Accesso Wi-Fi federato dell'Area della Ricerca di Pisa

Ing. Abraham Gebrehiwot

reparto: Rete Telematica del CNR di Pisa

Via G. Moruzzi 1

56124, Pisa

abraham.gebrehiwot@iit.cnr.it

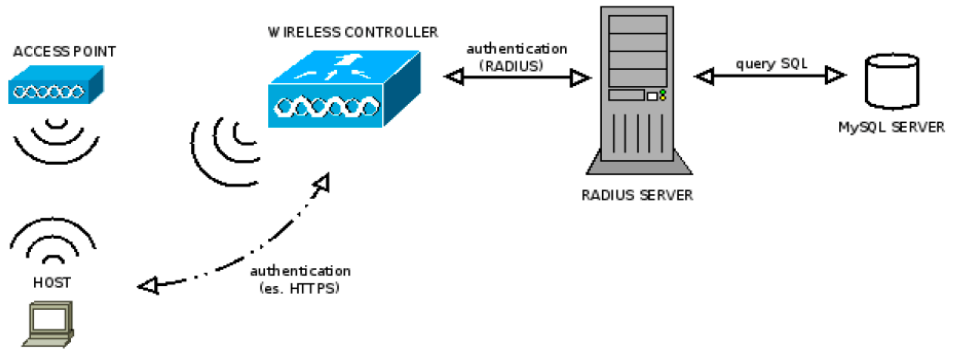
tel: +39-050-3152079

Obiettivo della presentazione

- Descrivere la soluzione accesso Wi-Fi "guest" del CNR di Pisa agli utenti della federazione IDEM
  - Mantenere l'infrastruttura esistente
- Cenno alla soluzione Wi-Fi federato CNR del Piemonte

Infrastruttura esistente

- il Wireless LAN Controller e AP della CISCO:
  - Cinque differenti SSID annunciati
  - Circa 50 access point
  - 2 WLC controller modello 44xx
- vari software di pubblico dominio:
  - free Radius, MySQL, Apache server ed infine codice sviluppato in PERL installati su un server Linux CentOS-5.



Gestione utenti Wi-Fi
RADIUS servre

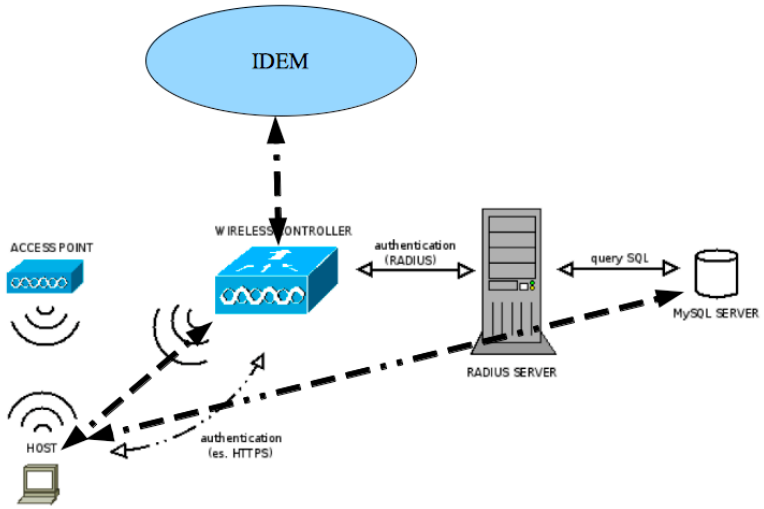
Infrastruttura esistente: copertura Wi-Fi

