THE ITALIAN RESEARCH & EDUCATION NETWORK | Consortium GARR

Identità digitali e servizi federati: SPID-IDEM quali opportunità?

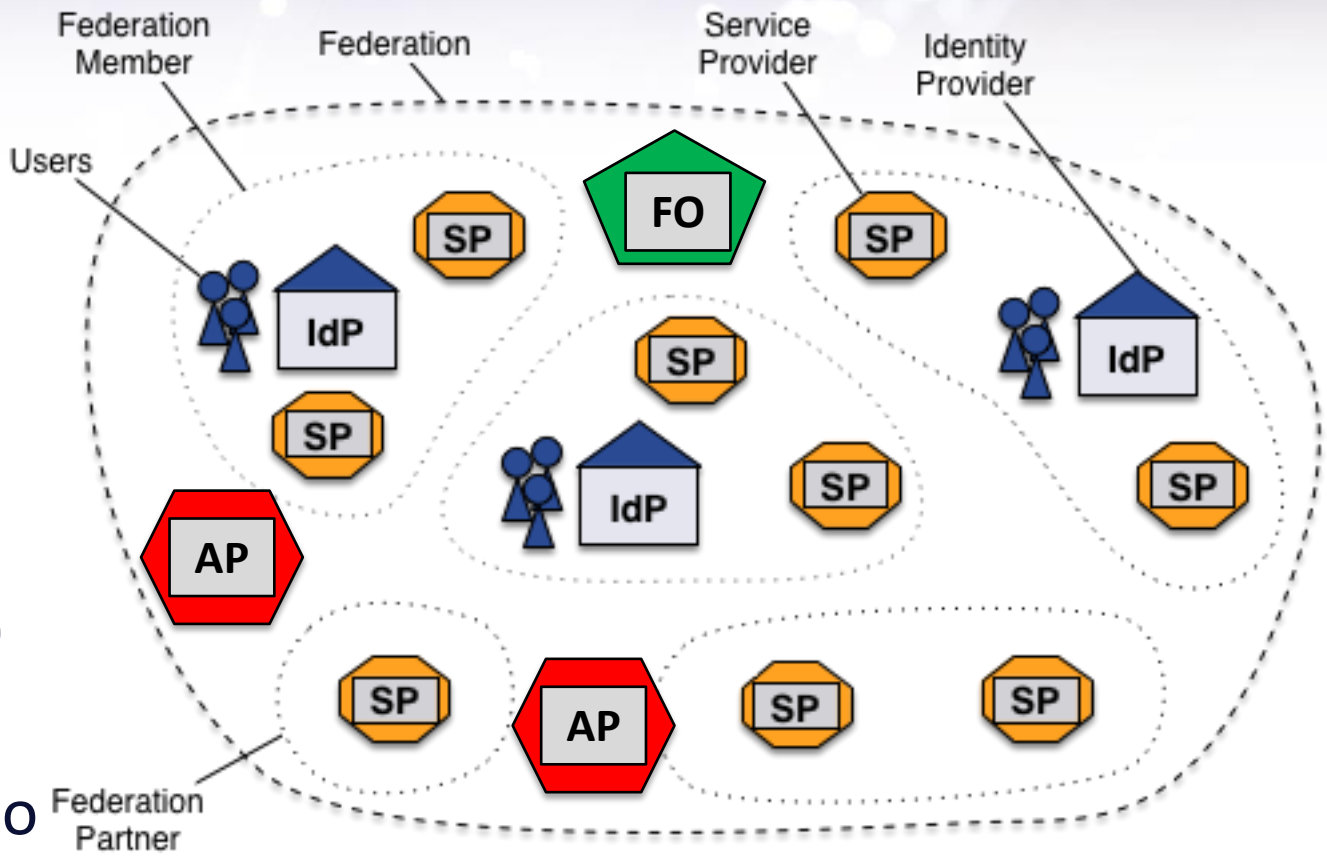
La federazione IDEM e le proposte di integrazione con SPID

Maria Laura Mantovani (GARR)

