Corso di formazione online

L'implementazione dei servizi con autenticazione SPID e CIE

Parte tecnica

Docente: Dott. Alfredo Visconti

Panoramica su OpenID Connect Core Specification

- impostazione progettuale è avvento delle Service Oriented Architecture (SOA), adatta a garantire l'interoperabilità tra molteplici sistemi software, scritti in diversi linguaggi di programmazione, ed implementati su differenti piattaforme hardware.

OpenID Connect

Un ecosistema digitale di identità federata permette ai fornitori di servizi di liberarsi del processo di autenticazione dell'identità e agli utenti di poter utilizzare una singola identità valida per tutti i servizi.

Si semplifica la gestione per le aziende e si rafforza la protezione dei dati personali per gli utenti, ma più è ampio il bacino di sistemi e utenze servite, più l'esposizione alle minacce aumenta. Ecco come garantire un elevato livello di sicurezza usando il protocollo OpenID Connect

Il mondo dell'identità federata è essenzialmente diviso tra due standard:
standard SAML2 (Security Assertion Markup Language 2.0) con una versione iniziale nel 2002, seguito dopo qualche anno nel 2014,
OpenID Connect 1.0 (**OIDC**), derivato dai precedenti protocolli OpenID 1.0 (2006) e 2.0 (2007) oramai obsoleti.

OpenID Connect non si occupa solo di autenticazione ma può essere anche utilizzato per autorizzazione, delega e API access management.
I punti di forza sono:

- facilità di integrazione;
- abilità di integrare applicazioni su diverse piattaforme, single-page app, web, backend, mobile, IoT;
- integrazione di componenti di terze parti in modalità sicura, interoperabile e scalabile;
- soluzione di diverse problematiche di sicurezza riscontrate in O Auth 2.0;
- utilizzo da parte di un gran numero di servizi social e di pagamento

Che cos'è OAuth

OAuth 2 è un **protocollo standard** aperto che consente alle applicazioni di accedere alle **risorse protette** di un servizio per conto dell'utente. OAuth 2.0 definisce flussi di autorizzazione per applicazioni native, applicazioni Web e dispositivi mobili.
Molte aziende offrono endpoint OAuth: Google, Facebook, LinkedIn, GitHub sono solo le prime che vengono in mente, ma il loro numero è in costante crescita.

In generale, un processo di autorizzazione può essere descritto come segue:
1. L'applicazione invia all'Authorization Server una richiesta di autorizzazione per accedere ad una risorsa protetta
2. Il proprietario della risorsa (di solito, l'utente) concede l'accesso
3. L'Authorization Server restituisce un Access Token da utilizzare in tutte le successive richieste come una sorta di "cartellino di riconoscimento"

Questa è solo una rappresentazione ad alto livello dell'intero processo, il flusso effettivo differirà in base al tipo di grant utilizzato.

Informazioni su SAML

Security Assertion Markup Language (SAML) è uno standard di federazione aperto che consente a un provider di identità (IdP) di autenticare gli utenti e trasferire il token di autenticazione a un'altra applicazione nota come provider di servizi (SP).
SAML consente all'SP di funzionare senza dover eseguire la propria autenticazione e di passare l'identità per integrare gli utenti interni ed esterni.
Consente la condivisione delle credenziali di sicurezza con un SP in rete, in genere un'applicazione o un servizio.
SAML consente una comunicazione sicura tra più domini e tra il cloud pubblico e altri sistemi abilitati a SAML, nonché un numero selezionato di altri sistemi di gestione delle identità posizionati on premise o in un altro cloud.
Con SAML, è possibile abilitare un'esperienza Single Sign-On (SSO) per gli utenti in due applicazioni qualsiasi che supportano il protocollo e i servizi SAML, consentendo così a un SSO di eseguire diverse funzioni di sicurezza per conto di una o più applicazioni.
SAML fa riferimento al linguaggio della variante XML utilizzato per codificare queste informazioni e può coprire anche vari messaggi e profili di protocollo che fanno parte dello standard.

Due funzioni di sicurezza principali di SAML

- **Autenticazione:** confermare che gli utenti sono chi dicono di essere
- **Autorizzazione:** passaggio dell'autorizzazione utente alle applicazioni per l'accesso a determinati sistemi o contenuti

1. Eseguire il login e accedere all'autenticazione SSO.
2. Esportare i metadati dal provider di identità e importarli.
3. Il sistema di identità comprenderà di più sul provider di identità SSO per esportare i metadati dal sistema
4. Fornire i metadati al team del provider di identità SSO.
5. Eseguire il test e abilitare SSO.

Un provider SAML è un sistema che consente agli utenti di ottenere l'accesso a un servizio necessario. SAML trasferisce i dati di identità tra due parti, un IdP e un SP. Esistono due tipi principali di provider SAML:

Provider di identità (IdP): esegue l'autenticazione e passa il livello di identità e autorizzazione dell'utente al provider di servizi (SP). L'IdP ha autenticato l'utente mentre l'SP consente l'accesso in base alla risposta dall'IdP.

Provider di servizi (SP): considera attendibile l'IdP e autorizza l'utente specificato ad accedere alla risorsa richiesta. Un SP richiede l'autenticazione dall'IdP per concedere l'autorizzazione all'utente e poiché entrambi i sistemi condividono lo stesso linguaggio, l'utente deve eseguire il login una sola volta.

Un'asserzione SAML è un documento XML che il provider di identità invia all'SP contenente lo stato di autorizzazione dell'utente. I tre tipi distinti di asserzioni SAML sono:

•Le asserzioni di autenticazione aiutano a verificare l'identificazione di un utente e a fornire l'ora in cui l'utente esegue il login e il metodo di autenticazione utilizzato (ad es. password).

•L'asserzione assegnata passa il token SAML all'SP. L'attributo utilizzato da SAML per identificare l'utente viene considerato uguale sia nella directory IdP che nella directory SP.

•Un'asserzione sulla decisione di autorizzazione indica se un utente è autorizzato a utilizzare un servizio o se il provider di identità ha negato la richiesta a causa di un errore della password o della mancanza di diritti per un servizio

SAML viene utilizzato principalmente per abilitare il Single Sign-On (SSO) del browser Web. L'obiettivo dell'esperienza utente per SSO consiste nel consentire a un utente di eseguire l'autenticazione una volta sola e ottenere l'accesso a sistemi protetti separatamente senza inviare nuovamente le credenziali. L'obiettivo di sicurezza è garantire che i requisiti di autenticazione siano soddisfatti a ciascun livello di sicurezza.

