## Scenario di riferimento

Il presente progetto si inserisce in uno scenario più ampio nel quale l’Assessorato alla Ricerca Scientifica della Regione Campania (AGC6) intende dotare tutti i cittadini della regione della cosiddetta Carta Regionale dei Servizi (CRS) e con questa tutta una serie di servizi a valore aggiunto.

Il progetto intende quindi cogliere una prima opportunità per sperimentare servizi in grado di valorizzare, all’interno di una comunità tecnologicamente avanzata e culturalmente predisposta come quella costituita dai 7 Atenei campani, la capacità di assegnare una identità digitale ad ogni suo membro che possa essere verificata on-line e fruita attraverso servizi in rete.

In particolare l’infrastruttura tecnologica prevede la piena integrazione/condivisione con il sistema nazionale ormai condiviso da tutte le regioni d’Italia denominato Carta Nazionale dei Servizi, che definisce tutti i dettagli sui media da utilizzare (Smart Card (anche contactless) /Token USB) sulle informazioni contenute sui dispositivi e sulla loro disposizione all’interno del file system perché si possa essere garantita la piena interoperabilità con applicazioni già sviluppate per la CNS e tra le varie regioni (in caso di cambi anche temporanei di residenza).

Il progetto condivide l’ipotesi iniziale, proposta dall’AGC6 di servirsi della società SOGEI indicata dal Ministero delle Entrate e Finanze (MEF) come società per l’emissione delle Tessere Sanitarie (TS) / CNS a tutti i cittadini d’Italia che prevede la riemissione (enrollment ed invio postale presso il domicilio fiscale di ogni cittadino) completa nell’arco di validità delle carte già emesse (tre anni).

Sarà cura dell’AGC6 negoziare una convenzione con il MEF per l’emissione delle carte necessarie per la sperimentazione per realizzare un sistema federato di gestione delle identità che coinvolge gli Atenei della Regione Campania.

Obiettivo principale della sperimentazione e del presente progetto è l’erogazione (diretta o indiretta) di servizi a valore aggiunto in grado di dimostrare gli enormi vantaggi ottenibili da un sistema per la gestione delle identità robusto e condiviso tra tutte le principali applicazioni fruibili in rete e che potranno beneficiare delle caratteristiche di robustezza e sicurezza insite nelle Smart Card e nell’architettura del sistema. Requisito essenziale è ancora una volta l’interoperabilità del sistema con le soluzioni realizzate o in fase di realizzazione secondo gli stessi standard nelle altre regioni.

Le Università Campane condividendo gli obiettivi esposti propongono quindi l’implementazione di un’infrastruttura federata e delocalizzata di gestione delle identità (profili e proprietà di ciascun utente / applicazione) che condivide un indice unico centralizzato ed un’unica infrastruttura tecnologica (Card Management System).

Nell'ambito di un'infrastruttura di identità federata, tutti i fornitori di servizi e i membri di appartenenza degli utenti, si scambiano informazioni sull'identità degli utenti stessi in modo sicuro e rispettoso, garantendo i diritti di riservatezza degli utenti finali.

La federazione proposta vedrà quindi i diversi attori coinvolti condividere politiche comuni sia per lo scambio di informazioni sugli utenti che per le risorse disponibili. In questo modo un’utente di una amministrazione potrà accedere ad un qualsiasi servizio tramite il sistema di autenticazione della propria organizzazione.

Il sistema di autenticazione sarà implementato a 2 livelli:

1. il primo, centralizzato, sarà basato sul principio della circolarità anagrafica e costituirà l’indice anagrafico complessivo degli utenti (13 campi anagrafici provenienti dal tracciato ad eventi denominato AP5 definito da CNSD per l’ INA / SAIA)
2. il secondo, distribuito localmente presso gli enti di appartenenza, dedicato alla gestione dei profili utente (application dipendent) consentirà anche di esportare altri metodi di autenticazione (ad esempio username/password) per garantire il passaggio graduale alla CNS o per affrontare il tema backup/account temporanei in caso di guasti o perdita delle SC.

In altre parole il sistema centrale di gestione degli indici anagrafici (sommatoria di tutte le identità presenti) costituirà un ulteriore metodo di autenticazione (il principale) per un sistema federato basato su tecnologie consolidate, facendosi carico esclusivamente della verifica delle credenziali basate su CRS sfruttando le sole informazioni presenti nel CMS ed in particolare le chiavi pubbliche relative ad ogni certificato rilasciato.

