Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

SPID: Avvio regolamentazione e pilota

9 Giugno 2014

CONTENUTI

1. SPID
2. Obiettivo dell'incontro
3. Presentazione team AgID
4. Elementi dello Schema di Decreto e normativa UE (S. Arbia)
5. Architettura e modello di riferimento (A. Raia)
6. Organizzazione del progetto
7. Gantt avvio regolamenti e pilota

CONTENUTI

1. SPID
2. Obiettivo dell'incontro
3. Presentazione team AgID
4. Elementi dello Schema di Decreto e normativa UE
5. Architettura e modello di riferimento
6. Organizzazione del progetto
7. Gantt avvio regolamenti e pilota

SPID /1

Art. 64. Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni

1. La carta d'identità elettronica e la carta nazionale dei servizi costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'identificazione informatica.

2. Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'identificazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio. Con l'istituzione del sistema SPID di cui al comma 2-bis, Le pubbliche amministrazioni possono consentire l'accesso in rete ai propri servizi solo mediante gli strumenti di cui al comma 1, ovvero mediante servizi offerti dal medesimo sistema spid. L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni.

2-bis. Per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID).

SPID /2

Art. 64. Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni

2-ter Il sistema SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia digitale, secondo modalità definite con il decreto di cui al comma 2-sexies, 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, in qualità di erogatori di servizi in rete, ovvero, direttamente, su richiesta degli interessati.

2-quater. Il sistema SPID è adottato dalle pubbliche amministrazioni nei tempi e secondo le modalità definiti con il decreto di cui al comma 2-sexies.

2-quinquies. Ai fini dell'erogazione dei propri servizi in rete, è altresì riconosciuta alle imprese, secondo le modalità definite con il decreto di cui al comma 2-sexies, la facoltà di avvalersi del sistema SPID per la gestione dell'identità digitale dei propri utenti. L'adesione al sistema SPID per la verifica dell'accesso ai propri servizi erogati in rete per i quali è richiesto il riconoscimento dell'utente esonera l'impresa da un obbligo generale di sorveglianza delle attività sui propri siti, ai sensi dell'articolo 17 del decreto legislativo 9 aprile 2003, n. 70.

SPID /3

Art. 64. Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni

2-sexies. Con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro delegato per l'innovazione tecnologica e del Ministro per la pubblica amministrazione e la semplificazione, di concerto con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali, sono definite le caratteristiche del sistema SPID, anche con riferimento:

a) al modello architetturale e organizzativo del sistema;

b) alle modalità e ai requisiti necessari per l'accreditamento dei gestori dell'identità digitale;

c) agli standard tecnologici e alle soluzioni tecniche e organizzative da adottare anche al fine di garantire l'interoperabilità delle credenziali e degli strumenti di accesso resi disponibili dai gestori dell'identità digitale nei riguardi di cittadini e imprese, compresi gli strumenti di cui al comma 1;

d) alle modalità di adesione da parte di cittadini e imprese in qualità di utenti di servizi in rete;

e) ai tempi e alle modalità di adozione da parte delle pubbliche amministrazioni in qualità di erogatori di servizi in rete;

f) alle modalità di adesione da parte delle imprese interessate in qualità di erogatori di servizi in rete.

CONTENUTI

1. SPID
2. Obiettivo dell'incontro
3. Presentazione team AgID
4. Elementi dello Schema di Decreto e normativa UE
5. Architettura e modello di riferimento
6. Organizzazione del progetto
7. Gantt avvio regolamenti e pilota

Obiettivo dell'incontro

- Condividere il quadro di attività;
- Condividere lo scenario normativo;
- Condividere lo scenario tecnologico;
- Presentazione del Gantt delle attività;
- Definire le attività con il maggior parallelismo possibile per attivare i servizi SPID, primariamente delle PA, entro aprile 2015;
- Definire gli impegni per ciascun soggetto;
- Definire il modello di relazione;
- Definire calendari di incontri e SAL

Lettere di ingaggio

L'avvio entro aprile 2015 del sistema SPID è una delle priorità indicate dal Presidente del Consiglio dei Ministri.

Lo schema di decreto attuativo è stato già rilasciato dall'Unità di missione per l'Agenda Digitale ed è stato avviato l'iter di approvazione/emanazione. ...

Per conseguire l'obiettivo indicato dal Presidente del Consiglio dei Ministri è necessaria la più ampia e fattiva collaborazione istituzionale per definire regole, modelli e interfacce e consentire l'avvio ed il dispiegamento del sistema.

