L'ABC per capire IDEM

e per capire cos'è l'Identità Digitale Federata

Gabriella Paolini – Consortium GARR (gabriella.paolini@garr.it)

IDEM DAY 2016 - 7 giugno 2016 - Roma - Università Roma Tre

Cos'è l'Identità Digitale?

- Facciamo un passo indietro.

Favorisca i documenti!

Da «Il Vigile» di Luigi Zampa con Alberto Sordi e Vittorio De Sica 1960 Fonte: Youtube

Cos'è l'Identità

- Cosa significa identificare una persona nella realtà?
  - Documento di identità (per stabilire che quella persona sia realmente quella persona)
  - Informazioni /documenti aggiuntivi che qualificano l'individuo (Studente, Dipendente pubblico, Giornalista, etc.)

Processo di identificazione nella realtà

- Devo partecipare ad un evento:
  - L'evento è pubblico. ⟹ Entro liberamente
  - L'evento è a pagamento con biglietto. ⟹ All'ingresso esibisco un biglietto, che non mi identifica, ma mi permette di entrare
  - L'evento è ad invito. ⟹ Esibisco un documento di identità che viene controllato e se sono sulla lista posso entrare.
  - L'evento è ad invito ed è riservato ai giornalisti. ⟹ Esibisco un documento di identità e la tessera dell'ordine dei giornalisti che attesta che sono un giornalista.

In what we trust?

- «Il documento di identità» è affidabile se rilasciato da **un'autorità**
- Le qualifiche se utilizzate ufficialmente devono essere dimostrate
- Concetti di
  - affidabilità
  - e fiducia

E allora l'Identità Digitale

- «L' insieme delle caratteristiche essenziali ed uniche di un soggetto che permettono di identificarlo».
  H. Abelson, L. Lessig, MIT - «Digital Identity in Cyberspace»
  http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall98-papers/identity/linked-white-paper.html
- «L'identità digitale è la rappresentazione virtuale dell'identità reale che può essere usata durante interazioni elettroniche con persone o macchine».
  E. Norlin, A. Durand, PingID Network - Whitepaper «Federated Identity Management»
  http://idkf.bogor.net/bio2/whitepaper/sso/whitepaper_identity_federation.pdf

- Credenziali ⟹ Il nostro documento di identità
- Attributi ⟹ le nostre qualifiche caratterizzanti

Credenziali e Attributi

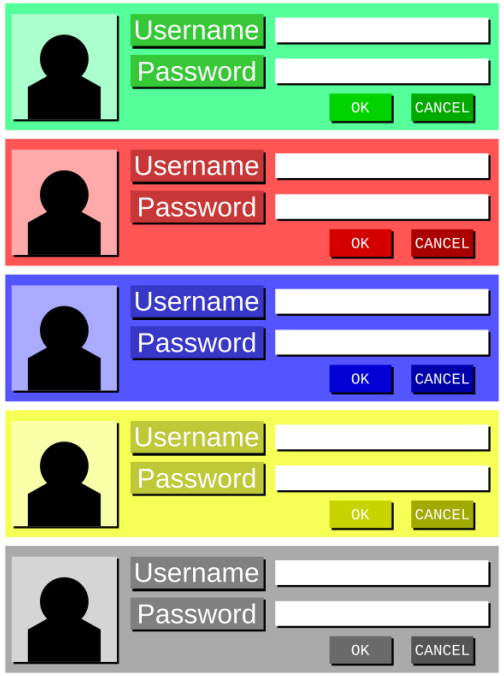
- Credenziali:
  - Informazioni che permettono di stabilire con certezza che la persona che le sta utilizzando è quella che dichiara di essere. Ad esempio:
    - La coppia di informazioni Username e Password
    - Un certificato elettronico
    - Una smartcard
    - Le impronte digitali
    - L'iride
- Attributi:
  - Informazioni accessorie che ci indentificano (più o meno importanti). Ad esempio:
    - Nome
    - Cognome
    - Indirizzo email
    - Codice fiscale
    - Datore di lavoro
    - Qualifica
    - Numero di Telefono

Come si ottiene la propria identità digitale

- Autocertificata:
  - Registrazione su un sito web
- Rilasciata da un organizzazione in base all'identificazione:
  - Identificazione verificata tramite altre modalità che già identificano la persona nel mondo reale: Numero di telefono, Carta di Credito, Indirizzo di residenza;
  - Identificazione verificata recandosi di persona presso l'organizzazione con un addetto che ne convalida la veridicità;
  - Identificazione verificata in digitale in base a dichiarazioni audio-video.

Autenticazione

- L'**autenticazione** è il *primo meccanismo* che attivo quando voglio accedere a informazioni protette che mi identificano in modo univoco **fornendo le mie credenziali**:
  - Sito web con la mia carriera scolastica (Registro scolastico),
  - Sito web di Home Banking,
  - Social Network,
  - Giornale in abbonamento,
  - etc.



