CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

# SPC-interoperabilità, cooperazione applicativa e sicurezza: la gestione delle Identità Federate

Francesco Tortorelli

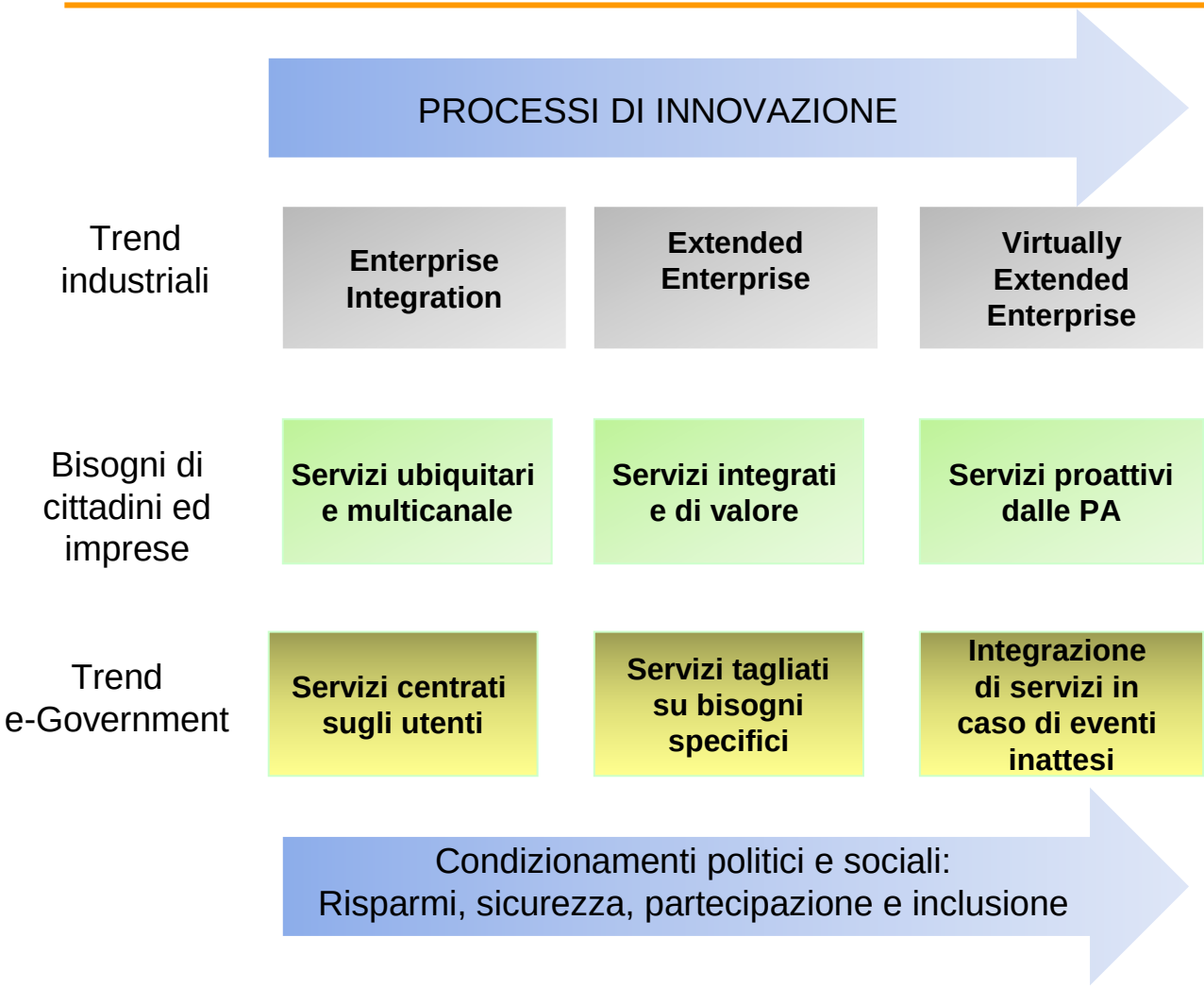
*Roma, 27 maggio 2008*

# AGENDA

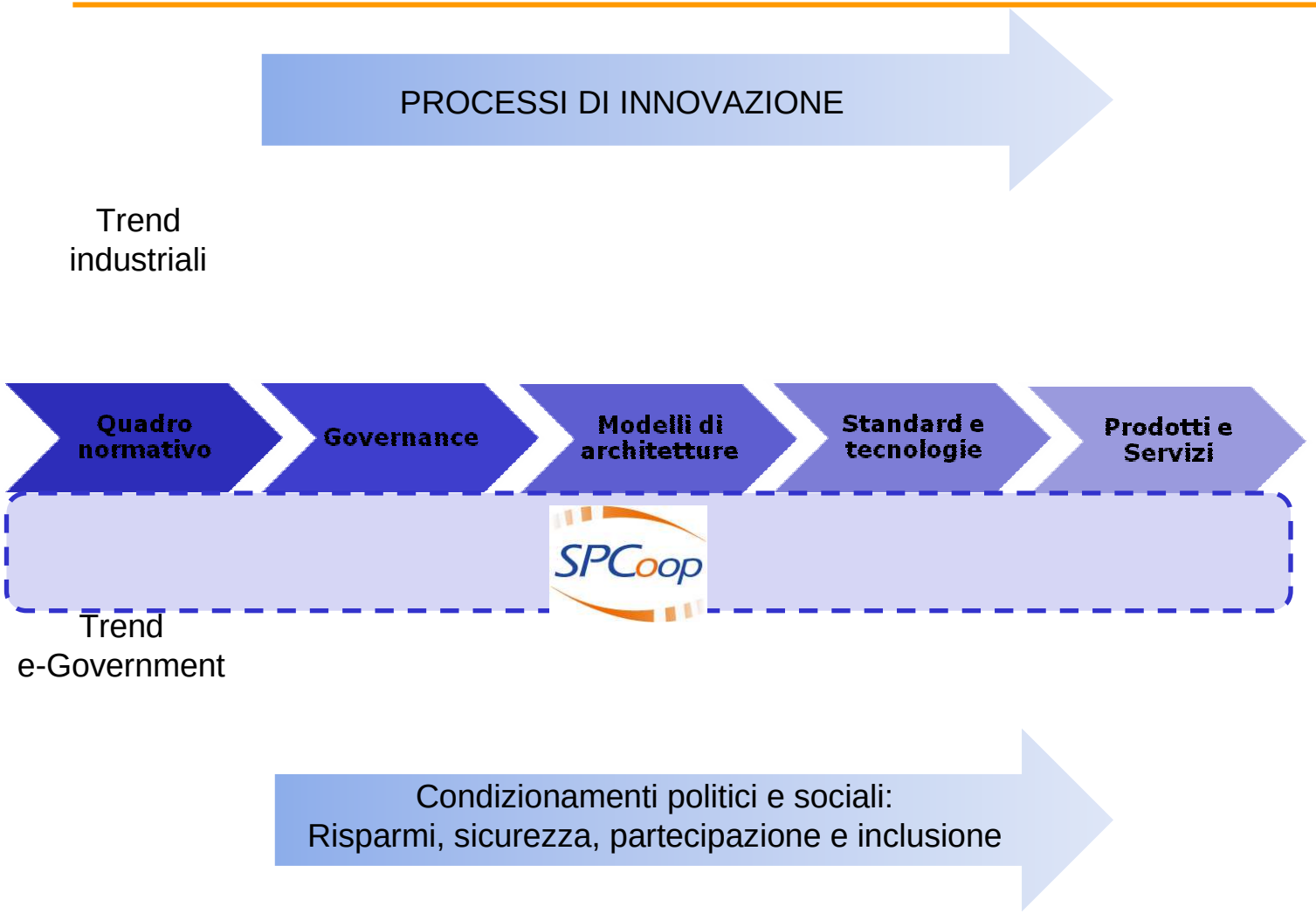
Contenuti della presentazione:

- e-Government trends
- le componenti di sicurezza indirizzate da SPC per l'interoperabilità e la cooperazione applicativa;
- Il modello di gestione (federata) delle identità digitali nell'ambito di SPC (scenari di interoperabilità e cooperazione applicativa)
- Infrastrutture  a supporto a livello nazionale
- modalità di partecipazione per le amministrazioni  e requisiti organizzativi, procedurali e tecnologici

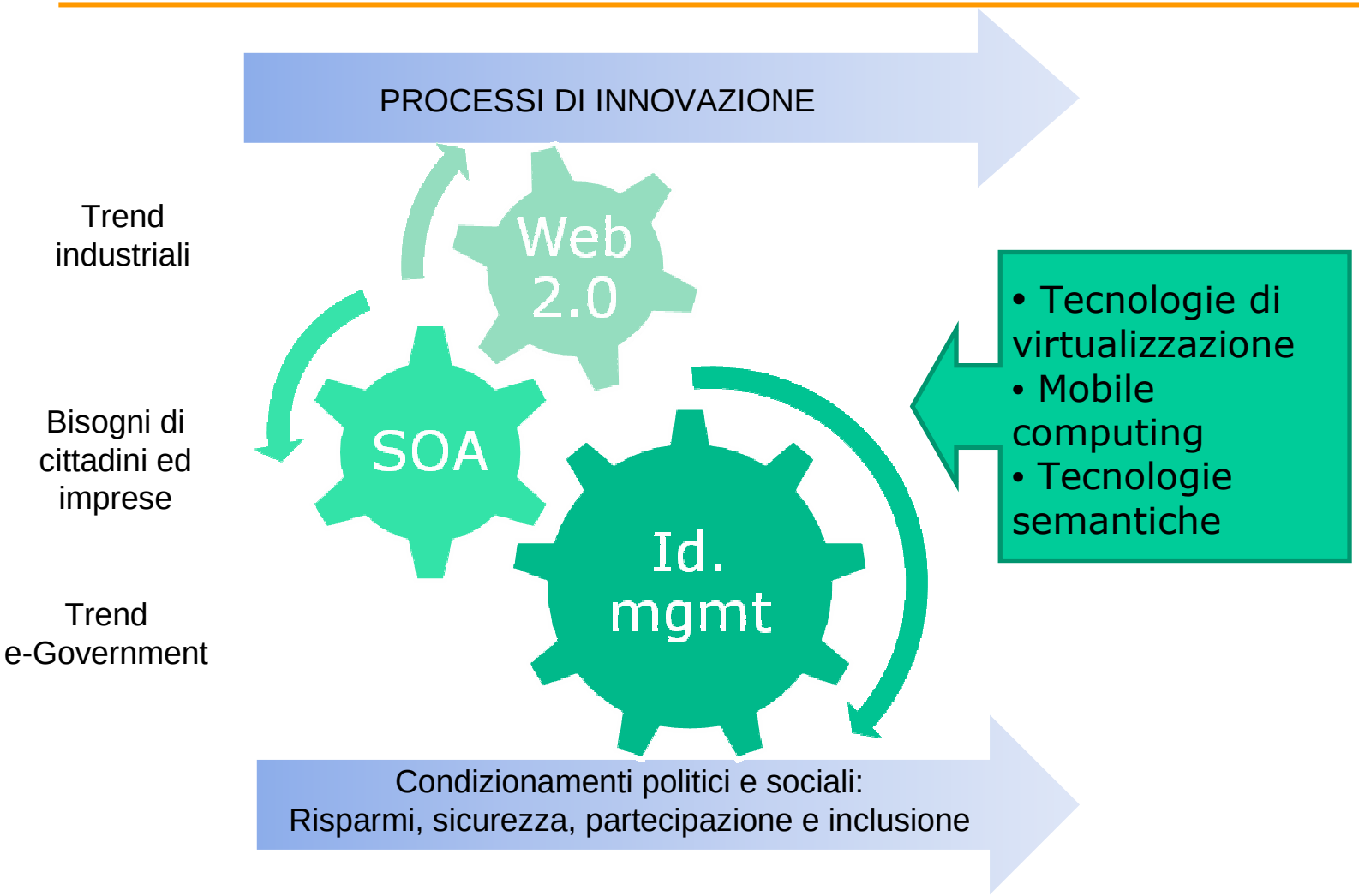
# Government & Industry trend



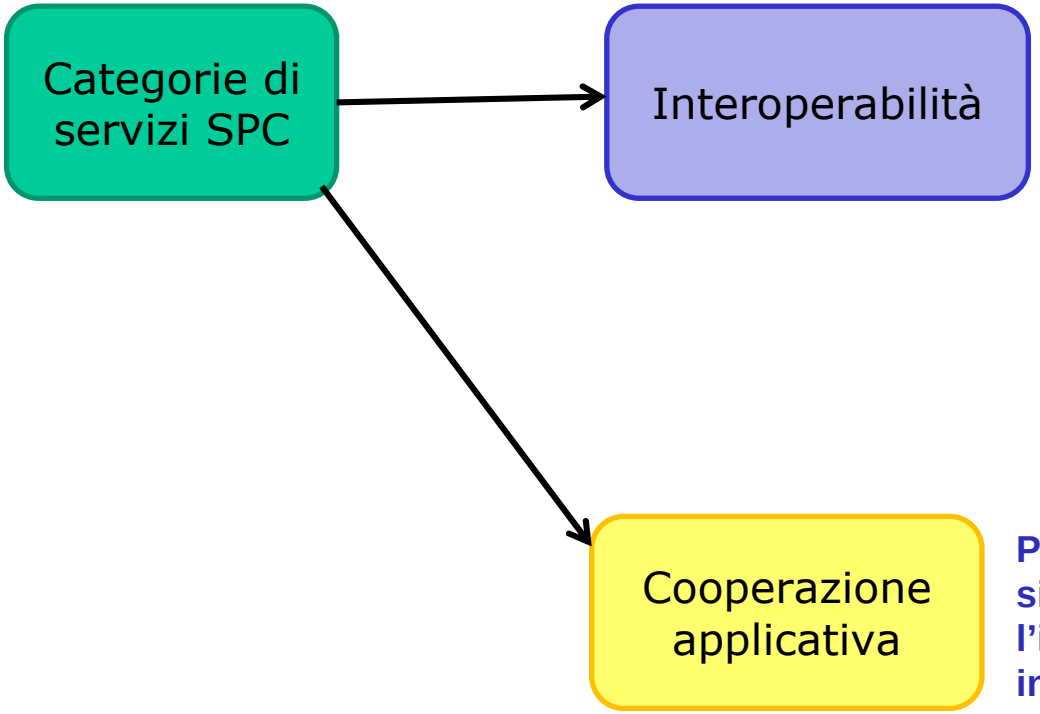
# Government & Industry trend



# Government & Industry trend



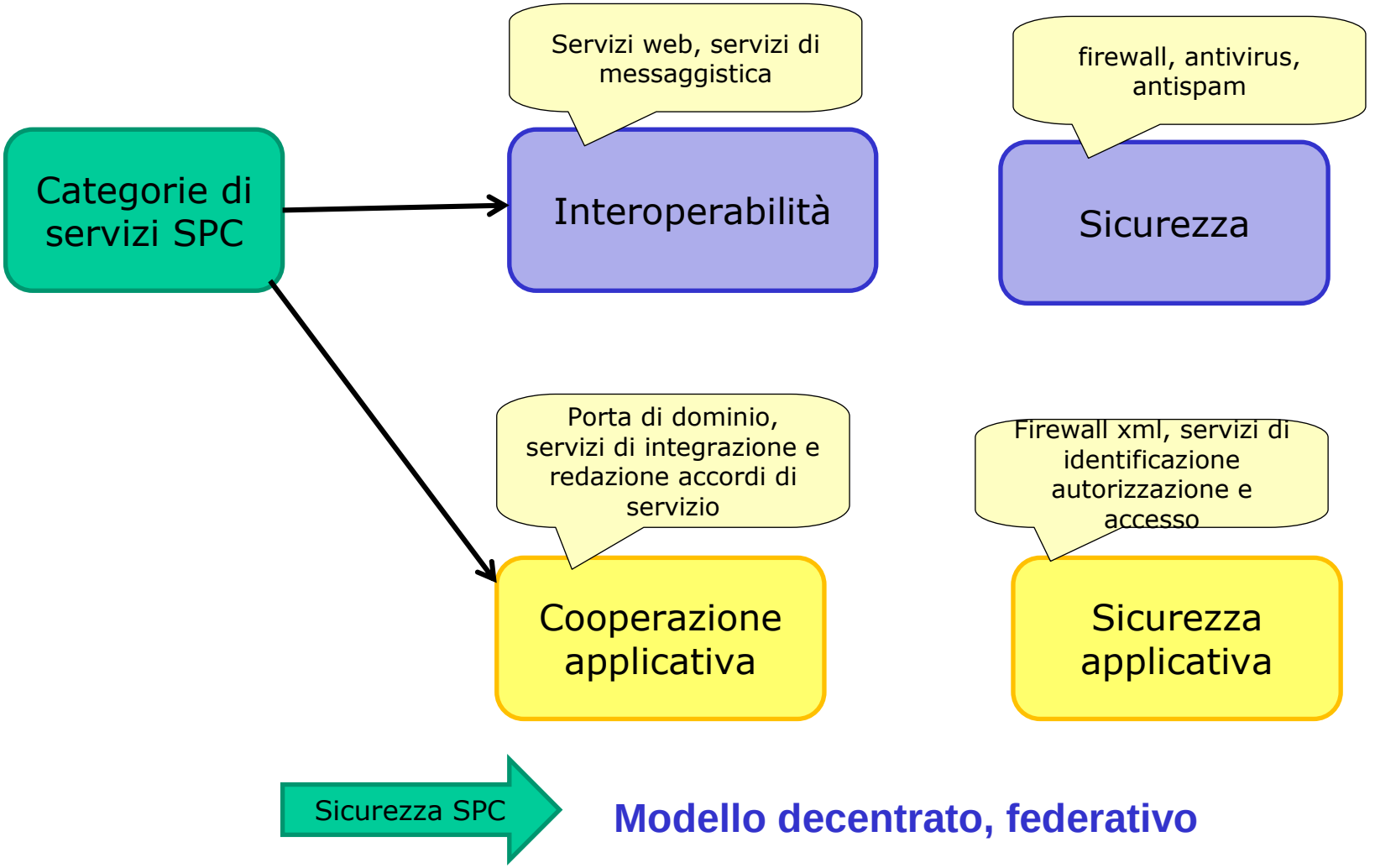
# I servizi di sicurezza SPC per interoperabilità e cooperazione