D'intesa con il Ministro per la semplificazione e la pubblica amministrazione, facendo leva sulla sensibilità e attenzione verso i processi di innovazione e contando sull'esperienza e capacità fin qui maturate …

… invitati i soggetti individuati in rappresentanza delle **PA centrali e locali, delle banche (nella veste di fornitore di servizi) e dei candidati al ruolo di gestore di identità** (identity provider).

Nel corso del predetto incontro verrà presentato lo scenario delle attività ed il relativo piano di progetto.

CONTENUTI

1. SPID
2. Obiettivo dell'incontro
3. Presentazione team AgID
4. Elementi dello Schema di Decreto e normativa UE
5. Architettura e modello di riferimento
6. Organizzazione del progetto
7. Gantt avvio regolamenti e pilota

Il team AgID

Francesco Tortorelli

Stefano Arbia

Gabriele Bocchetta

Marino Di Nillo

Massimiliano Pucciarelli

Alfio Raia

Le fasi di SPID

Regolazione e pilota

- Avvio delle fasi di regolazione
- Impostazione pilota

Privati e attribute

- Ampliamento ai soggetti disponibili e al mercato
- Completamento regolazione

Completamento

- Accreditamento e convenzioni
- Dispiegamento PA

CONTENUTI

1. SPID
2. Obiettivo dell'incontro
3. Presentazione team AgID
4. Elementi dello Schema di Decreto e normativa UE
5. Architettura e modello di riferimento
6. Organizzazione del progetto
7. Gantt avvio regolamenti e pilota

SPID Impianto normativo

SPID

Soggetti coinvolti:

- Gestori dell'identità digitale
- Fornitori di servizi
- Gestori di attributi qualificati
- Autorità di accreditamento e vigilanza

SPID RUOLI

Gestori dell'identità digitale

Ottengono l'accreditamento

Verificano l'identità degli *utenti* utilizzando anche i servizi previsti da apposita convenzione

Assegnano e gestiscono l'identità digitale

Rendono disponibili e gestiscono gli *attributi* dell'*utente*

Rendono disponibile gratuitamente alle pubbliche amministrazioni il servizio di autenticazione

Possiedono requisiti organizzativi e societari sostanzialmente uguali a quelli necessari per l'accreditamento dei certificatori di firma digitale

SPID RUOLI

Fornitori di servizi

Ottengono l'accreditamento

Inoltrano le richieste di *identificazione informatica* dell'*utente* ai *gestori dell'identità digitale*

Non discriminano gli *utenti* in base al *gestore dell'identità digitale* che l'ha fornita

Sono liberi di scegliere il livello di sicurezza delle identità digitali necessari per accedere allo specifico servizio

Sottoscrivono la convenzione predisposta

Soddisfano gli obblighi di cui all'articolo 17, comma 2, del decreto legislativo 9 aprile 2003, n. 70 con la comunicazione del codice identificativo dell'identità digitale utilizzata dall'utente

Possono fruire di servizi di autenticazione offerti dai gestori di identità UE 

Gestori di attributi qualificati

Ottengono l'accreditamento

Attestano il possesso e la validità di *attributi qualificati*, su richiesta dei *fornitori di servizi,* previo consenso degli *utenti* interessati

SPID RUOLI

Agenzia per l'Italia Digitale

- Accredita e vigila i gestori di identità
- Accredita e vigila i gestori di attributi qualificati
- Stipula Convenzioni

- Vigila sul rispetto delle convenzioni
- *Gestisce e pubblica il registro SPID* contenente l'elenco dei soggetti abilitati a operare in qualità di *gestori dell'identità digitale*, di *gestori degli attributi qualificati* e di *fornitori di servizi*
- Mantiene aggiornati i regolamenti attuativi

Agenzia per l'Italia Digitale

- Regola l'utilizzo di deleghe e procure da parte degli utenti

Coordina il pilota con l'obiettivo di emanare delle adeguate regole tecniche garantendone trasparenza e divulgazione

I provvedimenti AgID

Oggetto	Termine
Regole tecniche e modalità attuative	Entro 30 giorni dalla pubblicazione del DPCM
Modalità di accreditamento	Entro 60 giorni dalla pubblicazione del DPCM
Procedura per l'approvazione di sistemi di verifica dell'identità	Entro 60 giorni dalla pubblicazione del DPCM
Eventuale adeguamento dei regolamenti attuativi	Secondo necessità

SPID VERIFICA DELL'IDENTITÀ

La verifica dell'identità del richiedente un'identità digitale

a) identificazione tramite esibizione a vista di un valido documento d'identità da parte del soggetto richiedente, il quale sottoscrive il modulo di adesione allo *SPID*;

b) *identificazione informatica* tramite documenti digitali di identità, validi ai sensi di legge, che prevedono il riconoscimento a vista del richiedente all'atto dell'attivazione (TS-CNS, CNS, CRS, ATe,..);

c) *identificazione informatica* tramite altra *identità digitale SPID* di livello di sicurezza pari o superiore a quella oggetto della richiesta;

d) acquisizione del modulo di adesione allo *SPID* sottoscritto con firma elettronica qualificata o con firma digitale;

e) *identificazione informatica* per mezzo di sistemi informatici preesistenti all'introduzione dello *SPID* che risultino aver adottato, a seguito di apposita istruttoria dell'*Agenzia*, regole di *identificazione informatica* caratterizzate da livelli di sicurezza uguali o superiori a quelli definiti nel presente decreto.

