Lo stato dell'arte dell'identità digitale in Italia e in Europa

Giovanni MANCA
Esperto di digitalizzazione e sicurezza ICT

(Security Summit)
Roma – 7 giugno 2018

Argomenti

- **L’identità digitale nazionale.**
- **L’identità digitale in UE .**
- **Lo scenario di medio termine.**

Le basi di SPID

- «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)».

- Questo è l'articolo 64, comma 2-bis del CAD vigente e non sembra essere modificato dal decreto correttivo (2017).

- L'articolo 64 disciplina anche le modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni.

- DPCM 24 ottobre 2014 – Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese.

I regolamenti attuativi

- Modalità per l'accreditamento e la vigilanza dei gestori dell'identità.
- Le regole tecniche (protocolli di comunicazione e interazioni tra soggetti).
- Modalità attuative per la realizzazione dello SPID.
- Procedure per consentire ai gestori dell'identità digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio delle identità digitali.

Chi fa che cosa

- AgID accredita e vigila.
- I gestori delle identità rilasciano le credenziali.
- I gestori degli attributi qualificati certificano i «ruoli professionali».
- I fornitori dei servizi garantiscono l'accesso a questi ultimi tramite le credenziali SPID.
- Esistono, al momento, solo fornitori di servizi nella PA. E' disponibile da poco la regolamentazione (schema di convenzione) per i soggetti privati.

IL MODELLO SPID (Sistema Pubblico di Identità Digitale)

- **Garantire il raggiungimento degli obiettivi definiti all'interno dell'Agenda Digitale Europea** in relazione a:
  - ✓ **Standard e interoperabilità**: evolvere gli standard tecnici, definire delle regole di interoperabilità tra sistemi e organizzazioni
  - ✓ **Fiducia e sicurezza**: incrementare il livello di fiducia e sicurezza degli utenti rispetto all'online, migliorare le condizioni di riservatezza e tutela dei dati personali
- **Dare avvio al processo di semplificazione della Cittadinanza Digitale** attraverso la standardizzazione delle modalità di accesso e fruizione dei servizi delle Pubbliche Amministrazioni italiane e attraverso l'uniformità del front-end dei portali
- **Contribuire a ridurre i costi di gestione dei sistemi IT** delle Pubbliche Amministrazioni italiane.
- **Contribuire a ridurre la discrezionalità di investimento e la varietà di soluzioni IT** adottate dalle PPAA italiane di ogni ordine e grado
- **Contribuire a migliorare la performance digitale italiana** recuperando posizioni nel ranking del DESI, in particolare sulle dimensioni «Use of Internet», «Integration of Digital Technology» e «Digital Public Services»:
  - ✓ In virtù degli obblighi derivanti dal DPCM del 24 ottobre 2014, le Pubbliche Amministrazioni devono aderire a SPID. Ne deriva l'**omogeneizzazione dei livelli di sicurezza delle credenziali richieste per l'accesso ai servizi**
  - ✓ I soggetti privati hanno l'opportunità di accedere ad una federazione e di conseguenza ad una Customer Base certificata, **migliorando la capacità di vendita multicanale** (online; mobile)

La normativa di riferimento - 1

Normativa primaria: art. 64 D.Lgs. 7 marzo 2005, n. 82 – Stabilisce le regole primarie, il contesto di utilizzo e l'obbligo per le PA

Art. 64

(Sistema pubblico per la gestione delle identità digitali e modalità di accesso ai servizi erogati in rete dalle pubbliche 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).

2-ter. Il sistema SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'AgID, secondo modalità definite con il decreto di cui al comma 2-sexies, identificano gli utenti per consentire loro l'accesso ai servizi in rete.

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.

La normativa di riferimento - 2

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 ;

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.

2-octies. Le pubbliche amministrazioni consentono mediante SPID l'accesso ai servizi in rete da esse erogati che richiedono identificazione informatica.

2-nonies. L'accesso di cui al comma 2-octies può avvenire anche con la carta di identità elettronica e la carta nazionale dei servizi.