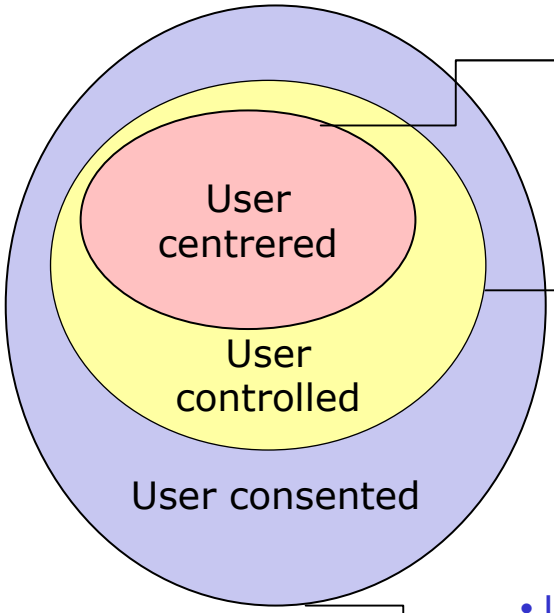

**servizi idonei a favorire la circolazione, lo scambio di dati e informazioni tra le amministrazioni e con i cittadini.**

**Parte di SPC finalizzata all'interazione fra sistemi informatici delle PA, per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti**

# I servizi di sicurezza SPC per interoperabilità e cooperazione



# Modelli di gestione delle identità digitali




- Identità viene fornita dall'utente
- Elevata interattività

- Utilizzo dell'identità sotto Il controllo dell'utente
- Possibili scenari di interattività
- Identity agent

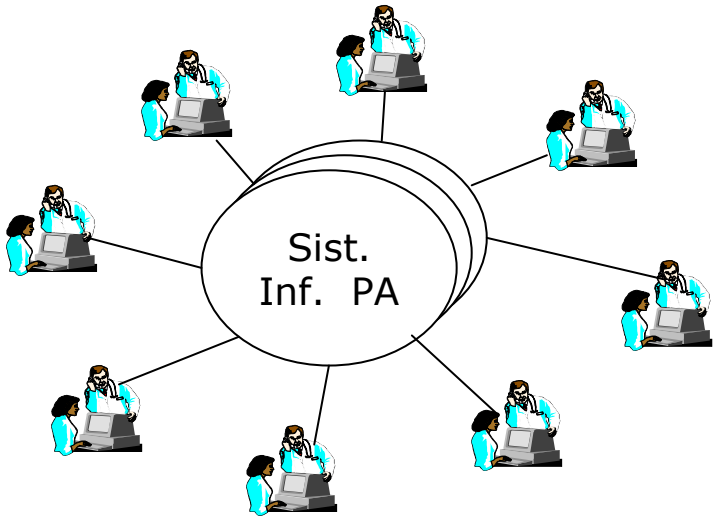
- Utilizzo dell'identità controllata da "Authorities" alle quali l'utente ha fornito delega in virtù di un "contratto"
- Interattività non prevista

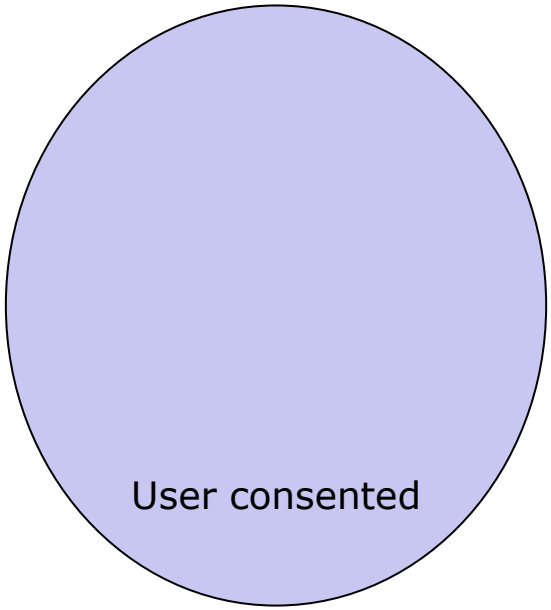
**Internet, web 2.0 like & more**

**Corporate, intranet**

# Modelli di gestione delle identità digitali /2

**Domain centric identity**

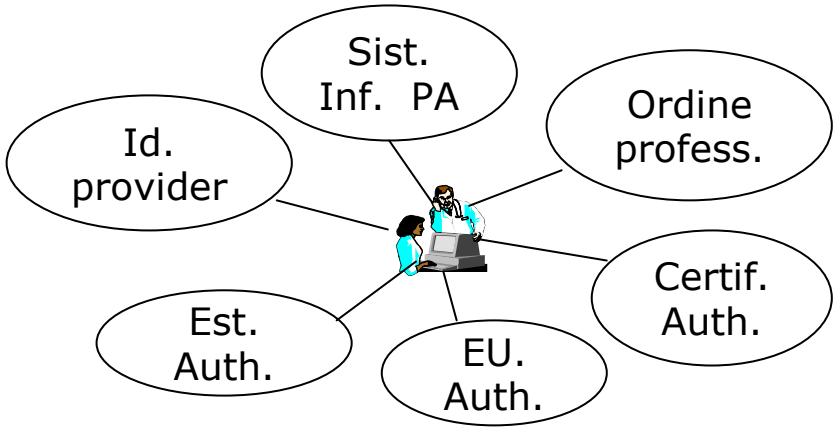


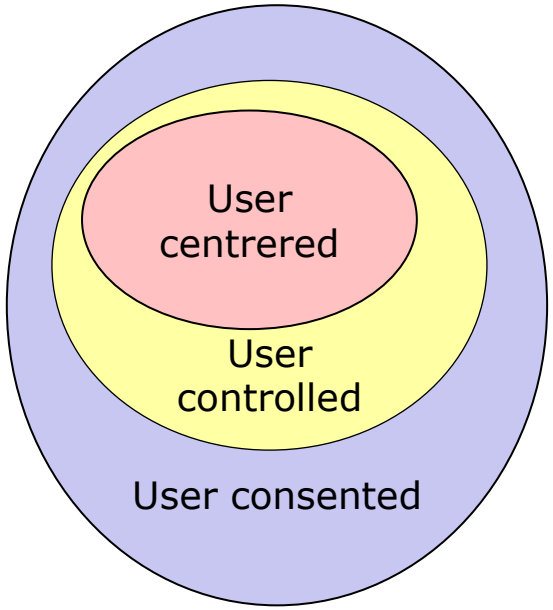




- **Responsabilità dell'amministrazione**
- **No interoperabilità con altre PA**
- **Scarsa automazione**
- **Bassa scalabilità**