Infrastruttura esistente: gestione utenti

- Utenti definiti su Free RADIUS server
  - Il RADIUS server esegue una query sul DBMS MySQL per la verificare le credenziali a lui trasmessi.
  - L'uso del server MySQL rende il processo di gestione degli utenti snello, flessibile e maggiormente manutenibile.
  - File sql.conf
    - Sono contenute le query SQL
    - Modifica alla "authorize_check_query" aggiungendo varie condizioni tra cui:
      - State=enum('enabled','disabled'), expiration='timestamp', wlan='varchar(50)'
  - categorie di utenti
    - (*SuperUser, Amministratori*, *Utenti interni*, *Collaboratori*, *Visitatori* e *gruppi di utenti per le conferenze*)
    - L'utente WiFi, in base alla propria categoria di appartenenza, può effettuare alcune operazioni
      - gestione completa del sito, gestione completa dei propri utenti, modifica della password, estensione del periodo temporale di validità delle credenziali, e modificare i propri attributi come indirizzo email e telefono.

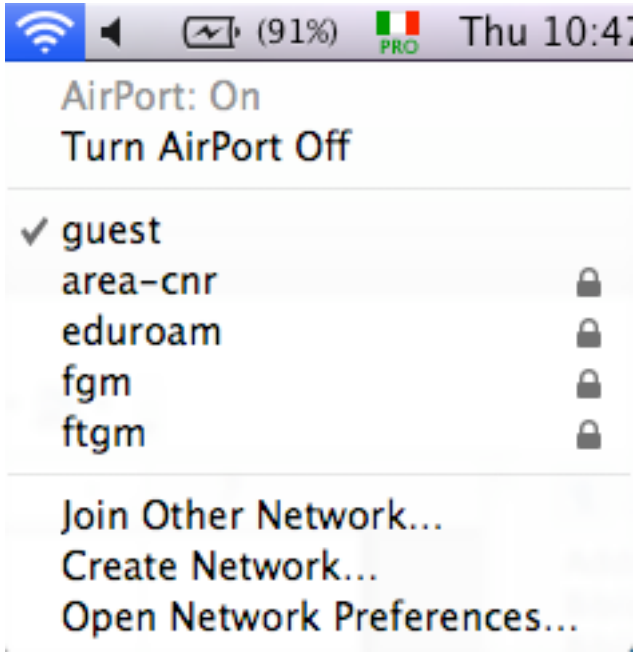
Infrastruttura modificata

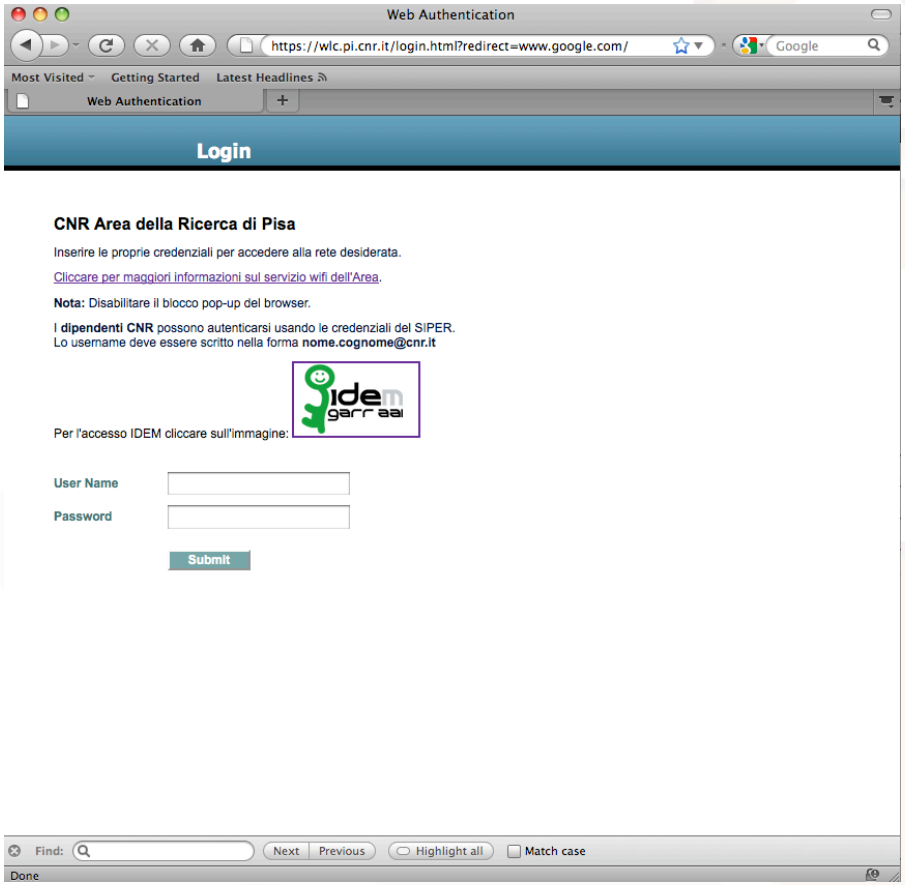
- Wireless LAN Controller e AP della CISCO
- vari software di pubblico dominio:
  - free Radius, MySQL, Apache server, SP Shibboleth ed infine codice sviluppato in PERL installati su un server Linux CentOS-5.