Al contrario, i vantaggi derivanti dallo schema di federazione (distribuito) sono molteplici tra cui si cita:

* l’utente potrà continuare ad utilizzare le proprie credenziali che una volta fornite dall’ente di appartenenza per l'accesso ai servizi convenzionati con la Federazione ed essere informato sui dati comunicati al fornitore di servizi per l'autorizzazione;
* l'organizzazione dell'utente manterrà il controllo sulla procedura di autorizzazione per l’accesso dei propri utenti ai servizi disponibili;
* i dati relativi al singolo utente (profilo utente) saranno conservati ed aggiornati unicamente dall’organizzazione di appartenenza, da cui le procedure per le modifiche avranno un singolo punto di accesso;
* il fornitore di servizi eviterà la gestione delle credenziali personali degli utenti e si avvarrà delle informazioni concordate con la Federazione e divulgate dall'organizzazione di appartenenza per la fase dell'autorizzazione che sarà basata sui ruoli.
* l’accesso ai diversi servizi erogati per tutti gli utenti avverrà attraverso un unico portale di autenticazione sia per i servizi della federazione che per i servizi specifici del proprio ateneo.

## Il livello federazione

Il sistema centrale alla base di questa proposta prevede la creazione di una federazione costituita dalla aggregazione dei diversi Atenei e la Regione Campania.

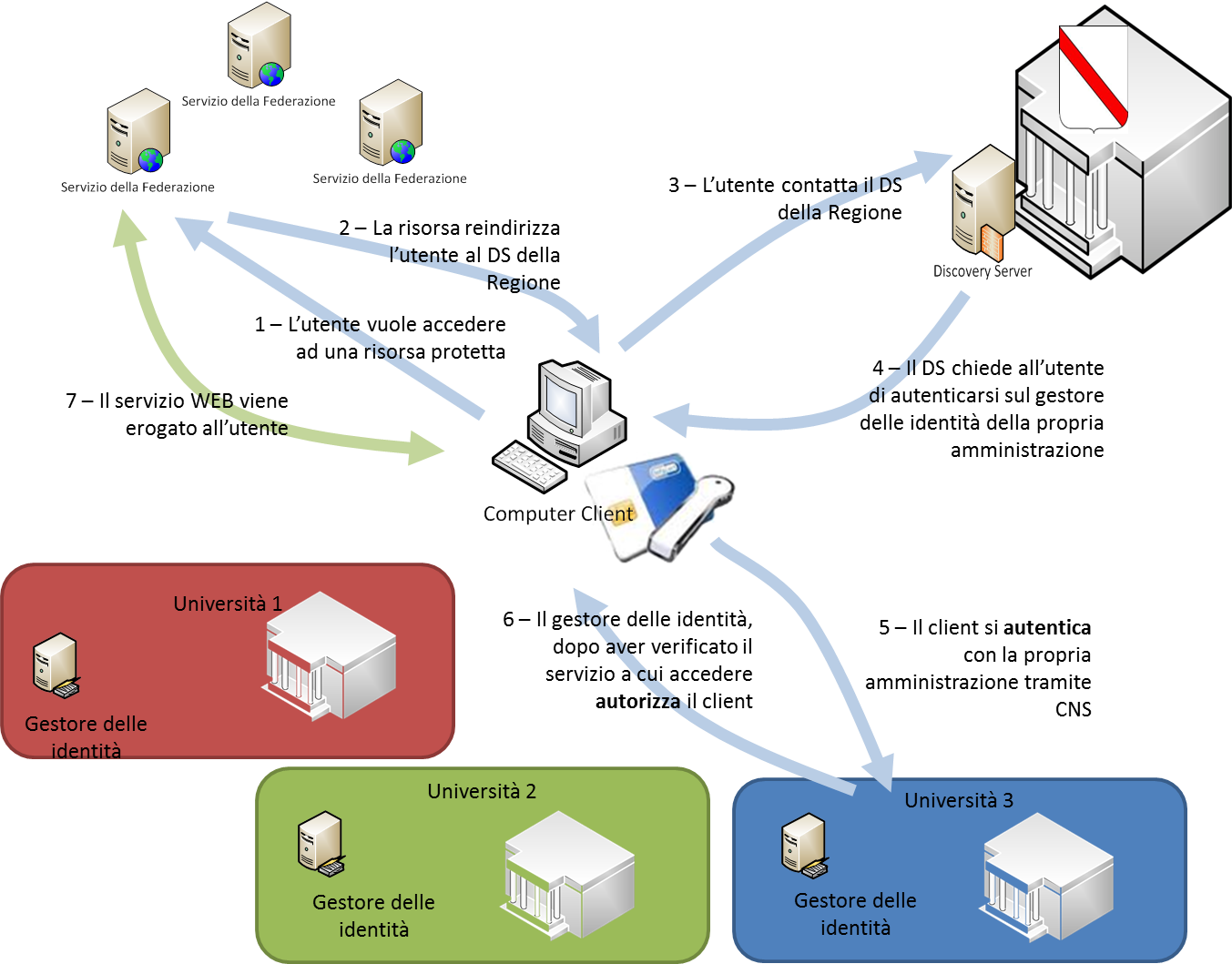
Per maggiore chiarezza lLa soluzione tecnica individuata è stata suddivisa in due strategie distinte in base alla tipologia di servizio erogato:

* applicativi web-based
* servizio di connettività Wi-FI

Di seguito una breve descrizione funzionale delle due soluzioni

#### Applicativi Web Based

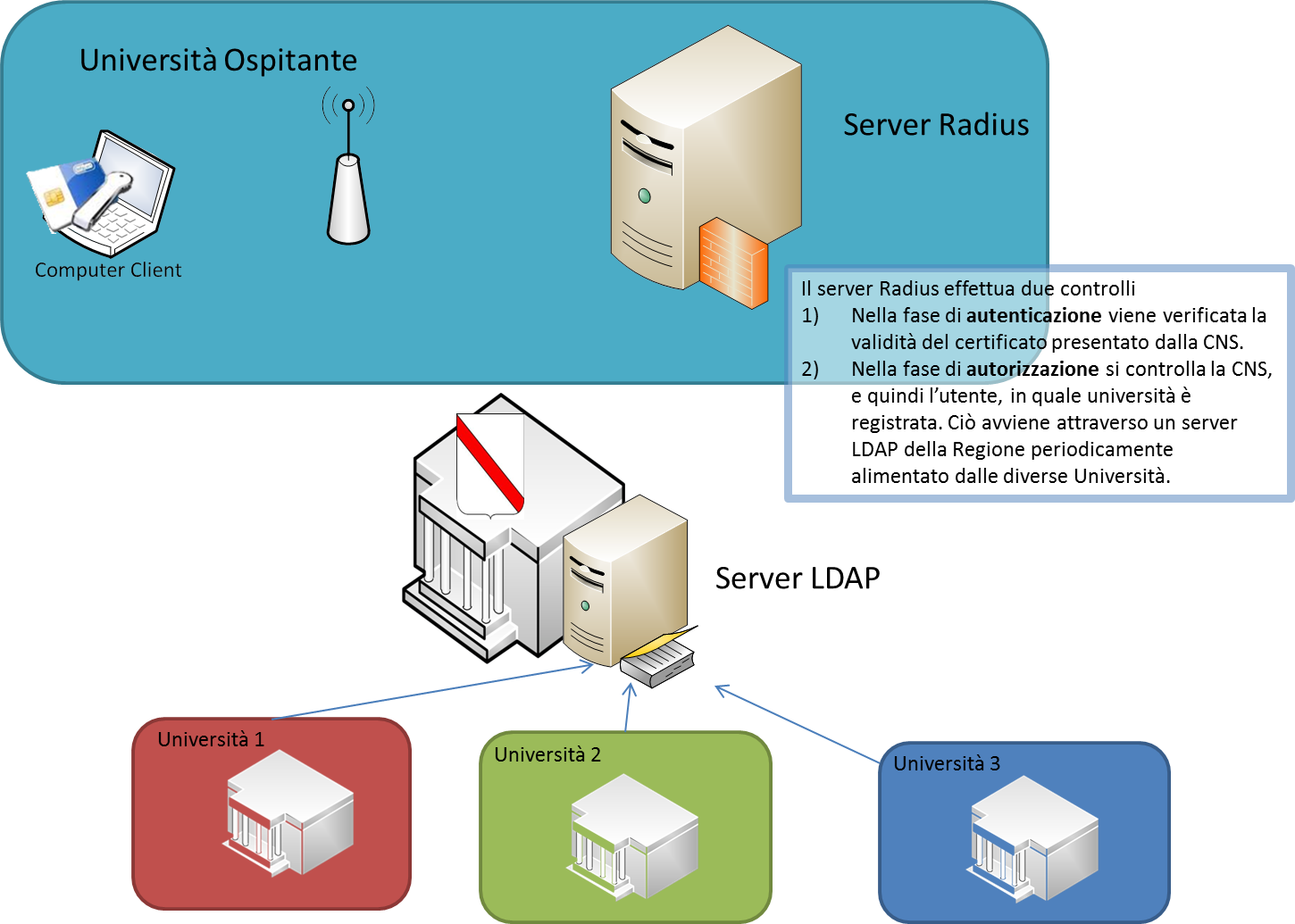
Per gli applicativi WEB-BASED l’autenticazione tramite CNS sarà implementata mediante una piattaforma software da installare parte in ciascun Ateneo e parte nella Regione. Questa architettura sarà in grado di autenticare i differenti utenti dei singoli Atenei ai molteplici servizi web forniti nella federazione.



