Identità Digitale Pubblica (SPID): contesto tecnologico e normativo

Indice

Introduzione

- **SPID** (Sistema Pubblico per la gestione dell'Identità Digitale) : framework per la gestione dell'Identitità Digitale
- *E' definito come: «il sistema di autenticazione che permette a cittadini ed imprese di accedere ai servizi online della pubblica amministrazione e dei privati aderenti con un'identità digitale unica»*
- E' stato introdotto attraverso il decreto della Presidenza del Consiglio dei Ministri del 24 ottobre 2014, pubblicato sulla Gazzetta Ufficiale n. 285 del 9 dicembre 2014
- SPID è stato è stato progettato in conformità al descritto nel Regolamento Europeo n°910/2014 **eIDAS** (*electronic IDentification Authentication and Signature*) .

Attori del Sistema SPID

- **Utenti**, persone fisiche o giuridiche, che utilizzano SPID per l'autenticazione. Ogni utente può essere associato a uno o più ID, contenere informazioni riservate.
- **Identity Provider (IdP)**, che creano e gestiscono ID. Sono soggetti pubblici o privati certificati da una terza parte fidata.
- **Attribute Authorities (o Provider)**, che hanno il compito di certificare specifici attributi per gli utenti.
- **Service Provider (SP)**, organizzazioni pubbliche o private che forniscono un servizio agli utenti autorizzati.
- **Una terza parte fidata (TTP),** che garantisce i livelli standard di sicurezza richiesti da SPID e certifica le entità coinvolte.

Livelli di Sicurezza

- SPID è pensato per servizi a diverso livello di criticità
- In base al tipo di servizio gli SP possono richiedere un'autenticazione più o meno robusta
- Sono previsti 3 livelli di robustezza dell'autenticazione: SpidL1, SpidL2 e SpidL3

Protocollo Utilizzato

- Il Protocollo utilizzato da SPID è SAML 2.0
- SAML: *Security Assertion Markup Language* è basato su XML (standard OASIS da Maggio 2005)
- E’ basato sul concetto di *Assertion*, come security token per autenticare, associare ad un attributo o autorizzare un subject in scenari *cross-domain*, *single-sign-on (SSO)*
- E’ un protocollo *Web-based.*

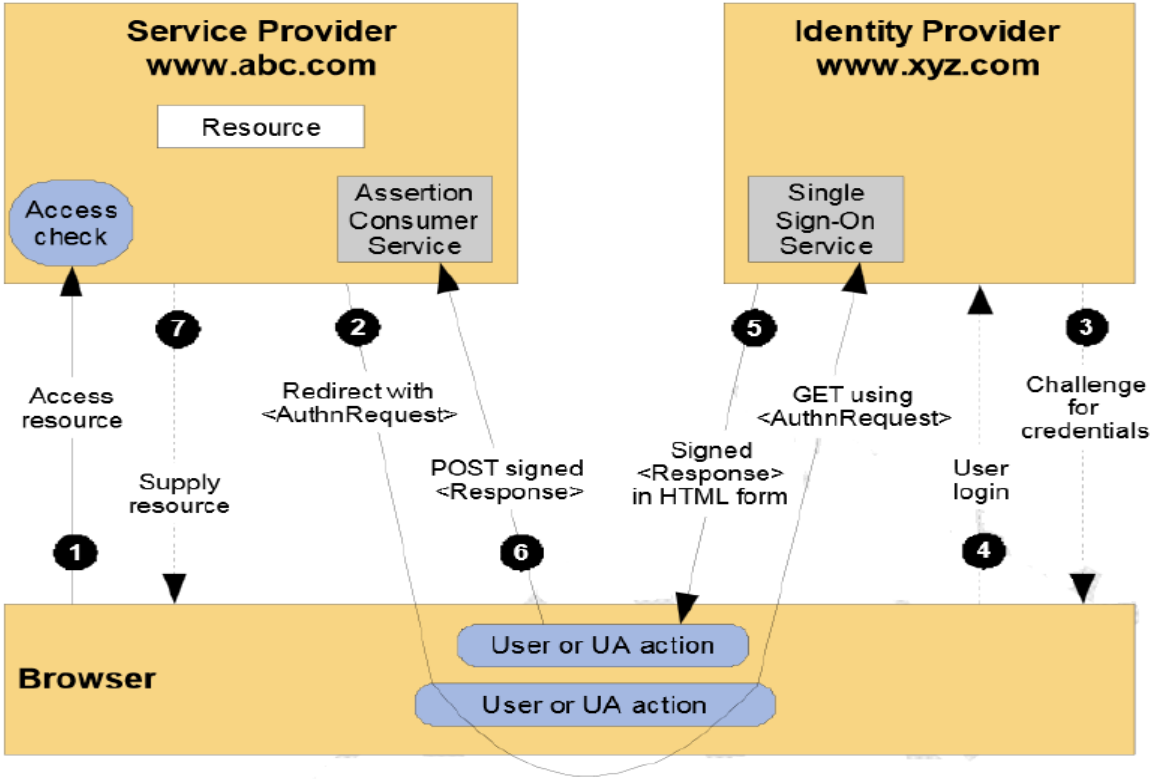
Identificazione Iniziale

- In un framework di identità digitale svolge un ruolo centrale la sicurezza del processo di identificazione iniziale
- Gli standard internazionali definiscono diversi livelli di sicurezza per tale processo (ad es. NIST)
- In SPID sono possibili diverse modalità, anche con verifica dei documenti da remoto