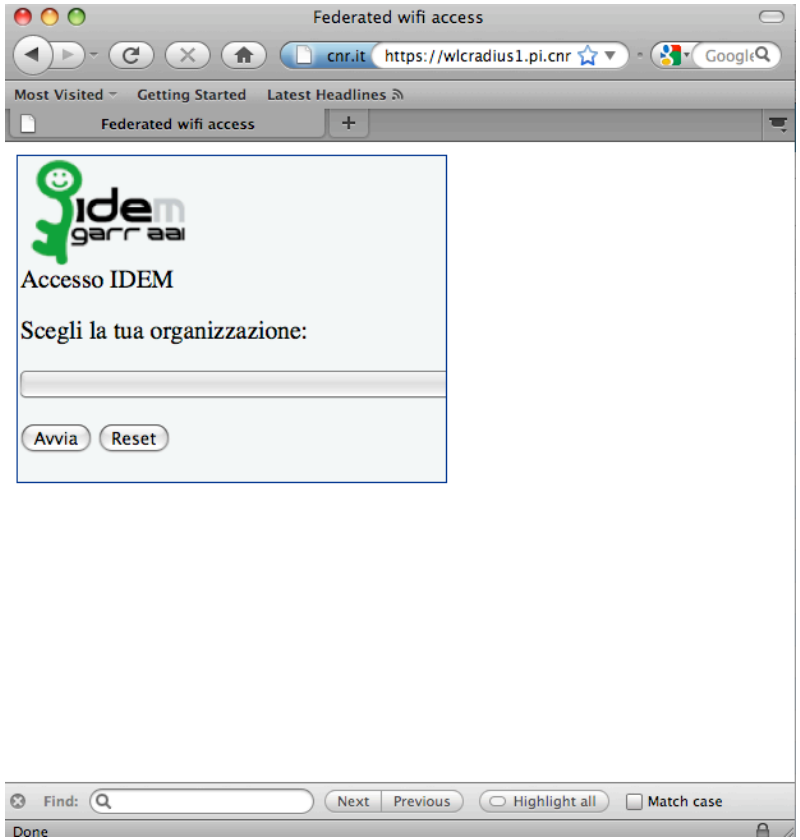
Gestione utenti Wi-Fi
SP IDEM
Embedded WAYF
RADIUS Server