Livelli di Autenticazione

- Sono io perché **so qualcosa che soltanto io posso conoscere** (something I know): username e password
- Sono io perché **ho qualcosa che soltanto io posso avere** (something I have): smartcard
- Sono io perché **sono finisicamente io** (something I am): impronte digitali

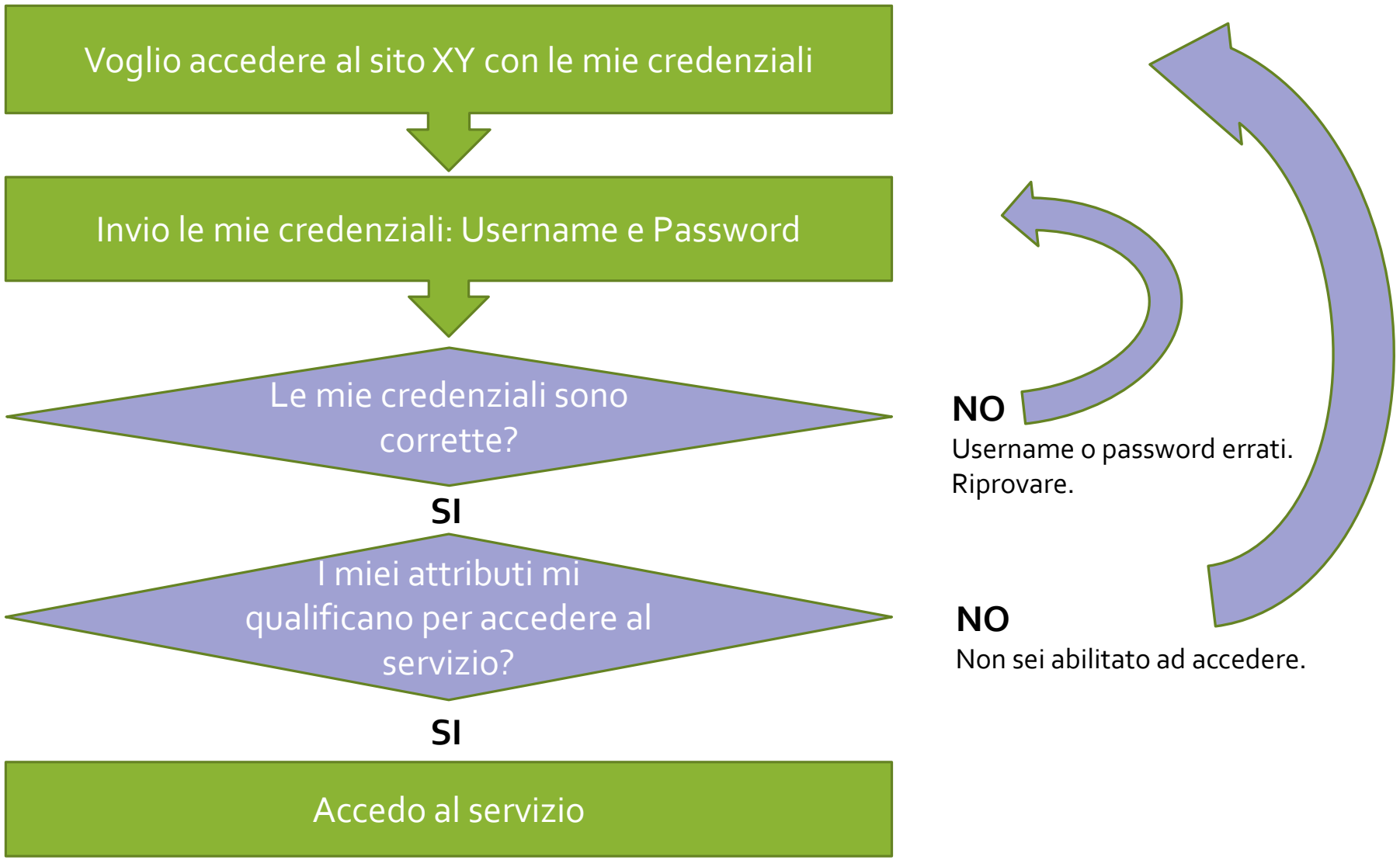
Identità Forte e Identità Debole

- In base alle modalità di rilascio dell'identità e ai livelli di autenticazione l'identità è definita Debole o Forte:
- **Identità Digitale Debole**: quando è associata a poche informazioni che identificano la persona. (Autocerficata – Username e password)
- **Identità Digitale Forte**: quando è associata a molte informazioni che identificano la persona. (Verificata di persona – Lettore di impronte digitali)

Autorizzazione

- L'**autorizzazione** è il *secondo meccanismo* che si attiva, una volta che la procedura di autenticazione è andata a buon fine.
  E' una verifica che viene svolta dal servizio al quale vogliamo accedere, in base alle informazioni che gli sono state fornite o che possiede.
  L'autorizzazione può non far accedere al servizio (non sei abilitato) oppure far accedere solo ad una parte del servizio.
- Es.
  - Accedo al Registro Elettronico, sono uno studente.
  - In base alla mia qualifica studente potrò accedere alla parte di sito dedicata agli studenti, ma non potrò accedere all'area riservata agli insegnanti.

