operanti a livello di Ateneo in coordinamento con analoghe iniziative a livello nazionale o internazionale (infrastruttura IDEM in ambito GARR, il progetto EDUROAM in ambito europeo, etc.). Le organizzazioni operanti all'interno della federazione consentiranno la gestione delle credenziali per l'accesso in roaming all'infrastruttura di rete wireless realizzata per tutti gli utenti attraverso il suddetto servizio di captive-portal erogato a livello federato.
Descrizione sintetica di ulteriori misure di sicurezza previste	Nell'ambito di questo progetto è prevista la realizzazione di una infrastruttura di sicurezza basata su smartcard, con meccanismi di SSO con diversi livelli di autenticazione, con l'obiettivo a lungo termine di utilizzare per tutte le applicazioni un livello di autenticazione forte.

### Utilizzo di soluzioni Open Source e/o riuso di soluzioni disponibili

Soluzioni Open Source utilizzate nel progetto	Il progetto prevede un largo utilizzo di software Open Source. In particolare i sistemi operativi dell'infrastruttura ed i tools di gestione saranno basati su software OS. L'interazione con l'intero sistema di autenticazione federata sarà realizzato attraverso sistemi del tipo Shibboleth, sviluppato nell'ambito del progetto MACE e facente parte del middleware di Internet2. L'eventuale cifratura di sessioni e la gestione di certificati X.509 sarà realizzata attraverso la suite OpenSSL. I servizi on-line saranno basati su piattaforma OS, codificati con le tecnologie XHTML 1.0 Strict e CSS Level 2, conformi alle specifiche del W3C, World Wide Web Consortium. In particolare, essi utilizzeranno il paradigma Linux Apache Tomcat prevedendo linguaggio di programmazione Java o PHP.
Soluzioni già realizzate, anche da terzi, e riutilizzate nel progetto	Sarà riutilizzato il sistema di autenticazione basato sulla coppia RADIUS/LDAP consentirà il riuso della piattaforma già in esercizio Cisco ACS/OpenLDAP.

### Piano di comunicazione

Piano di comunicazione del progetto (ad esempio, bacheche dedicate, poster, depliant illustrativi, ecc.)	Il problema della comunicazione sarà affrontata in accordo a una strategia multilivello che prevede di coinvolgere in momenti diversi i vari fruitori del servizio, a partire dagli studenti fino all'intera comunità che afferrisce all'Ateneo utilizzando sia i canali di comunicazione istituzionali (organi di Ateneo, centri orientamento studenti etc.) che quelli multimediali (Radio e Portale di Ateneo, TV cittadine) ed infine diffondendo sul territorio depliant, manifesti ed organizzando eventi di presentazione dell'iniziativa.
--	---



### Sezione 3 – Scheda Progetto

#### **Nome e descrizione del progetto**

UNISAIR – Unisa on the Air: Infrastruttura di accesso wireless per l'erogazione di servizi on-line agli studenti e alla comunità che afferisce all'Ateneo salernitano per attività di studio, ricerca, formazione e cultura in genere, piattaforma di identificazione degli utenti basata su smartcard multistandard con diverse tecnologie di identificazione.

Il progetto prevede la copertura totale della superficie dei campus di Fisciano e di Baronissi, che concentrano la quasi totalità delle strutture di proprietà dell'Ateneo e la realizzazione di una infrastruttura per l'utilizzo di smartcard per l'accesso attraverso autenticazione forte ai servizi con l'assegnazione a circa 20.000 studenti ed a 1.500 unità di personale strutturato.

Pertanto saranno realizzate di circa 300 isole di erogazione dei servizi di accesso in modalità hot-spot, ognuna delle quali coprirà una zona circolare con un raggio che va dai 30 ai 50 metri, in funzione delle caratteristiche delle aree interessate. La copertura realizzata andrà a servire sia tutte le strutture indoor (edifici deputati a ospitare facoltà, dipartimenti ed uffici, aule, sale riunioni e servizi) che gli spazi comuni all'aperto (aree di sosta, viali aree ricreative) messi a disposizione degli studenti e degli utenti dei servizi erogati dall'Ateneo in genere. Per la realizzazione della copertura il progetto prevede di far ricorso a una soluzione moderna ed estremamente scalabile, basata su un'architettura di wireless LAN completamente standardizzata in accordo ai paradigmi IEEE 802.11a/b/g-Wi-Fi con controllo centralizzato degli Access Point in grado di integrare all'interno di un'unica infrastruttura ibrida di accesso tutte funzionalità di rete, controllo e gestione necessarie.

L'infrastruttura di rete wireless realizzata verrà totalmente integrata con il sistema centralizzato di controllo degli accessi di Ateneo nonché resa disponibile in logica federata, a tutte le organizzazioni nazionali che aderiscono all'infrastruttura comune di Autenticazione e Autorizzazione della rete GARR (Idem AAI), ed internazionali associate alla comunità EDUROam. Ciò consentirà a tutti gli aventi diritto, all'interno del sistema di formazione universitaria a livello italiano ed internazionale, di connettersi alla rete di Ateneo ed attraverso di essa a quella GARR, senza alcun onere e in piena sinergia con gli obiettivi di internazionalizzazione e apertura dell'Ateneo.

Inoltre in parallelo sarà realizzata una infrastruttura di sicurezza basata su smartcard di tipo CNS (Carta Nazionale dei Servizi), per il riconoscimento e la profilazione degli utenti in ordine all'accesso a procedure informatiche. Detta infrastruttura consentirà l'attivazione, il rinnovo e la revoca delle credenziali di accesso. La singola smartcard sarà un unico sistema identificativo per l'utente per tutta la durata della relazione di appartenenza all'Università di Salerno, gestendo eventuali cambi di ruolo (p.e. studente->dottorando->ricercatore). Essa consentirà sull'unico supporto di identificare gli utenti con diverse metodologie e tecnologie (foto, certificato digitale, RFID, banda magnetica).