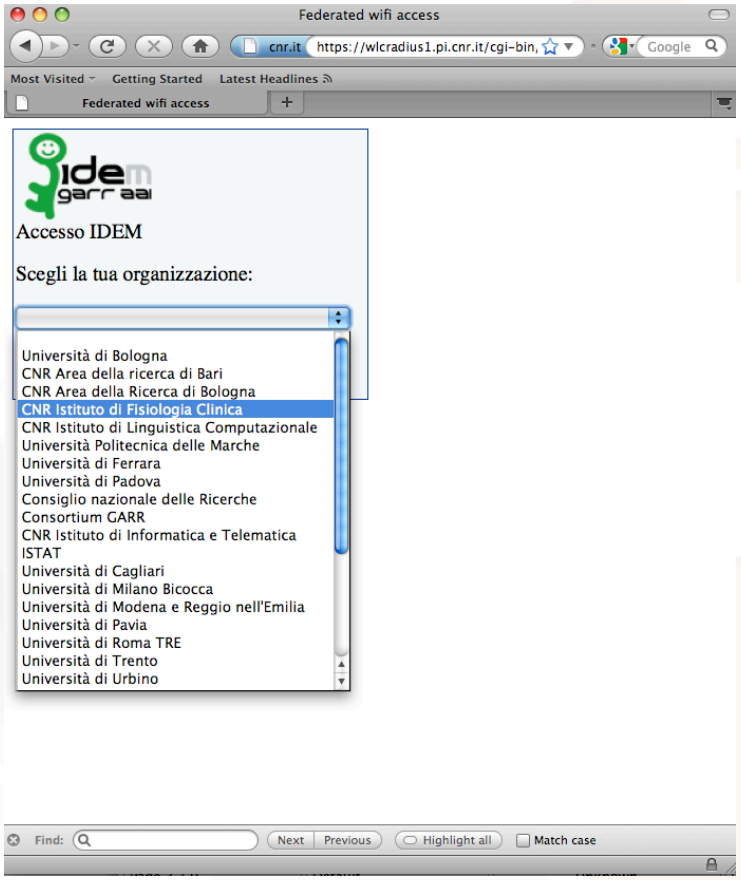
Servizio Wi-Fi federato: autenticazione utente finale