Le novità normative che fanno riferimento a SPID

- **Semplificazione gestione Attribute provider**: art. 6-bis, comma 2-bis «L'INI-PEC acquisisce dagli ordini e dai collegi professionali gli attributi qualificati dell'identità digitale ai fini di quanto previsto dal decreto di cui all'articolo 64, comma 2 –sexies»

- **Sistema di controllo integrato**: All'articolo 30 -ter del decreto legislativo 13 agosto 2010, n. 141, sono apportate le seguenti modificazioni:

  a) al comma 1, è aggiunto, in fine, il seguente periodo:

«Tale sistema può essere utilizzato anche per svolgere funzioni di supporto al controllo delle identità e alla prevenzione del furto di identità in settori diversi da quelli precedentemente indicati, limitatamente al riscontro delle informazioni strettamente pertinenti.»;

  b) al comma 5, dopo la lettera b) è inserita la seguente:
  «b -bis) i soggetti di cui all'articolo 27 del decreto legislativo 7 marzo 2005, n. 82;»

- **Antiriciclaggio**: All'articolo 28, comma 3, lettera c) , del decreto legislativo 21 novembre 2007, n. 231, sono aggiunte, in fine, le seguenti parole: «ovvero siano dotati di identità digitale di livello massimo di sicurezza nell'ambito del Sistema di cui all'articolo 64 del predetto decreto legislativo n. 82 del 2005».

Allineamento sistema creditizio

I principali processi di controllo

- IdP:
  - ✓ Relazione rilasciata da un organismo di valutazione della conformità accreditato
  - ✓ Esame da parte AgID della documentazione inerente processi, organizzazione, risorse, formazione, sicurezza, gestione privacy, business continuity, etc.
  - ✓ Processi certificati sotto il profilo della qualità e sicurezza (ISO relative)
  - ✓ Vulnerability assessment semestrale
  - ✓ Penetration test annuale
  - ✓ Sistema informativo condiviso con AgID
  - ✓ Vigilanza AgID

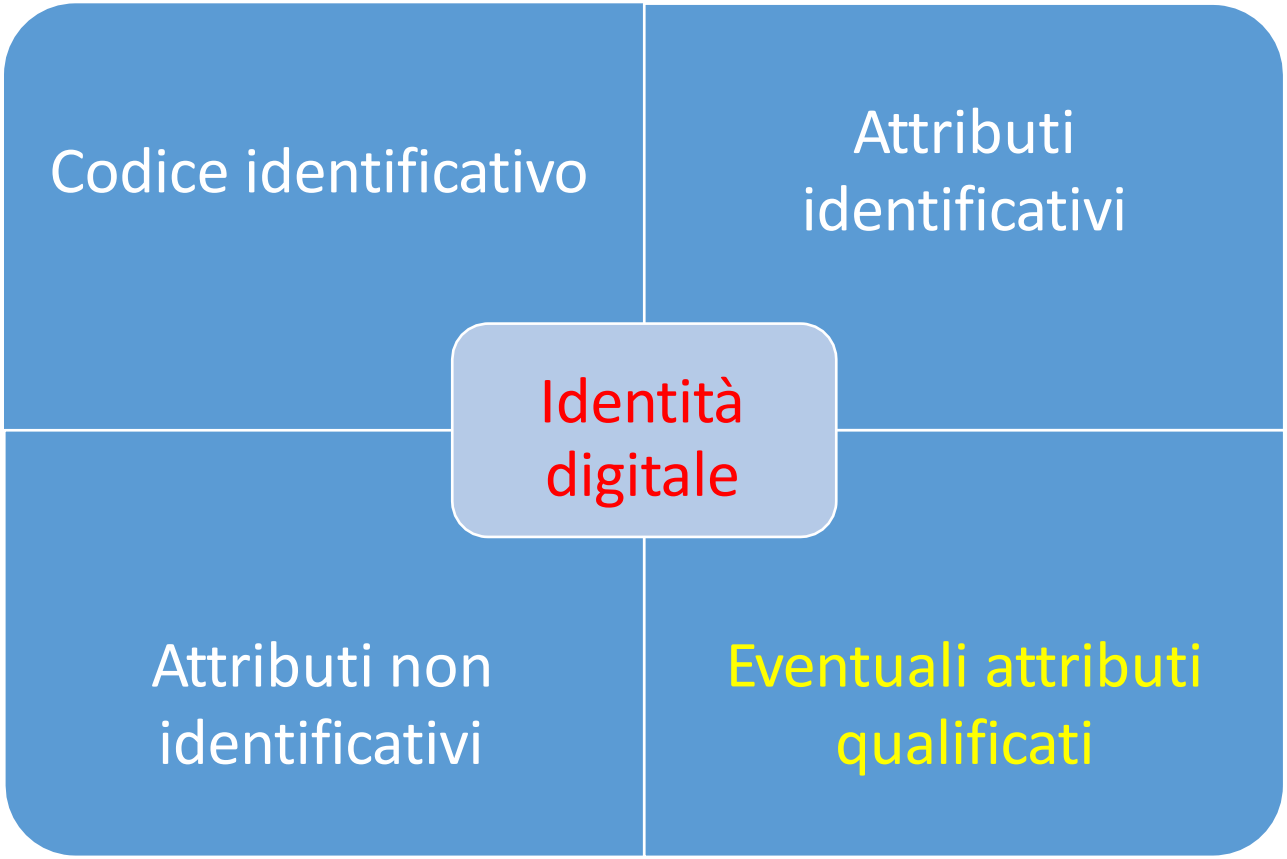
- SP:
  - ✓ Definizione di policy x livelli di accesso ai servizi
  - ✓ Sottoscrizione di una convenzione con precisi impegni
  - ✓ Validazione iniziale della compliance ai morsetti
  - ✓ Controlli sull'utilizzo delle regole da parte AgID