In pratica


Voglio accedere al sito XY con le mie credenziali
Invio le mie credenziali: Username e Password
Le mie credenziali sono corrette?
NO
Username o password errati.
Riprovare.
SI
I miei attributi mi qualificano per accedere al servizio?
NO
Non sei abilitato ad accedere.
SI
Accedo al servizio

Autenticazione e Autorizzazione

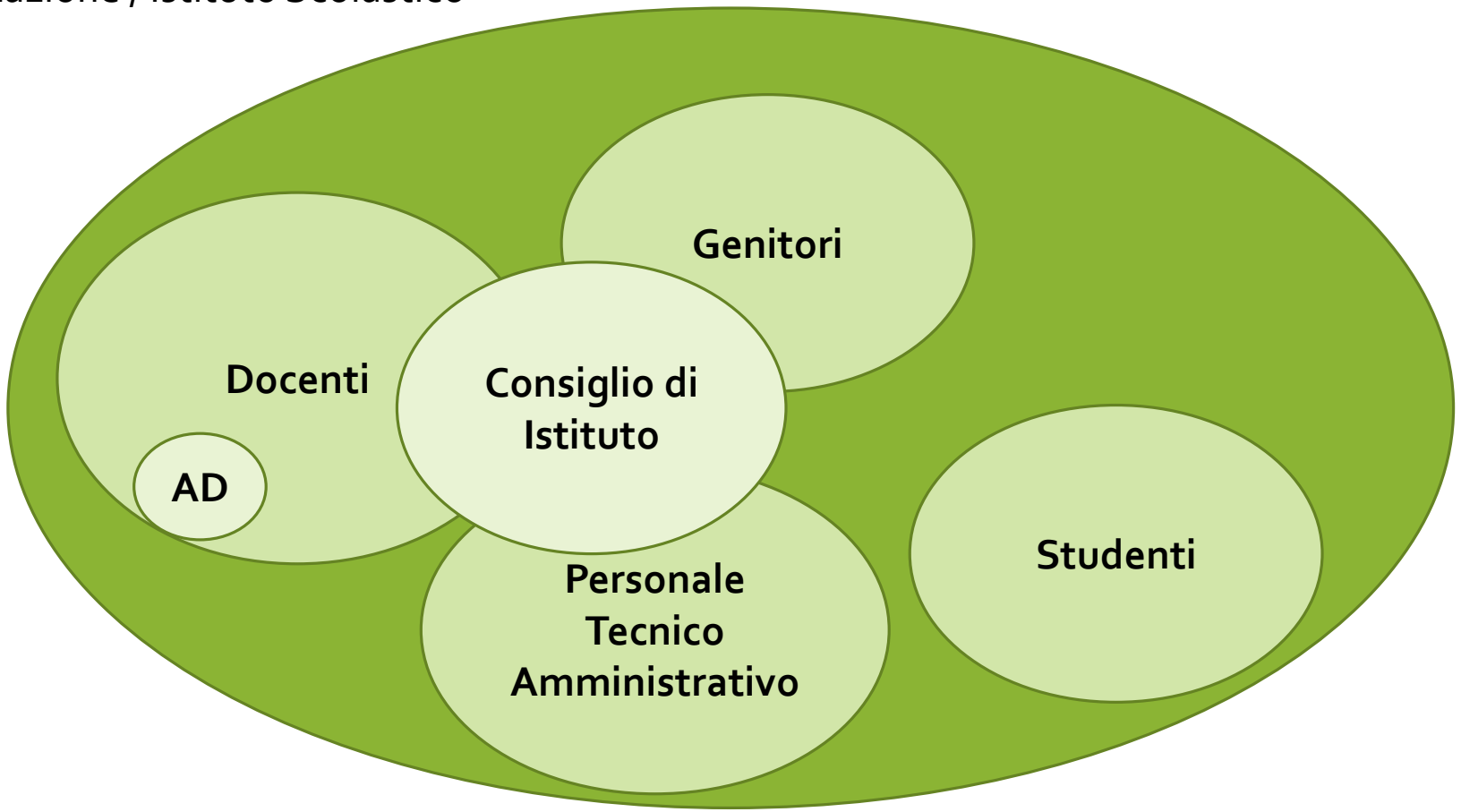
- Sono due processi diversi e distinti, eseguiti nella sequenza:
  1. Autenticazione
  2. Autorizzazione .
- Spesso fatti entrambi dallo stesso sistema/piattaforma/sito web, ma a volte no.

Chi gestisce l'identità?