#### **Obiettivi e ambito del progetto**

##### **Obiettivi**

L'esigenza della connettività a banda larga ovunque a beneficio delle moderne applicazioni di calcolo, automazione d'ufficio, collaborazione e comunicazione personale è ormai universalmente riconosciuta quale fattore chiave per lo sviluppo della competitività del sistema universitario, congiuntamente alla necessità di sviluppare sinergie nel processo di crescita del mondo della didattica, della ricerca e della società civile. Ciò non può che avvenire attraverso reti di connettività ubiqua e sempre disponibili che consentano la cooperazione forte e gli scambi tra le comunità degli studenti, dei docenti, dei ricercatori e dei tecnologi che operano sullo stesso territorio e insistono sul medesimo sistema informativo e su una piattaforma comune di servizi erogati a livello di Ateneo.

In tale logica, il progetto UNISAIR si prefigge di incrementare ulteriormente le possibilità di accesso alla rete da parte di chi frequenta l'Università, in primo luogo quindi gli studenti, che non sempre godono di accesso diretto e continuo alle aule multimediali e a locali cablati, ma anche a beneficio degli utenti "istituzionali" mobili, afferenti al mondo della didattica e della ricerca, che necessitano dell'accesso per un arco di tempo limitato (per esempio, per la durata di una visita o di una conferenza) o comunque di visitatori autorizzati che si trovano a gravitare nell'area di copertura. Con l'accesso wireless ubiquo alla rete di Ateneo, gli ospiti potranno quindi utilizzare i servizi on-line già disponibili, come quello delle iscrizioni on-line, delle biblioteche digitali, fruire della radio di Ateneo accedere alla posta elettronica e ai Servizi di portale, e quelli che saranno resi disponibili nell'ambito del presente progetto, come la verbalizzazione elettronica degli esami. Anche l'accesso alla rete Internet, per i cosiddetti servizi "commodity", sarà garantito ed è anch'esso essenziale per lo sviluppo della cultura in ambito universitario. Va sottolineato che nell'Ateneo salernitano gli studenti possono godere di ampi spazi messi a loro disposizione per poter utilizzare un notebook o un palmare e connettersi alla rete: sia apposite aule-studio, sia locali comuni, che biblioteche, ed anche spazi all'aperto, coperti o parzialmente coperti, ma fruibili. Pertanto, la realizzazione della piena copertura di questi spazi con gli "hot-spot", o punti di accesso, alla rete wireless, consentirà effettivamente di incrementare in termini sia quantitative che qualitative il "portfolio" Servizi e l'offerta dell'Ateneo.

Parallelamente alle esigenze di connettività è riconosciuta l'esigenza di identificare gli utenti per l'accesso ai servizi ed a seconda del tipo di applicazione prevedere diversi meccanismi di autenticazione e diversi livelli di autorizzazione. A tale scopo il progetto prevede di dotare inizialmente gli studenti iscritti regolarmente al primo livello di istruzione universitaria ed il personale strutturato di uno strumento identificativo del tipo CNS (Carta Nazionale dei Servizi). Lo strumento consentirà di identificare gli utenti tramite fotografia ed autenticarli con diversi livelli di sicurezza a seconda della tecnologia utilizzata. In particolare questo strumento diventerà il supporto indispensabile per la gestione della carriera dello studente e sarà strumento indispensabile per la verbalizzazione on-line degli esami consentendo a docenti e studenti

l'accesso alla procedura per l'identificazione e la firma da parte di entrambi alla cosiddetta camicia d'esame. Consentirà, tramite la banda magnetica, di integrarsi con il sistema di rilevazione delle presenze, già esistente, degli studenti e del personale. Permetterà tramite RFID di controllare l'accesso ad aree riservate/protette. Consentirà la virtualizzazione del libretto dello studente.

#### Ambito progettuale

Il progetto sarà realizzato all'interno di una infrastruttura consolidata che conta circa 12.000 punti accesso utente su rete cablata. Attualmente sono in esercizio circa 200 switches di accesso utente e 12 centri stella di edificio. La rete è sviluppata secondo una topologia gerarchica a tre livelli e suddivisa in VLAN per i vari servizi e per le diverse strutture. Ogni utente accede alla rete confinato nella VLAN di appartenenza ed ottiene un indirizzo IP nella maggior parte, ovvero in più dell'80 %, appartenente ad una classe privata.

L'infrastruttura dispone inoltre di uno strato proattivo di sicurezza trasversale, che include un sistema multilivello di firewalling, un sistema di antivirus con distribuzione centralizzata degli aggiornamenti, un sistema di antispam ed antivirus per il servizio di e-mail. Lo spazio per i dati è condiviso per i vari server che vi accedono tramite una S.A.N. FC, quest'ultima è replicata in una sede remota per la protezione dei dati. Il backup dei vari sistemi avviene tramite un software specializzato su un sistema unico di tape LTOg3 accessibile attraverso la S.A.N.

I servizi erogati sono fruibili con un uptime misurato del 99,5%, in particolare sono state adottate delle misure differenziate a seconda dei servizi, in particolare l'architettura dei database è stata progettata per gestire sia l'alta affidabilità che il bilanciamento del carico attraverso i vari nodi del sistema. Altri servizi sono stati portati in alta affidabilità attraverso la virtualizzazione degli stessi in un ambiente clusterizzato e distribuito.

Tutta l'infrastruttura è gestita e monitorata centralmente per consentire al personale di intervenire in tempi rapidi per la risoluzione dei guasti. Tutti i sistemi ad ogni livello sono dotati di sistemi di alimentazione ausiliaria, in particolare la server farm di Ateneo, dispone di due livelli di protezione per la mancanza di energia elettrica, che garantiscono la continuità operativa per circa 60 ore.

#### Finalità e risultati attesi dal progetto

L'iniziativa in questione è tesa a realizzare il substrato tecnologico capace di omogeneizzare le infrastrutture informatiche e telematiche a servizio dell'Ateneo disponibili a tutti gli utenti. In particolare essa mira ad abilitare l'Ateneo allo sviluppo di nuove modalità di comunicazione con i propri utenti per l'erogazione di servizi essenziali basati sulla massiva diffusione della connettività all'interno dei campus e quindi la disponibilità della larga banda ovunque e a chiunque sia autorizzato a fruirne, senza trascurare aspetti di sicurezza ed usabilità indispensabili per l'incremento della fruizione di suddetti servizi. La sicurezza prevede l'adozione di un sistema integrato di identificazione ed autenticazione degli utenti basato sui più evoluti standard tecnologici.

