

Pordenone, 14 novembre 2014

Strumenti di identificazione in rete

SABRINA CHIBBARO
sabrina@chibbaro.net



"On the Internet, nobody knows you're a dog."

PII - "Personally Identifiable Information"

- ❖ Nel mondo digitale, l'identità è un'informazione univoca associata ad un soggetto.
- ❖ Può consistere in una o più caratteristiche inerenti a quel soggetto o a lui assegnate

Confini del concetto di PII

- ❖ qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione
- ❖ Le pronunce giudiziarie USA sono poco coerenti:
 - ❖ l'indirizzo IP non è PII perché identifica non una persona ma un computer (*Seattle Court, defendant Microsoft*)
 - ❖ il ZIP code è PII quando associato ad una transazione con carta di credito (*Tyler v. Michaels Stores, Inc., 2012*)
 - ❖ l'Android ID non è PII, sebbene sia univoco per ogni utente e dispositivo (*class action contro Cartoon Network, 2014*)

Identificazione e Autenticazione

- ❖ L'identificazione è il processo con cui l'utente dichiara la sua identità
- ❖ L'autenticazione è il processo di verifica dell'identificazione

I tre fattori di autenticazione

- ❖ Something you **know** (password, PIN)
- ❖ Something you've **got** (OTP, token, PKI)
- ❖ Something you **are** (biometria)

L'autenticazione dovrebbe essere richiesta solo ove strettamente necessario e il livello di autenticazione va commisurato al fattore di rischio

Single sign-on

- ❖ funzionalità che consente ad un utente di effettuare un'unica autenticazione per l'accesso a più applicazioni, servizi o risorse
- ❖ SSO centralizzato: database unico e centralizzato dell'intera utenza
- ❖ SSO federato: le identità sono gestite da diversi IdM systems e condivise da domini autonomi

Benvenuto
SABRINA CHIBBARO

 **Crediti formativi**



**Conservazione
a norma**



**Firma
Digitale**



**Segnalazioni
Antiriciclaggio**



**Banca Dati
Notarile**

QUICK MENU

digita...

 CERCA



AREA LAVORO

Antiriciclaggio

Area clienti Notartel

Aste

Conservazione a norma

Manuali e Istruzioni operative

Servizi di Posta

Servizi on line con la PA

Certification Authority di Servizio CAs

Dati Statistici Notarili

Marca Temporale

Processo Civile Telematico

Ristrutturazione debiti agricoli I.N.P.S.