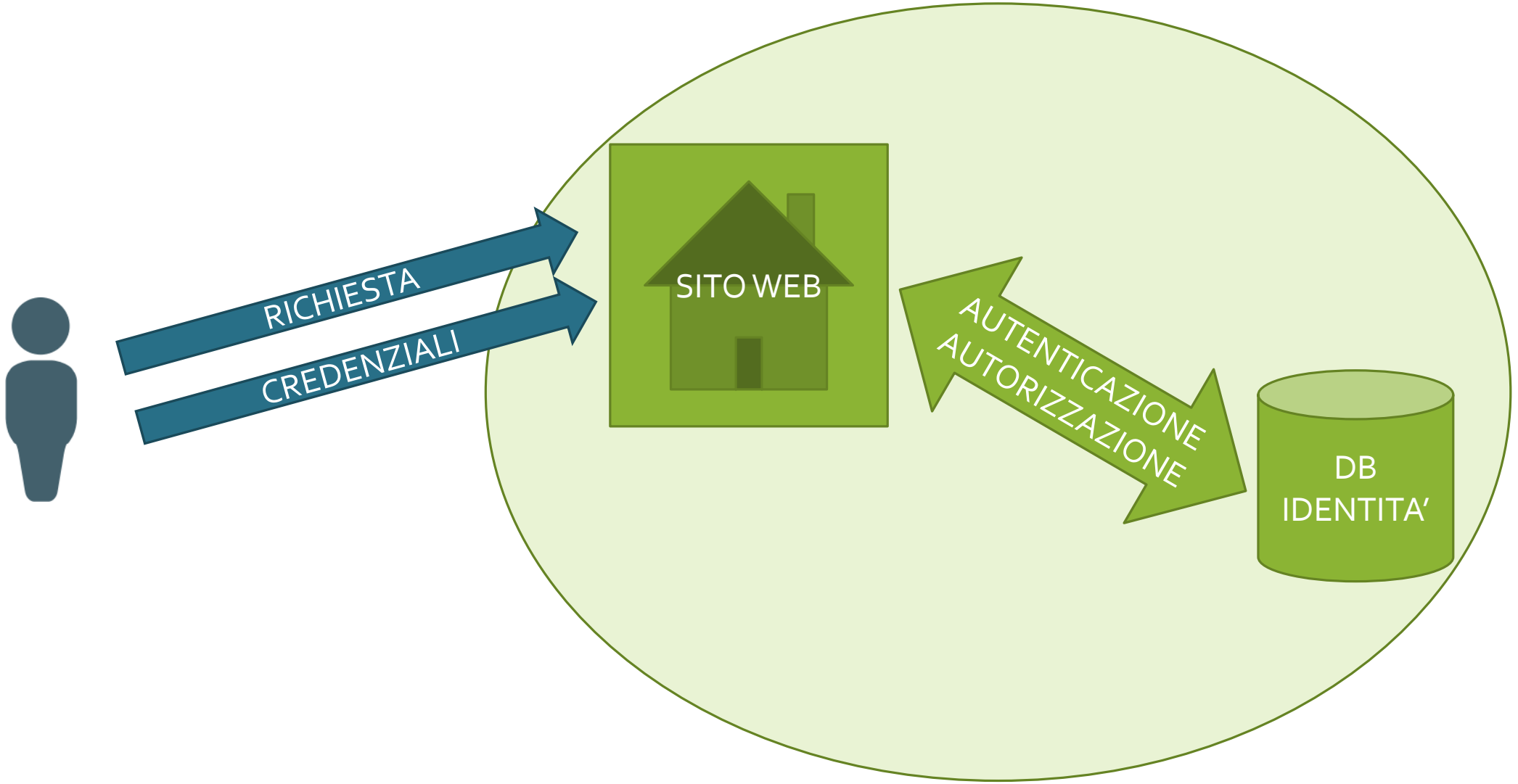
- Identità gestita personalmente
  - Registrazione a sito web, Facebook, Google, Apple (OpenID)
  - Di solito autocertificata
- Identità in contesti allargati – Identity Management
  - "L'Identity Management è un insieme di processi aziendali e un'infrastruttura di supporto per la creazione, la gestione e l'utilizzo di Identità Digitali"
    The Burton Group
  - In una organizzazione l'Identità Digitale può essere gestita in modo centralizzato, associando a quell'identità caratteristiche che ne permettono l'utilizzo qualificato.