Conservazione evidenze della verifica dell'identità del richiedente un'identità digitale

I gestori dell'identità digitale conservano per 20 anni:

- copia per immagine del documento di identità esibito
- il modulo sottoscritto dal richiedente l'identità digitale
- copia del log nel caso di uso di altre modalità previste/autorizzate

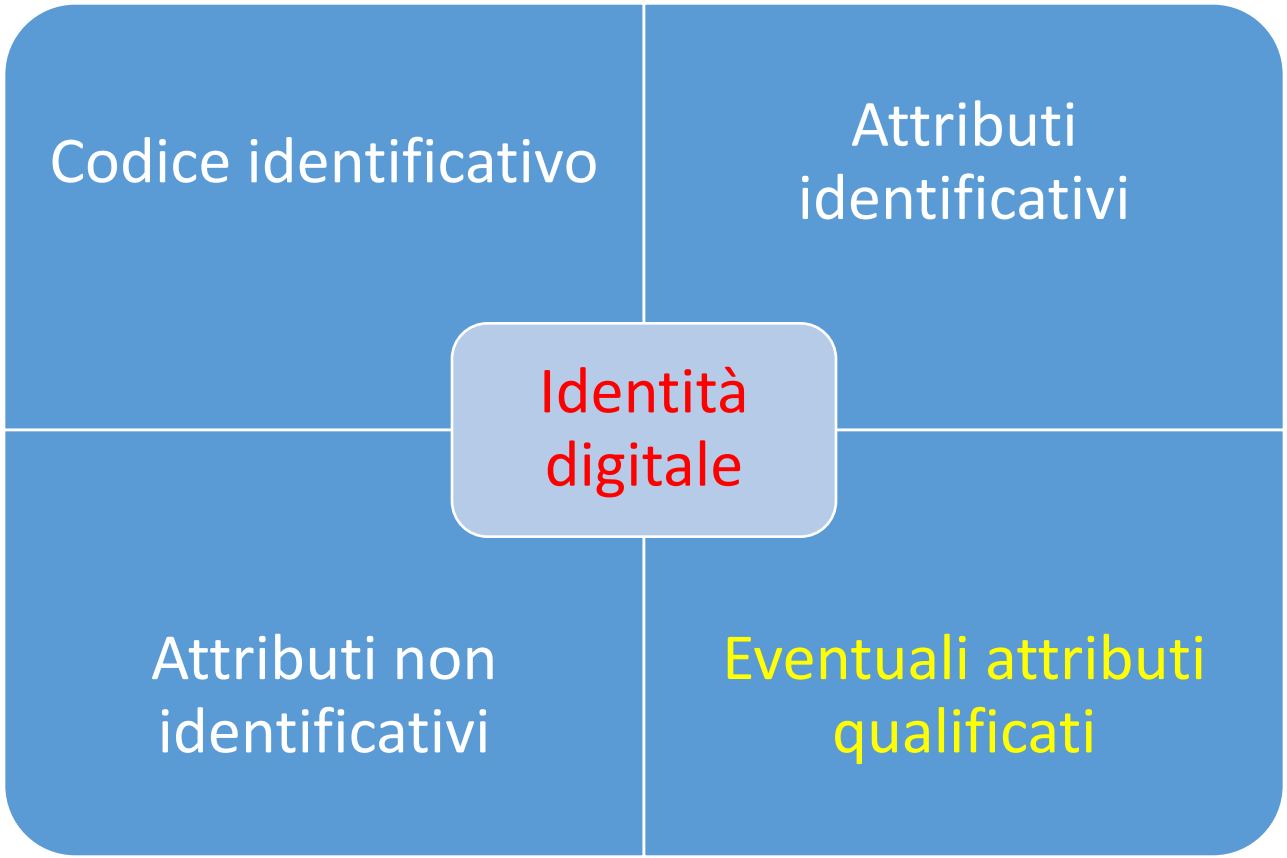
SPID ATTRIBUTI

attributi identificativi: nome, cognome, luogo e data di nascita, sesso, ovvero ragione o denominazione sociale, sede legale, nonché il codice fiscale e gli estremi del documento d'identità utilizzato ai fini dell'identificazione;

attributi non identificativi: il numero di telefonia mobile, l'indirizzo di posta elettronica, il domicilio fisico e digitale, nonché eventuali altri *attributi* individuati dall'*Agenzia*;

attributi qualificati: le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi altro tipo di *attributo* attestato da un *gestore di attributi qualificati*. Possono essere già contenuti nell'identità digitale.