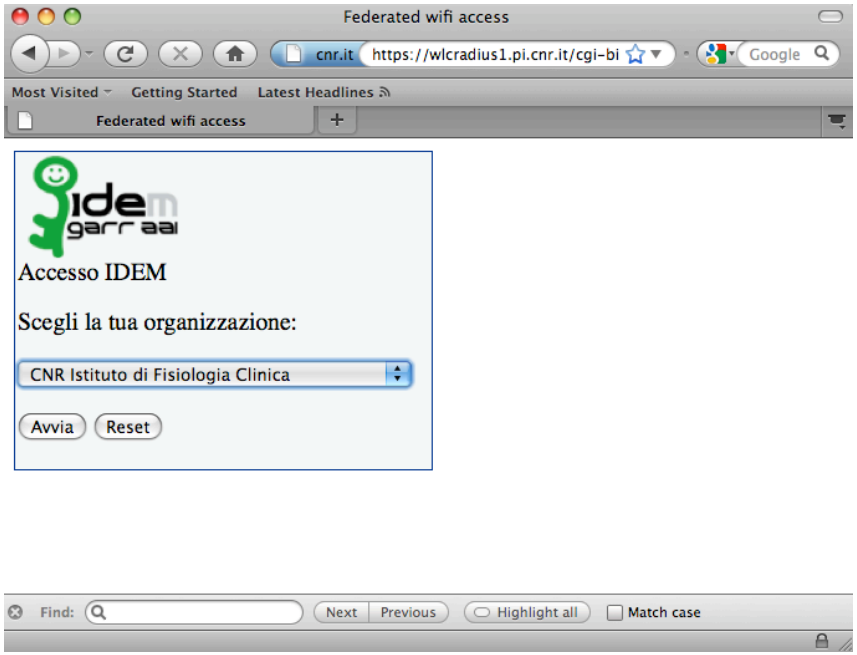


Servizio Wi-Fi federato: autenticazione utente finale

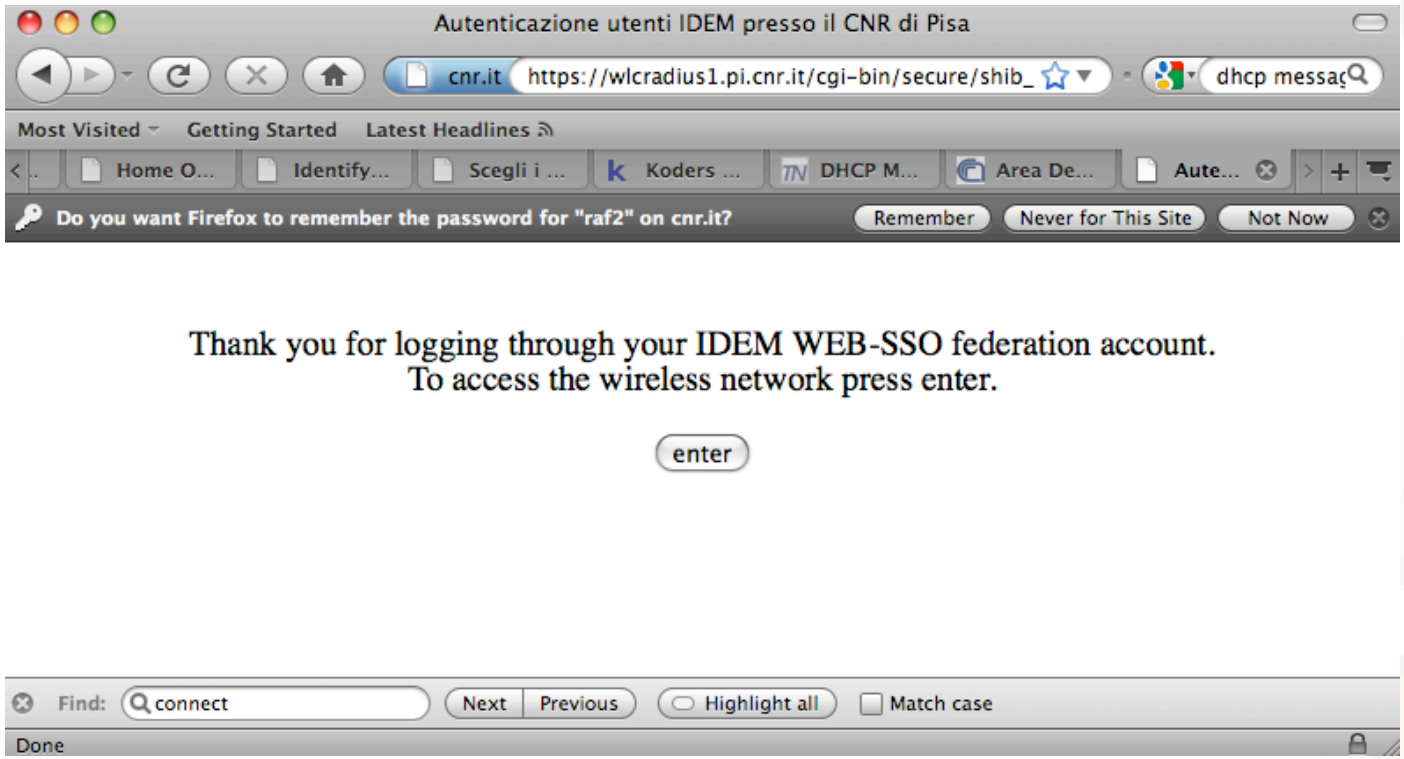




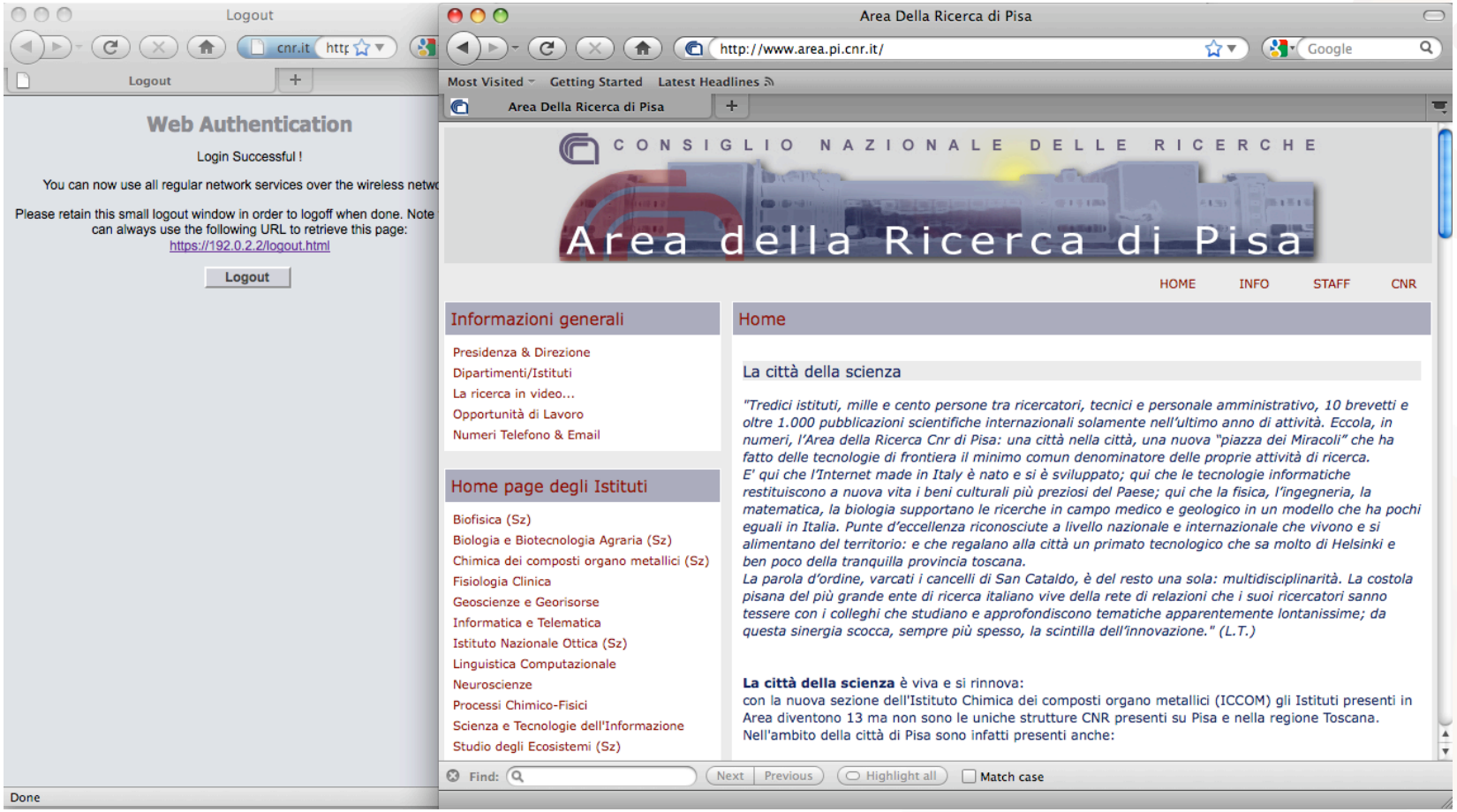
Servizio Wi-Fi federato: autenticazione utente finale



Servizio Wi-Fi federato: autenticazione utente finale



Servizio Wi-Fi federato: autenticazione utente finale



Descrizione funzionamento del Wi-Fi federato

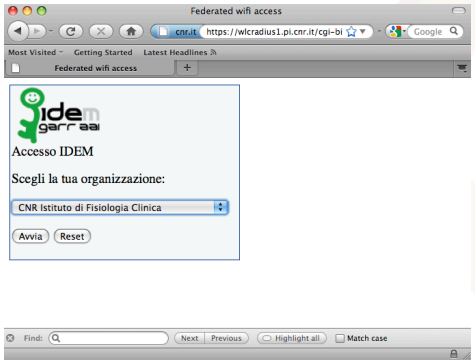
- Il browser dell'utente non autenticato deve interagire con le risorse IDEM
  - il WLC
    - presso il CNR di Pisa
  - l'embedded WAYF service
    - presso CNR di Pisa
  - l'SP che genera le credenziali per l'accesso alla rete Wi-FI
    - presso CNR di Pisa
  - i diversi IDP della federazione
    - risorse distribuite