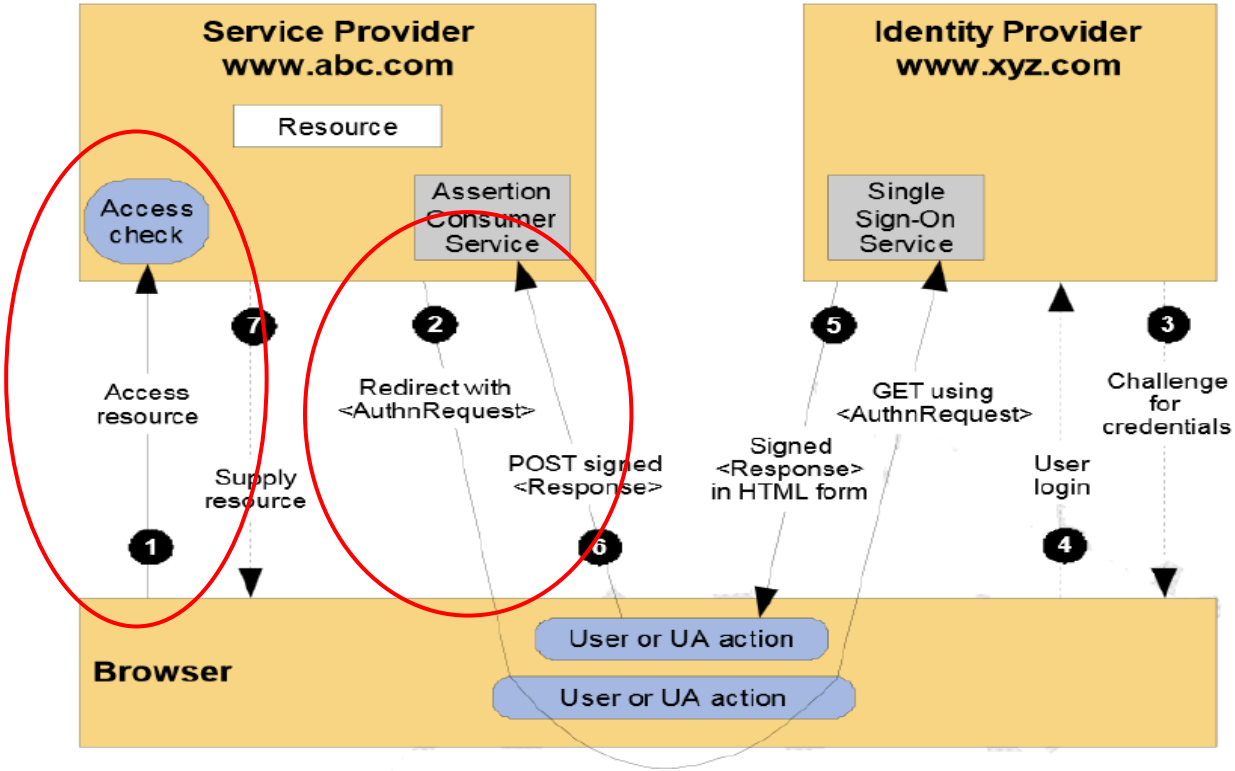
Federazione in SPID

- La federazione SPID è una federazione SAML 2
- E' costituita da:
  - **Attori**: utenti, IdP, SP, AA, TTP
  - **Assertion:** quali tipi di asserzioni sono usate (per SPID solo *Authentication* e *Attribute*)
  - **Protocolli**: Request e response per ottenere assertions e operare l'lidentity management
  - **Binding**: mapping tra protocolli SAML su messaggistica e protocolli standard di comunicazione
  - **Profili**: combinazione di Assertion, Protocolli e Binding per supportare i diversi usecase
  - **Authentication Context**: informazioni sul tipo e la robustezza del processo di autenticazione
  - **Federation Registry:** registro centrale delle entità
  - **Metadata** (IdP, SP e AA): descrizione delle entità e dati di configurazione (es. un IdP deve decidere se accettare o no richieste non firmate dagli SP, etc.)