WS GARR 2016 | Roma, 18.04.2016

SPID e IDEM: Federazioni di Identità tipo Mesh

- Gestori dell'identità digitale (IdP)
- Fornitori di servizi (SP)
- Gestori di attributi qualificati (AP)
- 1 Autorità di accreditamento e vigilanza (FO)



SPID e IDEM: framework

Autorità di Accreditamento:	SPID/Agenzia per l'Italia Digitale	IDEM/GARR The Italian Academic and Research Network
IdP, SP, AP:	insieme aperto di soggetti pubblici e privati	insieme circoscritto di soggetti pubblici e privati del settore Research and Education (R&E)
Cosa fanno gli IdP:	gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni.	gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi della community R&E (studenti, ex-studenti, docenti, ricercatori, dipendenti o affiliati).
Regole:	• DPCM 24.10. 2014, GU n. 285 del 9.12.2014 • Regolamento SPID: regole tecniche • Regolamento SPID: modalità attuative • Regolamento SPID: accreditamento gestori • Regolamento SPID: utilizzo identità pregresse • Modello Convenzione SPID tra AgID e Identity Provider/Pubbliche amministrazioni	• IDEM: Regolamento • IDEM: Norme di Partecipazione • IDEM: Specifiche tecniche • IDEM: Specifiche tecniche per la compilazione e l'uso degli attributi • IDEM: Metadata Profile • IDEM: Metadata registration practice statement • Richiesta di Adesione/Accordo Collabor. • DOPAU (Descrizione processo accreditamento)

SPID e IDEM: identità digitali

	SPID	IDEM
Sperimentazione	2014-2015 IdP: 4, SP: ?	2007-2008 IdP: 20, SP: 10
Operatività Dati 2016	Da 15.03.2016 IdP: 3, PA: 10, SP: 300	Da 01.04.2009 IdP: 75, M&P: 96, SP: 121, 1177, 2000ca., AA (standalone): 1, 3
Base utenti attivi Base utenti attesa	3 milioni (entro 2016) 60 milioni (tutta la popolazione italiana)	4 milioni ca. 8-10 milioni (tutti gli studenti e tutti i laureati)
Identificazione	• A vista con esibizione di doc identità • A vista da remoto con esibizione di doc identità • Identificazione informatica tramite documenti digitali di identità • Identificazione informatica tramite altre identità SPID • Identificazione informatica tramite firma elettronica qualificata o firma digitale	• A vista con esibizione di doc identità
Level of Assurance	• LoA2 • LoA3 • LoA4	• LoA2 • LoA3 (non usato) • LoA4 (non usato)

SPID e IDEM: attributi

	SPID	IDEM*
Identificativi:		
Codice identificativo	spidCode *(= <cod_IdP><nr. univoco>)*	ePPN *(=<stringa_univoca>@<domain>)* ePTID o SAML2name_id
Nome	Name	givenName
Cognome	familyName	sn
Codice fiscale	fiscalNumber *(=TINIT-<CodiceFiscale>)*	schacPersonalUniqueID *(=urn:schac:personalUniqueID:IT:CF:[CF<CodFis>]*
Secondari:		
Numero di telefono mobile	mobilePhone	mobile
Indirizzo di posta elettronica	email	mail
Qualificati:		
		eduPersonScopedAffiliation (ruolo)
		eduPersonEntitlement
		Titolo di studio

(*)I nomi degli attributi usati da IDEM sono conformi a: RFC 2798, 4519 e 4524, eduPerson schema e SCHAC schema. Uso internazionale.