L'articolazione temporale del progetto prevede la realizzazione delle infrastrutture e dei Servizi in 12 mesi dalla stipula della convenzione. Si tratta di tempi stretti, in considerazione della necessità di provvedere all'approvvigionamento delle componenti mediante le procedure idonee. L'approccio adottato, basato sull'esperienza acquisita, sarà dunque il seguente: la gara per l'acquisizione dell'HW e la realizzazione fisica della copertura sarà avviata con la massima rapidità, quindi il capitolato tecnico sarà predisposto appena si avrà notizia dell'approvazione del progetto.

Per quanto riguarda la pubblicizzazione dell'iniziativa, una prima fase verrà messa in atto nel primo mese della convenzione, per informare la popolazione studentesca dell'iniziativa e dei risultati attesi; un secondo momento di pubblicizzazione si avrà all'avvio dei lavori, ed un terzo momento di pubblicizzazione al termine della convenzione, contestualmente all'avvio del sistema nel suo complesso.

I servizi on-line saranno realizzati o ampliati, a seconda dei casi, in modo da essere fruibili al termine della realizzazione dell'infrastruttura hardware. I servizi saranno realizzati con personale interno e con risorse a contratto, sui fondi di progetto.

Per quanto attiene lo sviluppo dei servizi, la loro articolazione su 6 mesi prevede per ciascuno di essi una suddivisione in 5 fasi:

- 1) analisi formale dei processi in essere nell'amministrazione, loro revisione alla luce dei nuovi obiettivi e definizione dei nuovi processi.
- 2) fase di prototipizzazione e definizione delle piattaforme tecnologiche e del middleware a supporto.
- 3) fase implementativa dei processi individuati.
- 4) fase di dispiegamento delle applicazioni e attivazione dei servizi.
- 5) test funzionale del sistema realizzato.

#### Risultati attesi:

Realizzazione di una infrastruttura di rete che consenta di sfruttare al meglio ed ovunque all'interno delle strutture universitarie la possibilità connettersi ad Internet, sia per gli utenti afferenti all'Ateneo che ad eventuali ospiti accreditati presso altre strutture riconosciute all'interno di un progetto di Identità Federate tra gli enti di ricerca europei. Gli utenti potranno accedere indistintamente a tutte le risorse condivise dalle varie strutture di Ateneo con i propri mezzi. Gli studenti in particolare potranno accedere ai servizi on-line erogati esclusivamente nella intranet senza sottostare ai vincoli temporali di apertura degli spazi predisposti all'erogazione dei servizi. In conseguenza si avrà un notevole miglioramento delle procedure di Segreteria Studenti rendendo fruibili on-line diverse operazioni al momento effettuabili solo allo sportello. La dotazione degli utenti di un unico mezzo identificativo (smartcard multiservizio) consentirà di semplificare l'accesso ai vari servizi che

richiedono autenticazione a diversi livelli ed unificare le piattaforme tecnologiche a servizio delle diverse applicazioni, garantendo la piena compatibilità e conformità agli standard ed alle norme vigenti in materia di trattamento dei dati personali, di sicurezza ed ambientali. Inoltre dotare gli utenti di un sistema flessibile e capace di autenticazione ed identificazione forte potrà snellire le procedure di esame consentendo la verbalizzazione elettronica degli stessi ed allo stesso tempo utilizzare un pass unico per l'accesso ad eventuali aree riservate/protette. La razionalizzazione dell'infrastruttura wireless porterà all'eliminazione degli apparati wireless di tipo personale o comunque di piccole strutture con conseguente riduzione e controllo delle emissioni elettromagnetiche.

### **Caratteristiche dei servizi / Procedure di sicurezza**

#### Caratteristiche dei servizi

Gli utenti potranno accedere alla rete di Ateneo, previa autenticazione, da qualsiasi punto dei campus di Fisciano e Baronissi e di conseguenza connettersi alla rete Internet con strumenti personali. Il sistema di autenticazione centralizzato consentirà una semplificazione delle operazioni garantite da una unica credenziale valida per tutti i servizi/sistemi.

L'accesso sarà garantito con standard di qualità elevati sia in termini di banda disponibile per utente che in termini di uptime dell'infrastruttura che sarà monitorata e controllata centralmente dal centro di gestione. All'interno dei campus sarà garantita la copertura in mobilità, caratteristica che comporterà un innalzamento della fruibilità dei servizi, che a loro volta sono erogati con alta affidabilità e monitorati per garantire un elevato livello qualitativo.

I sistemi di autenticazione saranno compliant CC EAL 4+, in particolare le carte multifunzione prevedono una foto dell'utente stampata sul fronte ed i dati anagrafici dello stesso, il supporto conterrà una banda magnetica standard ISO 7811, un'interfaccia contact less di tipo RFID, una interfaccia smartcard ISO 7816. La multifunzionalità del supporto consentirà a breve termine la piena compatibilità con i dispositivi in uso quindi l'integrazione con le applicazioni esistenti; a medio termine consentirà l'autenticazione forte per alcune procedure in fase di rilascio (p.e. verbalizzazione elettronica degli esami, smart logon e SSO per l'accesso ai sistemi); a lungo termine si può prevedere l'uso di autenticazione forte per tutte le procedure.

#### Procedure di sicurezza

L'accesso alla rete sarà protetto e controllato attraverso meccanismi di cifratura WPA/TKIP ed autenticazione basati su captive-portal, e protocolli di AAA in grado di operare sia con credenziali "deboli" (username/password) che con certificati digitali X.509, presenti sulla smartcard di cui saranno forniti gli studenti ed il personale. Il software intercetterà le richieste di accesso e provvederà laddove le credenziali di accesso non siano presenti nei database di Ateneo re-instradamento delle stesse su servizi di condivisione delle identità on-line e delle relative attribuzioni (AAI) operanti in logica federata sia a livello di Ateneo che in coordinamento con analoghe iniziative a livello nazionale o internazionale (infrastruttura IDEM in ambito GARR, EDUROAM a livello della rete della ricerca europea etc.).

In un ambiente senza AAI federata un utente per poter accedere ad una risorsa deve di volta in volta essere autenticato utilizzando credenziali spesso diverse. Viceversa, in presenza di un'infrastruttura AAI federata ogni risorsa resa disponibile all'interno della federazione è accessibile attraverso controlli di autenticazione ed autorizzazione centralizzati: la procedura è gestita (di norma) presso il dominio di appartenenza (home) dell'utente.