SPID IDENTITÀ DIGITALE



Livelli di sicurezza delle identità digitali

Primo livello: corrispondente al Level of Assurance LoA2 dello standard ISO/IEC DIS 29115, il *gestore dell'identità digitale* rende disponibili sistemi di *autenticazione informatica* a un fattore (per esempio la password), secondo quanto previsto dal presente decreto e dai regolamenti di cui all'articolo 4.

Secondo livello: corrispondente al Level of Assurance LoA3 dello standard ISO/IEC DIS 29115, il *gestore dell'identità digitale* rende disponibili sistemi di *autenticazione informatica* a due fattori, non basati necessariamente su certificati digitali le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo, secondo quanto previsto dal presente decreto e dai regolamenti di cui all'articolo 4.

Terzo livello: corrispondente al Level of Assurance LoA4 dello standard ISO/IEC DIS 29115, il *gestore dell'identità digitale* rende disponibili sistemi di *autenticazione informatica* a due fattori basati su certificati digitali, le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo.

INDIVIDUAZIONE DEL LIVELLO DI SICUREZZA DEGLI STRUMENTI

L'*Agenzia* valuta e autorizza l'uso degli strumenti e delle tecnologie di *autenticazione informatica* consentiti per ciascun livello, nonché i criteri per la valutazione dei sistemi di *autenticazione informatica* e la loro assegnazione al relativo livello di sicurezza.

I *gestori dell'identità digitale* rendono pubbliche le decisioni dell'*Agenzia.*

Prossime azioni

1. *Acquisizione del parere tecnico di AgID*
2. *Sentire il Garante protezione dati personali per eventuali osservazioni*
3. *Espletare la procedura di notifica alla Commissione europea*
4. *Ottenere il concerto del Ministro dell'economia e delle finanze*
5. *Firme dei Ministri e pubblicazione*

Prossime azioni

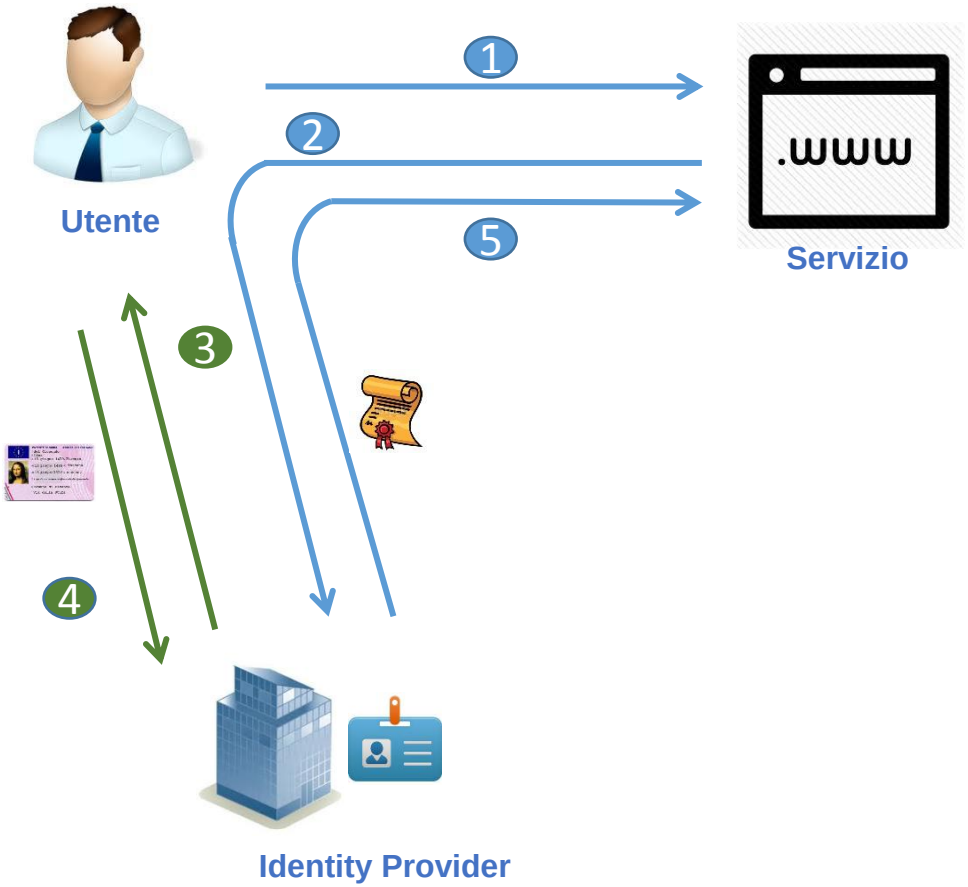
Avviare e condurre il Pilota in tempi coerenti con gli obiettivi temporali