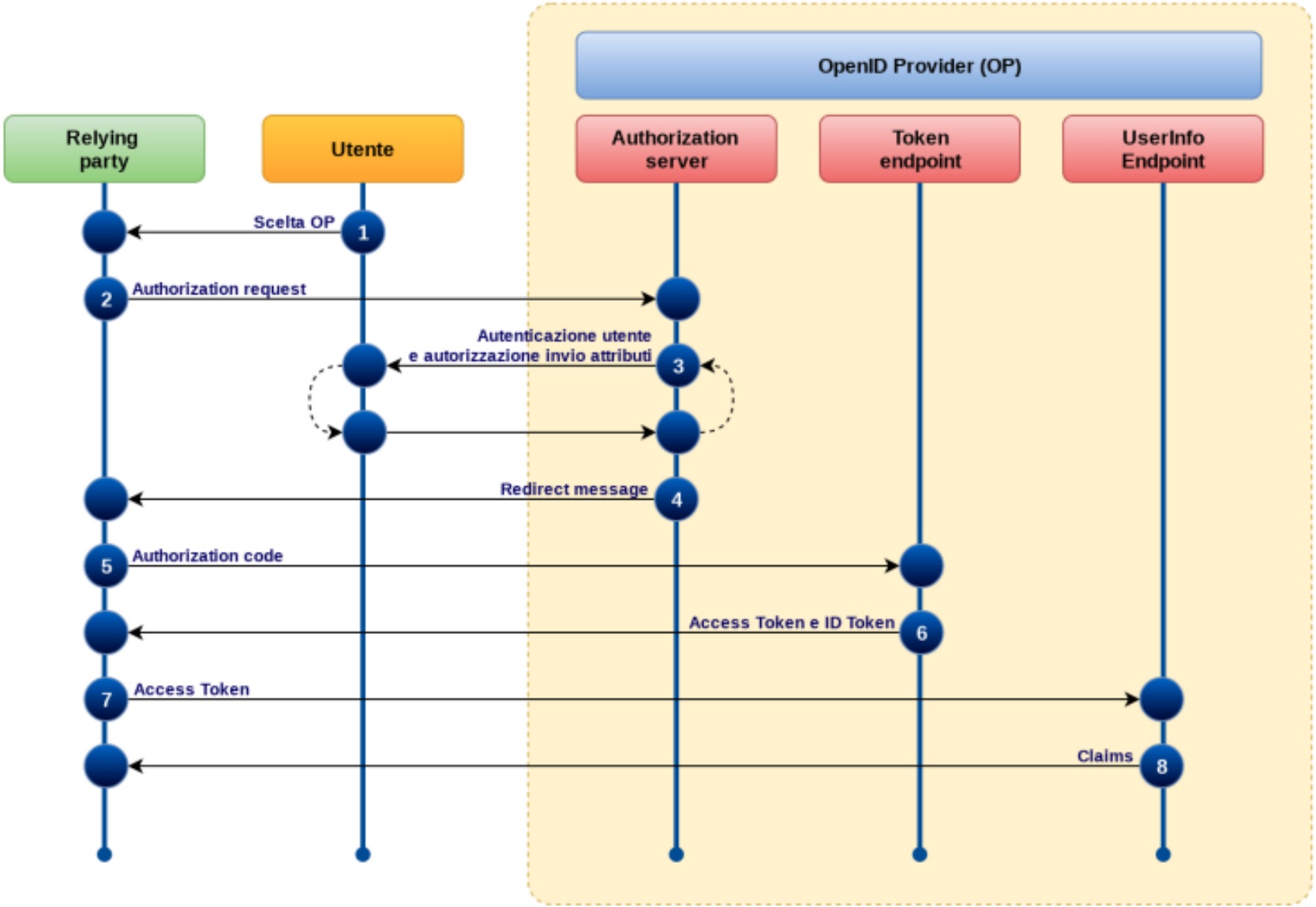
•**Gestire le identità nel cloud e on premise.** Promuovere un approccio unificato alla gestione delle identità e degli accessi con flussi di lavoro basati su cloud, provisioning degli utenti semplificato e self-service per gli utenti. L'integrazione degli standard aperti riduce il carico di lavoro e la manutenzione, fornendo il provisioning e la gestione semplificati degli utenti nel cloud e on-premise

•**Semplificare le attività relative alle identità.** Riduce la necessità di modifiche ricorrenti di utenti, ruoli o gruppi in più ambienti. Offre un bridge di identità che sincronizza le autorizzazioni delle identità tra servizi on premise e cloud

•**Strategia zero-trust.** Applicare i criteri di accesso utilizzando il servizio basato su cloud per Single Sign-On (SSO), l'applicazione efficace delle password e l'autenticazione a più fattori (MFA). Grazie all'autenticazione adattiva, i rischi si riducono aumentando i requisiti di login quando l'accesso degli utenti viene considerato ad alto rischio in base a dispositivo, posizione o attività

•**Gestire l'accesso digitale del consumatore.** Integra l'esperienza di accesso dei consumatori con interfacce utente self-service e schermate di login personalizzabili con il brand. L'accesso flessibile dei clienti consente di integrare servizi di terze parti e applicazioni personalizzate mediante le API REST e un'integrazione basata sugli standard

Flusso


OpenID Provider (OP)
Relying party
Utente
Authorization server
Token endpoint
UserInfo Endpoint
Scelta OP
1
2
Authorization request
Autenticazione utente
e autorizzazione invio attributi
3
Redirect message
4
5
Authorization code
Access Token e ID Token
6
7
Access Token
Claims
8

Che cos'è Open ID Connect - i punti di forza

Open ID Connect (OIDC) è lo **standard di autenticazione** che estende il protocollo di autorizzazione OAuth 2.0 ed è **caratterizzato da alti livelli di flessibilità e sicurezza, semplicità di implementazione ed efficacia nell'interoperabilità** in modo che le identità digitali, come **SPID** e **CIE**, possano essere facilmente utilizzata su servizi desktop e mobile.

le principali caratteristiche di OpenID Connect:

- Facilità di integrazione;
- Abilità di integrare applicazioni su diverse piattaforme, single-page app, web, backend, mobile, IoT;
- Integrazione di componenti di terze parti in modalità sicura, interoperabile e scalabile;
- Soluzione di diverse problematiche di sicurezza riscontrate in OAuth 2.0 al fine di garantire una maggiore resilienza informatica;
- Utilizzo da parte di un gran numero di servizi social e di pagamento.

Mentre OAuth 2.0 è un protocollo di delega delle autorizzazioni di accesso generico, consentendo così il trasferimento di dati, e non definisce i modi per autenticare gli utenti o comunicare informazioni su di essi, **Open ID Connect è un protocollo di identificazione aggiuntivo che consente ai client di verificare l'identità dell'utente finale** e di ottenere informazioni di base sul suo profilo in modo interoperabile.

OIDC consente agli sviluppatori di autenticare gli utenti su siti web e app senza dover possedere e gestire file di password, fornendo una risposta sicura e verificabile alla domanda: "*Qual è l'identità della persona che sta utilizzando il browser o l'applicazione nativa collegata a me?*".

L'utilizzo di questo protocollo serve a ridurre il rischio di potenziali attacchi da parte di cybercriminali e ad aumentare quindi il livello di sicurezza informatica delle tecnologie di autenticazione.

la tassonomia di Open ID Connect:

- **End-User**: è l'utente che richiede l'accesso ai servizi online;
- **User Agent**: è il browser che l'utente utilizza per accedere alle risorse online;
- **Claims**: è l'insieme di informazioni sull'utente di tipo nome-valore
- **Authorization Server**: è il server che possiede l'identità e le credenziali dell'utente;
- **OpenID Provider**: è l'Authorization Server capace di autenticare l'utente e rilasciare i Claims;
- **Relying Party**: è l'applicazione Client che richiede l'autenticazione dell'utente ed i Claims;
- **Resource Server**: è il server che ospita le risorse che saranno accedute;
- **ID Token**: è la stringa che contiene i Claims di autenticazione nel formato JWT (JSON Web Token), coppie del tipo nome:valore;
- **Subject Identifier**: è l'identificativo univoco dell'utente, rilasciato al Client;
- **UserInfo Endpoint**: è l'interfaccia che rilascia le informazioni autorizzate dell'utente.

vantaggi

Al fine di innalzare il livello di sicurezza delle credenziali di accesso di ciascun cittadino che possiede un'**identità digitale**, **il Sitema Pubblico di Identità Digitale ha adottato lo standard di autenticazione Open ID Connect** e l'Agenzia per l'Italia Digitale ha rilasciato le **linee guida** a cui i Gestori dell'identità digitale e i Fornitori di servizi pubblici e privati si sono dovuti adeguare a partire da maggio 2022.
Le linee guida di AgID stabiliscono l'obbligo di adottare il nuovo standard di sicurezza OpenID connect per continuare ad erogare i propri servizi attraverso il sistema di autenticazione SPID. L'obiettivo è garantire un potenziamento e un innalzamento della **cyber security**.