L'accesso alle procedure informatiche a disposizione degli utenti sarà protetto e controllato ed avverrà con meccanismi di autenticazione forte, mediante l'uso di smartcard standard CNS. A tale scopo saranno acquisite smartcard in numero sufficiente a coprire le esigenze dell'Ateneo e tutte le necessarie apparecchiature per l'integrazione con i sistemi esistenti per la chiusura dell'intera procedura.

Una tale organizzazione comporta significativi elementi a valore aggiunto:

- La possibilità di realizzare meccanismi di SSO (Single-Sign-On) che permettono ad un utente di autenticarsi una sola volta e di accedere, senza ri-autenticarsi, a tutte le risorse informatiche e ai servizi ai quali è autorizzato in ragione del proprio profilo.
- Eliminazione della ridondanza dei dati utente che sono presenti e gestiti solo presso il dominio di appartenenza.
- L'accesso alle risorse è basato completamente sulle credenziali/attributi dell'utente.
- Nasce il concetto di gestione dell'identità digitale federata.

Il paradigma federato costringe a ripensare i ruoli delle organizzazioni nella catena del servizio ed in particolare:

- implementa meccanismi di SSO in ambito federato e di conseguenza garantisce la sicurezza e la privacy degli utenti all'interno di uno specifico circle-of-trust;
- permette il mutuo scambio di attributi utente per consentire la piena condivisione dell'accesso alle risorse e/o servizi;
- consente di fare riferimento a infrastrutture a chiave pubblica (PKI) esterne per la certificazione delle entità coinvolte;
- garantisce meccanismi flessibili ed efficienti per la gestione del rilascio e dell'accettazione degli attributi;
- definisce un set di attributi ampliabile e completamente configurabile, a partire dallo schema standard eduPerson.

Ciascun tentativo di accesso a una risorsa protetta causa la redirectione automatica a un servizio che richiede all'utente di specificare

l'organizzazione all'interno della federazione che detiene tutte le informazioni relative alla propria identità digitale. Di conseguenza la procedura di autenticazione ed autorizzazione sarà ulteriormente rediretta verso l'apposito servizio erogato presso la "home institution" dell'utente. A valle di tale processo di autenticazione remota la componente operante localmente genererà un riferimento temporaneo per l'utente in questione, definito come "handle" che sarà inviato presso l'opportuno SP. L'SP potrà quindi utilizzare l'handle per richiedere informazioni di autorizzazione ed ulteriori attributi relativi all'utente. Sulla base di tali attributi l'SP deciderà se accordare l'accesso alle proprie risorse.

## Disegno di massima della soluzione

Il sistema di accesso wireless proposto è realizzato attraverso isole di copertura radio omogenee collegate alla rete wireline e operanti in modalità hot-spot. Ciascuna isola di copertura è costituita da un certo numero di AP in tecnologia 802.11b-g/WiFi raggruppati in un "Dominio Wireless" che coopereranno per l'assegnazione dinamica dei canali radio, l'autoregolazione delle potenze trasmissive e l'individuazione delle stazioni radio in copertura al fine di riconoscere e contenere i fenomeni di interferenza. All'interno di ogni dominio wireless saranno abilitate funzionalità di fast-roaming che consentiranno lo spostamento degli utenti già autenticati fra AP di uno stesso dominio senza effettuare la ri-autenticazione dell'utente. L'infrastruttura wireless sarà inoltre in grado di rilevare fonti anomale di interferenza, tipicamente costituite da access-point non operanti in maniera controllata all'interno dell'infrastruttura stessa (denominati "rogue access-points") e localizzare approssimativamente gli stessi attraverso operazioni di triangolazione.

La creazione di configurazioni ad elevata affidabilità sarà garantita dalla funzionalità di bilanciamento delle connessioni su più Access Point e dalla possibilità di definire su questi anche degli schemi di ridondanza a caldo.

Sofisticata funzionalità di filtering disponibili sia a livello Ethernet, che a livello Radio permetteranno di massimizzare le caratteristiche delle connessioni. La possibilità di funzionamento su più standard e bande di frequenza (IEEE802.11a/b/g, a 5 e 2,4GHz) e la relativa certificazione WiFi, permetteranno la realizzazione di reti estremamente scalabili, in cui la copertura radio su ciascuna banda di frequenza può essere ottimizzata in funzione del tipo di antenne e di potenza trasmissiva utilizzata.

L'architettura che si intende realizzare sarà in grado di integrarsi in modo semplice in tutti i contesti dove è già presente una rete wired già in esercizio. I principali elementi caratterizzanti la soluzione sono:

- adattamento a topologie di rete differenti;
- configurazione di sistema in grado di supportare diversi scenari;
- minimo impatto sull'infrastruttura di cablaggio esistente;
- architettura di gestione e controllo degli Access Point centralizzata;
- possibilità all'interno delle aree di copertura di roaming delle sessioni utente per client wireless nomadici;
- ammissibilità di una sola sessione per ciascun utente;
- separazione dei flussi di traffico dei partecipanti appartenenti a tipologie diverse (ricercatori, studenti, ospiti etc.);
- scalabilità gestionale e prestazionale;
- accesso controllato alla rete tramite autenticazione federata e accesso ai servizi attraverso SSO;
- conformità alla legislazione italiana per quanto concerne il tracciamento delle sessioni utente (tempo di connessione, tempo di disconnessione, durata della sessione, IP Address, MAC address dell'utenza) mantenendone l'anonimato;
- rispetto della privacy dell'utente mantenendo anonimi i messaggi di log (non registrando la reale identità dell'utente) e fornendo al contempo la possibilità di stabilire responsabilità personali (identità) in caso di abusi.