imposti dal Governo per la messa in produzione di SPID

CONTENUTI

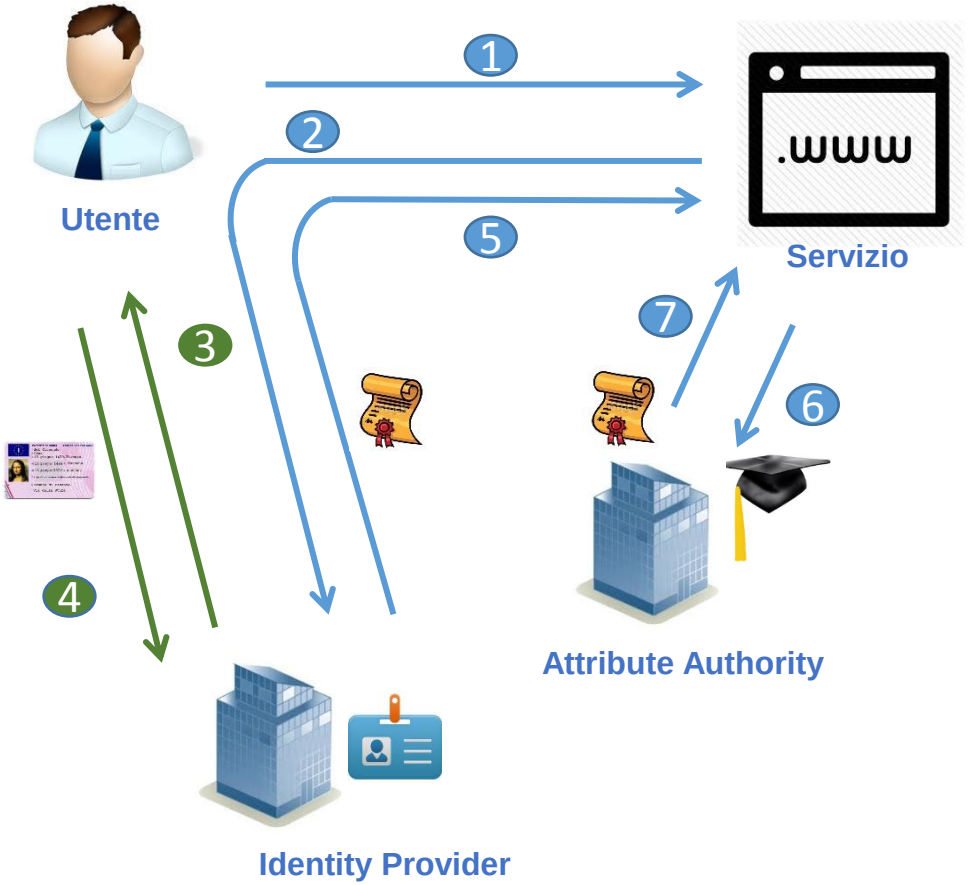
1. SPID
2. Obiettivo dell'incontro
3. Presentazione team AgID
4. Elementi dello Schema di Decreto e normativa UE (S. Arbia)
5. Architettura e modello di riferimento (A. Raia)
6. Organizzazione del progetto
7. Gantt avvio regolamenti e pilota

Infrastruttura SPID



1. **Richiesta di servizio**
2. **Inoltro verso Identity provider**
3. **Richiesta credenziali**
4. **Verifica credenziali**
5. **Rendirizzamento verso il service provider con asserzione di autenticazione**

Infrastruttura SPID



1. **Richiesta di servizio**
2. **Inoltro verso Identity provider**
3. **Richiesta credenziali**
4. **Verifica credenziali**
5. **Rendirizzamento verso il service provider con asserzione di autenticazione**
6. **Richiesta attributi**
7. **Risposta contenente certificazione attributi**

Chi fa cosa

Gestori identità SPID

- Realizzazione identity Provider
  - Specifiche di interfaccia IdP
- Presa in carico delle identità censite degli erogatori di servizi che partecipano al pilota

Services provider PA - Privati

- Identificazione servizi accessibili in modalità SPID
- Predisposizione sistemi di I&AM per l'accesso a tali servizi
  - Specifiche interfaccia IdP

AgID

- Predisposizione registro degli Identity Provider
  - Elenco degli identity provider SPID
  - metadata

Security Assertion Markup Language (SAML) V2.0

OASIS Security Services (SAML) TC, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005

OASIS Security Services (SAML) TC, Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005

OASIS Security Services (SAML) TC, Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005.