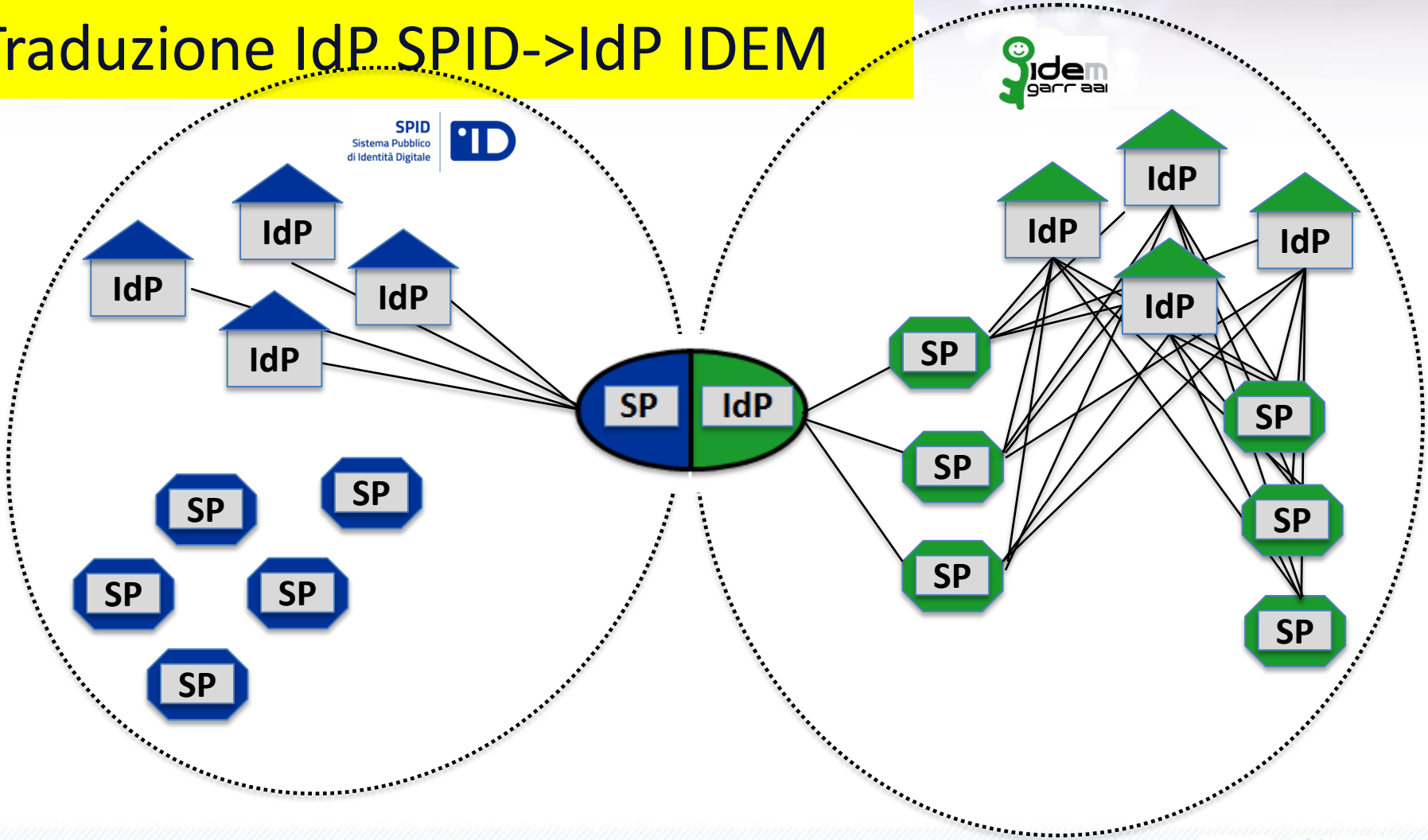
SPID-IDEM: specifiche tecniche

	SPID	IDEM
SAML v2 per il profilo “Web Browser SSO”	✓	✓
“SP-Initiated”: “Redirect/POST binding” e “POST/POST binding”	✓	✓
Subject dell’asserzione, NameID Format “urn:oasis:names:tc:SAML:2.0:nameidformat:transient”	✓	✓
Subject dell’asserzione, NameID NameQualifier	✓	✓
Nell’asserzione: <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameidformat:entity">*(entityID)*</saml2:Issuer>	✓	*Stessa info in altro campo*
Ogni asserzione, da Idp e da SP, deve essere firmata SHA256	✓	*Per IdP* ✓
SP deve richiedere <RequestedAuthnContext> e IdP deve essere in grado di rispondere	✓	*Da implementare /Facoltativo*
Nei Metadati: gli IdP "WantAuthnRequestSigned"	✓	*Da implementare*
Sicurezza del canale SSL o TLS ultima versione disponibile	✓	✓
SAML V2 Profile	$SAML2_{SPID}$	$SAML2_{INT}$*