I principali vantaggi di OpenID Connect in SPID:
• **Evitare d'inserire la password ad ogni accesso**, riducendo così i rischi legati ad attacchi informatici da parte di cybercriminali che potrebbero intercettare i flussi di informazioni tra gli attori coinvolti nel processo di autenticazione;
• **Migliorare la User experience** soprattutto per quel che riguarda l'utilizzo delle applicazioni da dispositivi mobili, allo scopo di garantire agli utenti maggiore flessibilità e sicurezza;
• Dare ai cittadini in possesso di un'identità digitale SPID la **possibilità di bloccare tutte le autenticazioni effettuate per l'accesso a un determinato servizio**.
OpenID Connect in SPID si inserisce nell'ambito della strategia Cyber Resilience Act, ovvero la proposta di Regolamento europeo sui requisiti dei prodotti con elementi digitali che mira a rafforzare le norme di cybersecurity per garantire prodotti hardware e software più sicuri.

Area Riservata

ACCEDI

Uffici giudiziari

ACCEDI

Punti di accesso

ACCEDI

Consultazione pubblica dei registri

ACCEDI

Consultazione pubblica registri Corte di Cassazione

ACCEDI

Servizio online giudice di pace

ACCEDI

Portale delle procedure concorsuali

ACCEDI

Piattaforma e-learning

ACCEDI

Portale liquidazione spese di giustizia, istanze Pinto e imputati assolti

Class Action - Azioni di Classe

Pagamenti online tramite pagoPA - utenti non registrati

Registro nazionale degli incarichi di curatore, commissario giudiziale e liquidatore giudiziale

Portale dei Servizi Telematici del Ministero della Giustizia

Servizi Online Uffici Giudiziari

Seguici

Accedi con smartcard

Per accedere con **Smartcard**

Accedi con SPID

Per accedere con **Entra con SPID**

Accedi con SPID

Per accedere con **Entra con SPID**

502 Bad Gateway

SPID Selfcare

Genera il codice OTP e copialo qui.

Credenziale :

ArubaOTP Mobile (M7670859373286301)

Codice OTP : Non puoi generare il codice?

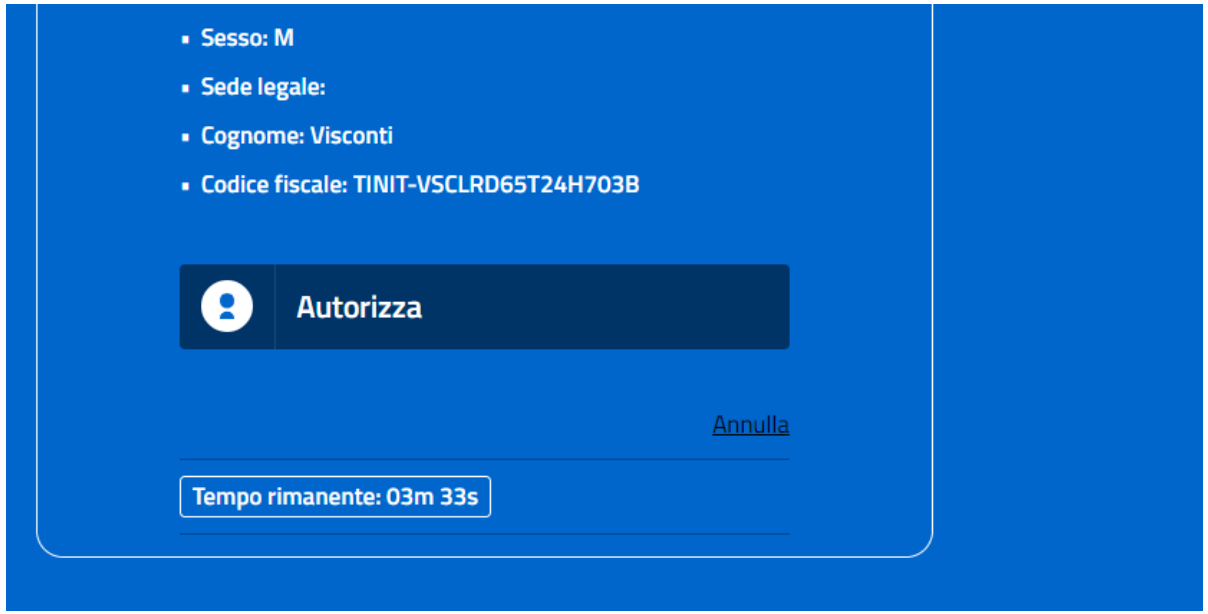
Codice OTP

Annulla

ACCEDI

Come fare se


UTILIZZA
spid 2
IN ALTERNATIVA USA
spid 3
MINISTERO DELLA GIUSTIZIA
Per accedere al servizio richiesto è necessario l'utilizzo dei seguenti dati personali:
Partita IVA:
Domicilio digitale:
Indirizzo di posta elettronica: amministrazione@viscontisoluzioni.it
Provincia di nascita: SA
Data di scadenza identità: 2024-07-21
Ragione o denominazione sociale:
Codice identificativo SPID: AIDP0002259027
Documento d'identità: cartaIdentita CA80399EE comuneNapoli 2019-05-28 2029-12-24
Domicilio fisico: via G. Marconi 41 84013 Cava de' Tirreni SA
Numero di telefono mobile: +393939063440
cookie policy


Sesso: M
Sede legale:
Cognome: Visconti
Codice fiscale: TINIT-VSCLRD65T24H703B
Autorizza
Annulla
Tempo rimanente: 03m 33s

Servizi

Consultazione registri

Informazioni sullo stato dei procedimenti e consultazione del fascicolo informatico.

Accedi

Consultazione registri Corte di Cassazione

Consultazione registri Corte di Cassazione

Accedi

Registro Generale degli Indirizzi Elettronici

Per conoscere l'indirizzo di posta elettronica certificata e il domicilio legale dei soggetti registrati. I professionisti ausiliari del giudice possono registrarsi, ai sensi dell'art 9 del provvedimento 18 luglio 2011, con un click sul codice fiscale che comparirà in alto nella pagina dopo l'operazione di Login.

Accedi

Registro PP.AA.

Registro contenente gli indirizzi di Posta Elettronica Certificata delle Amministrazioni pubbliche ai sensi del DL 179/2012 art 16, comma 12 - consultabile esclusivamente dagli uffici giudiziari, dagli uffici notificazioni, esecuzioni e protesti, e dagli avvocati -

Pagamenti online

Sistema integrato con pagoPA

Accedi

Service Oriented Architecture

L'architettura orientata ai servizi (SOA) è un metodo di sviluppo del software che utilizza componenti chiamati servizi per creare applicazioni aziendali.

Ogni servizio fornisce una funzionalità aziendale e i servizi possono comunicare tra loro attraverso piattaforme e lingue diverse. Gli sviluppatori utilizzano la SOA per riutilizzare i servizi in sistemi diversi o per combinare più servizi indipendenti ed eseguire compiti complessi.