Sistema Videoconferenza VDC/CNN

Studi di Settore

Firma Digitale

Rettifica Mod. F24 Tobin Tax 2013

Servizi anagrafici e ICI

Adempimenti telematici - Procedure di
emergenza

Entratel

Friuli Venezia Giulia - Libro Fondiario

Reti Amiche

Sister - Contact center

Sister

InfoCamere - Visure Camerali

InfoCamere - Pratiche telematiche

ComunicaStarweb

ACI - Visure automobilistiche

Archinota - Ricerca atti notarili

IPZS - Servizio inserzioni

Trento - Visure Catastali e Tavolari

Bolzano - Visure Catastali e Tavolari

Verifica Codice Fiscale

Verifica Partita IVA

Vincoli in rete

INI-PEC



AGORÀ



blog



forum sigillo



twitter



ANNUARIO

albo unico

altri organismi

annuario europeo



AGENDA UNICA

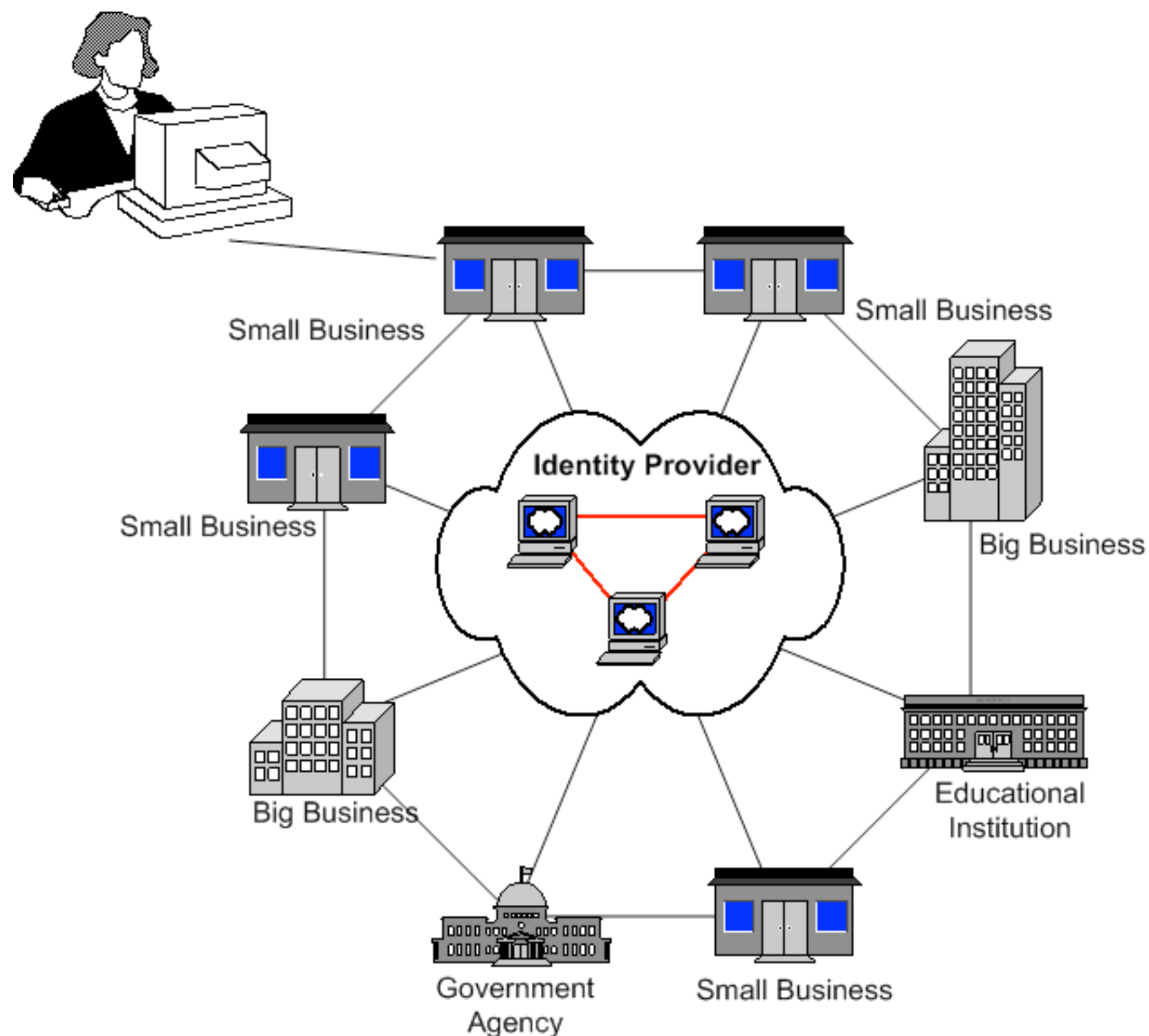
< Novembre 2014 >

L	M	M	G	V	S	D
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23

CHIUDI 

Identità federata

FIIdM
("federazione" di
identità) indica le
tecnologie e gli
standards che
servono a consentire
la portabilità delle
informazioni
relative all'identità
tra domini di
sicurezza distinti



Security Assertion Markup Language (SAML)

- ❖ è uno standard informatico aperto, basato su XML, per lo scambio di dati di autenticazione e autorizzazione (dette asserzioni) tra domini di sicurezza distinti basato su XML. Definisce tre ruoli:
 - ❖ Identity Provider (fornisce le informazioni sull'identità)
 - ❖ Service Provider (fornisce servizi)
 - ❖ Principal (utente)

Su richiesta del Principal, l'Identity Provider passa una asserzione SAML al Service Provider sulla base della quale quest'ultimo decide se permettere o negare l'accesso ai propri servizi al Principal.

Regolamento eIDAS

- ❖ Consente a persone fisiche e giuridiche di utilizzare gli strumenti di ID nazionali per accedere ai servizi pubblici negli altri paesi dell'unione europea dove tali strumenti sono disponibili
- ❖ Crea un mercato interno europeo per le firme digitali assicurando che saranno riconosciute oltre frontiera e siano equiparate alle firme autografe

eID - eTS

- ❖ Definisce tre di garanzia dei regimi di identificazione elettronica: basso, significativo ed elevato
- ❖ Firme elettroniche qualificate, sigilli elettronici, validazione temporale elettronica, servizi elettronici di recapito certificato, autenticazione dei siti web, documenti elettronici

Il progetto SPID

Il DL 21 giugno 2013, n. 69 ha modificato l'art. 64 del CAD

- ❖ **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', e' 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 e' costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia digitale, ..., 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.

SPID

I soggetti pubblici o privati che partecipano allo SPID sono:

- a) i gestori dell'identità digitale;
- b) i gestori degli attributi qualificati;
- c) i fornitori di servizi;
- d) l'Agenzia;
- e) gli utenti.