Organizzare l'identità

Organizzazione / Istituto Scolastico



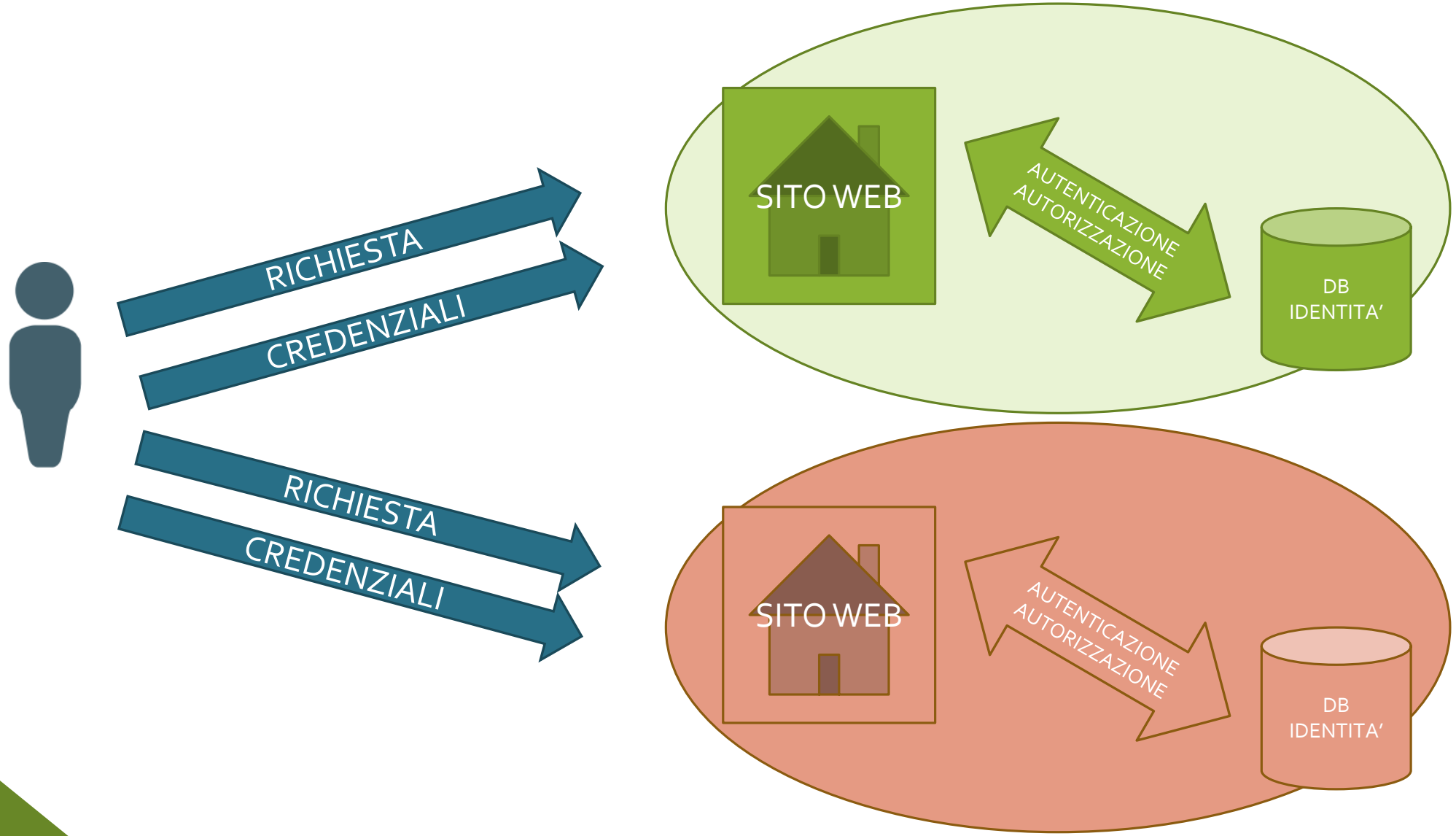
Come funziona? Un sito



Siamo ancora noi…

Da «Non ci resta che piangere» di e con Massimo Troisi e Roberto Benigni 1984 Fonte: Youtube

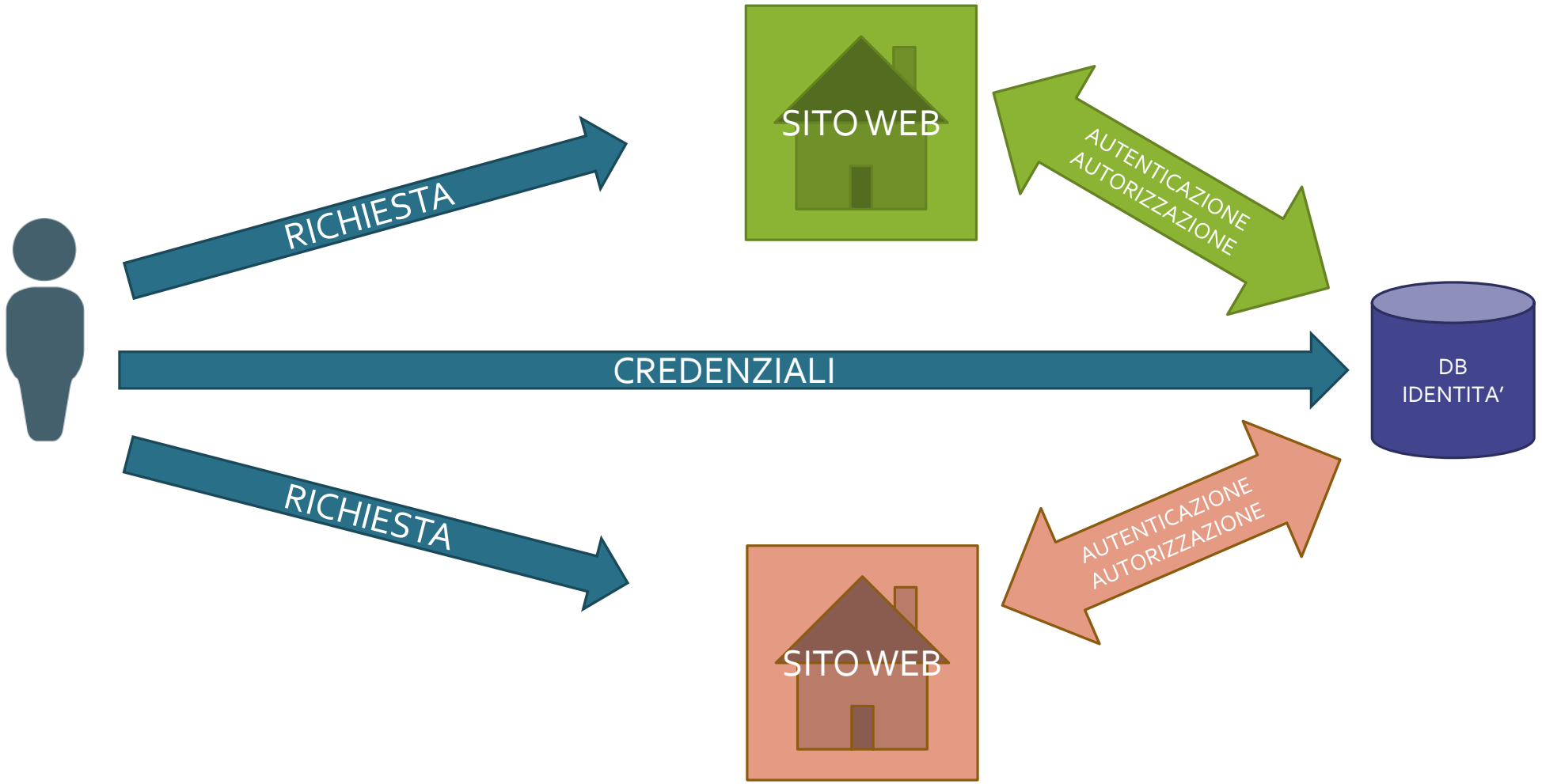
Come funziona? Due siti, tre siti, … un fiorino



Single Sign On (SSO)

- Quando nella mia organizzazione ho un'unica infrastruttura che gestisce la mia identità posso utilizzare
  un unico sistema
  che mi permette di utilizzare
  le stesse credenziali per accedere a più servizi.