Ad esempio, diversi processi aziendali in un'organizzazione richiedono la funzionalità di autenticazione degli utenti. Invece di riscrivere il codice di autenticazione per tutti i processi aziendali, è possibile creare un unico servizio di autenticazione e riutilizzarlo per tutte le applicazioni.

Allo stesso modo, la maggior parte dei sistemi di un'organizzazione sanitaria, come i sistemi di gestione dei pazienti e i sistemi di cartelle cliniche elettroniche (EHR), devono registrare i pazienti. Questi sistemi possono ricorrere a un unico servizio comune per eseguire la registrazione del paziente.

Vantaggi dell'architettura orientata ai servizi

L'architettura orientata ai servizi (SOA) presenta numerosi vantaggi rispetto alle tradizionali architetture monolitiche in cui tutti i processi vengono eseguiti come una singola unità. Alcuni dei principali vantaggi della SOA includono quanto segue:

Time-to-market ridotto
Gli sviluppatori riutilizzano i servizi in diversi processi aziendali per risparmiare tempo e costi. Possono assemblare applicazioni molto più velocemente con la SOA che scrivendo codici ed eseguendo integrazioni da zero.

Manutenzione efficiente
È più facile creare, aggiornare ed eseguire il debug di piccoli servizi rispetto ai blocchi di codice di grandi dimensioni nelle applicazioni monolitiche. La modifica di qualsiasi servizio in una SOA non influisce sulla funzionalità complessiva del processo aziendale.

Maggiore adattabilità
La SOA è più adattabile ai progressi tecnologici. È possibile modernizzare le applicazioni in modo efficiente ed economico. Ad esempio, le organizzazioni sanitarie possono utilizzare la funzionalità dei vecchi sistemi di cartelle cliniche elettroniche nelle nuove applicazioni basate su cloud.

Principi base dell'architettura orientata ai servizi

Non esistono linee guida standard ben definite per l'implementazione dell'architettura orientata ai servizi (SOA). Tuttavia, alcuni principi base sono comuni a tutte le implementazioni SOA.

Interoperabilità

Ciascun servizio in SOA include documenti descrittivi che specificano la funzionalità del servizio e i relativi termini e condizioni. Qualsiasi sistema client può eseguire un servizio, indipendentemente dalla piattaforma o dal linguaggio di programmazione sottostante. Ad esempio, i processi aziendali possono utilizzare servizi scritti sia in C# che in Python. Poiché non esistono interazioni dirette, le modifiche in un servizio non influiscono sugli altri componenti che utilizzano il servizio.

Accoppiamento debole

I servizi in SOA dovrebbero essere accoppiati debolmente, con la minor dipendenza possibile da risorse esterne come modelli di dati o sistemi informativi. Dovrebbero anche essere indipendenti senza mantenere alcuna informazione da sessioni o transazioni passate. In questo modo, se si modifica un servizio, non avrà un impatto significativo sulle applicazioni client e sugli altri servizi che utilizzano il servizio.

Astrazione

I client o gli utenti del servizio in SOA non devono conoscere la logica del codice del servizio o i dettagli di implementazione. Per loro, i servizi dovrebbero apparire come una scatola nera. I clienti ottengono le informazioni richieste su ciò che fa il servizio e su come utilizzarlo tramite contratti di servizio e altri documenti di descrizione del servizio.

Granularità

I servizi in SOA dovrebbero avere una dimensione e un ambito appropriati, idealmente racchiudendo una discreta funzione aziendale per servizio. Gli sviluppatori possono quindi utilizzare più servizi per creare un servizio composito per l'esecuzione di operazioni complesse.

Componenti principali nell'architettura orientata ai servizi

Servizio

I servizi sono gli elementi costitutivi di base della SOA. Possono essere privati, cioè disponibili solo per gli utenti interni di un'organizzazione, o pubblici, cioè accessibili a tutti via Internet. Individualmente, ciascun servizio ha tre caratteristiche principali.

Implementazione di servizi è il codice che costruisce la logica per eseguire la specifica funzione del servizio, come l'autenticazione dell'utente o il calcolo della fattura.

Contratto di servizi definisce la natura del servizio e i termini e le condizioni associati, come i prerequisiti per l'utilizzo del servizio, il costo del servizio e la qualità del servizio fornito.

Interfaccia di servizi altri servizi o sistemi comunicano con un servizio attraverso la sua interfaccia di servizi. L'interfaccia definisce come richiamare il servizio per eseguire attività o scambiare dati. Riduce le dipendenze tra i servizi e il richiedente di servizi.

Fornitore di servizi

Il fornitore di servizi crea, mantiene e fornisce uno o più servizi che altri possono utilizzare. Le organizzazioni possono creare i propri servizi o acquistarli da fornitori di servizi terzi.

Utente di servizi

L'utente di servizi richiede al fornitore di servizi di eseguire un servizio specifico. Può essere un intero sistema, un'applicazione o un altro servizio. Il contratto di servizi specifica le regole che il fornitore e l'utente di servizi devono seguire quando interagiscono tra loro. I fornitori e gli utenti di servizi possono appartenere a diversi dipartimenti, organizzazioni e persino settori.

Registro di servizi

Un registro di servizi, o repository di servizi, è una directory accessibile in rete di servizi disponibili. Memorizza i documenti di descrizione del servizio dei fornitori di servizi. I documenti descrittivi contengono informazioni sul servizio e su come comunicare con esso. Gli utenti di servizi possono facilmente individuare i servizi di cui hanno bisogno utilizzando il registro di servizi.

Come funziona l'architettura orientata ai servizi

Nell'architettura orientata ai servizi (SOA), i servizi funzionano in modo indipendente e forniscono funzionalità o scambi di dati ai propri utenti. L'utente richiede informazioni e invia i dati di input al servizio. Il servizio elabora i dati, esegue l'attività e invia una risposta. Ad esempio, se un'applicazione utilizza un servizio di autorizzazione, fornisce al servizio il nome utente e la password. Il servizio verifica il nome utente e la password e restituisce una risposta appropriata.

Protocolli di comunicazione

I servizi comunicano utilizzando regole stabilite che determinano la trasmissione dei dati su una rete. Queste regole sono chiamate protocolli di comunicazione. Alcuni protocolli standard per implementare la SOA includono quanto segue:

- Simple Object Access Protocol (SOAP)
- RESTful HTTP
- Apache Thrift
- Apache ActiveMQ
- Servizio messaggi Java (JMS)

È persino possibile utilizzare più di un protocollo nella tua implementazione SOA.

Cosa sono i microservizi

L'architettura dei microservizi è costituita da componenti software molto piccoli e completamente indipendenti, chiamati microservizi, che si specializzano e si concentrano su un'unica attività. I microservizi comunicano tramite le API, che sono regole create dagli sviluppatori per consentire ad altri sistemi software di comunicare con il loro microservizio.

Lo stile architettonico dei microservizi è più adatto ai moderni ambienti di cloud computing. Spesso operano in container, unità software indipendenti che impacchettano il codice con tutte le sue dipendenze.

Vantaggi dei microservizi

I microservizi sono scalabili in modo indipendente, veloci, portatili e indipendenti dalla piattaforma (caratteristiche native del cloud). Sono anche disaccoppiati, il che significa che non hanno dipendenze limitate da altri microservizi. Per raggiungere questo obiettivo, i microservizi hanno accesso locale a tutti i dati di cui hanno bisogno invece dell'accesso remoto ai dati centralizzati a cui accedono e utilizzano anche altri sistemi. Ciò crea una duplicazione dei dati che i microservizi compensano in termini di prestazioni e agilità.