# Modelli di gestione delle identità digitali /3

**Federated identity**




- **Responsabilità ripartita**
- **Interoperabilità con altre PA**
- **Scalabile**
- **Adatto a processi automatizzabili**

# Alcuni concetti di base

CAD

**autenticazione informatica**: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, …

DECRETO REGOLE TECNICHE SPC

**autorità di autenticazione**: la struttura che consente l'autenticazione in rete di un soggetto o di un sistema informatico o di un servizio

**L'autenticazione in ambito SPC viene effettuata sotto la responsabilità dell'ente che eroga un servizio sulla base di un insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto**

**autorità di identificazione**: la struttura che consente l'identificazione di un soggetto attraverso le modalità previste dall'art. 66 del Codice;

**autorizzazione**: l'insieme di attività che consentono l'accesso ad un servizio o una risorsa a chi, preventivamente identificato o autenticato, possiede gli attributi o il ruolo necessario;

**autorità di attributo e ruolo**: la struttura che ha la potestà di attestare attributi e ruoli ai fini dell'erogazione di un servizio;

# DPCM Regole tecniche: principi generali

## Economicità nell'utilizzo dei servizi di rete, di interoperabilità e di supporto alla cooperazione applicativa

Gli Organismi di attuazione e controllo, secondo gli indirizzi e le indicazioni della Commissione e nel rispetto delle presenti Regole tecniche, **progettano e realizzano, anche attraverso la stipula dei contratti quadro** di cui all'art. 83 del Codice, gli interventi che facilitino e sostengano lo sviluppo di servizi di rete, di interoperabilità e di cooperazione applicativa tra le Amministrazioni che utilizzano il SPC . **A tal fine, attuano misure che favoriscano, in particolare:**

**l'accesso ai servizi attraverso sistemi di autenticazione distribuiti e federati, al fine di gestire con maggiore efficienza identità digitali e ruoli attribuiti e certificati dalle autorità di autenticazione e dalle autorità di attributo e ruolo**;

# DPCM R. tec.: gestione delle identità digitali

1. **Nell'ambito del SPC l'autorizzazione all'accesso ai servizi si basa sul riconoscimento delle identità digitali delle persone fisiche e dei sistemi informatici utilizzati per l'erogazione dei servizi medesimi**. L'autorizzazione ricade sotto la responsabilità **dell'ente erogatore e può avvalersi di meccanismi di mutuo riconoscimento nell'ambito di sistemi federati di gestione delle identità digitali**, secondo criteri e modalità stabiliti dalla Commissione.

2. **I servizi disponibili in SPC** possono operare secondo diversi livelli di gestione delle identità digitali:
   - **servizi che non richiedono alcuna identificazione o autenticazione;**
   - **servizi che richiedono l'autenticazione in rete da parte di un'autorità di autenticazione;**
   - **servizi che richiedono, per le persone fisiche, l'identificazione in rete da parte di un'autorità di identificazione;**
   - **servizi che richiedono per gli utenti, oltre all'identificazione, l'attestazione di attributi e/o ruoli, che ne qualifichino ulteriormente le funzioni e/o i poteri.**

# Le funzioni di “sicurezza” dei servizi Infrastrutturali di CA

Amministrazione

Delegato
x i registri

Registro

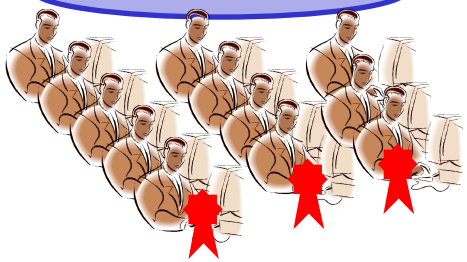
(ora IndicePA)

Acc
di
ser
v.

Indice dei
soggetti

(ora RubricaPA)

Strutture org, caselle PEC, Servizi telematici,
sito istituzionale, Acc. di servizio Porte di Dominio,



**Modelli di architetture**

**Standard e tecnologie**

**Prodotti e Servizi**

?