(*) http://saml2int.org/

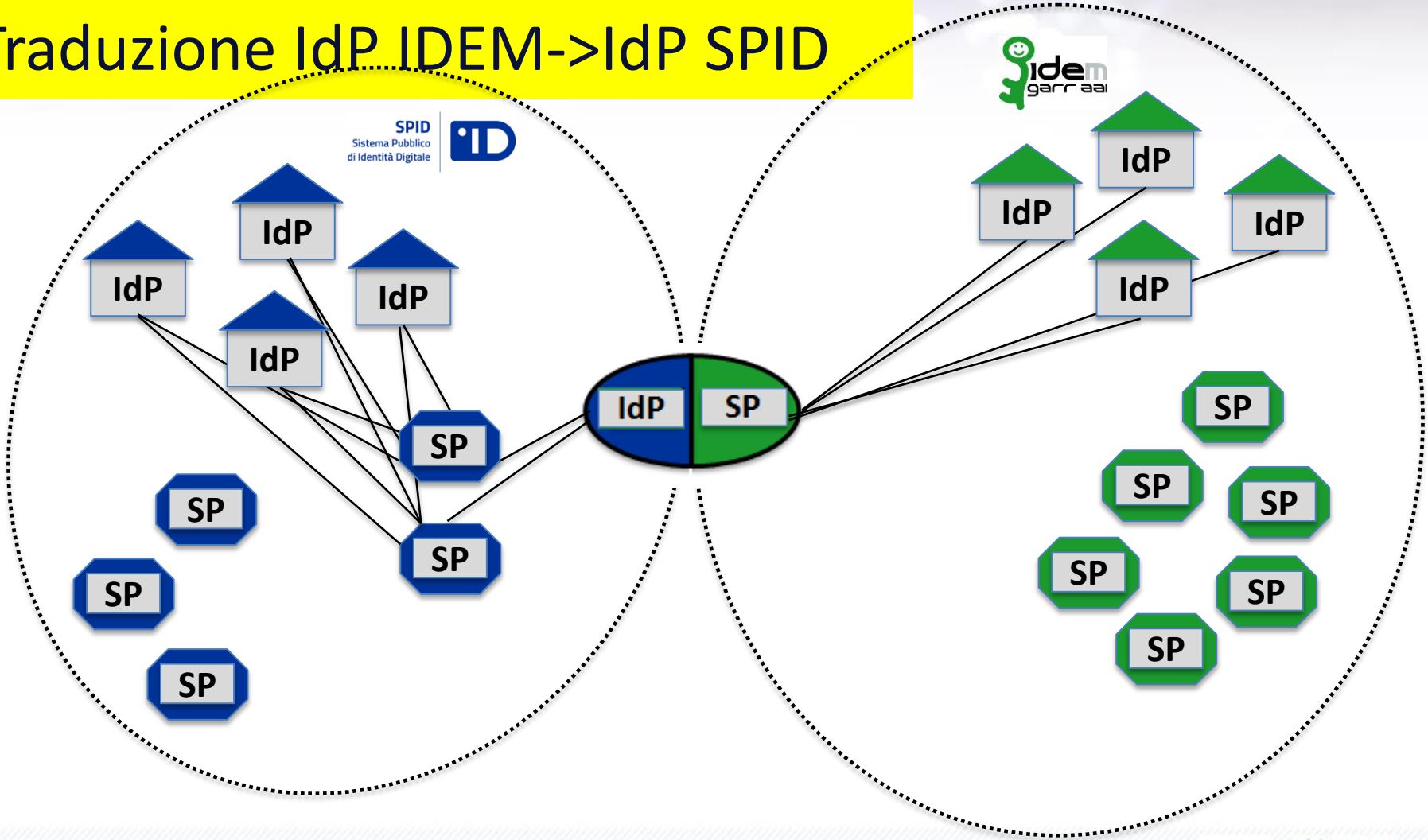
Casi di integrazione 1
SP IDEM accettano IdP SPID