#### Servizio di connettività Wi-FI

Per l’autenticazione WI-FI tramite CNS si prevede che ciascun Ateneo aderente al progetto, implementi un proprio server RADIUS in grado di scomporre le fasi della AAA in diversi passi:

1. La prima fase di autenticazione: l’utente che si vuole autenticare su una rete della federazione mediante smartcard dovrà utilizzare il certificato presente nel proprio dispositivo CNS per farsi riconoscere. Questa fase avviene come di consueto e già normato per la CNS attraverso una challange tra la Certification Authority che ha emesso il certificato (RC) e il client direttamente. A tal fine esistono già molti applet per l’autenticazione con CRS/CNS o il documento di InfoCert “Accesso ai Siti Internet.pdf“.
2. Nella fase di autorizzazione: il server RADIUS, dopo aver riconosciuto l’utente le cui credenziali sono state ricevute direttamente dal risultato della challange nella fase di autenticazione verificherà l’associazione della chiave pubblica (o del codice fiscale) su un server comune della federazione[[1]](#footnote-1).
3. A di Accounting: dopo aver riconosciuto l’utente in fase di autenticazione, e dopo averlo autorizzato, in fasi di autorizzazione, l’accounting prevede che l’amministrazione erogante il servizio conservi i log di accesso alla sessione legata al profilo dell’utente.