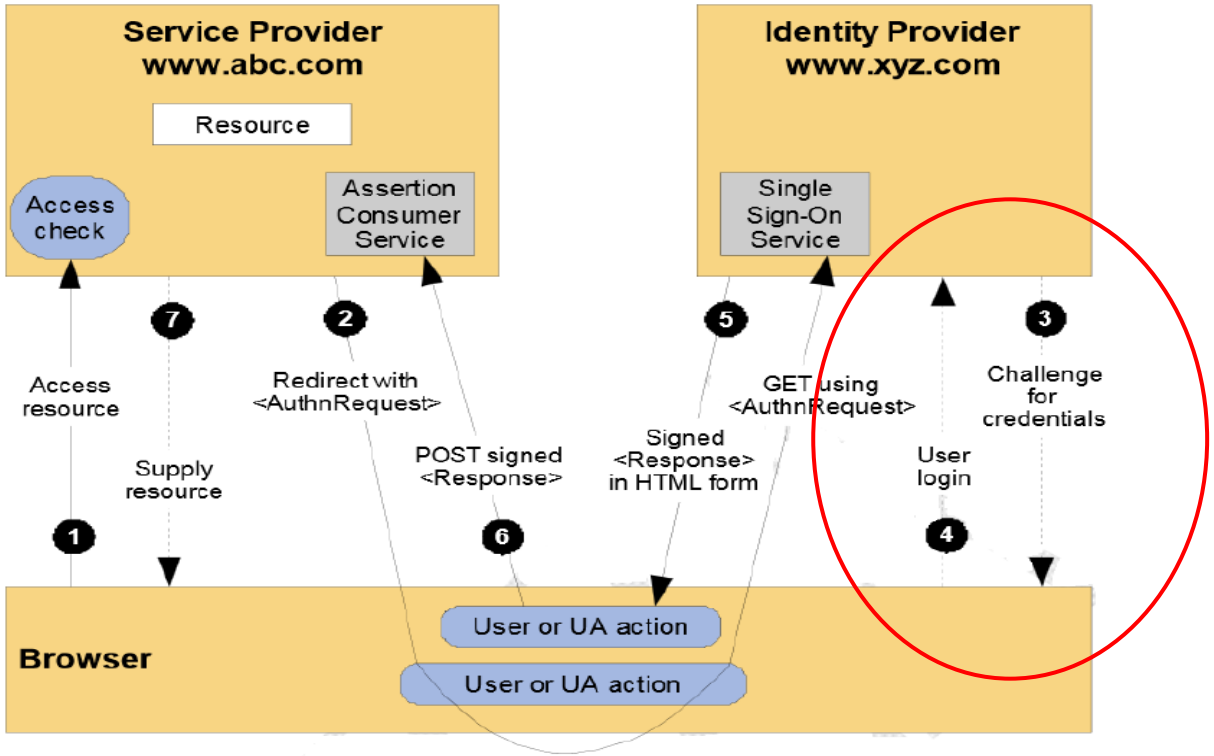
Processo di autenticazione in SPID



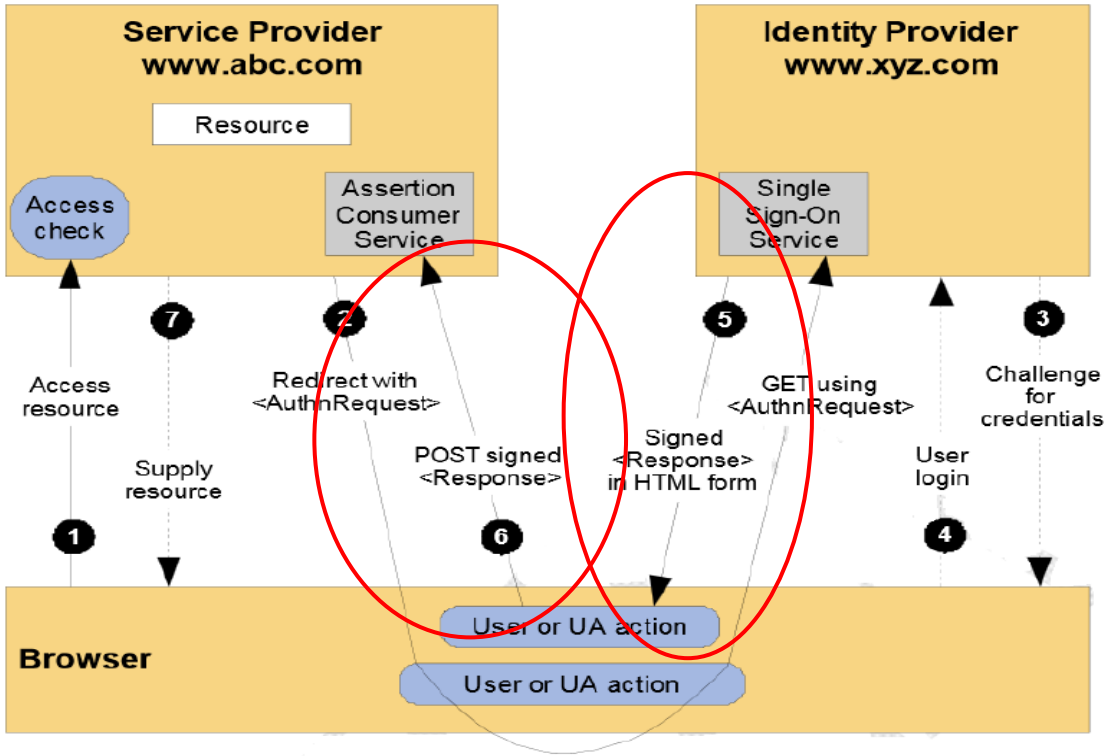
Processo di autenticazione in SPID



Processo di autenticazione in SPID



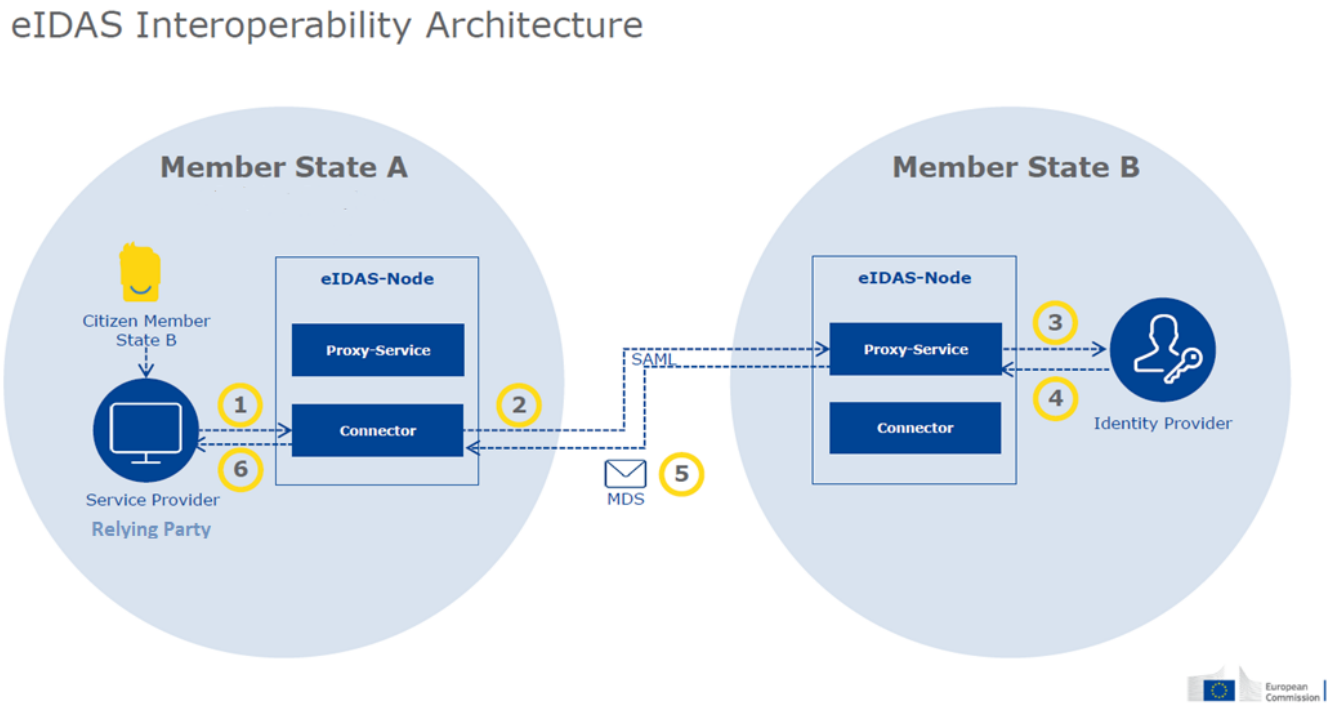
Processo di autenticazione in SPID



Interoperabilità Europea

- eIDAS Interoperability Architecture, versione 1.2, 31 27 settembre 2019 (eIDAS Technical Specifications)
- Regole e infrastruttura per l'interoperabilità: i cittadini potranno autenticarsi presso SP esteri sulla base dei propri IdP
- L'architettura si basa sulla presenza di nodi eIDAS che interconnettono i domini nazionali

Processo di autenticazione



Sicurezza del Sistema SPID

- Gli IdP sono attori critici, assunti trusted
- Gli IdP devono garantire stringenti requisiti sia per l'accreditamento che in fase di esercizio, come stabilito dal:
  - Regolamento AGID RECANTE LE MODALITÀ PER L'ACCREDITAMENTO E LA VIGILANZA DEI GESTORI DELL'IDENTITA' DIGITALE (articolo 1, comma 1, lettera l) , DPCM 24 ottobre 2014)
- Anche i SP possono hanno un ruolo rilevante per la sicurezza del sistema

Conclusioni

- L’identità digitale pubblica è uno strumento fondamentale per l’erogazione di servizi di e-government (e non solo)
- L’interoperabilità al livello almeno europeo rappresenta un fattore abilitante
- L’identità digitale pubblica si presta a diverso scenari innovativi di utilizzo (es. integrazione in soluzioni blockchain-based, controllo fisico dell’accesso, firma elettronica avanzata, etc.)