Ruolo dell'Agid

- ❖ 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

I gestori degli attributi qualificati

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

Sono accreditati di diritto i seguenti gestori di attributi qualificati:

a) ...;

b) i Consigli, gli Ordini e i Collegi delle professioni regolamentate relativamente all'**attestazione dell'iscrizione agli Albi professionali**;

c) le Camere di Commercio, industria e artigianato per l'**attestazione delle cariche e degli incarichi societari iscritti nel Registro delle imprese**;

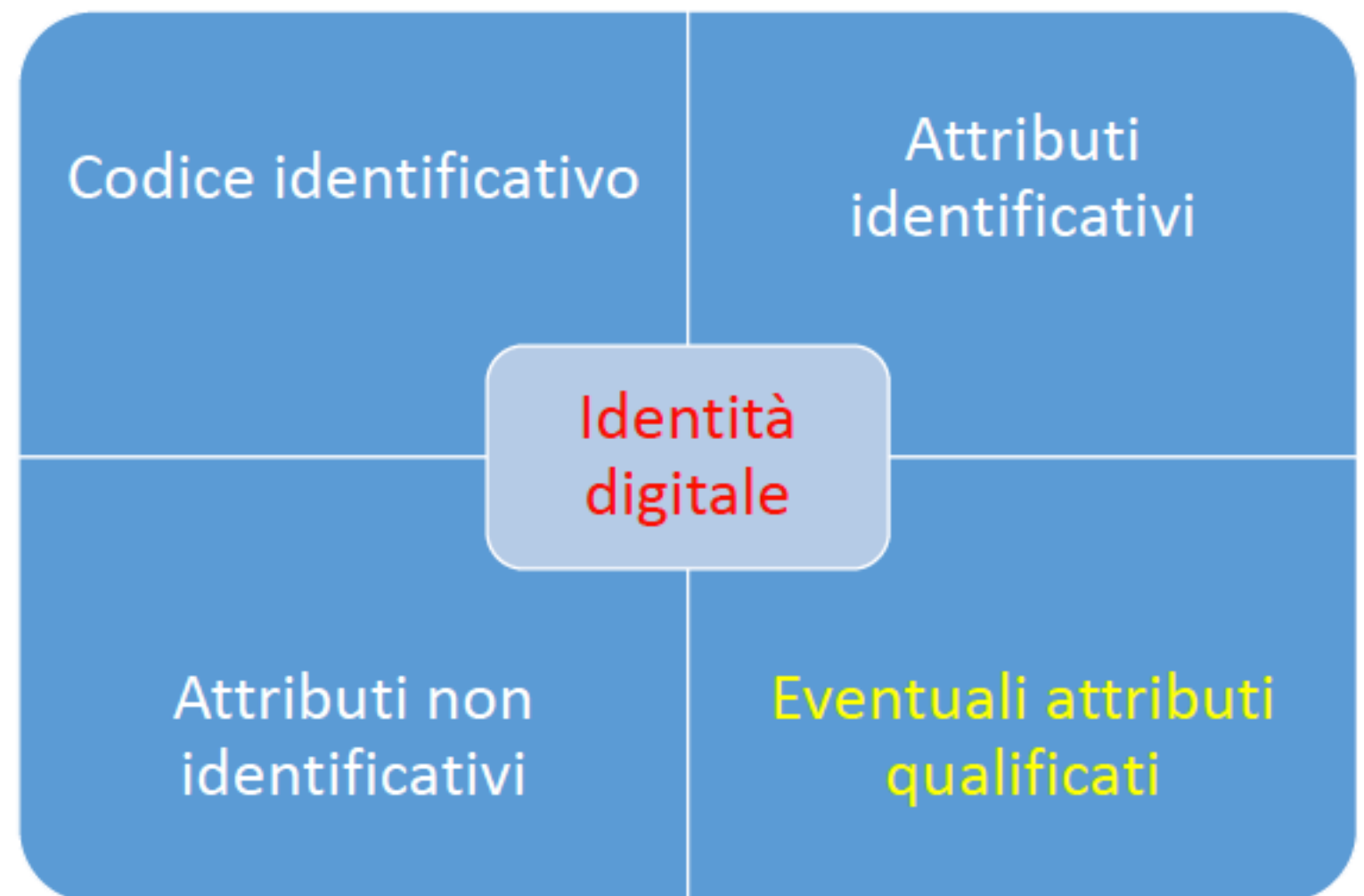
L'identità

attributi identificativi: nome, cognome, luogo e data di nascita, sesso, ovvero 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;

attributi qualificati: le qualifiche, le abilitazioni professionali e i poteri di rappresentanza.