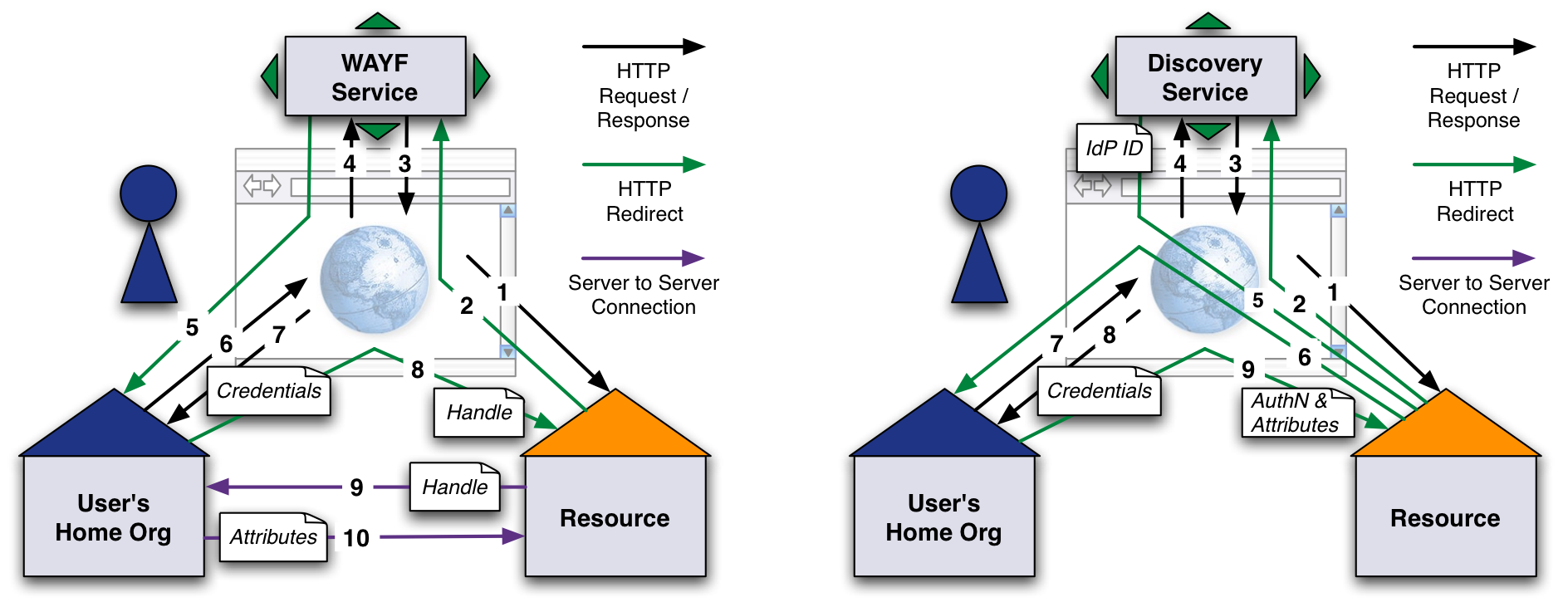
## L’infrastruttura informatica

Nei precedenti paragrafi si è vista, in modo estremamente sintetico, una macro descrizione funzionale. In questo paragrafo si vuole descrivere, sempre sinteticamente, l’infrastruttura tecnica informatica con cui verranno gestite le due tipologie di servizi erogabili. Una spiegazione dettagliata, così come le configurazioni dei prodotti da installare, saranno presentati in un successivo documento.

Una delle principali specifiche progettuali perseguite da questo progetto è quella che prevede che ciascun membro della federazione garantisca la gestione delle identità dei propri utenti in modo autonomo. In tal modo nessuna amministrazione dovrà esporre i dati personali (in particolar modo quelli sensibili) all’esterno del proprio ente.

La Regione, come preannunciato al paragrafo precedente, costituirà il collante amministrativo e tecnologico tra le differenti amministrazioni e sarà quindi l’entità che andrà a legare le singole amministrazioni nella federazioni proposta:

* dal punto di vista amministrativo dovrà curare e approvare i “DOcumenti descrittivi del Processo di Accreditamento degli Utenti dell’Organizzazione” (secondo le specifiche fornite dal progetto IDEM per il modello DOPAU) delle singole Università. Dovrà inoltre farsi garante e definire le linee guida e le condizioni da rispettare tra tutti i membri.
* dal punto di vista tecnico dovrà erogare i due servizi centralizzati presentati al paragrafo precedente, ovvero sia il servizio “Where Are You From” (WAYF) o “Discovery Service”[[2]](#footnote-2) (DS) utilizzato per l’autenticazione dei servizi Web che il servizio LDAP necessario per la fase di autorizzazione del servizio WI-FI. Tale servizio LDAP prevede che ciascun ente membro della federazione esporti, per ciascun utente della propria amministrazione, gli attributi (da concordare e standardizzare tra le differenti amministrazioni) in un ramo di propria competenza che sia però interrogabile da tutti i membri della federazione.



## Un esempio - l’Università degli Studi di Salerno

L’implementazione di una infrastruttura AAI (Authentication and Authorization Infrastructure) rappresenta, a nostro avviso, l’opportunità concreta per razionalizzare e semplificare i sistemi di autenticazione presenti nella proprie infrastruttura informatica. Di fatto, l’implementazione di un sistema AAI prevedere una prima fasi di analisi dei propri applicativi e delle basi di dati disponibili; successivamente occorre individuare le fonti autorevoli dei dati e infine integrare i dati disponibili dai vari database in un unico repository centralizzato (repository non necessariamente fisico ma logico). Questa analisi deve essere effettuata per ogni tipologia di utente (personale tecnico- amministrativo, personale docente, studenti e laureati, erasmus ecc) che deve accedere ai servizi dell’Ateneo e che di conseguenza deve utilizzare il servizio di Identity and Access Management (IAM).

L’Università di Salerno, ha implementato una prima piattaforma IAM, ovvero un sistema di gestione delle identità finalizzato a collezionare e mantenere aggiornati i dati di tutti gli utenti (personale tecnico-amministrativo, personale docente, studenti, laureati e altri) prelevando direttamente le singole informazioni dalle fonti dati autoritative.