Specificamente, l'architettura di rete in oggetto sarà composta da quattro layer logici:

- Apparati Utente (Handeld/Pc/Notebook). Gli utenti accederanno alla rete wireless in diverse modalità attraverso dispositivi equipaggiati con le opportune interfacce standard.
- Layer2 Transport. L'infrastruttura di accesso alla rete wireless sarà realizzata attraverso AP collegati a switch tradizionali che trasportano il traffico verso la componente di instradamento operante a livello 3.
- Layer3 Transport. Il traffico degli utenti verrà instradato verso le altre LAN di Ateneo e l'esterno (internet) attraverso gli apparati di rete Layer3 che gestiranno anche le funzionalità di authentication-proxy utilizzate nel contesto dei servizi di Single-Sign-On.
- Network Services. Attraverso la funzionalità di authentication-proxy sarà garantita l'intercettazione dell'accesso degli utenti alla rete e il relativo reinstradamento automatico ai servizi di web captive-portal necessari alla gestione dell'autenticazione federata.

Apparati utente

Per la definizione del servizio wireless lato client è necessario considerare che i meccanismi più diffusi di trasporto del framing Ethernet su

infrastruttura wireless sono definiti dagli standard IEEE 802.11b/g a 2.4GHz e IEEE 802.11a 5GHz e che la maggioranza dei dispositivi disponibili sul mercato utilizza la versione 802.11b/g a 2.4GHz che gestisce soltanto 3 canali wireless senza sovrapposizione.

Infrastruttura di accesso wireless

L'architettura di controllo degli Access Point all'interno dei domini wireless realizzati sarà basata sul protocollo Lightweight Access Point Protocol (LWAPP) e sul concetto di "Wireless LAN controller" che permetterà di gestire in modo centralizzato e coordinato un'infrastruttura di tipo Wi-Fi controllandone dinamicamente la configurazione nonché la gestione dinamica dei canali e dei fenomeni di interferenza.

La rete wireless realizzerà le aree di copertura sia attraverso il deployment di Access Point modulari e non, controllati a livello centralizzato via LWAPP, che tramite rete wired sono collegati al controller che permette la supervisione e la gestione degli stessi. Tutti gli AP da utilizzare per l'erogazione dell'accesso wireless dovranno presentare le seguenti caratteristiche costruttive e funzionali evolute che garantiranno un livello adeguato di qualità e la protezione dell'investimento nel tempo (ROI):

- Supporto degli standard IEEE 802.11b/g ed eventualmente 802.11n;
- Facilities di autenticazione 802.1X, EAP-Flexible Authentication via Secure Tunneling, Protected EAP (PEAP MSCHAPv2), EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled TLS (EAP-TTLS), EAP-Subscriber Identity Module (EAP-SIM);
- Protocolli di cifratura AES-CCMP per cifratura WPA2, Temporal Key Integrity Protocol (TKIP): key hashing (per-packet keying), Message Integrity Check (MIC) e sistema di rotazione delle chiavi broadcast via TKIP o WPA TKIP, IEEE 802.11 WEP con chiavi a 40 e a 128 bit;
- Conformità allo standard IEEE 802.11i e alle direttive ETSI;
- Supporto alimentazione PoE IEEE 802.1af.

Gli AP modulari potranno ospitare sia antenne omnidirezionali che unidirezionali di tipo patch con o senza diversity, e diversi livelli di guadagno per ottimizzare il livello di copertura negli spazi aperti e nelle grandi strutture. Gli stessi potranno inoltre ospitare sia moduli radio a 2,4 GHz (802.11b/g) che a 5 GHz (802.11a).

Per semplificare le problematiche di realizzazione e successiva gestione, l'alimentazione di tutti gli access point dovrà sfruttare il cablaggio dati in rame, in accordo alla modalità in-line power, utilizzando appositi apparati di switching operanti in accordo allo standard PoE IEEE 802.1af o utilizzando apparati preesistenti a cui saranno associati power injectors. Tutti gli AP installati all'esterno prevedranno quanto necessario per l'installazione in sicurezza ed alta affidabilità (scatola a tenuta stagna, protezione al surriscaldamento, etc.).

La sicurezza e il controllo degli utenti avverrà tramite tecnologie AAA combinate con sistemi di sicurezza esterni in grado di erogare funzioni di firewalling e di captive portal e con tecnologie di rete layer 2 in grado di garantire l'isolamento in apposite LAN virtuali dei singoli client in ragione del loro profilo e delle rispettive attribuzioni/diritti di accesso.

Tutti i dispositivi di accesso wireless dovranno essere monitorati attraverso una suite di sistemi di controllo e management evoluta che consentirà una gestione proattiva degli stessi. Tali saranno sono responsabili delle funzionalità di governo della rete wireless, come le policy di sicurezza, l'intrusion prevention, la gestione delle interfacce radio, la QoS, la RF prediction, l'ottimizzazione della rete, il troubleshooting, il tracking degli utenti, il security monitoring, la gestione degli Access Point e i servizi di mobilità (a partire dal roaming). In tal modo il centro di gestione della rete potrà localizzare dinamicamente e tracciare gli spostamenti di dispositivi wireless, persone e oggetti, ottimizzando i processi interni e identificando velocemente le minacce alla sicurezza.

Differenziazione logica dei profili di accesso alla rete

All'interno della rete coesisteranno simultaneamente utenti con profili di utilizzo differenti (ricercatori, docenti, studenti, amministrazione, cittadini e ospiti in aree pubbliche); per separare tali traffici saranno creati gruppi distinti, assegnando a ciascuno di essi una proprietà di accesso. Per ragioni di robustezza ed affidabilità il dominio wireless globale verrà suddiviso in sottodomini, ciascuno dei quali sarà univocamente identificato tramite l'utilizzo di uno specifico SSID. L'SSID è un identificatore univoco di 32 caratteri presente nell'header della frame 802.11 inviata sulla WLAN che agisce come un qualificatore/selettore di accesso quando un utente si connette ad un determinato AP. A ciascuna Wireless LAN (WLAN) indipendente, realizzata per il supporto di uno specifico profilo, con i relativi diritti ed attribuzioni di accesso, viene associato uno specifico SSID, che consentirà a ogni utilizzatore di effettuare l'associazione esclusivamente ad un particolare sottodominio.