Approfondimento 1: introduzione

- **SPID** (Sistema Pubblico per la gestione dell'Identità Digitale) è uno strumento che prevede il rilascio e la gestione di identità digitali al fine di consentire ai Fornitori di servizi che aderiscono al sistema la possibilità di identificare i propri utenti attraverso un meccanismo di autenticazione federata.
- I sistemi di autenticazione federata sono fondati su un insieme di standard, tecnologie ed protocolli che permettono ad un insieme di Service Providers (SP) – Fornitori di Servizio -- di avvalersi dell'autenticazione che gli utenti effettuano presso gli Identity Providers (IdP) – Gestori dell'Identità Digitale. Questi ultimi svolgono il ruolo di gestori dell'identità digitale degli utenti, facendosi pertanto garanti della loro identità durante il processo di autenticazione presso i servizi forniti dai Service Provider. L'insieme delle organizzazioni formate da SP e IdP forma la Federazione.
- Con il decreto della Presidenza del Consiglio dei Ministri del 24 ottobre 2014, pubblicato sulla Gazzetta Ufficiale n. 285 del 9 dicembre 2014 è stata avviata l'attuazione del sistema SPID che rappresenta "*il sistema di autenticazione che permette a cittadini ed imprese di accedere ai servizi online della pubblica amministrazione e dei privati aderenti con un'identità digitale unica*". SPID è stato è stato progettato in conformità al descritto nel Regolamento Europeo n°910/2014 **eIDAS** (*electronic IDentification Authentication and Signature*) .
- eIDAS è un provvedimento normativo direttamente applicabile negli Stati Membri (essendo un Regolamento) senza necessità di esplicito recepimento. La finalità di questo Regolamento è quello di permettere la diffusione delle transazioni digitali nei Paesi dell'Unione Europea, fornendo "*una base normativa comune per interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni*". Tra le altre cose eIDAS fornisce un quadro di riferimento per firme elettroniche, per la firma di documenti informatici e identità digitale per l'interazione online tra cittadini, imprese e Pubblica Amministrazione. Secondo eIDAS, « l'Identificazione elettronica» è il "*processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica*", realizzato attraverso un "mezzo di identificazione elettronica" e cioè "*un'unità materiale e/o immateriale contenente dati di identificazione personale, utilizzata per l'autenticazione nei servizi online*". eIDAS è un Regolamento che rispetta il principio della neutralità tecnologica, per cu ogni stato membro può scegliere la tecnologia con cui attuare l'identità digitale pubblica. Sono tuttavia imposti, attraverso ulteriori provvedimenti normativi tecnologici, stringenti vincoli di interoperabilità tra gli Stati.
- Le tecniche e protocolli su cui si basa SPID sono già stati sperimentati a livello europeo e adottate dai progetti sperimentali Stork e Stork II (Secure idenTity acrOss boRders linKed).

Approfondimento 2: Attori

- **Gli attori dell'ecosistema di SPID sono:**
  - *Utenti*, persone fisiche o giuridiche che utilizzano il sistema SPID per accedere a servizi della Pubblica Amministrazione o di Imprese. Ogni utente può essere associato a uno o più ID SPID.
  - *Identity Provider*, che creano e gestiscono identità digitali nel sistema SPID. Sono soggetti privati o pubblici accreditati da una terza parte fidata.
  - *Service Provider* (Fornitori di servizi), organizzazioni pubbliche o private registrati nella federazione che forniscono servizi agli utenti autorizzati identificati attraverso SPID
  - *Attribute Provider*, che certificano un particolare insieme di attributi qualificati (come il possesso di un diploma, l'appartenenza a un corpo professionale, ecc.) relativi a utenti che possiedono un'identità digitale. Esempi di Attribute Provider sono Ordini e collegi professionali, Camere di Commercio, Ministero dello Sviluppo Economico, etc.
  - Una Terza *parte fidata* (TTP), che garantisce i livelli standard di sicurezza richiesti da SPID e accredita le entità coinvolte (nel concreto, in Italia, la TTP è AGID: Agenzia per l'Italia digitale).

Approfondimento 3: livelli di sicurezza

- Il sistema SPID prevede tre diversi livelli di sicurezza per l'autenticazione informatica. I service Provider possono scegliere, servizio per servizio, quale dei tre livelli richiedere per l'accesso al servizio. Come vedremo, l'identificazione di un utente da parte di un Service Provider richiede una contestuale autenticazione dell'utente presso un Identity Provider. Il livello di sicurezza richiesto, quindi, si mappa sul livello di sicurezza dell'autenticazione presso l'Identity Provider richiesta per l'accesso al servizio.
  - Nel primo livello, l'Identity Provider rende disponibili sistemi di autenticazione informatica ad un fattore (ad esempio username e password). Tale livello corrisponde al "Level of Assurance LoA2" dello standard ISOIIEC DIS 29115;
  - Nel secondo livello l'Identity Provider rende disponibili sistemi di autenticazione informatica a due fattori, non basati necessariamente su certificati digitali. Tale livello corrisponde al "Level of Assurance LoA3" dello standard ISOIIEC DIS 291 15;
  - Nel terzo livello l'Identity Provider rende disponibili sistemi di autenticazione informatica basati su certificati digitali, le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999193lCE del Parlamento europeo. Tale livello corrisponde al "Level of Assurance LoA4" dello standard ISOIIEC DIS 291 15.
-

Approfondimento 4: SAML

- Il framework del Sistema Pubblico di Identità Digitale (SPID), dal punto di vista tecnologico, è basato sul protocollo di autenticazione /autorizzazione Security Assertion Markup Language (SAML) versione 2.
- SAML è un formato di dati open-standard basato su XML per lo scambio di dati di autenticazione e autorizzazione tra un Identity Provider e un Service Provider.
- Il meccanismo su cui si basa il protocollo è lo scambio di token di sicurezza.
- SAML supporta autenticazioni via web tramite cross-domain single sign-on e permette di ridurre il sovraccarico dovuto alla distribuzione di più token di autenticazione tra gli utenti.
- I messaggi SAML brevi possono essere inviati in modalità HTTP GET se di lunghezza inferiore ai limiti imposti per gli URL, mentre quelli più lunghi devono essere trasmessi attraverso HTTP POST Binding.
- Il primo step per l'utente è registrarsi presso un Identity Provider
- L'IdP identifica l'utente e rilasciare un'identità digitale SPID insieme alle credenziali di sicurezza per diversi livelli di assurance visti prima.

Approfondimento 5: livelli si assurance NIST per identificazione

- NIST Special Publication 800-63 (Revision 3): Digital Identity Guidelines
- IAL: *Identity Assurance Level (si riferisce al processo di identificazione), che viene considerato separato da quello di autenticazione (i cui livelli sono indicati dall'acronimo AAL). Si noti che i livelli SPID che vedremo successivamente sono riferiti all'autenticazione, non all'identificazione*
- *Gli IAL previsti sono 3 e definiti come segue:*
  - **"IAL1**: There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted or should be treated as such (including attributes a Credential Service Provider, or CSP, asserts to an RP).
  - **IAL2**: Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing. Attributes can be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.
  - **IAL3**: Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the CSP. As with IAL2, attributes can be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes."
- Il Sistema SIPD è quindi ricondicibile al livello IAL2 per quanto concerne il processo di identificazione.