ATTRIBUTI NELLO SPID

- ***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.


Codice identificativo
Attributi identificativi
Identità digitale
Attributi non identificativi
Eventuali attributi qualificati

Fonte AgID

I livelli di sicurezza delle identità digitali - 1

- **Tre livelli di sicurezza di autenticazione informatica.**
  - ✓**Un fattore: es. password.**
  - ✓**Due fattori: es. password e PIN dinamico.**
  - ✓**Due fattori: basati su certificati digitali.**
- **Lo standard ISO/IEC di riferimento è il 29115.**

I livelli di sicurezza delle identità digitali - 2

Primo livello: corrispondente al Level of Assurance LoA2 dello standard ISO/IEC 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.

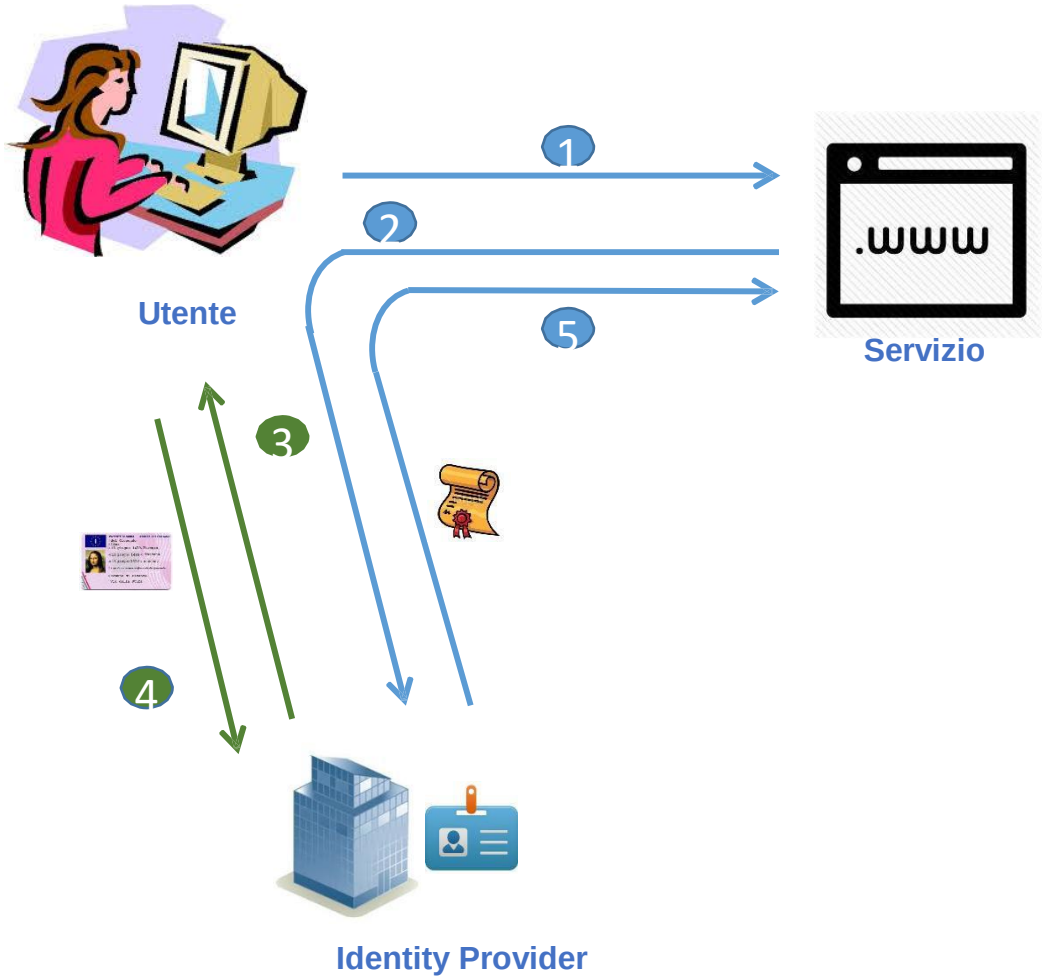
Secondo livello: corrispondente al Level of Assurance LoA3 dello standard ISO/IEC 29115, il *gestore dell'identità digitale* rende disponibili sistemi di *autenticazione informatica* a due fattori, non basati necessariamente su certificati digitali le cui chiavi private siano custodite su dispositivi 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 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.

SPID – Avanzamento alla data

- 8 gestori dell'identità attivi.
- Il rilascio delle credenziali è iniziato il 15 marzo 2016.
- Al 1 giugno 2018 sono state rilasciate circa 2.540.319 credenziali (fonte AgID).
- 4.000 amministrazioni attive (fonte AgID).
- La scadenza formale per gli obblighi per la PA di erogazione dei servizi tramite SPID era il 31 marzo 2018, ma….