SOA rispetto ai microservizi

L'architettura dei microservizi è un'evoluzione dello stile architettonico delle SOA. I microservizi affrontano le carenze della SOA per rendere il software più compatibile con i moderni ambienti aziendali basati su cloud. Sono granulari e favoriscono la duplicazione dei dati rispetto alla condivisione dei dati. Ciò li rende completamente indipendenti con i propri protocolli di comunicazione che vengono esposti tramite API leggere. È essenzialmente compito degli utenti utilizzare il microservizio tramite la sua API, eliminando così la necessità di un ESB centralizzato.

Caratteristiche e vantaggi dei microservizi

Autonomi - Ciascun servizio nell'architettura basata su microservizi può essere sviluppato, distribuito, eseguito e ridimensionato senza influenzare il funzionamento degli altri componenti. I servizi non devono condividere alcun codice o implementazione con gli altri. Qualsiasi comunicazione tra i componenti individuali avviene attraverso API ben definite.

Specializzati - Ciascun servizio è progettato per una serie di capacità e si concentra sulla risoluzione di un problema specifico. Se gli sviluppatori aggiungono del codice a un servizio rendendolo più complesso, il servizio può essere scomposto in servizi più piccoli.

I vantaggi sono

Agilità - I microservizi promuovono le organizzazioni di team indipendenti di dimensioni ridotte che diventano proprietari del servizio che gestiscono. I team agiscono in contesti ridotti e ben delineati così che possano lavorare in modo più indipendente e rapido. Ciò riduce i tempi del ciclo di sviluppo. Potrai trarre un enorme vantaggio dal throughput aggregato dell'organizzazione.

Scalabilità e flessibilità - I microservizi ti consentono di scalare ciascun servizio in modo indipendente per rispondere alla richiesta delle funzionalità. Ciò permette di ridimensionare in modo corretto l'infrastruttura in base alle necessità, misurare in modo accurato i costi di una funzionalità e proteggere la disponibilità dell'applicazione nel caso in cui il servizio sperimenti un amento nella richiesta.

Semplicità di distribuzione - I microservizi supportano l'integrazione continua e la distribuzione continua, così da poter provare nuove idee in modo più semplice e ripristinare impostazioni precedenti quando qualcosa non funziona

Libertà tecnologica - Le architetture non applicano un unico approccio all'intera applicazione. I team hanno la libertà di scegliere gli strumenti migliori per risolvere i loro problemi specifici.

Codice riutilizzabile - Dividere il software in moduli piccoli e ben definiti permette di utilizzare funzioni per più scopi. Un servizio scritto per una certa funzione può essere utilizzato come blocco costruttivo per un'altra funzionalità. Ciò permette all'applicazione di effettuare il bootstrap in modo indipendente, gli sviluppatori possono creare nuove capacità senza dover scrivere codice da zero.

Panoramica su OpenID Connect Federation 1.0 Specification

- Spiegazione di AVISPA (Automated Validation of Internet Security Protocols and Applications) che è un tool integrato per la validazione automatica di protocolli ed applicazioni di sicurezza per sistemi distribuiti
- Breve accenno al linguaggio HLPSL

•

OpenID Connect 1.0 le federazioni

OpenID Connect 1.0 è un semplice “identity layer”, basato sul protocollo OAuth 2.0, che permette ai Client di verificare l'identità dell'End-User attraverso l'autenticazione eseguita da un Authorization Server, nonché di ottenere informazioni di base dell'End-User stesso

Lo scopo è di evitare che ogni utente necessiti di registrare un account in ogni fornitore di servizi.

Una Federazione delle Identità Digitali è una infrastruttura all'interno della quale tante organizzazioni, afferenti a domini differenti, aderiscono ad un medesimo quadro regolatorio per costruire un meccanismo di fiducia sia amministrativo, mediante la stipula di convenzioni e accreditamento presso una o più autorità super partes, che tecnologico, mediante l'adozione di standard di interoperabilità sicuri che consentono l'interscambio dei dati.

Questa configurazione stabilisce i livelli di garanzia e di sicurezza adeguati affinchè un individuo possa autenticarsi presso un servizio web (Service Provider) mediante la propria identità digitale, rilasciata da un altro servizio web (Identity Provider).

I partecipanti che si riconoscono all'interno della medesima Federazione, ottengono i Metadata gli uni degli altri. I Metadata contengono le chiavi pubbliche per le operazioni di firma digitale e criptazione e le definizioni necessarie all'interscambio delle informazioni.

I Metadata sono certificati da un parte fidata che all'interno della Federazione SPID è AgID, mentre all'interno della Federazione CIE è il Ministero dell'Interno.

SPID e CIE id implementano OpenID Connect Federation 1.0 e ne estendono alcune funzionalità, realizzano una implementazione concreta e producono le buone pratiche per la sua adozione.

Configurazione della Federazione

La configurazione della Federazione è pubblicata dal Trust Anchor all'interno della sua Entity Configuration, disponibile presso un web path ben noto e corrispondente a **.well-known/openid-federation**.

Tutti i partecipanti **DEVONO** ottenere, prima della fase di esercizio, la configurazione della Federazione e mantenerla aggiornata su base giornaliera. All'interno della configurazione della Federazione sono pubblicate le chiave pubbliche del Trust Anchor usate per le operazioni di firma, il numero massimo di Intermediari consentiti tra una Foglia e il Trust Anchor (**max_path length**) e le autorità abilitate all'emissione dei Trust Mark (**trust_marks_issuers**).

Modalità di partecipazione

Per aderire alle Federazioni SPID e CIE id un partecipante deve pubblicare la propria configurazione (Entity Configuration) presso il proprio web endpoint .well-known/openid-federation.
Gli incaricati tecnici ed amministrativi della Foglia completano la procedura amministrativa per la registrazione di una nuova Entità o l'aggiornamento di un'Entità preesistente definita dalla Autorità di Federazione o da un suo Intermediario (SA).
L'Autorità di Federazione o il suo Intermediario, dopo aver effettuato tutti i controlli amministrativi e tecnici richiesti, registra le chiavi pubbliche della Foglia e rilascia una prova di adesione alla Federazione sotto forma di Trust Mark (TM).
La Foglia DEVE includere il TM all'interno della propria configurazione di Federazione (Entity Configuration) come prova del buon esito del processo di onboarding.
L'Autorità di Federazione o suo Intermediario DEVE pubblicare la dichiarazione di riconoscimento della Foglia (Entity Statement) contenente le chiavi pubbliche di Federazione della Foglia e i TM a questa rilasciati.

AVISPA

AVISPA (Automated Validation of Internet Security Protocols and Applications) è un tool integrato per la validazione automatica di protocolli ed applicazioni di sicurezza per sistemi distribuiti.
È stato sviluppato nell'ambito di un progetto avente l'obiettivo dello sviluppo di una tecnologia che permetta di accelerare l'elaborazione di protocolli di rete sicuri e la diffusione di applicazioni distribuite avanzate basate su di essi. AVISPA è già stato utilizzato con successo per l'analisi di diversi protocolli nel corso della standardizzazione da parte di enti quali IETF, ITU e W3C.
Risultati sperimentali, ottenuti dall'analisi di una vasta libreria di protocolli di sicurezza per Internet, indicano inoltre che AVISPA rappresenta lo stato dell'arte per l'analisi dei protocolli di rete.
L'applicazione fornisce un linguaggio di alto livello (High Level Protocol Specification Language, o HLPSL) per la specifica formale dei protocolli e delle loro proprietà di sicurezza. Inoltre, AVISPA integra più componenti che implementano molteplici tecniche di analisi automatica.