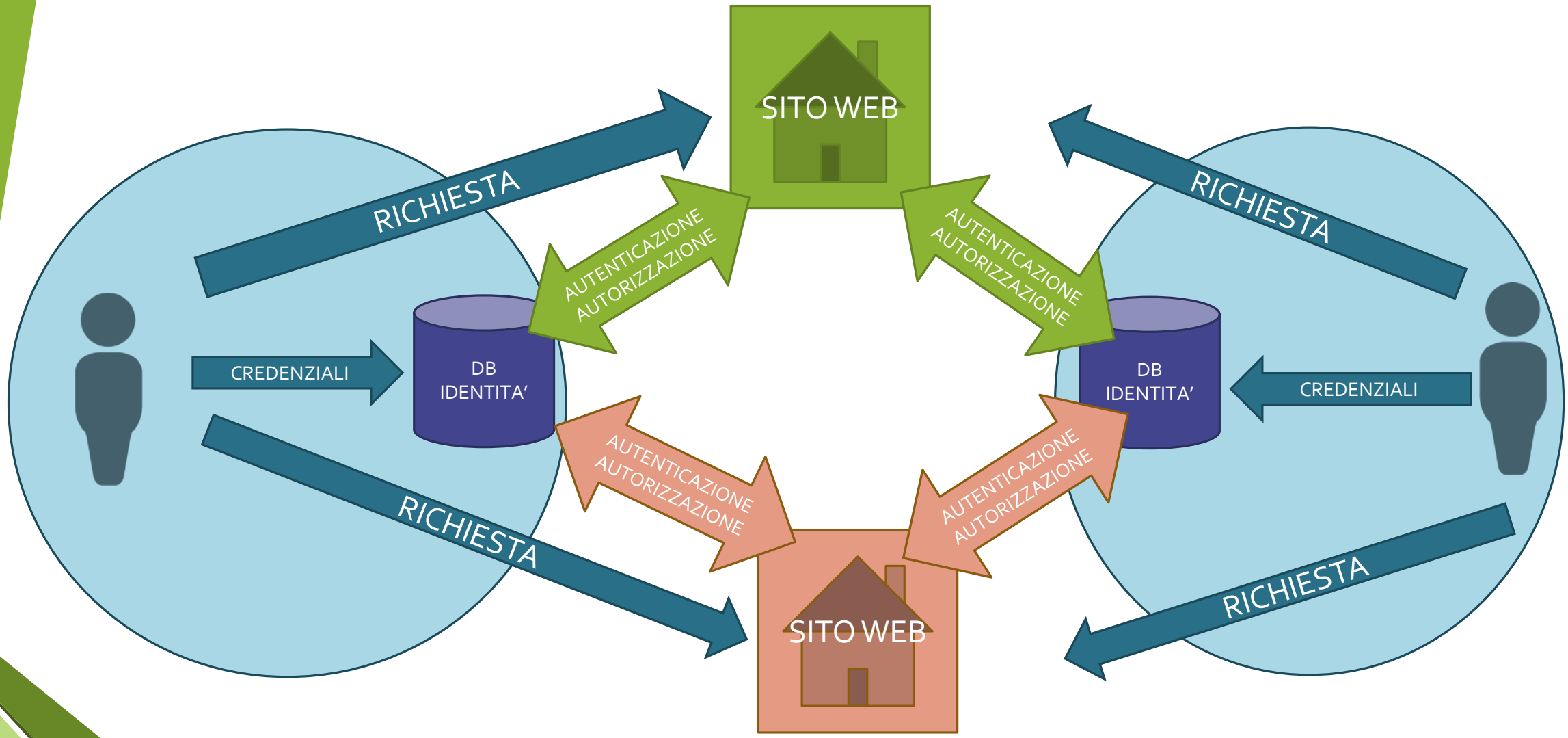
Come funziona?