Approfondimento 6: verifica identità

- La verifica dell'identita' del soggetto richiedente e la richiesta di adesione al sistema SPID da parte degli utenti avvengono in uno dei seguenti modi:
  - a) identificazione del soggetto richiedente che sottoscrive il modulo di adesione allo SPID, tramite esibizione a vista di un valido documento d'identita' e, nel caso di persone giuridiche, della procura attestante i poteri di rappresentanza;
  - b) identificazione informatica tramite documenti digitali di identita', validi ai sensi di legge, che prevedono il riconoscimento a vista del richiedente all'atto dell'attivazione, fra cui la tessera sanitaria-carta nazionale dei servizi (TS-CNS), CNS o carte ad essa conformi;
  - c) identificazione informatica tramite altra identita' 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 fornita da 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 per SPID
- L’identificazione a vista della persona fisica richiedente un’identità SPID da parte del gestore dell’identità può essere effettuata dai gestori dell’identità digitale anche **in digitale da remoto tramite strumenti di registrazione audio/video nel rispetto del decreto legislativo 30 giugno 2003, n.196.**

Approfondimento 7: identificazione da remoto (regolamento ai sensi dell'articolo 4, comma 2, DPCM 24 ottobre 2014) 1/2

- Il gestore deve implementare un sistema che garantisca, preliminarmente all'instaurazione della sessione audio/video, la cifratura del canale di comunicazione mediante l'adozione di meccanismi standard, applicativi e protocolli aggiornati alla versione più recente. Inoltre deve garantire l'utilizzo di applicativi orientati all'usabilità e all'accessibilità da parte dell'utente.
- L'identificazione da remoto deve avvenire in una modalità tale da consentire la raccolta di elementi probanti, utili in caso di un eventuale disconoscimento dell'identità da parte dell'utente nel rispetto delle seguenti condizioni:
  - a) le immagini video devono essere a colori e consentire una chiara visualizzazione dell'interlocutore in termini di luminosità, nitidezza, contrasto, fluidità delle immagini;
  - b) l'audio deve essere chiaramente udibile, privo di evidenti distorsioni o disturbi.
  - c) la sessione audio/video, che ha ad oggetto le immagini video e l'audio del soggetto richiedente l'identità e dell'operatore, deve essere effettuata in ambienti privi di particolari elementi di disturbo.

- Il gestore è responsabile della valutazione in merito alla sussistenza delle condizioni suddette e l'operatore preposto all'attività può sospendere o non avviare il processo di identificazione nel caso in cui la qualità audio/video sia scarsa o ritenuta non adeguata a consentire la verifica dell'identità del soggetto.
- L'operatore che effettua l'identificazione accerta l'identità del richiedente tramite la verifica di un documento di riconoscimento in corso di validità, purché munito di fotografia recente e riconoscibile e firma autografa del richiedente stesso, rilasciato da un'Amministrazione dello Stato e verifica il codice fiscale tramite la tessera sanitaria in corso di validità.
- L'operatore che effettua l'identificazione può escludere l'ammissibilità della sessione audio/video per qualunque ragione, inclusa l'eventuale inadeguatezza del documento presentato dal richiedente (ad esempio perché logoro o carente delle caratteristiche elencate).
- La sessione audio/video è interamente registrata e conservata per venti anni decorrenti dalla scadenza o dalla revoca dell'identità digitale con modalità crittografiche atte a garantirne l'accesso esclusivamente dietro richiesta dell'autorità giudiziaria, dell'Agenzia nel corso delle attività di vigilanza, dell'utente e dell'autorità giudiziaria in caso di disconoscimento della stessa.

Approfondimento 8: identificazione da remoto (regolamento ai sensi dell'articolo 4, comma 2, DPCM 24 ottobre 2014) 2/2

- La sessione audio/video deve essere condotta seguendo una procedura scritta e formalizzate dal gestore che prevede almeno le seguenti attività:
  - a) l'acquisizione del consenso, **qualora necessario**, alla videoregistrazione e alla sua conservazione per 20 anni come previsto dalla normativa vigente in materia. L'operatore informa che la videoregistrazione sarà conservata in modalità protetta;
  - b) l'operatore dichiara i propri dati identificativi;
  - c) il soggetto conferma le proprie generalità;
  - d) il soggetto conferma la data e l'ora della registrazione;
  - e) il soggetto conferma di volersi dotare di un'identità digitale e conferma i dati inseriti nella modulistica online in fase di pre-registrazione;
  - f) il soggetto conferma il proprio numero di telefonia mobile e l'indirizzo mail;
  - g) l'operatore invia un sms che il soggetto richiedente è tenuto a esporre al dispositivo di ripresa e una mail all'indirizzo di posta elettronica dichiarato, con un link ad una URL appositamente predisposta per la verifica;
  - h) l'operatore chiede e ottiene conferma dal soggetto circa la conoscenza delle tipologie di credenziali di cui disporrà per l'accesso ai servizi in rete;
  - i) l'operatore chiede di inquadrare, fronte e retro, il documento di riconoscimento utilizzato dal soggetto, assicurandosi che sia possibile visualizzare chiaramente la fotografia e leggere tutte le
  - informazioni contenute nello stesso (dati anagrafici, numero del documento, data di rilascio e di scadenza, amministrazione rilasciante);
  - j) l'operatore chiede di mostrare la tessera sanitaria su cui è riportato il codice fiscale del soggetto;
  - k) il soggetto conferma di aver preso visione e di accettare le condizioni contrattuali e d'uso disponibili sul sito web del gestore di identità;
  - l) l'operatore chiede al soggetto di compiere una o più azioni casuali volte a rafforzare l'autenticità della richiesta;
  - m) l'operatore riassume sinteticamente la volontà espressa dal soggetto di dotarsi di identità digitale e raccoglie conferma dallo stesso.
  - I dati di registrazione, costituiti da file audio-video, immagini e metadati strutturati in formato elettronico, vengono conservati a norma di legge

Approfondimento 9: Federation Registry

- Il Federation Registry contiene tutte le informazioni relative agli Identity Provider accreditati dall'Agenzia per l'Italia Digitale). Per ogni entità, il registro contiene una voce ***AuthorityInfo***

- • ***AuthorityInfo*** *entry del registro relativa ad una entità; a sua volta costituita da:*
  - • ***EntityId :*** *identificatore SAML dell'entità;*
  - • ***Soggetto:*** *denominazione del soggetto a cui afferisce l'entità della federazione;*
  - • ***EntityType:*** *tipo di entità (Identity Provider, Attribute Authority, Service Provider);*
  - • ***MetadataProviderURL:*** *l'URL del servizio di reperimento metadati;*
  - • ***AttributeList:*** *elenco di attributi qualificati certificabili da una entità di tipo Attribute Authority.*

- Esiste un metodo HTTP-GET per l'accesso al Federation Registry che fa parte dell'interfaccia *IRegistryAccess*. Il metodo riceve come input un entityID, un authorityType, oppure, un attributeType per selezionare un'entità in grado di certificare un particolare attributo qualificato. Il risultato è fornito attraverso un file XML firmato da AGID.
- E' supportato anche l'accesso LDAP.