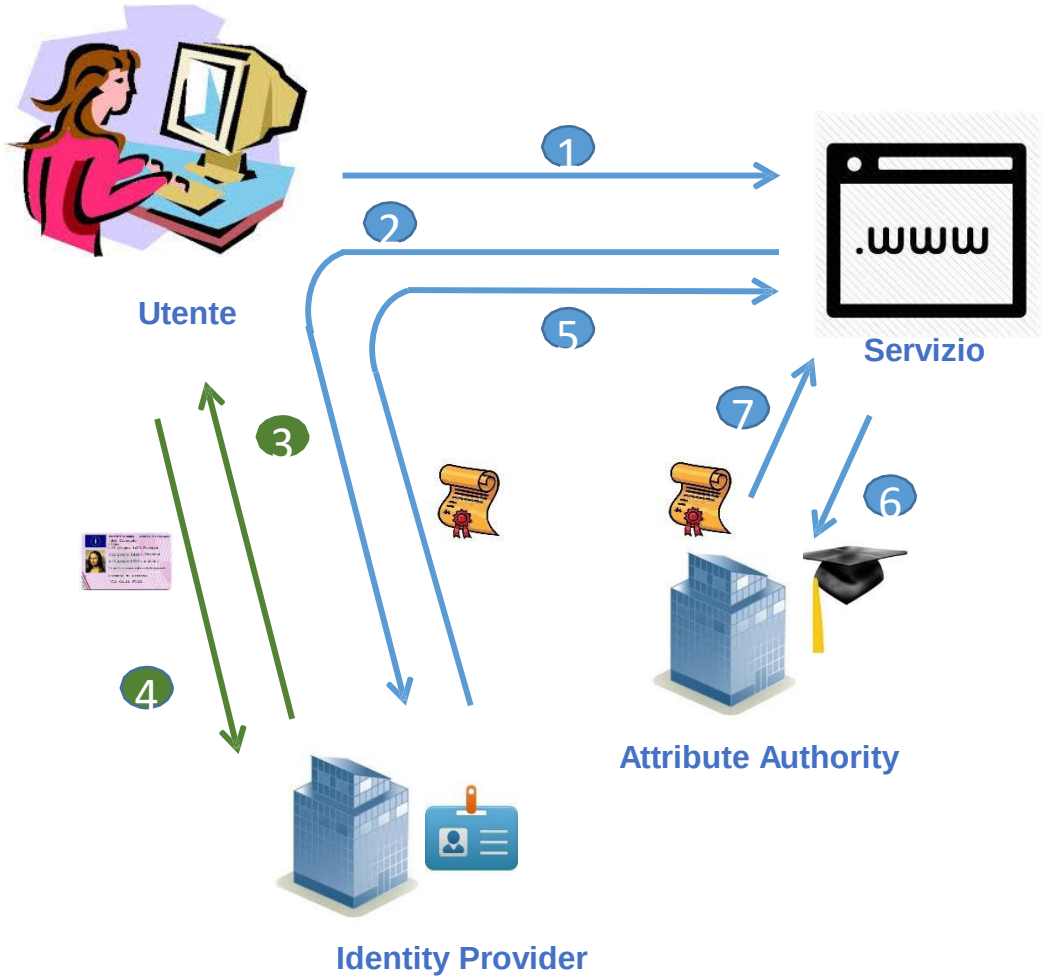
Infrastruttura SPID



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

Da AgID

Infrastruttura SPID

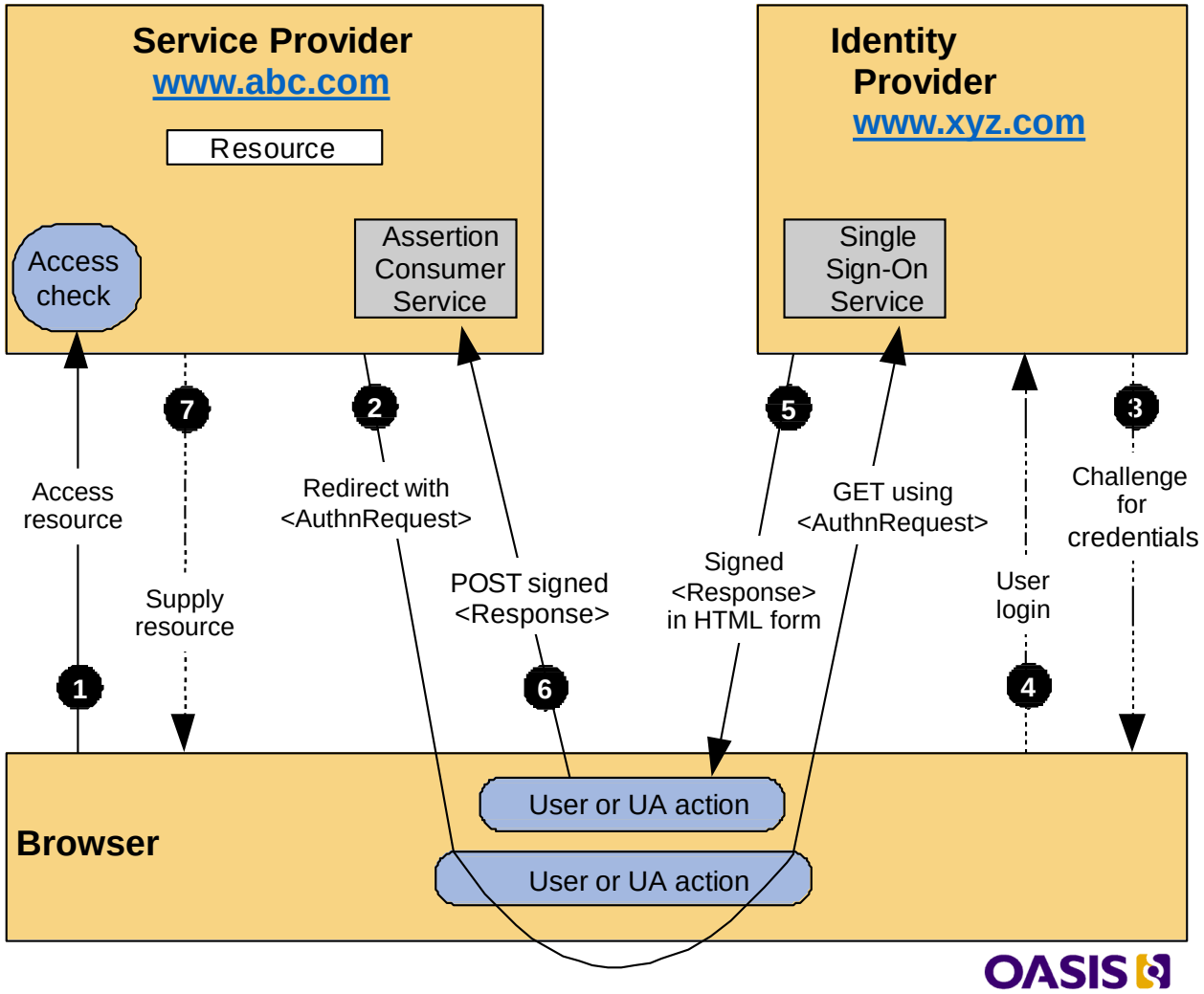


1. Richiesta di servizio
2. Inoltro verso Identity provider
3. Richiesta credenziali
4. Verifica credenziali
5. Rendirizzamento verso il service provider con asserzione di autenticazione
6. Richiesta attributi
7. Risposta contenente certificazione attributi

Da AgID

Lo standard SAML per SPID

SP- Initiated SSO: Redirect / POST Bindings



Fonte AgID

Argomenti

- **L’identità digitale nazionale.**
- **L’identità digitale in UE .**
- **Lo scenario di medio termine.**

L’identità digitale in eIDAS - 1

- **Articolo 8 del Regolamento eIDAS «Livelli di garanzia dei regimi (una migliore traduzione direbbe «schemi») di identificazione elettronica.**

- **Livelli di garanzia:**
  - ✓ **basso;**
  - ✓ **significativo;**
  - ✓ **elevato.**

- **Le specifiche sono dettagliate nella decisione di esecuzione 2015/1502.**

- **L’articolo 24 del Regolamento eIDAS stabilisce ulteriori dettagli sulla verifica e, se del caso, eventuali attributi specifici della persona fisica o giuridica. Questo nell’ambito delle regole per il rilascio di un certificato qualificato per un servizio fiduciario.**

L’identità digitale in eIDAS - 2

- **Si deve tenere in conto che il tutto è nei confini della regola «conformemente al diritto Nazionale».**

- **Le verifiche possono essere effettuate:**
  - **in presenza fisica;**
  - **a distanza tramite mezzi di identificazione elettronica (CNS, SPID, CIE, ecc.);**
  - **mediante l’uso di un certificato elettronico per la firma o il sigillo qualificato;**
  - **mediante altri metodi equivalenti alla presenza fisica (tipo web cam). L’equivalenza è confermata da un organismo di valutazione della conformità.**

- **L’identità del titolare è nazionale e viene attribuita esclusivamente secondo tali regole.**

