6 AUTENTICAZIONE FEDERATA PER L'ACCESSO A INTERNET E A RISORSE IN RETE

QUESTE LINEE GUIDA indicano quali scenari e tecnologie si devono implementare nelle università per giungere all'obiettivo nel rispetto delle indicazioni normative vigenti. Il capitolo è articolato in due parti: una contiene la descrizione generale, l'ambito di applicazione e la normativa; l'altra contiene la esemplificazione in casi specifici.

6.1 Descrizione generale del servizio e ambito di applicazione

L'utente, registrato presso un soggetto - detto "Organizzazione di appartenenza", OdA - che gli ha fornito un'identità digitale e le relative credenziali (username e password, o certificato), utilizza le credenziali fornite dall'OdA per accedere ad Internet attraverso le risorse di rete di un secondo soggetto, detto "Fornitore di servizio" (FdS).

Condizioni d'uso:

1. **Registrazione**: la procedura di registrazione adottata dall'OdA per assegnare e/o abilitare le credenziali all'utente deve garantire l'integrità, la disponibilità e la riservatezza delle credenziali e l'identificazione certa dell'utente nel rispetto della normativa vigente in materia di antiterrorismo e di protezione dei dati personali. Sono ammesse:
   a. procedure di registrazione a seguito di identificazione diretta de visu attraverso l'acquisizione dei dati di un documento di identità personale;
   b. procedure di registrazione a seguito di identificazione indiretta basata sull'acquisizione dei dati di una carta di credito o di una SIM card rilasciata in Italia;
   c. procedure di registrazione a seguito di identificazione indiretta basata sull'acquisizione di token o la verifica di credenziali precedentemente rilasciati dalla OdA stessa con modalità di tipo a) o b).
2. **Gestione dell'identità digitale**: l'OdA deve garantire il trattamento dei dati e delle credenziali dell'utente nel rispetto della normativa vigente in materia di protezione dei dati personali e, nel caso in cui l'identità digitale comprenda username e password, deve mettere a disposizione dell'utente procedure sicure per modificare o reimpostare la propria password.

3. **Autenticazione**: la procedura di autenticazione deve prevedere l'utilizzo di canali sicuri per la trasmissione delle credenziali attraverso opportune tecnologie, e evitare di esporre le credenziali al FdS o a terzi.
4. **Accesso:** la procedura di accesso deve prevedere lo scambio tra l'OdA e il FdS dei dati minimi indispensabili a permettere: l'identificazione dell'utente presso l'OdA, la verifica del possesso dei requisiti di accesso, l'erogazione del servizio nel rispetto della normativa vigente e delle *usage policies* della rete del FdS e della rete (ad esempio NREN) a cui questo è connesso.
5. **Tracciamento**: l'OdA e il FdS devono collaborare ai fini del tracciamento e dell'identificazione dell'utente nel rispetto della normativa vigente in materia di antiterrorismo e di protezione dei dati personali. A tal fine l'OdA e il FdS devono condividere riferimenti univoci associati alle tracce mantenute dal FdS e all'identità dell'utente mantenuta dall'OdA.
6. **Fiducia**: l'OdA e il FdS devono darsi garanzie reciproche di rispetto delle condizioni espresse ai precedenti punti 1, 2, 3, 4 e 5. Tali garanzie possono essere formalizzate da un accordo bilaterale tra OdA e FdS, o dall'adesione dell'OdA e del FdS ad una federazione o confederazione che preveda il rispetto delle suddette condizioni.
7. **Informazione**: l'utente deve essere informato in modo chiaro e compiuto:
   - ❖ delle finalità e delle modalità di trattamento dei propri dati personali eventualmente richiesti;
   - ❖ dei servizi, delle federazioni e delle confederazioni a cui le credenziali danno accesso;
   - ❖ dell'identità del soggetto che fornisce il servizio (FdS) e dell'identità del soggetto che opera la validazione delle credenziali all'atto dell'autenticazione (OdA)
   - ❖ dello scambio di informazioni tra OdA e FdS ai fini della fornitura del servizio, nei casi in cui ciò sia indispensabile ai fini dello stesso;
   - ❖ delle condizioni di utilizzo del servizio di accesso;
   - ❖ delle modalità di interruzione dell'accesso (*logout*).
8. **Consenso**: prima di effettuare l'accesso l'utente deve acconsentire, caso per caso o *una tantum* allo scambio di informazioni tra OdA e FdS eventualmente necessarie ai fini della fornitura del servizio.
9. **Controllo**: l'utente deve avere controllo della durata della connessione ad Internet e deve poterne verificare in ogni momento la sussistenza o la cessazione.