Approfondimento 10: Identity Provider Metadata

- Le caratteristiche dell'*Identity Provider* devono essere definite attraverso *metadata* conformi allo standard SAML v2.0 :
  - *Nell'elemento <**EntityDescriptor**> devono essere inclusi almeno i seguenti componenti:*
    - *un attributo **entityID** indicante l'identificativo (URI) dell'entità, univoco in ambito SPID;*
    - *l'elemento **<IDPSSODescriptor>** specifico che contraddistingue l'entità di tipo Identity provider deve riportare i seguenti attributi:*
      - ***protocolSupportEnumeration**: che enumera gli URI indicanti i protocolli supportati dall'entità (poiché si tratta di un'entità SAML 2.0, deve indicare almeno il valore del relativo protocollo: "urn:oasis:names:tc:SAML:2.0:protocol");*
      - ***WantAuthnRequestSigned**: attributo con valore booleano che, quando è true impone ai service provider che fanno uso di questo Identity Provider l'obbligo della firma delle richieste di autenticazione;*
      - *un elemento <**KeyDescriptor**> che contiene l'elenco dei certificati e delle corrispondenti chiavi pubbliche dell'entità, utili per la verifica della firma dei messaggi prodotti da tale entità nelle sue interazioni con le altre*
      - *un elemento <**NameIDFormat**> riportante l'attributo che specifica il formato con cui indicare il nome del subject a cui si riferisce l'assertion*
      - *uno o più elementi<**SingleSignOnService**> che specificano l'URL del Single Sign-On Service per ricevere le richieste e il tipo di binding (POST o REDIRECT)*
      - *uno o più elementi <**attribute**> ad indicare nome e formato degli attributi certificabili dell'Identity provider*
      - *un elemento <**Signature**> riportante la firma detached sui metadata . La firma deve essere prodotta utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore;*
      - *opzionalmente (ma consigliato), un elemento <**Organization**> che indica l'organizzazione (name, URL) a cui afferisce l'entità specificata.*

- I ***metadata Identity Provider** sono disponibili per tutte le entità SPID federate attraverso l'interfaccia **IMetadataRetrive** alla URL https://<dominioGestoreIdentita>/metadata, ove non diversamente specificato nel Registro SPID, e sono firmate in modalità detached dall'Agenzia per l'Italia Digitale. L'accesso deve essere effettuato utilizzando il protocollo TLS nella versione più recente disponibile.*

Approfondimento 11: Service Provider Metadata

- Le caratteristiche del *Service Provider* devono essere definite attraverso *metadata* conformi allo standard SAML v2.0 :
  - *Nell'elemento <**EntityDescriptor**> devono essere inclusi almeno i seguenti componenti:*
    - *un attributo **entityID** indicante l'identificativo (URI) dell'entità, univoco in ambito SPID;*
    - *l'elemento **<SPSSODescriptor>** specifico che contraddistingue l'entità di tipo Service Provider deve riportare i seguenti attributi:*
      - ***protocolSupportEnumeration**: che enumera gli URI indicanti i protocolli supportati dall'entità (poiché si tratta di un'entità SAML 2.0, deve indicare almeno il valore del relativo protocollo: "urn:oasis:names:tc:SAML:2.0:protocol");*
      - ***WantAuthnRequestSigned**: attributo con valore booleano che, quando è true impone ai service provider che fanno uso di questo Identity Provider l'obbligo della firma delle richieste di autenticazione;*
      - *un elemento <**KeyDescriptor**> che contiene l'elenco dei certificati e delle corrispondenti chiavi pubbliche dell'entità, utili per la verifica della firma dei messaggi prodotti da tale entità nelle sue interazioni con le altre*
      - *uno o più elementi<**AssertionConsumerService**> che specificano l'URL a cui contattare il Service Provider per l'invio di risposte SAML e il tipo di binding fissato a POST*
      - *uno o più elementi <**AttributeConsumingService**> che descrive il set di attributi richiesti dal Service Provider con l'identificazione del set minimo e del set richiesto (attraverso un attributo **index** -- riferito dalla **AuthReq** --che individua l'i-mo servizio, il sottoelemento <**ServiceName**> per il set minimo associato all'i-mo servizio e il sottoelemento <**RequestedAttribute**> per gli attributi associati all''i-mo servizio)*
      - *un elemento <**Signature**> riportante la firma detached sui metadata . La firma deve essere prodotta utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore;*
      - *opzionalmente (ma consigliato), un elemento <**Organization**> che indica l'organizzazione (name, URL) a cui afferisce l'entità specificata.*

- I ***metadata Iservice Provider** sono disponibili per tutte le entità SPID federate attraverso l'interfaccia **IMetadataRetrive** alla URL https://<dominioGestoreIdentita>/metadata, ove non diversamente specificato nel Registro SPID, e sono firmate in modalità detached dall'Agenzia per l'Italia Digitale. L'accesso deve essere effettuato utilizzando il protocollo TLS nella versione più recente disponibile.*

Approfondimento 12: AuthRequest

- In primo luogo, l'utente utilizzando un browser (User Agent) invia al Service Provider una richiesta per accedere ad un determinato servizio (Step 1). Quindi il Service Provider inoltra all'Identity Provider (indicato dall'utente) una richiesta di autenticazione attraverso il browser (Step 2). La informazioni principali della richiesta di autenticazione **AuthnRequest** sono le seguenti:

- ***<AuthnRequest** > è un messaggio che contiene quanto segue:*
  - *un attributo univoco **ID**. Esso è generalmente ottenuto dalla combinazione origine e timestamp della richiesta (quest'ultimo generato con una precisione di almeno un millesimo di secondo per evitare replay attack);*
  - *un attributo **Version**, che indica la versione della specifica SAML adottata (che deve valere sempre 2);*
  - *un attributo **IssueInstant**, che specifica l'istante in cui la richiesta è stata rilasciata in formato UTC;*
  - *un attributo **Destination**, a indicare l'URI a cui è inviata la richiesta;*
  - *un attributo booleano **ForceAuthn**, true solo nel caso di autenticazioni SpidL2 o SpidL3;*
  - *un attributo **AssertionConsumerServiceIndex** (eventualmente sostituito da una coppia di attributi **AssertionConsumerServiceURL** e **ProtocolBinding***) che ha lo scopo di comunicare l'URL del servizio cui deve essere inviata la risposta alla richiesta di autenticazione e il tipo di binding *(GET o POST)* da utilizzare.
  - *un attributo opzionale **AttributeConsumingServiceIndex**, che specifica gli attributi che devono essere attestati nell'asserzione;*
  - *un elemento opzionale <**Subject**>, che identifica la persona che ha richiesto la procedura di autenticazione;*
  - *un elemento <**Issuer**>, che rappresenta il Service Provider;*
  - *un elemento <**NameIDPolicy**>, che definisce il formato del name identifier che l'Identity Provider deve usare nella risposta;*
  - *un elemento opzionale <**Conditions**>, che specifica il tempo di validità (notBefore, notAfter in UTC) – si noti che l'IdP non è obbligato a tener conto di questo vincolo;*
  - *un elemento <**RequestedAuthnContext**>, che indica la robustezza delle credenziali richieste SpidL1, SpidL2 o SpidL3 e* il metodo per stabilire il rispetto del vincolo (valori ammessi "*exact*", "*minimum*", "*better*", "*maximum*").
  - *un elemento <**Signature**> presente nel caso di binding HTTP POST, contenente la firma detached del Service Provider con chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore.*
  - *Un elemento opzionale <**Scoping**> per la delega dell'autenticazione e uno o più elementi <**RequesterID**> ad essa correlati. Al momento questi elementi non devono essere utilizzati, sono previsti dalle regole tecniche solo per scopi futuri.*

Approfondimento 13: challenge-response

- Se la richiesta è valida, l'Identity Provider esegue il processo di autenticazione con l'utente (Step 3 e 4). Nel caso in cui l'autenticazione viene eseguita con successo, il Gestore dell'identità digitale prepara la dichiarazione di autenticazione dell'utente per il Fornitore dei servizi, chiamata ***Assertion***.
- Il Processo di autenticazione con l'utente dipende dal LoA richiesto (SpidL1, SpidL2, SpidL3), attraverso l'elemento: <***RequestedAuthnContext***>

Approfondimento 14: Response

- A questo punto, l'Identity Provider restituisce all'User Agent il messaggio **Response** contenente l'**Assertion** (Step 5), che viene inoltrato al Service Provider tramite HTTP POST Binding (Step 6).