A causa dell'attuale immaturità intrinseca di buona parte dei software nativi di gestione delle connessioni wireless (supplicants) su buona parte dei dispositivi commerciali è opportuno, a scopo di garantire l'accesso a tutti gli utenti, inviare gli SSID in broadcast e non utilizzare meccanismi di sicurezza Layer 2 tipo 802.1x per il controllo degli accessi. Tale impostazione permette ad un utente di collegarsi liberamente in rete utilizzando uno degli SSID disponibili, in ragione delle proprie attribuzioni di accesso. Il Wireless Controller centralizzato consentirà di mappare il traffico proveniente da un SSID su una specifica VLAN già configurata a livello dell'infrastruttura di trasporto wireline. Una VLAN sarà costituita da un gruppo chiuso o dominio di broadcast di livello 2 la cui funzione è quella di ripartire logicamente gli utenti di un campus in gruppi di utenti affini a prescindere dalla loro posizione fisica. Una VLAN possiede tutte le caratteristiche fisiche di una LAN (in particolare, i dispositivi all'interno di una VLAN possono comunicare tra di loro senza la necessità di ricorrere a politiche di routing), fornendo

all'amministratore la possibilità di raggruppare al suo interno client siti su differenti segmenti LAN. Poiché le VLAN dovranno essere instradate (attraverso funzionalità di routing, previste a livello della rete di trasporto) verso le reti esterne, gli apparati di accesso wireless e wireline saranno impostati utilizzando il mapping WLAN SSID VLAN Subnet IP

Su ciascuna VLAN verrà configurato un DHCP server per l'assegnazione agli utenti dell'indirizzamento IP. Esiste la possibilità che un utente si colleghi ad SSID diversi ed allochi un IP su ciascuna delle VLAN ad essi associate. L'esaurimento degli indirizzi disponibili verrà evitato utilizzando un numero di indirizzi (classi private RFC1918 che saranno oggetto di NAT verso le reti esterne) eccedenti rispetto al numero complessivo di utilizzatori.

Tutte le operazioni di NAT saranno a carico del border router/firewall di Ateneo che provvederà a loggare tutte le operazioni di translazione insieme a tutti gli accessi effettuati da ciascun dispositivo collegato alla rete wireless.

#### Logging e tracciamento

Su tutti gli AP e sul sistema di AAI realizzato a livello dell'intera federazione saranno attivate funzioni di logging che abiliteranno il tracciamento di qualsiasi evento che interessi l'apparato o il servizio in questione, dedicando uno specifico server alle funzioni di collettore degli eventi e realizzando quindi un servizio SYSLOG centralizzato a livello della federazione.

#### Identità federata

L'architettura del sistema di autenticazione federata in questione è caratterizzata da tre componenti fondamentali:

- Il Service provider (SP) che fornisce la risorsa o il servizio da proteggere – per esempio l'accesso alla rete, a un sito o ad una applicazione.
- L'Identity provider (IdP), di norma implementato nella "Home Institution" degli utenti con il compito di realizzare l'autenticazione e di fornire gli attributi richiesti dai vari SP.
- Il servizio WAYF (Where Are You From), che permette all'utente di scegliere/scoprire l'IdP di appartenenza dove autenticarsi o ottenere autorizzazioni ed attributi.

Figura 1: architettura federata di gestione delle identità.

La componente SP sarà caratterizzata a sua volta da tre elementi fondamentali: il servizio "Assertion Consumer" (ACS), l'"Attribute Requester" (AR), e il "resource manager" (RM). Tali servizi sono implementati in maniera nativa nella distribuzione standard di Shibboleth e sono in grado di girare sullo stesso o su differenti server web. Nel contesto di una transazione di autenticazione federata, l'utente, attraverso un browser formulerà al RM una richiesta di accesso a una specifica risorsa. Il RM convocherà l'ACS che attraverso il servizio WAYF acquisirà l'identità di un handle service (HS) da contattare per tutte le successive richieste relative all'utente. L'HS potrà quindi rispondere attraverso una SAML "authentication assertion" che conterrà un handle che sarà passato dall'ACS all'AR. L'AR utilizzerà tale handle insieme all'indirizzo dell'Attribute Authority (AA) associata per richiedere tutte le attribuzioni che necessita di conoscere e per cui è autorizzato. L'AR analizzerà e validerà i dati ottenuti sulla base di opportune policy di ammissibilità degli attributi (AAP's). Infine i risultanti valori di attributo saranno forniti al RM, che è responsabile del loro utilizzo al fine di garantire l'accesso alla risorsa controllata.

L'IdP sarà invece caratterizzato da quattro sub-componenti primari: l'Attribute Authority (AA), l'Handle Service (HS), le fonti di attributi, e il sistema di SSO. Le componenti AA e HS sono realizzate nativamente all'interno di Shibboleth. E' infine possibile usare qualsiasi servizio standard di Single-Sign-On in grado di gestire l'attributo REMOTE\_USER. Dal punto di vista dell'IdP la prima azione effettuata nella gestione di una transazione è la redirectione dell'utente verso l'Handle Service corrispondente, che provvederà a consultare il sistema SSO per determinare se l'utente è stato già autenticato. In caso contrario, l'utente riceverà una richiesta di autenticazione attraverso il proprio browser che sarà poi inviata a ritroso al SP con un opportuno handle. Successivamente, una richiesta formulata dall'Attribute Requester del SP, che include il suddetto handle, sarà inoltrata all'Attribute Authority, come descritto in precedenza.

Il servizio WAYF potrà essere gestito in outsourcing, operare a livello centralizzato all'interno di una specifica federazione oppure essere realizzato all'interno dell'ACS. Tale servizio è responsabile della realizzazione delle associazioni degli utenti con le home institution da esse specificate e della successiva redirectione automatica verso gli HS specifici di tali istituzioni.

Lo schema seguente mostra il flusso completo di una transazione di autenticazione federata con l'utente che si interfaccia direttamente attraverso il proprio browser al sito del Service Provider attraverso una nuova sessione e senza conoscere alcuna informazione circa l'Identity Provider.

Figura 2: AAI federata – schema funzionale dei flussi.

1. L'utente cerca di accedere a una risorsa controllata collegandosi con l'Application Server del SP.
- 2,3,4. L'utente è automaticamente re-instradato verso un server WAYF, attraverso il quale ha la possibilità di indicare la propria home institution e quindi accedere al proprio IdP.
5. L'utente è rediretto verso l'Handle Service disponibile presso il proprio IdP.
- 6,7. L'autenticazione viene portata a termine presso l'IdP, usando le credenziali dell'utente note localmente.
8. L'Handle Service genera un identificativo univoco (Handle) associato alla transazione e redirige l'utente verso l'Assertion Consumer Service (ACS) del service provider. L'ACS valida l'asserzione di accesso richiesta, crea una corrispondente sessione e trasferisce il controllo della

transazione all'Attribute Requestor (AR).