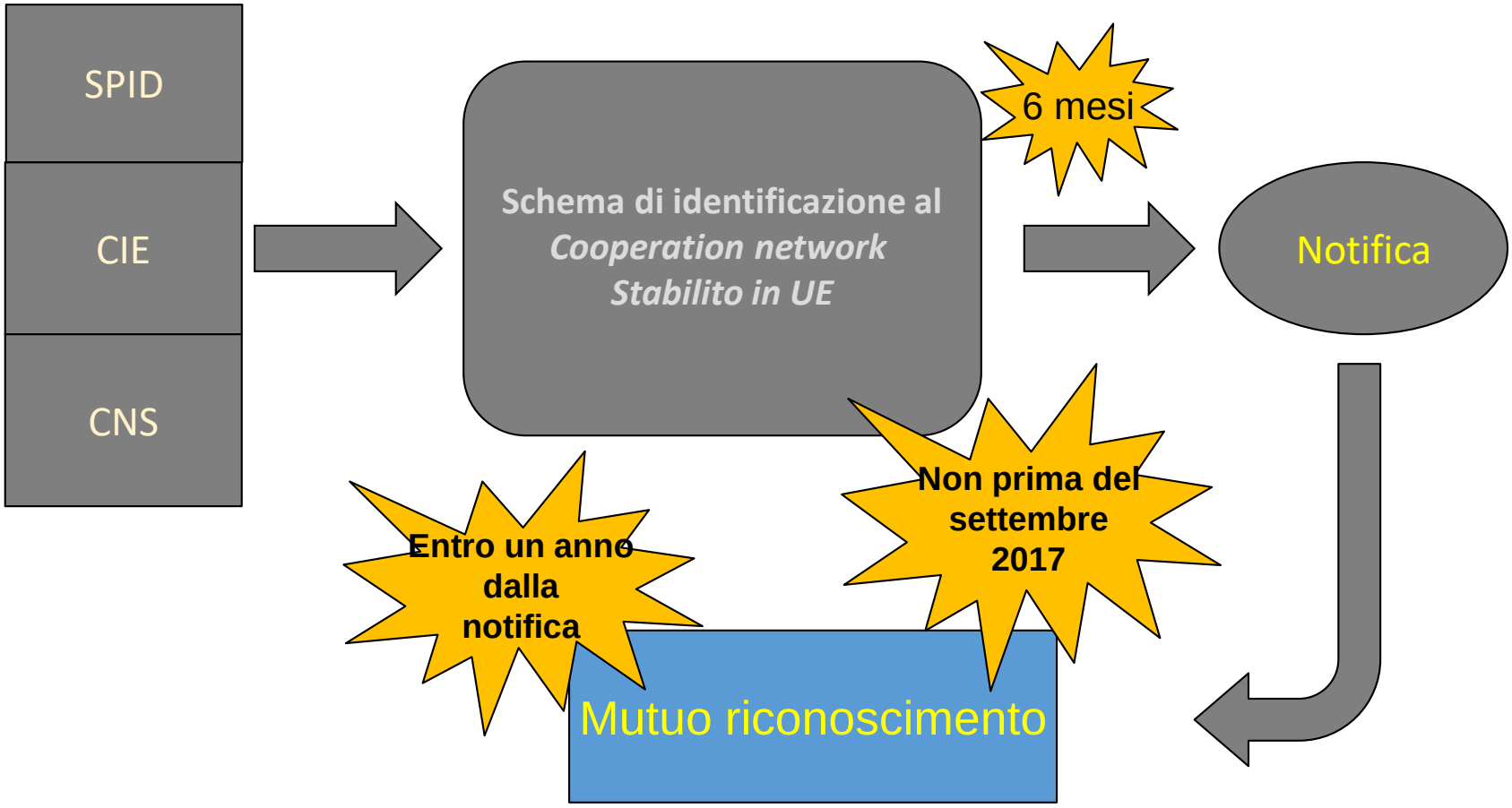
Standard per l'eID - 1

- Non è una standardizzazione delle identità attribuite dallo Stato membro.
- Lo scopo è quello di eliminare le barriere transfrontaliere dei mezzi di identificazione elettronica utilizzati negli Stati membri almeno per l'autenticazione nei servizi pubblici.
- Il meccanismo adottato è quello della conformità a regole generali che possono essere notificate alla Commissione UE che valuta la loro ammissibilità secondo le regole dell'articolo 7 del Regolamento eIDAS.
- In sostanza lo Stato membro notifica la descrizione, il tipo di vigilanza adottato, le responsabilità applicabili e i livelli di garanzia dei regimi/schemi di identificazione elettronica.