6.2 Modalità Operative: i casi Eduroam ed Idem - Autenticazione Federata per Il Wi-Fi in ambito Universitario

Le linee guida generali di cui sopra si riferiscono all'autenticazione federata per accesso ad Internet in qualsiasi ambito e con qualsiasi tecnologia. Nel presente paragrafo si fornisce invece una particolarizzazione esemplificativa riferita all'autenticazione federata per il wi-fi in ambito universitario. In questo specifico ambito, le due modalità suggerite per implementare quanto espresso nel paragrafo "Descrizione generale del servizio e ambito di applicazione" sono le federazioni **eduroam ed IDEM**.

eduroam (*education roaming*) è il servizio di accesso sicuro e globale (mondiale) alla rete Internet in modalità wi-fi per gli utenti mobili a disposizione della comunità internazionale della ricerca e della formazione universitaria. eduroam permette agli studenti, ai ricercatori e al personale universitario di sfruttare la connettività Internet nei propri campus e presso ogni altra istituzione partecipante che si ha l'occasione di vi sitare senza ulteriori necessità di registrazione o configurazione (**http://www.eduro- am.org**).

IDEM è la Federazione Italiana di Infrastrutture di Autenticazione e Autorizzazione dedicata alla comunità della ricerca e della formazione universitaria (https://www.IDEM.garr.it). La federazione IDEM permette l'accesso a molteplici risorse web, utilizzando profili SAML. L'utente beneficia anche del *Single Sign On* e mediante l'unica identità fornita dalla sua organizzazione di appartenenza accede a molteplici risorse (contenuti, dati, applicazioni) della propria organizzazione e delle altre organizzazioni della federazione.

Mediante le tecnologie messe in opera dalla federazione IDEM è possibile realizzare speciali *Service Provider* per autorizzare l'accesso alla rete in modalità wi-fi gli utenti della federazione che si trovano presso la propria organizzazione di appartenenza o presso altre organizzazioni della federazione. Questa particolare configurazione permette una modalità di accesso alla rete Internet per gli utenti mobili analoga, ma non alternativa, a quella fornita da eduroam.

È auspicato che ogni università aderisca ad entrambe le federazioni seguendo una roadmap personalizzata che conduce alla realizzazione di:

- un sistema di Identity Management (IM)
  - ✓ è a carico di questo componente dare garanzia del rispetto delle condizioni 1 e 2 prima definite
  - ✓ il sistema di IM non è un componente tecnologico né della federazione IDEM, né della federazione eduroam
  - ✓ ciascuna università stabilisce in autonomia come realizzarlo

- ✓ il sistema di IM dovrebbe essere unico per l'università e ad esso dovrebbero attingere le informazioni sulle identità digitali sia l'Identity Provider di IDEM che l'Identity Provider di eduroam;

- un *Identity Provider* (IDP) in IDEM
  - ✓ le condizioni 3 e 5 sono garantite dall'implementazione tecnologica del componente;
- un Identity *Provider* (IDP) in eduroam
  - ✓ le condizioni 3 e 5 sono garantite dall'implementazione tecnologica del componente;
- un servizio di accesso alla rete (*Resource Provider, RP*) in modalità wireless tramite la federazione eduroam
  - ✓ le condizioni 4, 5 e 9 sono garantite dall'implementazione tecnologica del componente;
- un servizio di accesso alla rete in modalità wireless tramite la federazione IDEM
  - ✓ le condizioni 4 e 5 sono garantite dall'implementazione tecnologica del componente
  - ✓ la condizione 9 è fattibile, ma richiede esplicita configurazione.

L'adesione ufficiale di una università a ciascuna delle due federazioni attua la condizione 6.

Rimane a carico dell'università stabilire come attuare le condizioni 7 e 8, con la precisazione che quest'ultima può essere acquisita in forma tradizionale oppure in modalità informatica con l'implementazione tecnologica di un modulo aggiuntivo (uAp- prove).