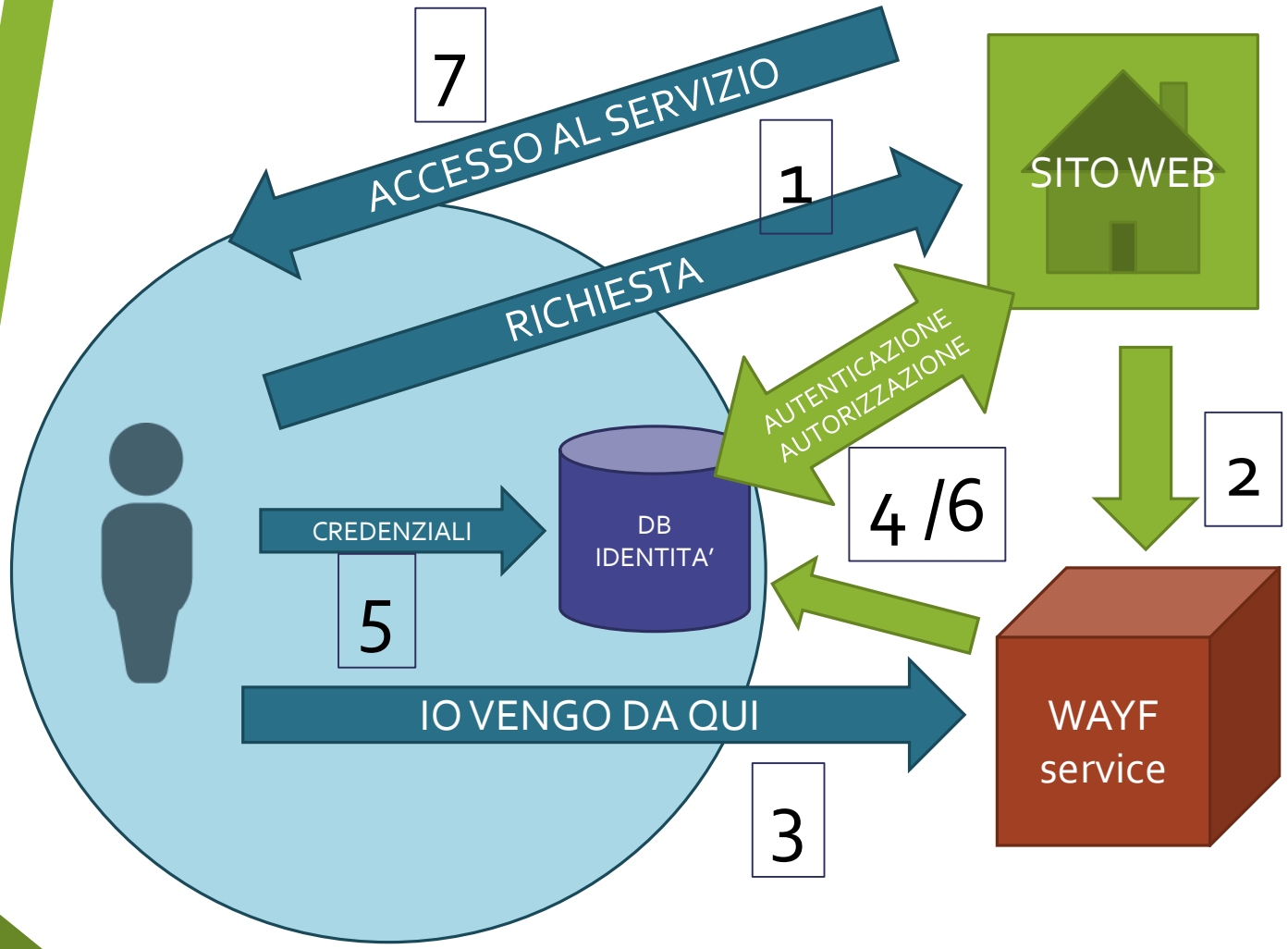
Quando l'identità digitale diventa federata?

- L'Identità Digitale diventa federata quando il meccanismo di Single Sing-On si estende fuori dalla propria organizzazione e si può accedere ad una molteplicità di servizi forniti da più organizzazioni usando sempre le stesse credenziali.

Come funziona?



Come funziona?



Where Are You From Service

I vantaggi dell'Identità Federata

- Per l'Utente:
  - Utilizza un unico sistema di credenziali per accedere a molteplici servizi.
  - Non deve dare a tutti le proprie credenziali (privacy) e ricordarle

- Per il gestore del sito web:
  - Non deve mantenere le credenziali di tutti gli utenti (privacy)
  - Può rendere più semplici le procedure di accesso al sistema.
  - Con la Federazione sa che può fidarsi di chi garantisce l'Identità.

I ruoli nell'Identità Digitale Federata

- Identity provider
- Service provider
- La Federazione

Gestore dell'Identità – IDentity Provider - IDP

- Il gestore dell'Identità, Identity Provider o IDP, mantiene le credenziali dell'utente, gestisce il meccanismo di autenticazione e fornisce le informazioni che caratterizzano l'utente (attributi) verso l'SP.