Traduzione IdP SPID->IdP IDEM

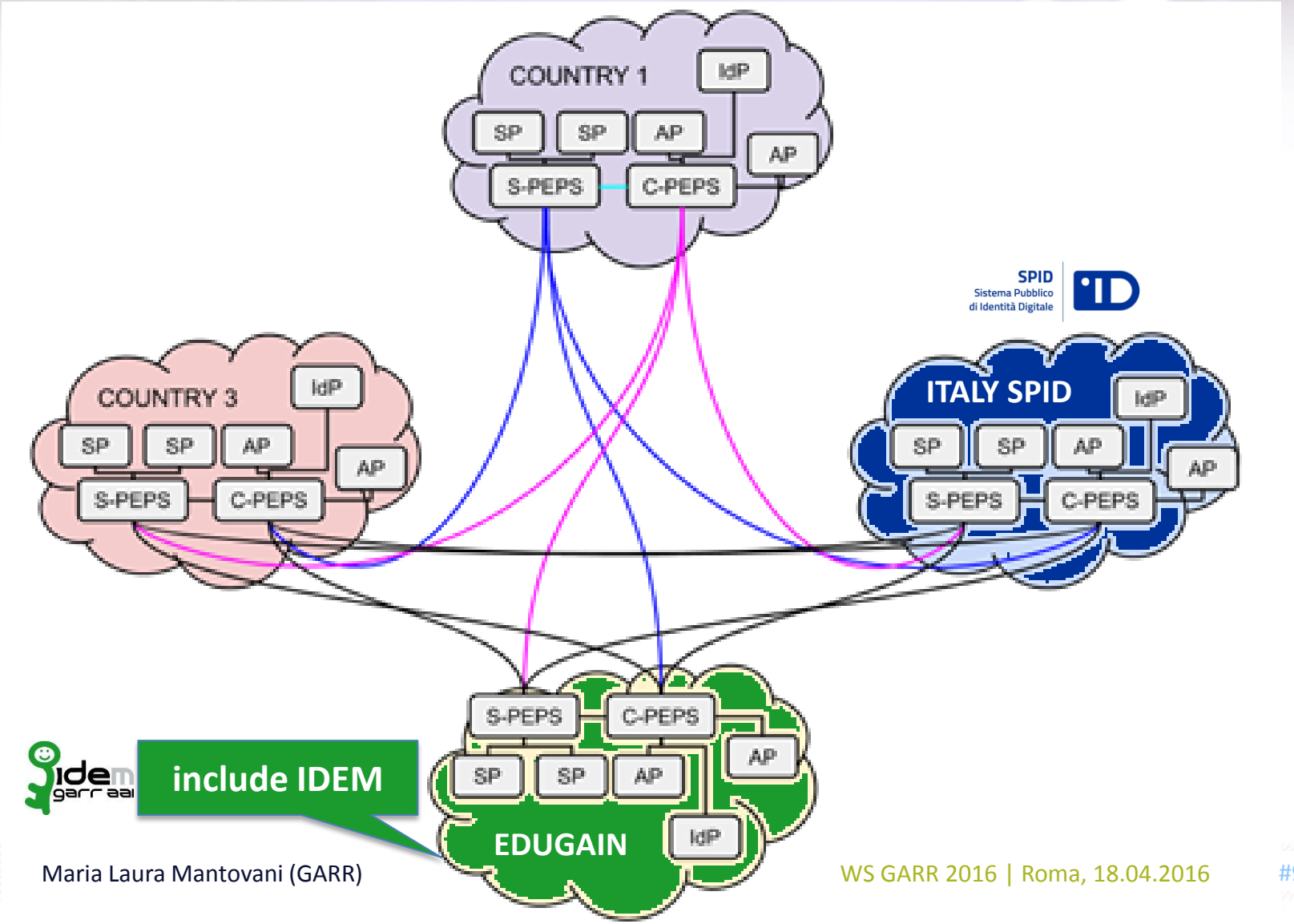


Casi di integrazione 2
SP SPID accettano IdP IDEM

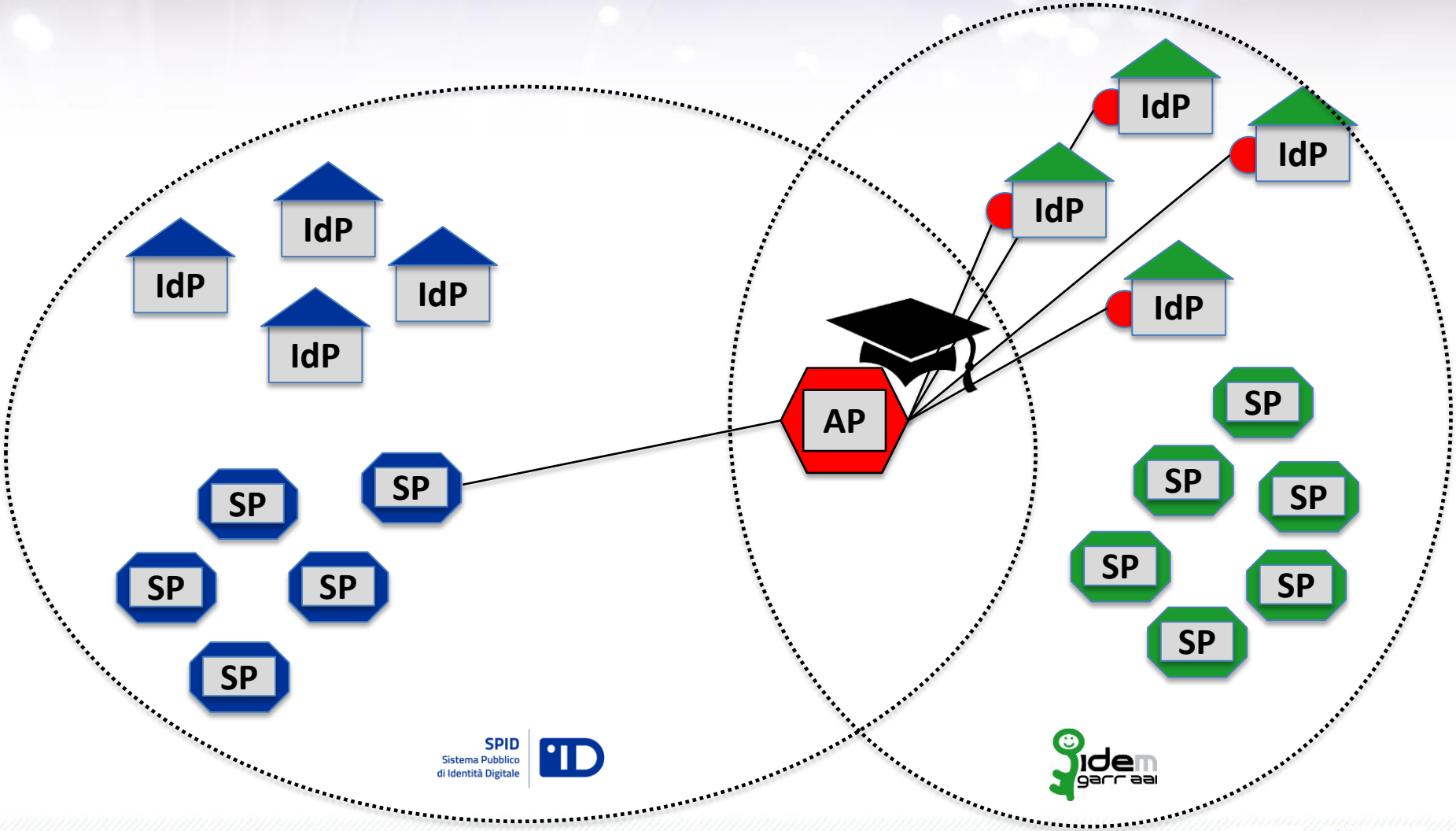
Traduzione IdP IDEM->IdP SPID



Casi di integrazione 3 modello STORK2



Casi di integrazione 4 fornitore di attributi qualificati



Conclusioni

Possibilità di collaborazione:

- Con AGID:
  - regolamento per AP
  - mappatura attributi
  - interoperabilità **SAML2SPID <-> SAML2INT**
- Con IDP SPID:
  - prove proxy SP-IDP
- Con SP SPID:
  - prove proxy IDP-SP
  - prove con AP

Grazie per l'attenzione

marialaura.mantovani@garr.it