**GFID**

# Le funzioni dei Servizi Infrastrutturali di CA /2

**5) Gestione federata delle identità digitali** di quel cosiddetto “circle of trust” attraverso:

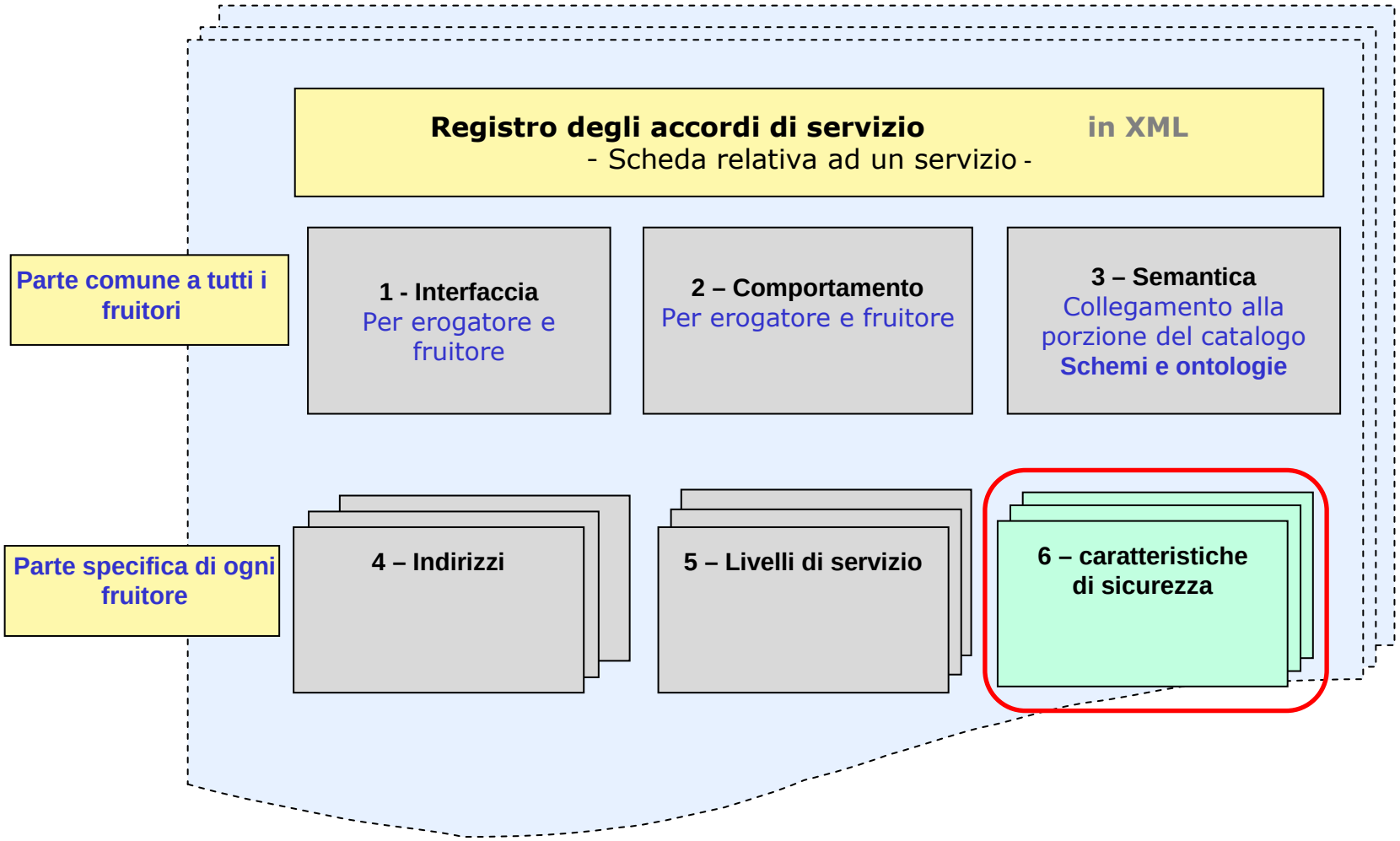
• l’accreditamento e la validazione all’interno del dominio federativo;

• la pubblicazione degli enti che ricoprono il ruolo di certificatori/validatori delle identità digitali e dei ruoli;

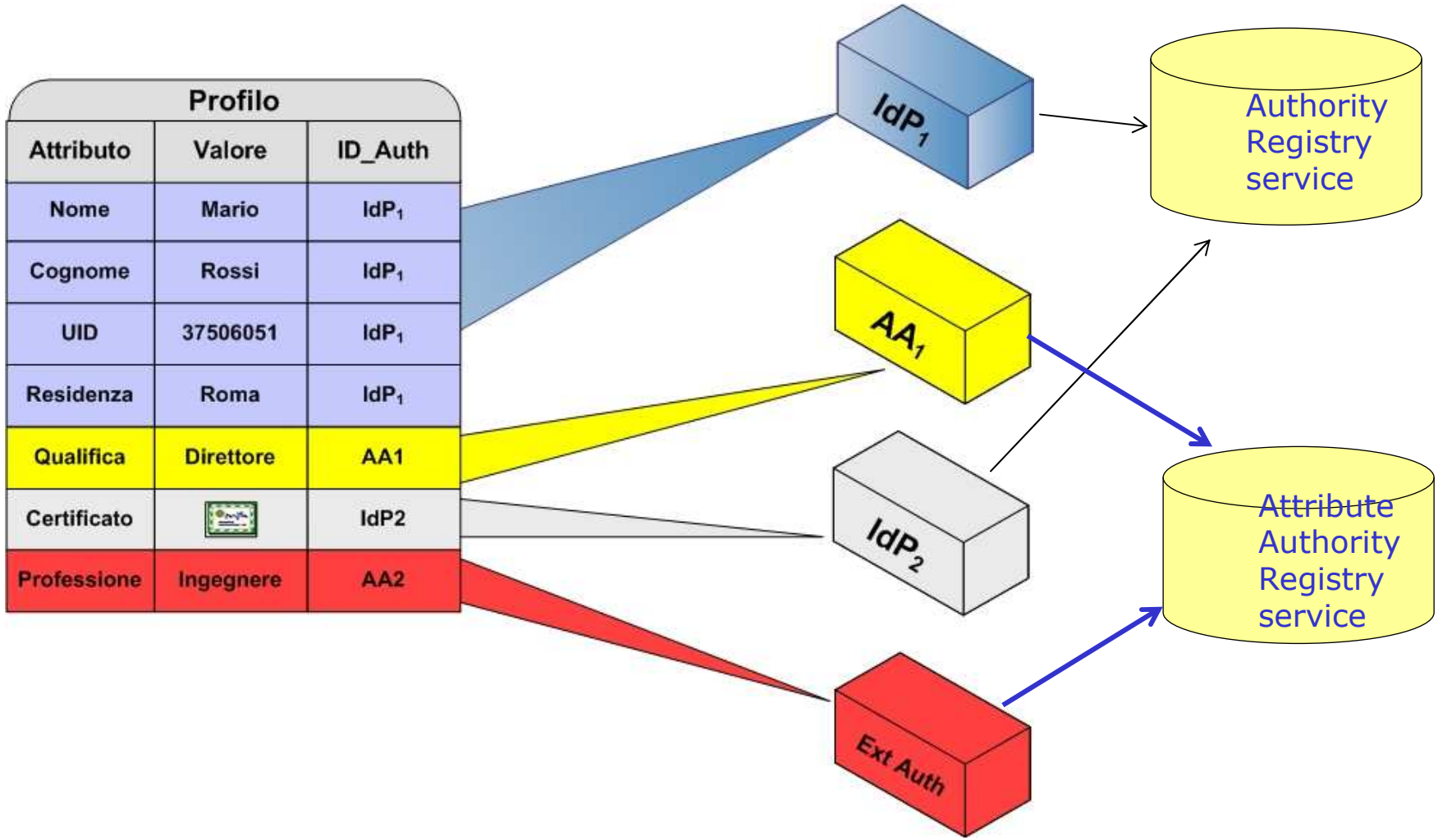
• la definizione di un insieme di accordi (policy) che comprendono un modello comune di cooperazione all’interno della federazione;

• la definizione delle responsabilità nell’ambito della cooperazione, utilizzando gli accordi di servizio.