#### Identity Management

Nell’infrastruttura dell’Ateneo è stato implementato il sistema di gestione di Identity and Access Management (Iam@UniSA) basato su Shibboleth, ovvero un framework open source fondato su SAML e sviluppato dal consorzio Internet2. Per utilizzare Shibboleth nella nostra realtà è stata effettuata, come già accennato, una dettagliata analisi sugli utenti dell’Ateneo e sono stati individuati i singoli database autoritativi.

L’individuazione delle fonti autorevoli dei dati di autorizzazione e di identificazione è stato di fatto uno dei passi principali nell’implementazione della piattaforma IAM. Il lavoro è stato alquanto complesso essendo partiti da diversi database con dati ridondati e spesso non corretti.

I passi seguiti sono stati:

1. Individuazioni delle diverse tipologie di utenti a cui offrire i servizi di autenticazione centralizzata:
   * Personale docente
   * Personale tecnico-amminsitrativo
   * Studenti (considerando studenti anche i dottorandi)
   * Personale esterno all’Ateneo ma con rapporto di lavoro più o meno stabile o più o meno ufficiale (ditte esterne, aziende partecipate, consorzi, studenti esterni, collaboratori senza contratto)
2. Per ciascuna tipologia di utente sono stati individuati gli attributi anagrafici comuni e quelli specifici delle diverse categorie. Gli attributi sono stati poi “normalizzati” per avere tutti la stessa semantica.
3. I singoli attributi sono stati successivamente associati ai diversi database autoritativi: ad esempio ESSE3 per gli studenti, CSA per il personale TA e Docente. Infine è stato creato un nuovo Database per la gestione dei rapporti “di lavoro più o meno stabili o più o meno ufficiali” di cui spesso non esistevano tracce formali.
4. Infine sono state create delle viste intermedia delle tabelle dei differenti DB autoritativi e utilizzate da applicazioni sviluppate ad hoc per la gestione delle piattaforma IAM.

Il passo 4 si è reso necessario per motivi prestazionali in modo da avere un'unica applicazione per la gestione dei profili e dei servizi anziché accedere a diversi applicativi o database contemporaneamente.



Una volta completata la fase di predisposizione delle fonti dati si è proceduto a configurare il sistema di Identity Provider (IP) e diversi sistemi Service Provider (SP). Nel mondo Shibboleth l’IP è un server web sui cui l’utente si autentica mentre il SP è il servizio web a cui l’utente vuole accedere.

Un importante conseguenza del consolidamento delle identità svolto è stato la creazione di un preciso e dettagliato censimento non solo dei database applicativi in esercizio ma anche un’omogeneizzazione dei dati delle identità. In fine sono state predisposte le procedure amministrative per la gestione degli utenti.

Le credenziali uniche hanno consentito la semplificazione e standardizzazione delle varie procedure:

* rilascio di nuove credenziali per le diverse tipologie di utenti;
* provisioning e de-provisioning automatizzato degli utenti dai database autoritativi;
* creazione di una procedura unica per il recupero delle credenziali in caso di smarrimento;
* creazione di una procedura unica per la gestione della scadenza password.

#### Accesso ai servizi

L’accesso ai servizi informatici erogati sotto qualsiasi forma, con accesso remoto via internet o con acceso fisico dall’interno delle strutture universitarie pone il problema del riconoscimento dell’utente e quindi Autenticazione e Autorizzazione.

Il sistema IAM implementato svolge questo ruolo e garantisce un accesso unificato a tutti i servizi interni dell’Ateneo, con uno strato intermedio per le applicazioni che non erano compatibili con questo tipo di sistemi. Inoltre il sistema si pone come requisito base per l’implementazione di nuovi servizi che devono prevedere la compatibilità applicativa ed architetturale con il esso.

L’infrastruttura ha portato diverse implicazioni positive tra cui:

lo sgravio per le singole procedure applicative di un database locale per gli accessi e le autorizzazioni;

ogni utente ha una sola CAU (Credenziale di Acceso Unificata) che gli viene rilasciata al primo contatto con l’Università e lo segue fino al termine del rapporto. Con una significativa riduzione di tempi e di costi per la gestione dei processi di accreditamento per le singole procedure.

1. La Regione Campania ospiterà il servizio di autorizzazione utilizzato da tutti i membri appartenenti alla federazione. [↑](#footnote-ref-1)
2. Il DS è nuovo e sostituisce il WAYF ma non è compatibile con Shibboleth 1 [↑](#footnote-ref-2)