9,10. L'AR utilizza l'Handle per richiedere le necessarie attribuzioni presso l'Attribute Authority dell'IdP. L'Attribute Authority risponde con un'asserzione di attributo vincolata alle politiche di gestione degli attributi e a questo punto il Service Provider dispone degli attributi necessari per garantire l'accesso controllato alla risorsa e per condizionare ulteriori decisioni a livello di applicazione.

Il ruolo fondamentale di mediazione tra gli apparati che forniscono il servizio di accesso alla rete e l'Authentication e Authorization Infrastructure (AAI) federata cui è deputata la verifica dell'identità utente sarà assolto dalla funzionalità di authentication-proxy. L'utilizzo della funzione di authentication-proxy impone dei vincoli sull'implementazione della logica di routing. In particolare l'authentication-proxy è gestita a livello di controllo centralizzato della rete wireless. Una volta autenticato a livello centrale, il traffico potrà essere instradato utilizzando le normali funzioni di routing offerte dalla sottostante infrastruttura di trasporto wired. Le policy di sicurezza utilizzate dal meccanismo di authentication-proxy prevedono modalità di autenticazione tramite tipiche credenziali di accesso username/password o certificati X.509. Il meccanismo di authentication-proxy si basa sulla scansione di una tabella al cui interno viene memorizzato a livello centralizzato lo stato delle connessioni. L'utente per ottenere l'accesso alla rete deve obbligatoriamente interagire con il meccanismo di authentication-proxy attraverso l'inizializzazione di una sessione HTTP (es. accesso ad un sito tramite web browser).

Per accelerare il secure-roaming tra celle gli AP svolgeranno la funzione di riautenticazione all'interno delle singole isole di copertura senza comunicare con il server di autenticazione.

### **Approccio e Piano di realizzazione**

L'approccio al progetto prevede uno studio iniziale, già in fase di sviluppo, per la verifica della copertura e le problematiche delle interferenze, e per la definizione di un progetto esecutivo per l'acquisizione delle smartcard da distribuire agli studenti.

Il piano di realizzazione verrà avviato successivamente alla stesura dei progetti esecutivi e della loro approvazione da parte degli organi di controllo. Parallelamente sarà avviato il piano di comunicazione coinvolgendo le associazioni degli studenti presenti all'interno dell'Ateneo per una diffusione capillare delle informazioni. L'acquisizione di beni e servizi verrà effettuata secondo le norme vigenti e a seguito della scelta del fornitore verranno realizzate le infrastrutture.

### **Utilizzo di soluzioni Open Source e riuso di soluzioni già disponibili**

Il progetto prevede un largo utilizzo di software Open Source sia per la realizzazione dei tool di gestione della infrastruttura di autenticazione federata, sia per la realizzazione e/o potenziamento dei servizi on-line, che per i sistemi operativi.

I servizi on-line utilizzeranno prevalentemente software public domain, ed in particolare le tecnologie XHTML 1.0 Strict e CSS Level 2, conformi alle specifiche del W3C, World Wide Web Consortium. In particolare, essi utilizzeranno il paradigma Linux – Apache – Tomcat prevedendo come linguaggio di programmazione Java e PHP.

L'interfaccia degli apparati di accesso verso il sistema di autenticazione implementata con un server RADIUS, già in esercizio basato su Cisco ACS, che analizzerà le richieste e inoltrerà le stesse verso un LDAP locale o remoto in caso di utenti federati. Il repository LDAP deputato a contenere l'anagrafica, le credenziali di accesso e le attribuzioni di ciascun utente utilizzerà la soluzione già in esercizio basata su OpenLDAP, tutte le eventuali sessioni cifrate, le operazioni di cifratura e la gestione di certificati X.509v3 sarà realizzata attraverso la suite OpenSSL.

Per il sistema di autenticazione federata e la realizzazione della logica SSO si prevede di utilizzare una soluzione elaborata dall'INTERNET2 Consortium ([www.internet2.edu](http://www.internet2.edu)) che sviluppa tecnologie di rete avanzate per l'utilizzo in ambito scientifico ed accademico. Tale soluzione dell'INTERNET2 Consortium è rappresentata dal progetto Shibboleth, realizzato nel contesto del gruppo MACE, e che si è concretizzato nello sviluppo di un sistema Open Source, scalabile ed efficace, per l'accesso a risorse/servizi web condivisi tramite credenziali di autorizzazione. La tecnologia Shibboleth è fondata sull'uso del framework SAML (Security Assertion Markup Language), basato su XML per lo scambio di informazioni ("assertions") per l'autenticazione e autorizzazione ed è in grado di interfacciarsi con servizi LDAP o RADIUS esterni e con database relazionali che supportino connessioni JDBC.

### **Iniziative e Piano di comunicazione**

Il piano di comunicazione si articola in tre fasi distinte. In ciascuna fase i destinatari principali della comunicazione sono gli studenti ed il personale dipendente dell'Ateneo. Ogni fase ha durata di 2 settimane circa.

La prima fase avrà inizio subito dopo la stipula della convenzione, quindi nel primo dei dodici mesi del progetto. In questa fase verrà emesso un

comunicato stampa per pubblicizzare il progetto nel suo complesso ed il finanziamento ricevuto, e verrà inoltre data comunicazione alle rappresentanze studentesche negli organi collegiali di Ateneo. Il contenuto della comunicazione verterà sui vantaggi del sistema wireless, in particolare per l'accesso ai servizi on-line, e sui servizi on-line che verranno creati e/o potenziati nell'ambito del progetto. Il sito web di Ateneo verrà aggiornato con gli stessi contenuti.