OASIS Security Services (SAML) TC, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005

OASIS Security Services (SAML) TC, Authentication Context for The OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005.

Specifiche SPID

Le specifiche proposte sono quelle già previste per l'identity Provider dal modello GIFID di SPC

- Il funzionamento dell'Identity provider è quello previsto da SAML v2 per il profilo "Web Browser SSO" ([SAML-TechOv] sez. 4.1)
- Devono essere previste le due versioni "SP-Initiated": "Redirect/POST binding" e "POST/POST binding". in cui il meccanismo di autenticazione è innescato dalla richiesta inoltrata dall'utente (tramite il suo User Agent) ad un Service Provider, il quale a sua volta si rivolge opportunamente all'autorità di certificazione d'identità in modalità "pull".
- La richiesta di autenticazione SAML (basata sul costrutto <AuthnRequest>) può essere inoltrata da un Relying Party all'Identity Provider usando il binding HTTP Redirect o il binding HTTP POST.
- La relativa risposta SAML (basata sul costrutto <Response>) può invece essere inviata dall'Identity Provider al Relying Party solo tramite il binding HTTP POST.
- Specifiche delle interfacce riporteranno dettagliatamente:

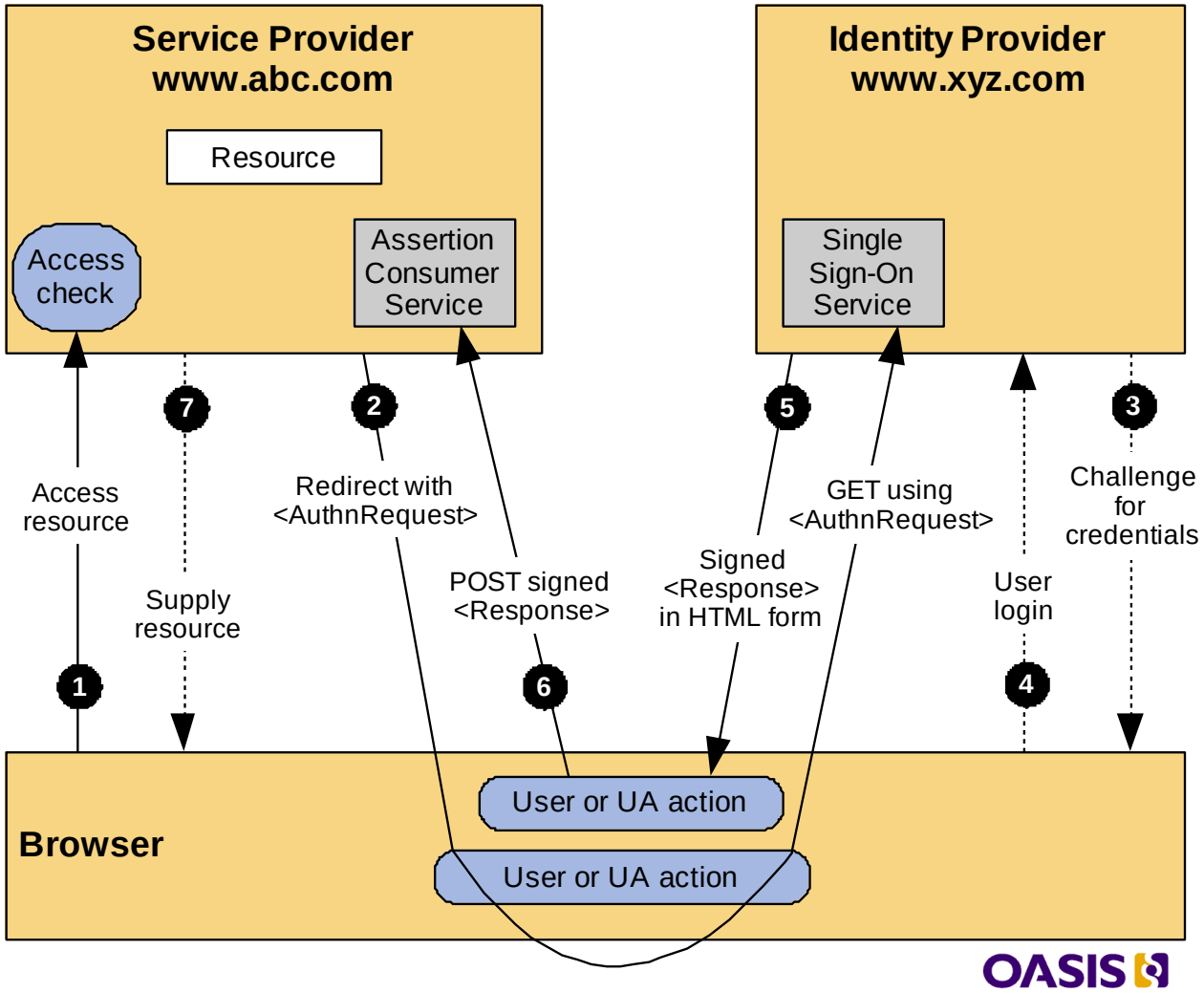
  Le caratteristiche delle asserzioni prodotte