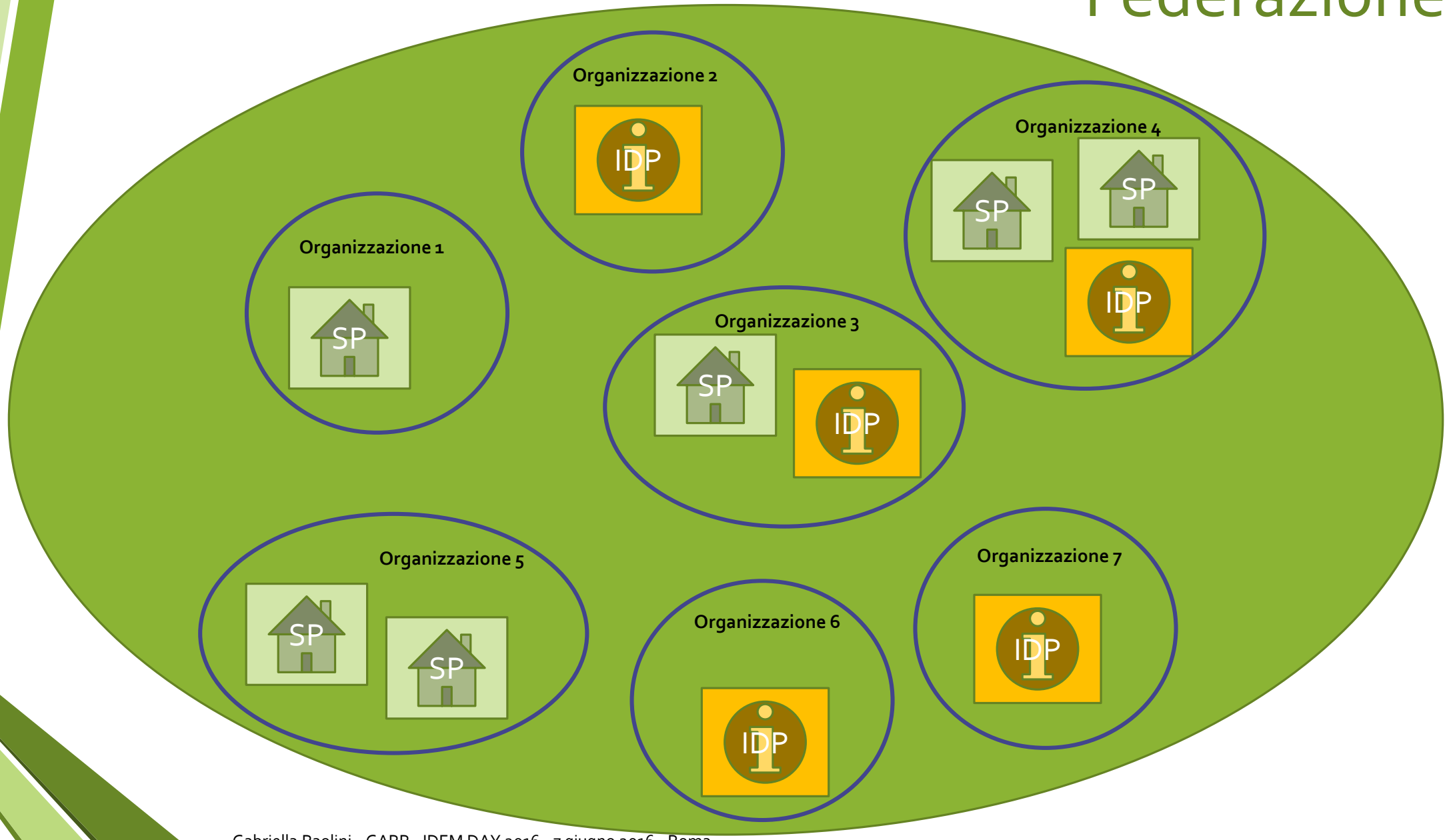
Gestore del Servizio – Service Provider - SP

- Il gestore del servizio, Service Provider o SP, apprende le informazioni di autenticazione e gli attributi relativi all'utente dall'IDP e li passa all'applicazione (di solito un server web) che risponde all'utente con quanto richiesto in base agli attributi presentati.

La Federazione

- La Federazione è un gruppo di organizzazioni che decidono di collaborare per condividere le proprie informazioni in un rapporto di fiducia reciproca. Ogni organizzazione può avere un IDP e/o uno o più SP.
- I partecipanti alla federazione condividono:
  - Accordi tecnici (protocolli, schemi di attributi, sistemi di AAI,…)
  - Accordi amministrativi basati sulla reciproca fiducia.

Federazione



I vantaggi per la sicurezza e la privacy

- Le credenziali dell'utente sono al sicuro
  - Soltanto l'IDP mantiene le credenziali dell'utente e soltanto l'IDP gestisce l'autenticazione dell'utente.
- Le informazioni sull'Identità dell'utente
  - L'IDP fornisce all'SP solo la parte necessaria di informazioni sull'utente. In questo modo l'IDP fornisce ad ogni SP gli attributi essenziali e specifici in base alla richiesta.

La Federazione IDEM

- IDEM è la Federazione Italiana delle Università e degli Enti di Ricerca per l'Autenticazione e l'Autorizzazione. Gli obiettivi di IDEM sono quelli di creare e supportare un framework, comune agli enti di formazione e di ricerca italiani, per la gestione condivisa degli accessi alle risorse on-line.
- Per raggiungere questi obiettivi IDEM favorisce lo sviluppo di una **comunità basata sulla fiducia reciproca**, cosi da facilitare i partecipanti a prendere decisioni appropriate, per il controllo degli accessi, sulla base delle informazioni fornite dai partecipanti stessi.
- IDEM per il sistema federato è aperta all'utilizzo di ogni framework basato sullo standard SAML. Poiché la maggior parte dei partecipanti utilizza Shibboleth è necessario che ogni nuovo servizio, per poter interoperare nella federazione, sia **conforme a SAML2 e interoperabile con Shibboleth**.

dal sito http://www.idem.garr.it

Grazie!

gabriella.paolini@garr.it

Le immagini usate nella presentazione sono state selezionate dal sito https://openclipart.org

http://www.garr.it