In particolare AVISPA è costituita da diversi moduli:

- un traduttore chiamato HLPSL2IF per trasformare le specifiche HLPSL scritte dagli utenti in specifiche IF (Intermediate Format)
- quattro differenti back-end (OFMC, CLAtSe, SATMC, TA4SP) in grado di analizzare le specifiche IF per la verifica dei protocolli di rete

Il linguaggio HLPSL

HLPSL è un linguaggio espressivo utile per la modellazione della comunicazione e dei protocolli di sicurezza.

Nonostante HLPSL risulti efficace scrivere le specifiche dei protocolli in HLPSL non è altrettanto semplice.
HLPSL è un linguaggio basato sui ruoli.
I protocolli scritti in HLPSL, infatti, sono definiti ruolo dopo ruolo piuttosto che messaggio dopo messaggio

HLPSL è un linguaggio basato sulla logica temporale. I protocolli, pertanto, sono modellati come sistemi di transizioni mediante la descrizione dello stato del sistema e la specifica delle modalità con cui tale stato può cambiare.
In HLPSL, come già accennato, la specifica del sistema è suddivisa in ruoli.
Per ogni ruolo viene definito l'insieme delle sue variabili tra le quali vi sono le variabili di stato.

Ruoli

In HLPSL le specifiche dei protocolli sono organizzate e suddivise in ruoli.
Un ruolo può essere considerato come la descrizione di un comportamento.
Alcuni ruoli (ruoli base, *basic roles*) rappresentano ogni agente partecipante allo svolgimento di un protocollo e ne descrivono le azioni.
Altri (ruoli composti, *composed roles*) istanziano i ruoli base al fine di modellare l'interazione degli agenti nel corso dell'intera esecuzione del protocollo (ruoli sessione, *session roles*) oppure definiscono le sessioni del protocollo di effettivo interesse (ruoli ambiente, *environment roles*).

Goal di Sicurezza

Dopo aver definito l'insieme di ruoli necessario alla descrizione del protocollo, le specifiche in HLPSL prevedono la dichiarazione dei goal di sicurezza.
Essi, in combinazione con i goal facts con cui vengono dettagliate le transizioni dei ruoli base, descrivono le condizioni che indicano un attacco.
Attualmente HLPSL prevede solamente goal di autenticazione e segretezza.

Il goal di segretezza secrecy of kab, ad esempio, insieme al goal fact corrispondente secret(Kab, kab, {A,B}), indica che una certa variabile Kab deve rimanere sempre nota soltanto agli agenti A e B.

I goal di autenticazione previsti da HLPSL sono di due tipi e corrispondono rispettivamente alle definizioni di Gavin Lowe di autenticazione forte e debole.

Nel caso dell'autenticazione forte, nessun agente accetta lo stesso valore una seconda volta dallo stesso agente con cui è in comunicazione.
Nel caso dell'autenticazione debole, invece, non vi è alcuna protezione contro le ripetizioni.

Linee guida
Art 3

1. Al fine di rilasciare l'*identità digitale uso professionale della persona fisica*, il gestore dell'identità deve verificare l'identità personale della persona fisica richiedente. La verifica dell'identità è assolvibile anche attraverso un servizio in rete accessibile con l'uso di identità digitale SPID della medesima persona fisica, a condizione che le credenziali utilizzate per l'autenticazione siano state rilasciate dallo stesso IdP al quale vengono richieste le credenziali per uso professionale e siano di livello pari o superiore a quelle richieste. Tale limitazione non si applica nel caso in cui siano intervenuti specifici accordi di natura privata fra gli IdP.

2. Al fine di rilasciare l'*identità digitale uso professionale per la persona giuridica* il gestore dell'identità deve:
   a) verificare l'identità personale della persona fisica richiedente;
   b) verificare che il richiedente abbia titolo per richiedere l'*identità digitale per la persona giuridica*.
3. La verifica di cui ai precedenti commi 1 e 2 lettera a) è effettuata con le modalità e i controlli previsti dalla normativa vigente in materia di rilascio dell'identità digitale della persona fisica.
4. La verifica di cui al comma 2, lettera b) è effettuata con modalità preventivamente sottoposte dal gestore dell'identità ad AgID per l'approvazione.

Articolo 5

Attributo uso professionale

1. L'*identità digitale uso professionale* contiene l'attributo-estensione *Purpose* valorizzato con codice **P**.
2. L'attributo oggetto del presente articolo consente ai fornitori di servizi SPID di regolare l'accesso ai servizi dedicati a professionisti e a persone giuridiche.
3. Resta in carico ai fornitori dei servizi SPID la definizione del livello di autorizzazione associato alla persona fisica risultante dall'*identità digitale uso professionale*.
4. Il fornitore di servizi SPID che intende far autenticare un soggetto con l'*identità digitale uso professionale*, inserisce la seguente estensione SAML nell'authRequest:

```
<samlp:Extensions
```

Token di autorizzazione

1. Il *token di autorizzazione* è il risultato dell'algoritmo di hash SHA-256 della stringa di dati contenente i dati personali del soggetto cui rilasciare l'*identità digitale uso professionale per la persona giuridica*, un *token* costituito da una stringa alfanumerica casuale di cinque caratteri e il *codice di controllo* di cui al precedente art. 9, comma 3, lettera b).
   Il contenuto di tale stringa è il seguente:

nome_cognome_codiceFiscale_numeroDocumento_indirizzoMail_numeroCellulare_token_codiceControllo

Articolo 11

Sistema di gestione

Linee guida per OpenID Connect in SPID

- OpenID Connect Core – Definisce il core delle funzionalità OpenID Connect: l'autenticazione basata sul protocollo OAuth 2.0 e l'uso dei claims per comunicare le informazioni relative all'End-User
- OpenID Connect Discovery – (Optional) Definisce come i Client possono trovare dinamicamente le informazioni relative agli OpenID Providers
- OpenID Connect Dynamic Registration – (Optional) Definisce come i Client si registrano dinamicamente con gli OpenID Providers Regole tecniche OpenID Connect per CIE

OpenID Connect è uno strato (layer) d'identità semplice basato sul protocollo OAuth 2.0.

Esso consente ai Client di verificare l'identità di un Utente Finale sulla base della autenticazione effettuata da un Server di Autorizzazione, nonché di ottenere informazioni di base sul profilo dell'Utente Finale in maniera interoperabile e REST-like.

Le specifiche che lo descrivono si suddividono in più parti:

- **OpenID Connect Core** – Definisce il core delle funzionalità OpenID Connect: l'autenticazione basata sul protocollo OAuth 2.0 e l'uso dei claims per comunicare le informazioni relative all'End-User
- **OpenID Connect Discovery** – (Optional) Definisce come i Client possono trovare dinamicamente le informazioni relative agli OpenID Providers
- **OpenID Connect Dynamic Registration** – (Optional) Definisce come i Client si registrano dinamicamente con gli OpenID Providers

Questa specifica assume che il Relying Party abbia già ottenuto sufficienti credenziali ed abbia fornito informazioni necessarie per usare l'OpenID Provider, incluso il suo indirizzo dell'Authorization Endpoint e del Token Endpoint. Questa informazione è generalmente ottenuta attraverso la Discovery, come descritto nell'OpenID Connect Discovery 1.016, o può essere ottenuta attraverso altri meccanismi.

Relying party (RP) è un termine informatico utilizzato per fare riferimento a un server che fornisce l'accesso a un'applicazione software protetta.