  Le caratteristiche delle AuthnRequest e della AuthnResponse

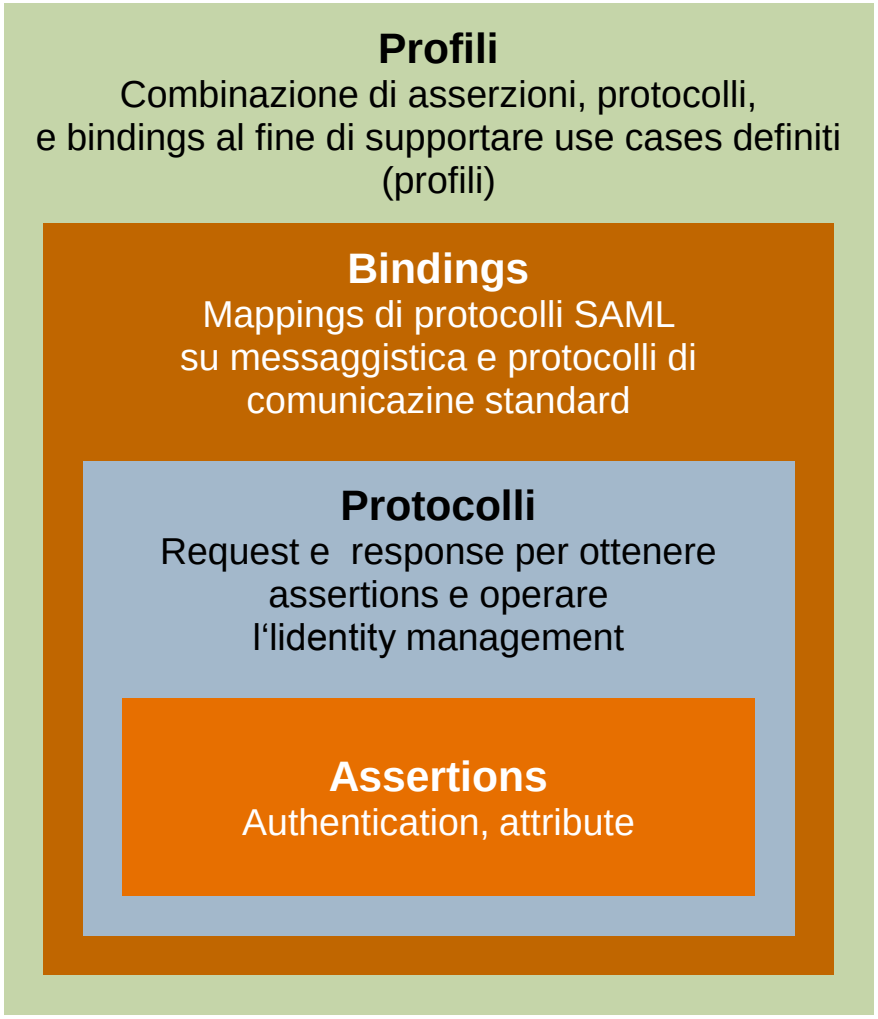
  Le caratteristiche del binding

  I metadati

SP- Initiated SSO: Redirect / POST Bindings



SAML vs SPID



Authentication Context
Informazioni sul tipo e sulla forza
del processo di autenticazione

Metadata
Dati di configurazioni per
identity e service providers

CONTENUTI

1. SPID
2. Obiettivo dell'incontro
3. Presentazione team AgID
4. Elementi dello Schema di Decreto e normativa UE
5. Architettura e modello di riferimento
6. Organizzazione del progetto
7. Gantt avvio regolamenti e pilota

Organizzazione del progetto

AgID (coordinamento e conduzione del progetto)

- Predisposizione e gestione ambienti di Comunicazione e collaborazione per il gruppo pilota e generale
- Gestione del Gantt, SAL periodici (settimanali, quindicinali e mensili)
- Stesura specifiche con gruppo tecnico