Descrizione funzionamento del Wi-Fi federato: ACL

- Configurazione di Access Control Lists del WLC
  - Tramite WEB o command line
  - Per ogni risorsa IDP di IDEM
  - Non supporta IPv6

11	Permit	146.48.68.189 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0
12	Permit	0.0.0.0 / 0.0.0.0	146.48.68.189 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0

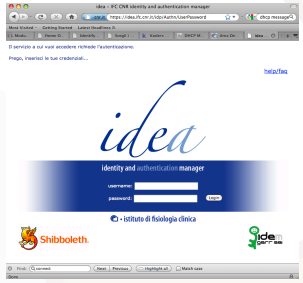
Descrizione funzionamento del Wi-Fi federato: embedded WAYF



- E' composto da due script
  - Il primo script:
    - elabora i metadati della federazione IDEM
    - Per ciascun IDP estrae i campi "entityID" e "OrganizationDisplayName" e restituisce un un menu a tendina:
      - L'utente vede l'OrganizationDisplayName
      - Lo script restituisce l'entityID allo script successivo

Descrizione funzionamento del Wi-Fi federato: embedded WAYF

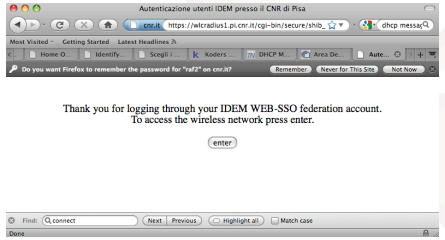
- Il secondo script:
  - Prende in input l'entityID selezionato e compone la URL di redirezione verso il DiscoveryResponse del SP passando gli argomenti target ed entityID. Ad esempio:
    - https://wlcradius1.pi.cnr.it/Shibboleth.sso/DS?target=https://wlcradius1.pi.cnr.it/cgi-bin/secure/shib_guest.pl&entityID=https://idea.ifc.cnr.it/idp/shibboleth



  - Questa stringa è sufficiente al DiscoveryResponse del SP ad autenticare l'utente finale presso il suo IDP e dare accesso allo script target presso il SP
  - Questa operazione è trasparente all'utente finale

Descrizione funzionamento del Wi-Fi federato: Account linking

- Generare un account locale con il target script:
  - target=https://wlcradius1.pi.cnr.it/cgi-bin/secure/shib_guest.pl
    - Crea un account sul RADIUS server
    - Utilizza il campo eduPersonTargetedID come username ed una password casuale
    - In realtà si consulta il campo "REMOTE_USER" configurato sul SP per consultare i variabili eduPersonTargetedID ed mail in ordine
    - Se l'utente esiste estende la validità dell'account per un solo giorno e resetta la password
    - Prepara un form nascosto per accedere alla rete Wi-Fi



Conclusioni

- Autenticazione WEB SSO Shibboleth per accedere la rete
- Il traffico IP viene trasmesso in chiaro
- Bisogna definire le ACL sul WLC manualmente
- Le ACL sul WLC hanno il limite di non controllare il traffico IPv6
- La necessità di avere un WEB browser per accedere alla rete
- Non si ha la possibilità di assegnare la VLAN di appartenenza agli utenti in modo dinamico
- Difficoltà di uso per utenti con dispositivi mobili (come telefoni di ultima generazione)
- Attualmente la soluzione WiFi federato non è ancora accettata a livello di inter federazioni al di fuori di IDEM
- Vantaggio: comunità di utenza IDEM accede alla nostra rete

Cenno alla soluzione Wi-Fi federato presso CNR del Piemonte

Sonicwall Network Security Appliance
NSA-5500