Standard per l'eID - 2

- Le regole di interoperabilità (web services SAML) sono mutuate dal Progetto pilota su larga scala della UE denominato STORK 2 (Secure idenTity acrOss boRders linKed).
- L'utilizzo di meccanismi basati sui web services e in particolare su SAML 2.0 rende il sistema SPID omogeneo con l'approccio comunitario.
- La norma tecnica di riferimento è la ISO/IEC 29115 e SPID nella propria normativa di riferimento fa esplicito riferimento ai livelli di garanzia 2, 3 e 4.
- Sono state avviate le attività per notificare SPID alla Commissione UE con la cosiddetta pre-notifica.

Il mutuo riconoscimento per l'identità elettronica



Identità digitale transnazionale

- **Se l'identificazione elettronica è prevista dalla Legge nazionale per accedere ad un servizio fornito da un soggetto pubblico in uno Stato membro, gli strumenti di identificazione di un altro Stato membro devono essere riconosciuti a condizione che:**
  - ✓ **gli strumenti di identificazione sono rilasciati nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione;**
  - ✓ **il livello di sicurezza sia corrispondente o superiore a quello richiesto dallo Stato membro al cui servizio si vuole accedere;**
  - ✓ **il livello di sicurezza sia effettivamente utilizzato per accedere al servizio.**

Argomenti

- **L’identità digitale nazionale.**
- **L’identità digitale in UE .**
- **Lo scenario di medio termine.**

SPID – Prospettive di medio e lungo termine

- **Non è definito se i cittadini dovranno pagare le credenziali SPID (gratuite certamente per il 2019).**
- **Le PPAA non devono nulla. I privati le tariffe pubblicate con la recente determinazione 366/2017.**
- **Se un servizio è disegnato per l'accesso tramite password/PIN non è complicato erogare il servizio tramite SPID.**
- **E' indispensabile una adeguata e forte partecipazione dei soggetti privati.**

Convenzione servizi per i soggetti privati

- **Determinazione AgID n. 366/2017 del 18 dicembre 2017.**
- **Profilazione dei servizi.**
- **Tariffe per i fornitori di servizio.**
- **Regole di ingaggio e pagamento per gli stakeholder.**

La convenzione

http://www.agid.gov.it/notizie/2018/02/07/spid-pubblicata-convenzione-lingresso-fornitori-servizi-privati.

- **Aggiornamento delle convenzioni pubblico e privato.**
- **Indicazioni sul pagamento delle tariffe demandate ad accordi tra gestori dell'identità.**
- **Responsabilità aggiornate per i soggetti coinvolti e sanzioni irrogate ai sensi dell'ultimo CAD. Minima 40.000 €, massima 400.000 €.**

Le tariffe

- **Articolo del docente con qualche dettaglio su scenari futuri.**

- **Il link all'articolo è il seguente:**

https://www.agendadigitale.eu/cittadinanza-digitale/identita-digitale/servizi-spid-dei-privati-cosa-comporta-la-convenzione-agid/

Lo scenario dei servizi forniti da privati

- **Le tariffe indicate e obbligatorie, anche con il periodo di «sconto» biennale sono giudicate alte da molti potenziali fornitori di servizi privati.**
- **Nel breve periodo potremo valutare chi aderisce a queste tariffe. Utilities, trasporti, banche, assicurazioni, ecc.**
- **Il mondo della Sanità privata si sta dimostrando «perplesso».**
- **Anche il mondo bancario/finanziario ci sta pensando.**

Siti di riferimento:

www.spid.gov.it

http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/spid

Il logo SPID è quello ufficiale del progetto.

Conclusioni

- **Il numero di credenziali rilasciate è lontano dagli obiettivi prefissati.**
- **Alla data circa il 90% delle credenziali è stato rilasciato da Poste Italiane.**
- **Quando tutte le PPAA erogheranno il loro servizi solamente tramite SPID non è definito.**
- **L'adesione dei soggetti privati a SPID è iniziata con Lottomatica.**

Contatti

Giovanni Manca
e-mail: mncgnn59@gmail.com