La seconda fase avrà inizio all'avvio dei lavori di installazione dell'infrastruttura hardware. Verrà emesso un comunicato stampa e verranno di nuovo informate le rappresentanze studentesche, ed in più verrà data informativa diretta a tutti gli studenti, mediante due sistemi: il sistema di posta elettronica di Ateneo e la radio di Ateneo, che si rivolgerà alla comunità scolastica e universitaria del territorio campano, costituita da studenti, docenti ed operatori del settore. L'uso della radio ha il duplice obiettivo di favorire le attività di diffusione di notizie istituzionali rivolte all'interno ed all'esterno dell'Ateneo e di orientare gli studenti della Scuola e dell'Università che, oltre ad essere il target di riferimento della radio stessa, rappresentano il soggetto attivo dell'ideazione, conduzione e realizzazione dei programmi. Il sito web di Ateneo verrà aggiornato con gli stessi contenuti.

La terza fase avrà inizio nell'ultimo dei dodici mesi di progetto, e precisamente quando tutti i servizi e le infrastrutture previste saranno disponibili e operativi. La pubblicizzazione prevede sia, la pubblicazione di appositi articoli ed informative sui principali quotidiani locali, e a diffusione di comunicati attraverso le televisioni locali, sia la realizzazione di manifesti, brochure e depliant illustrativi che saranno diffusi sia all'interno dell'Ateneo che sul territorio, a tutta l'utenza interessata. Sarà previsto inoltre l'invio di comunicati via e-mail diretta a tutto il personale e agli studenti. Continuerà la diffusione delle informative attraverso la radio di Ateneo. Il sito web di Ateneo verrà aggiornato con gli stessi contenuti, ed in più con le istruzioni di accesso all'infrastruttura. Sarà infine organizzato un evento/convegno per la presentazione dell'iniziativa aperto a tutta la comunità universitaria e alla cittadinanza.

### Struttura finanziaria del progetto

Il valore totale del Progetto è pari a € 600.000, di cui:

€ 300.000 a carico dell'Università di Salerno pari al 50,00 % del totale

€ 300.000 su finanziamento richiesto al Dipartimento pari al 50,00 % del totale

=====

100.0 %

Il finanziamento richiesto al Dipartimento è pari a € 300.000, di cui:

€ 214.000 per la realizzazione di reti di connettività pari al 70,16 %

€ 76.000 per l'implementazione dei servizi (compresi i servizi minimi) pari al 25,33 %

€ 10.000 per l'attuazione delle attività di comunicazione agli studenti pari al 03,33 %

Il valore totale del Progetto è pari a € 600.000, di cui:

€ 300.000 a carico dell'Università di Salerno pari al 50,00 % del totale

€ 300.000 su finanziamento richiesto al Dipartimento pari al 50,00 % del totale

=====

100.0 %

Il finanziamento richiesto al Dipartimento è pari a € 300.000, di cui:

€ 214.000 per la realizzazione di reti di connettività pari al 70,16 %

€ 76.000 per l'implementazione dei servizi (compresi i servizi minimi) pari al 25,33 %

€ 10.000 per l'attuazione delle attività di comunicazione agli studenti pari al 03,33 %

### Eventuali ulteriori informazioni

\_\_\_\_\_

Figura 2: AAI federata – schema funzionale dei flussi.

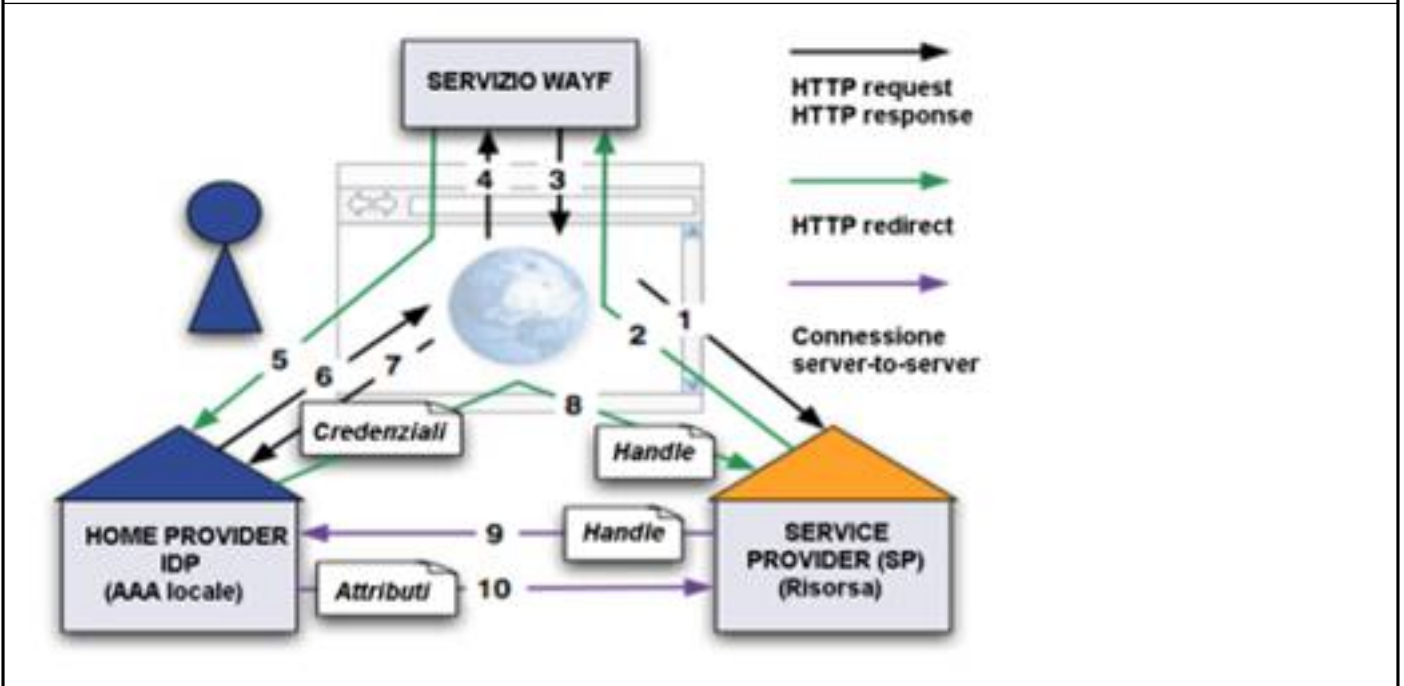


Figura 1: architettura federata di gestione delle identità.