- *⟨**Response**⟩ contiene i seguenti campi:*
  - *un attributo univoco **ID** generato allo stesso modo dell'AuthRequest;*
  - *un attributo **Version**, che indica la versione della specifica SAML adottata (obbligatoriamente 2.0);*
  - *un attributo **IssueInstant**, che indica l'istante di emissione della richiesta, in formato UTC;*
  - *un attributo **InResponceTo**, che fa riferimento all'ID della richiesta a cui si risponde;*
  - *un attributo **Destination**, a indicare l'URI a cui la risposta deve essere inviata;*
  - *un elemento ⟨**Status**⟩, che specifica l'esito della richiesta (ad esempio, successo);*
  - *un elemento ⟨**Issuer**⟩, che rappresenta l'Identity Provider;*
  - *un elemento ⟨**Assertion**⟩, solo se l'autenticazione ha avuto successo, definita come segue (prossima slide);*
  - *Può esservi l'elemento ⟨**Signature**⟩.*

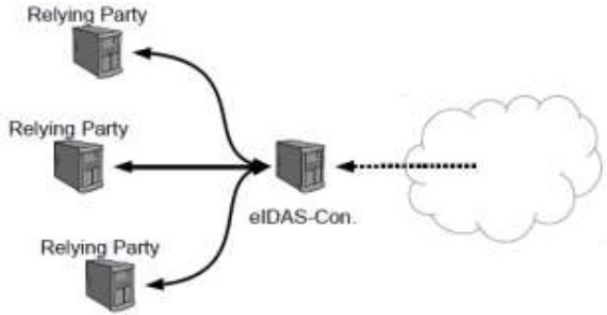
- *⟨**Assertion**⟩ contiene i seguenti elementi:*
  - *un attributo univoco **ID**, generato come negli altri casi;*
  - *un attributo **Version**, che indica la versione della specifica SAML adottata (obbligatoriamente 2.0);*
  - *un attributo **IssueInstant**, che specifica l'istante in cui la richiesta è stata rilasciata;*
  - *Un elemento ⟨**Subject**⟩, che identifica l'utente autenticato contentente, tra l'altro,* l'elemento <**SubjectConfirmation**> che, a sua volta, contiene l'attributo *⟨**SubjectConfirmationData**⟩* riportante gli attributi:
    - • ***Recipient*** *riportante l'AssertionConsumerServiceURL relativa al servizio per cui è stata emessa l'asserzione e l'attributo*
    - • ***NotOnOrAfter*** *che limita la finestra di tempo durante la quale l'asserzione può essere propagata*.
    - • ***InResponseTo***, *il cui valore deve fare riferimento all'ID della richiesta*;
  - *un elemento ⟨**Issuer**⟩, che specifica il Gestore dell'identità digitale;*
  - *un elemento ⟨**Conditions**⟩, che riporta il periodo temporale di validità e include un elemento ⟨**AudienceRestriction** ⟩ , che include a sua volta un elemento ⟨**Audience** ⟩ che ha come valore l'EntityID del Service Provider (unica entità che può usare quella asserzione).*
  - *un elemento ⟨**AuthnStatement**⟩, che è la descrizione del contesto di autenticazione includendo quindi il livello (SpidL1, SpidL2 o SpidL3);*
  - *opzionalmente un elemento ⟨**AttributeStatement**⟩, che contiene gli attributi certificati nell'assertion;*
  - *un elemento ⟨**Signature**⟩, la firma detached dell'Identity Provider sull'assertion RSA 104 e SHA-256.*
  - *opzionalmente, un elemento ⟨**Advice**⟩, che include a sua volta eventuali assertion di altre autorità o identity provider (previsto per sviluppi futuri, non utilizzato al momento)*

Approfondimento 15: Entità funzionali alla Interoperabilità EU 1/2

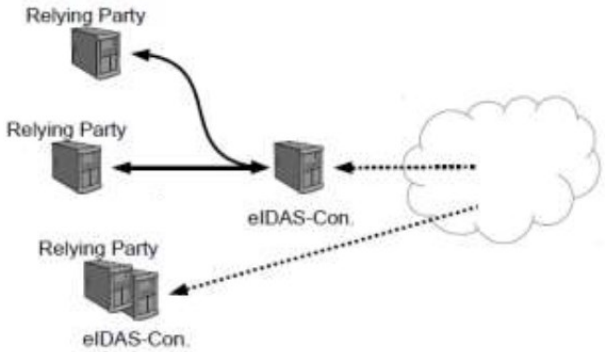
- **Member State (MS)**, uno stato facente parte dell'UE e/o dell'Area Economica Europea che segue il regolamento eIDAS.
- **Relying Party (RP),** è l'entità che richiede l'autenticazione (può coincidere con il SP o essere delegato dal SP
- Il **cittadino**, che si autentica in MS diverso da quello di appartenenza (e dove risiede il suo IdP)
- **MS mittente**, cioè quel MS il cui schema eID è usato nel processo di autenticazione e manda i dati autenticati al MS ricevente.
- **MS ricevente**, quel MS che ospita il RP dove è necessaria l'autenticazione per un servizio.
- **Nodo eIDAS**, un'entità operativa coinvolta nell'autenticazione di persone tra gli stati membri. Questi nodi, a seconda del loro ruolo, possono essere distinti in **eIDAS-Connector**, quando richiedono autenticazione tra i MS, e **eIDAS-Service,** quando offrono autenticazione tra i MS. Un'ulteriore differenza va fatta in questi ultimi se il servizio è effettuato attraverso Proxy (come in figura) o se gli **eIDAS-Service** eseguono un Middleware che è imposto dal MS mittente. In tal caso l' **eIDAS-Connector** del MS ricevente è eseguito insieme agli eIDAS-Middleware-Services necessari per ricevere le risposte secondo lo schema imposto dal Middleware

Approfondimento 16: Entità funzionali alla Interoperabilità EU 2/2

- Abbiamo visto come le interazioni all' interno di eIDAS sono principalmente effettuate dai MS mittenti e riceventi e operate dai nodi. Tali nodi, che siano di tipo Connector o Service possono operare sia su base Proxy o Middleware e utilizzano il linguaggio SAML v2 (Security Assertion Markup Language) per comunicare. Ogni MS ricevente dovrebbe utilizzare più Connector e decidere dove posizionarli sul territorio nazionale. I Connector stessi possono essere usati anche da RP pubblici o privati all' interno del MS. Se il numero di Connector in un MS è pari ad uno si parlerà di MS centralizzato, altrimenti si dirà MS decentralizzato e si avrà un connector per ogni RP