PA (Pac, Regioni, Comuni)

- Partecipazione alla definizione delle specifiche
- Realizzazione accesso SPID ai servizi
- Diffusione e comunicazione

ASSOCERTIFICATORI

- Realizzazione IdP e servizi di autenticazione
- Diffusione regole e modelli

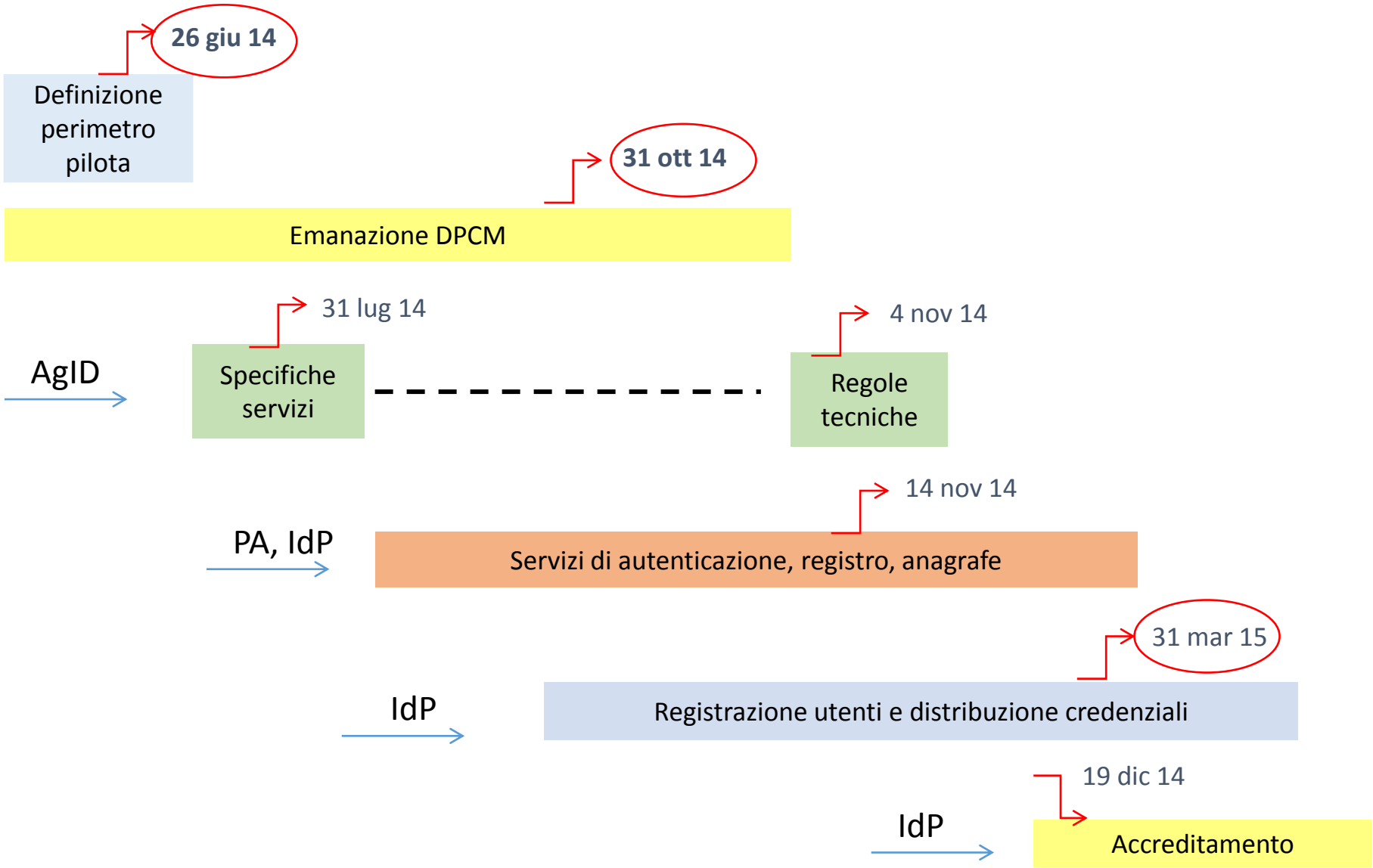
ABI

- Diffusione regole e modelli
- Attivazione degli associati

CONTENUTI

1. SPID
2. Obiettivo dell'incontro
3. Presentazione team AgID
4. Elementi dello Schema di Decreto e normativa UE
5. Architettura e modello di riferimento
6. Organizzazione del progetto
7. Gantt avvio regolamenti e pilota

Gantt sintetico



Grazie !