# La struttura degli accordi di servizio

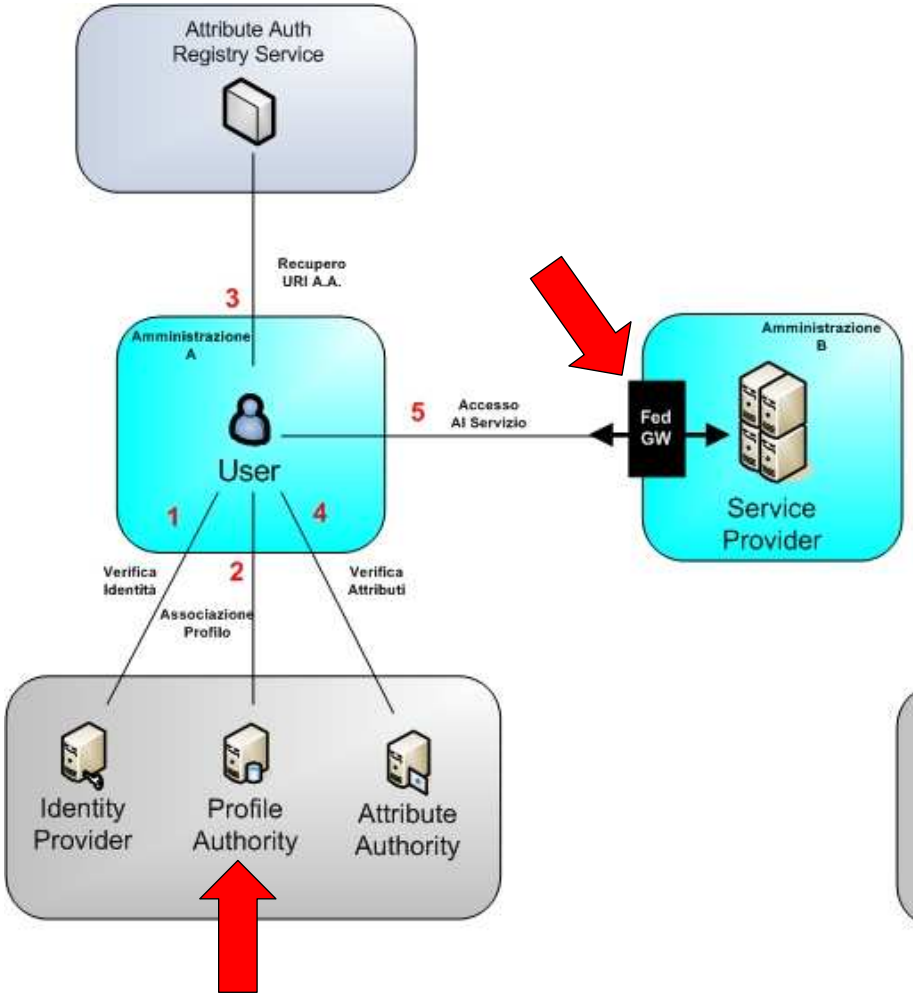


# Il modello di Gestione Federata delle Identità Digitali SPCoop

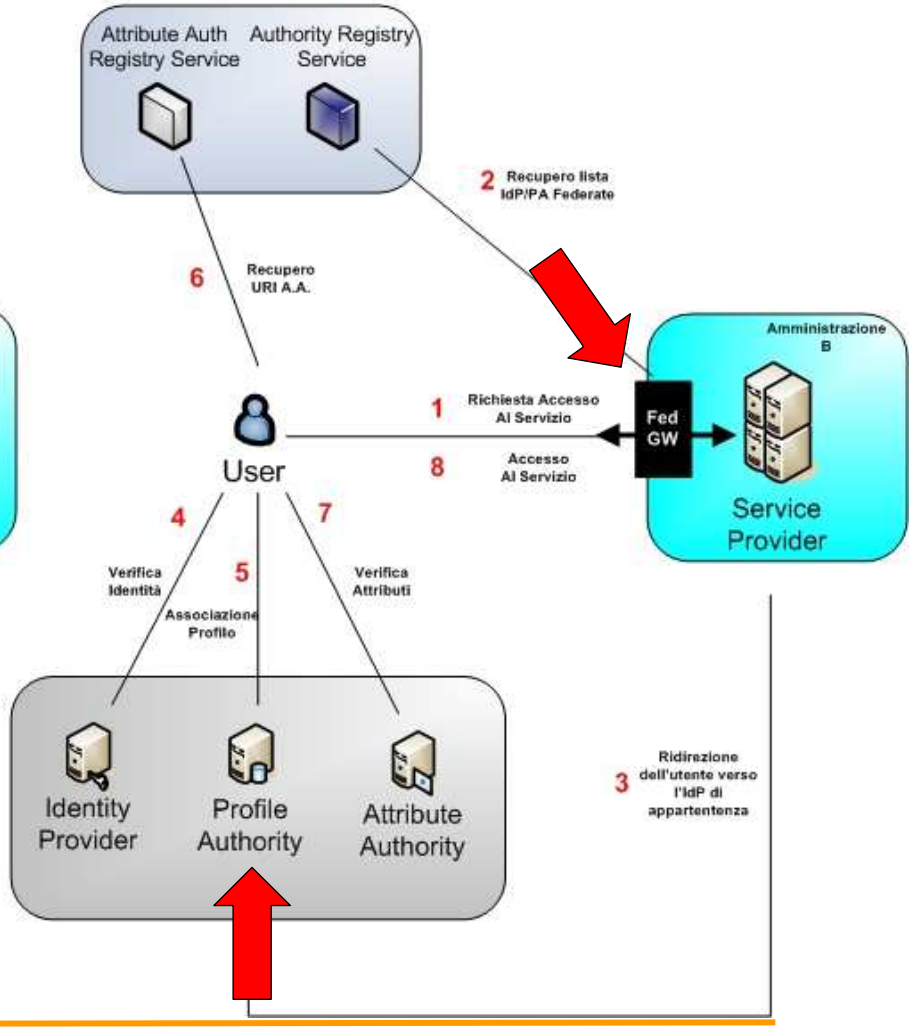


# Il modello di Gestione Federata delle Identità Digitali SPCoop /2

**Utente interno ad un'amministrazione**

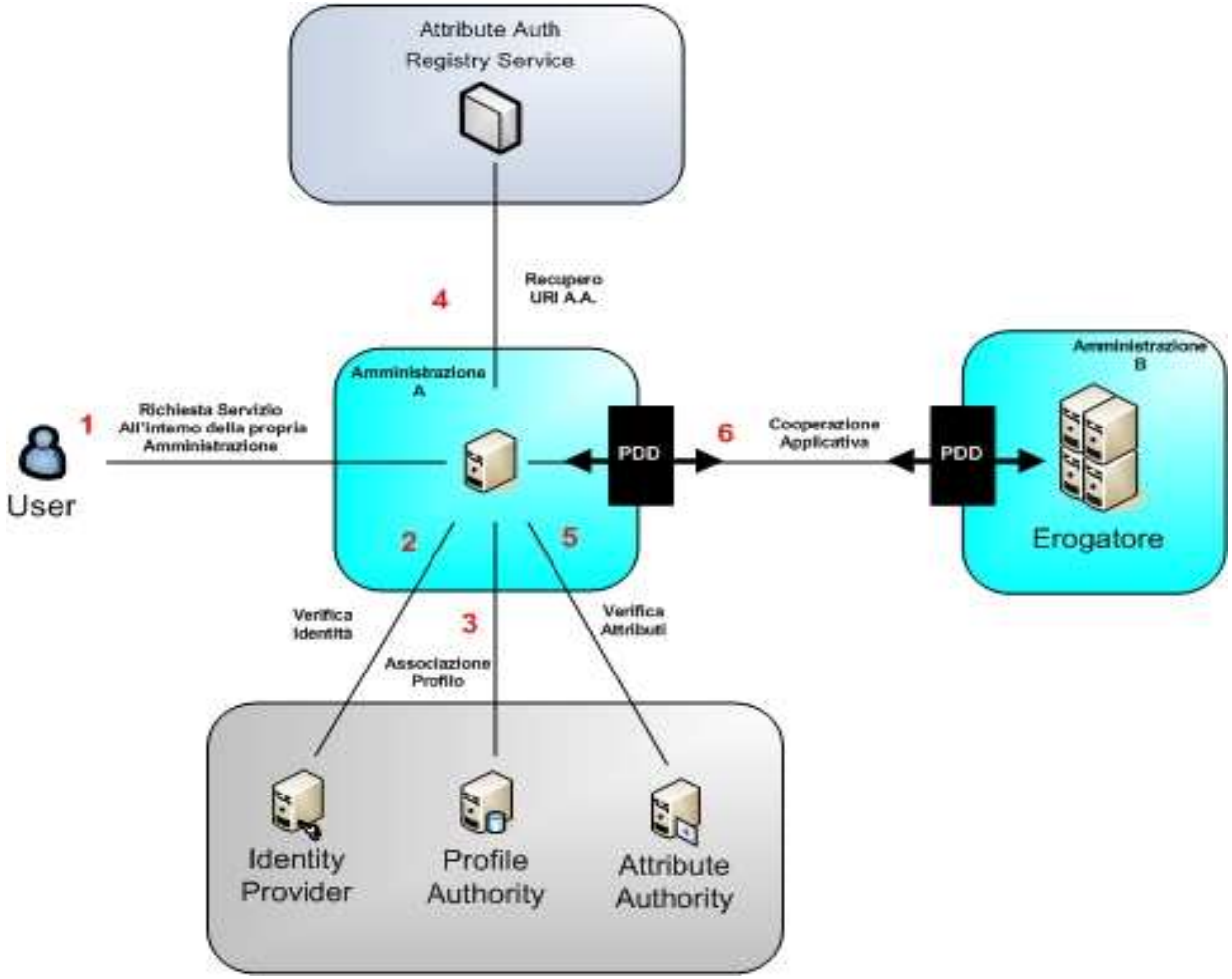



**Utilizzo Applicazione Federata via Web**

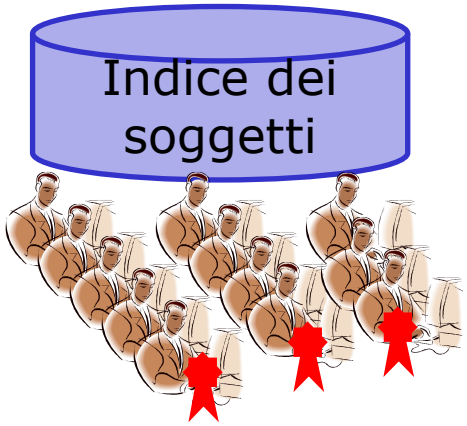


# Il modello di Gestione Federata delle Identità Digitali SPCoop /2

**Utilizzo Applicazione in cooperazione applicativa**

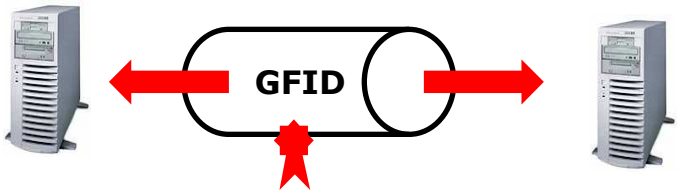


# modalità di partecipazione per le amministrazioni e requisiti organizzativi, procedurali e tecnologici




Due categorie di servizi infrastrutturali x:

- Sussidiarietà
- Utilizzo authorities terze
- Utilizzo PA come authorities




Identity providers
Attribute autorities
Modelli per federarsi
Sono possibili: scenari:Web e di cooperazione applicativa

# modalità di partecipazione per le amministrazioni e requisiti organizzativi, procedurali e tecnologici /2

- utilizzo dell'indice dei soggetti (opz.)
- utilizzo di un IDP federato
- federarsi come ALD
- accettazione del modello di interscambio (profili di collaborazione)
- definizione dei propri ruoli (opz.)
- utilizzo di ruoli esterni federati
- utilizzo servizi (web service) definendo negli accordi di servizio il profilo di collaborazione per la cooperazione applicativa
- utilizzo delle "primitive", messe a disposizione dal modello, per lo scambio di asserzioni

# Grazie !