Centralized MS



Decentralized MS

Approfondimento 17: processo di autenticazione (step)

- **Processo di autenticazione**
  - Il processo di autenticazione è avviato dal RP che invia una richiesta di autenticazione al nodo Connector responsabile, quest' ultimo può essere direttamente collegato al RP (nel caso di MS decentralizzato) oppure implementato da un'entità esterna (nel caso di MS centralizzato). La richiesta potrebbe contenere un identificativo di MS qualora il MS mittente è già noto al RP (perché indicato dall'utente).
  - Nel caso che quest' informazione non sia presente, il Connector deve richiederla al MS.
  - Il Connector deve inviare una richiesta SAML all' eIDAS-Service corrispondente al MS selezionato che deve essere dettagliata con tipo e nome del RP (pubblico o privato).
  - L'eIDAS-Service deve verificare l'autenticità della richiesta ed in particolare:
    - -Se l' eIDAS-Service utilizza più schemi eID, deve fornire un'interfaccia di selezione dello schema per l'utente.
    - -Se il RP richiedente è un'entità privata, l' eIDAS-Service potrebbe anche respingere la richiesta nel caso che i termini di accesso allo schema non siano rispettati.
    - -Se il livello di sicurezza richiesto non può essere soddisfatto dall'eIDAS-Service allora la richiesta deve essere respinta.
  - L' eIDAS-Service deve operare l'autenticazione della persona in accordo con lo schema eID e rispettarne il livello di sicurezza; deve successivamente inviare una risposta SAML al Connector richiedente che contiene un'assertion criptata SAML.
  - Il Connector deve verificare l'autenticità della risposta ricevuta e decriptare l'assertion. Inoltre deve verificare che il livello di sicurezza indicato sia uguale o maggiore a quello indicato nell'assertion così da poter inviare i dati di identificazione autenticati al RP richiedente.
  - Se uno qualsiasi di questi passi fallisce, la procedura deve essere immediatamente interrotta (Abort) e la gestione degli errori deve seguire le specifiche SAML.

Approfondimento 18: processo di autenticazione (metadata)

- **Metadata**
  - Lo scambio dei metadati è basato sui seguenti principi:
    - I **Trust Anchors** (entità autorevoli che garantiscono la fiducia) per i tutti i nodi eIDAS sono i MS e non sono presenti ulteriori trust anchors centrali.
    - I **metadati** dei Connector e dei Proxy-Service sono distribuiti nel formato SAML, e sono firmati dal Trust Anchor o da un'altra entità (ad esempio l'operatore del nodo) trusted sulla base di una catena di certificati che raggiunge un Trust Anchor.
    - Per garantire l'interoperabilità si deve seguire il profilo SAML relativo ed i certificati devono essere incapsulati in elementi **<X509Certificate>.** L'effettiva locazione dei metadati SAML è raggiungibile pubblicamente tramite un indirizzo HTTPS URL, mentre i metadati SAML dei servizi Middleware sono esportati in file. Per ovviare a problemi di performance e di affidabilità causati da possibili interruzioni di rete, i nodi eIDAS possono memorizzare in cache i metadata, ed usare tale capacità anche per velocizzare accessi futuri.

Approfondimento 19: Sicurezza del Sistema SIPD (1/2)

- Ogni vulnerabilità del SP che possa portare alla compromissione del protocollo lato service provider può inficiare la sicurezza del sistema.
- Volendo definire un modello di sicurezza significativo, nel quale assumiamo trusted l'Identity Provider e potenzialmente corrotto il Service Provider, è comunque opportuno identificare due tipologie di attacchi che hanno significative differenze in termini di impatto:
  - Attacchi che compromettono l'autenticazione permettendo l'autenticazione con successo di un impostore su uno specifico SP vulnerabile
  - Attacchi che compromettono l'autenticazione permettendo l'autenticazione con successo di un impostore su diversi SP (furto di identità SPID)
- La prima tipologia di attacchi si basa essenzialmente sull'exploit di vulnerabilità tecniche lato SP che permettano all'attaccante di compromettere la veridicità dell'esito del protocollo, nella fase di verifica dei messaggi inviati dall'IdP legale al service provider.
- Nel secondo caso, invece, la compromissione del SP (a titolo di esempio attraverso XSS sul portale web) ha l'obiettivo di contattare un Identity Provider fittizio, eventualmente attuando un man-in-the-middle tra SP e IdP legale.
- L'impatto di questa tipologia di attacchi è significativamente maggiore della precedente perché espone la vittima alla possibile sottrazione delle credenziali SPID. Ciò permetterebbe all'attaccante di effettuare impersonation su qualsiasi service provider che richiede un'autenticazione SPID di livello 1, o attraverso combinazione con altri attacchi (esempio SIM swap o sms hijacking), anche per autenticazioni di livello 2 su un qualsiasi service provider.

Approfondimento 20: Sicurezza del Sistema SIPD (2/2)

- Dal punto di vista tecnico, deve essere considerato che il browser dell'utente, per come è definito il protocollo SAML2, è il veicolo attraverso il quale passano tutti i messaggi delle varie fasi del protocollo di autenticazione, fino alla trasmissione dell'assertion dall'Identity Provider al Service Provider. Pertanto, la compromissione del Service Provider può certamente rappresentare il mezzo attraverso il quale l'attaccante riesce a compromettere il browser dell'utente, e quindi, invalidare la correttezza e l'affidabilità del processo di autenticazione.
- Il Service provider pertanto, oltre ad adottare tutte le misure organizzative e tecniche idonee ad evitare la compromissione dei propri sistemi e il conseguente danno ad altri (utenti ed Identity provider), dovrà curare alcuni specifici aspetti di sicurezza procedurali ed organizzativi.
- Il primo è la piena conoscenza dell'ambito di utilizzo delle identità digitali, le limitazioni di responsabilità e i limiti di indennizzo che l'Identity Provider prevede nel Manuale Operativo, oltre il rispetto di quanto previsto dall'art. 13 del DPCM del 24 ottobre 2014 e dagli eventuali Regolamenti di cui all'art. 4 dello stesso DPCM.
- Il secondo è la scelta adeguata del livello di autenticazione SPID (LoA) che deve essere richiesto per i diversi servizi. È richiesto che tale scelta venga effettuata attraverso un approccio di tipo risk-based, che deve modellare l'incidente informatico per il quale stimare impatto e probabilità come l'errore di autenticazione o uso improprio delle credenziali. In particolare vi è una correlazione positiva tra LoA e significatività dell'impatto dell'incidente informatico (assunta costante la probabilità).
- La metodologia suggerita dall'Agenzia, prevede l'identificazione dei rischi per ogni specifico sistema/applicazione/servizio e l'associazione ai livelli di sicurezza previsti in ambito SPID, ovviamente l'assegnazione del potenziale impatto (basso, moderato, alto) di questi rischi dipende dallo specifico contesto e dalle entità coinvolte da impropria autenticazione.