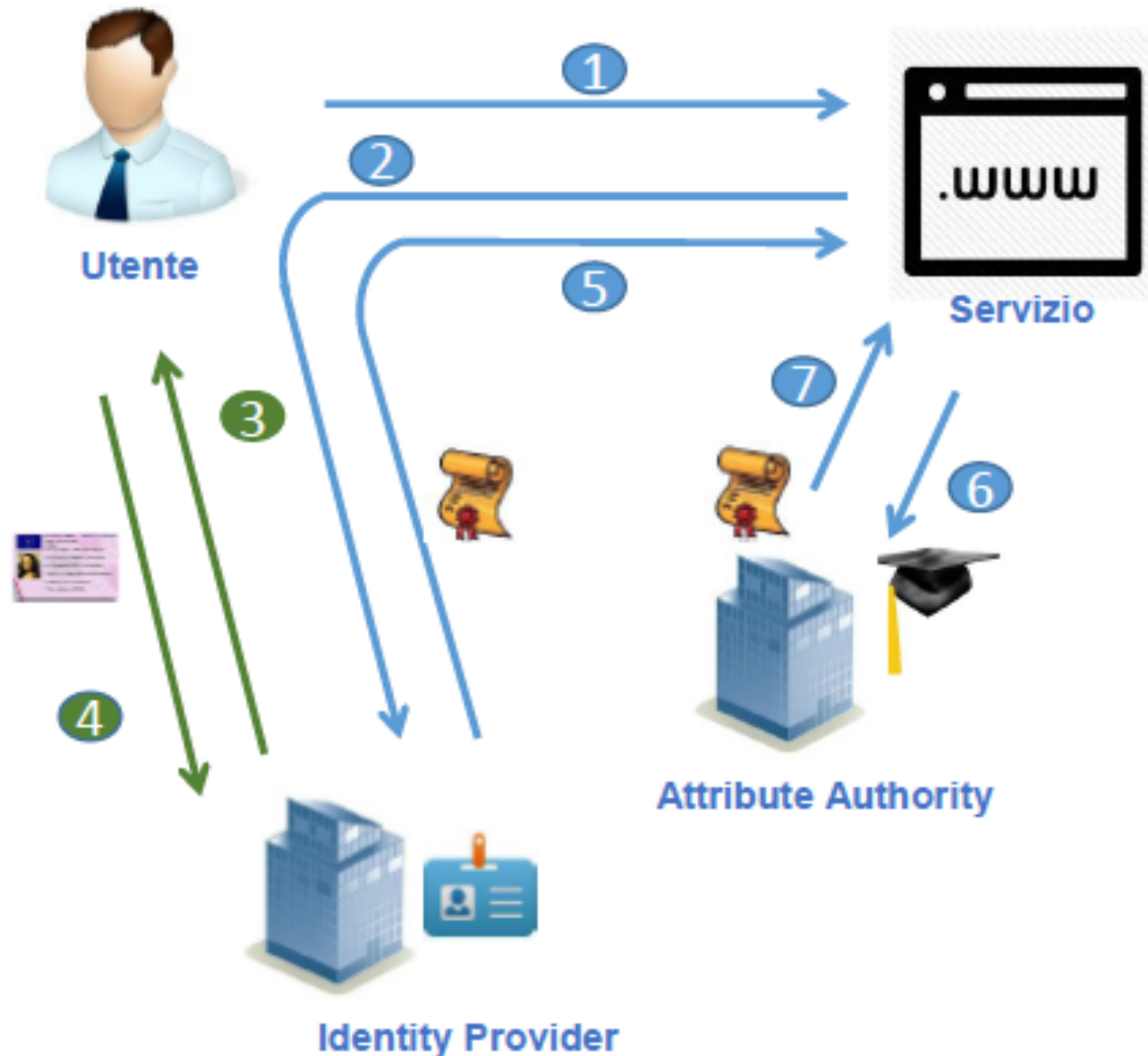
Possono essere già contenuti nell'identità digitale.



Livelli di sicurezza delle identità digitali

- ❖ **Primo livello:** sistemi di autenticazione informatica a un fattore (per esempio la password).
- ❖ **Secondo livello:** sistemi di autenticazione informatica a due fattori, non basati necessariamente su certificati digitali le cui chiavi private siano custodite su dispositivi sicuri.
- ❖ **Terzo livello:** sistemi di autenticazione informatica a due fattori basati su certificati digitali, le cui chiavi private siano custodite su dispositivi sicuri.

Schema di funzionamento



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

“All identity is ‘local’. The further away from a pre-specified business context an identity credential becomes, the less valuable it is.”

– *Dazza Greenwood*