OpenID Provider: è l'Authorization Server capace di autenticare l'utente e rilasciare i Claims.

Resource Server: è il server che ospita le risorse che saranno accedute.

Il protocollo OpenID Connect, in astratto, segue i seguenti passaggi:

1. Il RP (client) invia una richiesta al OpenID Provider (OP).
2. L'OP autentica l'utente finale e ottiene l'autorizzazione.
3. L'OP risponde con un ID Token e di solito con un Access Token.
4. La RP può inviare una richiesta con l'Access Token all'UserInfo Endpoint.
5. Il UserInfo Endpoint restituisce asserzioni relative all'utente finale

OpenID Connect esegue l'autenticazione per loggare l'utente finale o per determinare se l'utente finale è già connesso.

restituisce il risultato dell'autenticazione effettuata dal Server al client in maniera sicura in modo tale che il client possa contare su di esso.

Per questo motivo in questo caso il Client è chiamato Relying Party (RP).

Il risultato di autenticazione viene restituito sotto forma di un ID token. Esso contiene asserzioni che esprimono informazioni quali l'Emittente (Issuer) , il Subject Identifier, quando scade l'autenticazione, ecc.

L'autenticazione

L'autenticazione, l'atto di verifica dell'identità,
è progettata per proteggere da attività di accesso fraudolente, o più genericamente l'idoneità dell'utente ad accedere a informazioni protette. Parliamo di informazioni computerizzate e l'identità dell'utente da autenticare è quella digitale.
Non è un tema che richiama la necessità di identificare in modo certo un soggetto fisico ma di garantire la correttezza formale di credenziali di accesso digitali

Il framework di autenticazione nel nostro caso OAuth 2.0 è uno standard aperto che consente ad un utente di concedere ad un sito Web o ad un'applicazione di terze parti l'accesso alle proprie risorse protette, senza necessariamente rivelare a terzi le proprie credenziali o addirittura l'identità.

Pensiamo, ad esempio, a quando per accedere a un sito web ci viene offerta una o più opportunità di accesso, utilizzando l'esito dell'autenticazione su uno dei siti web o servizi visualizzati. Selezioniamo uno di questi e ci autentichiamo con le nostre credenziali per quel sito/servizio. Di conseguenza, il primo sito riceverà dal sito ove ci siamo appena autenticati, l'autorizzazione per il nostro accesso. Questo è OAuth.

Token

OAuth 2.0 è un protocollo di autenticazione basato sui token (token-based authentication). Il token è una stringa, firmata da un server per le verifiche di integrità, che può contenere molte informazioni sull'utente, quali autorizzazioni, gruppi di appartenenza ed indicatori di tempo.

L'utente mantiene l'accesso finché il token rimane valido.
Un tipico token di accesso (access token) contiene tre parti distinte, che lavorando insieme, verificano il diritto dell'utente di accedere ad una risorsa. I tre elementi chiave sono:

1. **Header** (*intestazione*): i dati sul tipo di token e l'algoritmo utilizzato per realizzarlo sono inclusi qui.
2. **Payload** (*carico utile*): le informazioni sull'utente, comprese le autorizzazioni e le scadenze, sono incluse qui. Questa parte è anche detta sezione delle richieste (claims section).
3. **Signature** (*firma*): i dati di verifica, affinché il destinatario possa garantire l'autenticità del token, sono inclusi qui. Questa firma è in genere di tipo hash, perciò è difficile da forzare e riprodurre.

Tipi di Token

1.token d'accesso utente: è necessario per concedere le autorizzazioni ad interagire con i dati dell'utente. Generalmente, preventivamente è richiesto il consenso dell'utente tramite un opportuno form;

2.token d'accesso dell'app: è necessario per concedere le autorizzazioni ad interagire con i dati dell'app. Per la generazione viene utilizzata una password predefinita tra app ed il sito che si vuole visitare ad es. Facebook;

3.token d'accesso della pagina: è necessario per concedere le autorizzazioni ad interagire con i dati della pagina. Per ottenere questo token, è necessario avere prima ottenuto un token d'accesso utente;

4.token client: è un identificativo che si può incorporare nel codice binario delle app e serve per l'identificazione della particolare app.

L'uso dei token conferisce grande flessibilità ma soprattutto riduce la necessità di trasmettere continuamente le credenziali di autenticazione di lungo periodo (complete di dati personali), a favore di permessi di autenticazione temporanei (token).

La struttura dati dell'ID Token è la principale estensione che l'OpenID Connect fa all'OAuth 2.0 per abilitare l'Utente Finale ad essere autenticato.
L'ID Token è un token di sicurezza che contiene asserzioni (claims) relative all'autenticazione di un Utente Finale, per un Authorization Server, quando si utilizza un Client

exp - OBBLIGATORIO.
Il tempo di scadenza oltre il quale l'ID Token non deve essere accettato per l'elaborazione. L'elaborazione di questo parametro richiede che la data e l'ora corrente deve essere antecedente alla data e ora della scadenza indicata nel valore. Gli implementatori possono prevede un margine di tolleranza di pochi minuti che tenga conto dello scostamento degli orologi.
auth_time
L'ora in cui è avvenuta l'autenticazione dell'Utente Finale. Il suo valore è un JSON number. Quando è fatta una richiesta max_age o quando auth_time è una richiesta come un asserzione essenziale, allora questo Claim è OBBLIGATORIO; in caso contrario, la sua inclusione è FACOLTATIVA

Flusso di autenticazione di OAuth 2.0

Se consideriamo il flusso di autenticazione secondo il punto di vista dell'utente, abbiamo una serie ben precisa di passaggi per accedere al server delle risorse dal proprio browser:

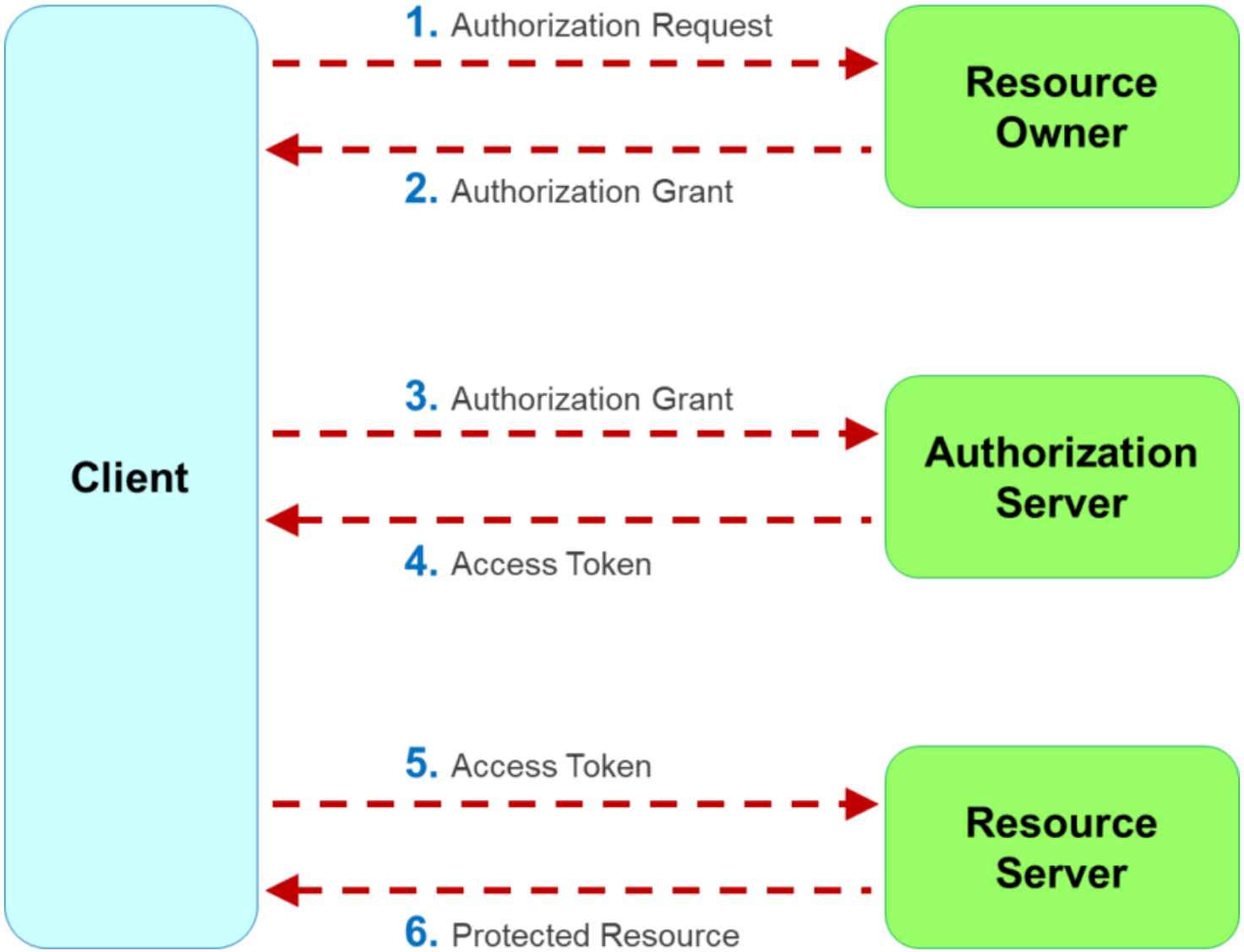
1. **Accesso**: utilizziamo il nome utente ed una password (credenziali) per dimostrare la nostra identità.
2. **Verifica**: il server autentica le credenziali ricevute ed emette il token d'accesso.
3. **Immagazzinamento**: il token viene inviato al browser per essere conservato localmente.
4. **Comunicazione**: ogni volta che si accede a qualcosa di nuovo sul lato server, il token viene sempre verificato.
5. **Cancellazione**: al termine della sessione, il token viene eliminato.

Se consideriamo il modello tecnico/funzionale su cui si basa il processo di autenticazione nel suo complesso, dobbiamo descrivere l'interazione di quattro tipi di ruoli:

1. **Client**: è l'applicazione che richiede l'accesso ad una risorsa protetta per conto del proprietario della risorsa. L'applicazione può essere quella dell'End-User oppure del Service Provider (talvolta detto anche *relying party*).
2. **Resource Owner**: è l'entità in grado di concedere l'accesso ad una risorsa protetta. Quando l'entità è un individuo allora viene definito utente finale (end-user).
3. **Resource Server**: è il server che ospita le risorse protette, capace di accettare e rispondere alla richieste usando il token di accesso. Tipicamente è gestito da un Service Provider.
4. **Authorization Server**: è il server che autentica il Resource Owner ed emette i token di accesso dopo aver ottenuto la giusta autorizzazione. Tipicamente è gestito da un Identity Provider.

Il **flusso generale di funzionamento** del protocollo di autorizzazione è sintetizzato in sei passi, descrivendo le interazioni tra i quattro ruoli:

1. Il Client invia una richiesta di autorizzazione al Resource Owner. Può avvenire direttamente o per tramite dell'Authorization Server che agisce come intermediario.
2. Il Client riceve una concessione di autorizzazione (authorization grant), che rappresenta una credenziale con l'autorizzazione del Resource Owner e può essere espressa in uno dei quattro modi previsti, purché supportati dall'Authorization Server.
3. Il Client richiede un token di accesso autenticandosi sull'Authorization Server, presentando la concessione di autorizzazione.
4. L'Authorization Server autentica il Client, convalida la concessione di autorizzazione e, se valido, emette un token di accesso.
5. Il Client richiede la risorsa protetta dal server delle risorse, presentando il token di accesso.
6. Il Resource Server convalida il token di accesso e, se valido, soddisfa la richiesta.


Client
1. Authorization Request
2. Authorization Grant
Resource Owner
3. Authorization Grant
4. Access Token
Authorization Server
5. Access Token
6. Protected Resource
Resource Server

Il protocollo **OAuth 2.0** prevede i seguenti flussi per i quattro tipi di concessione dell'autorizzazione (*grant type*):

1. **Codice di autorizzazione (*Authorization Code*):** il codice di autorizzazione viene ottenuto utilizzando un Authorization Server come intermediario tra il Client e il Resource Owner. Il Client indirizza direttamente il Resource Owner sull'Authorization Server per autenticarsi, ed in questo modo il Resource Owner non condivide le sue credenziali con Client.
2. **Implicito (*Implicit*):** è un flusso di codice di autorizzazione semplificato ed ottimizzato per i Client su browser che utilizzano un linguaggio di scripting come JavaScript. Viene emesso il token di accesso direttamente senza scambio della concessione di autorizzazione.
3. **Credenziali della password del Resource Owner (*Resource Owner Password Credentials*):** le credenziali di sicurezza del Resource Owner (cioè utente e password) sono usate come concessione di autorizzazione per ottenere il token di accesso.
4. **Credenziali client (*Client Credentials*):** le credenziali del Client sono utilizzate come concessione di autorizzazione, tipicamente quando il Client è anche Resource Owner. Può essere utilizzato per la comunicazione machine-to-machine.

Claims

Con l'uso dei Claims, generalmente trattati come cookie di sessione, OpenID Connect permette all'utente di controllare quali parti sono inviate al Client, garantendo che solo quelle necessarie vengano condivise.

Il vantaggio per la privacy si accompagna però alla necessità di un uso più consapevole delle credenziali stesse, poiché l'eventuale compromissione coinvolgerebbe un insieme ampio di risorse accessibili.

Il parametro claims definisce gli attributi e il livello SPID richiesti.

All'interno dell'elemento «*userinfo*» si elencano gli attributi, da richiedere come chiavi di oggetti JSON, i cui valori devono essere *null*. Gli attributi elencati sotto «userinfo» sono disponibili al momento della chiamata allo UserInfo Endpoint.

Errori di autenticazione

Una risposta di errore di autenticazione è un messaggio OAuth 2.0 Authorization Error Response restituito dall'OP's Authorization Endpoint in risposta al messaggio di richiesta di autorizzazione inviato dal Relying Party (RP).
Se l'utente finale nega la richiesta oppure l'autenticazione dell'utente finale non riesce, l'OP (Authorization Server) informa il RP (Client) utilizzando i parametri di risposta di errore di OAuth 2.0 a meno che il reindirizzamento URI non sia valido, l'Authorization Server restituisce una risposta di errore al Cliente, al URI di reindirizzamento specificato nella richiesta di autorizzazione, con i parametri di stato error. Altri parametri non devono essere restituiti.
Oltre ai codici di errore definiti di OAuth 2.0, esistono i seguenti codici di errore:

- interaction_required - richiestal'interazione dell'utente. Es. è necessario un passaggio di autenticazione aggiuntivo
- login_required – Accesso richiesto
- account_selection_required - è richiesta la selezione dell'account
- consent_required - consenso richiesto
- invalid_request_uri - uri della richiesta non valida
- invalid_request_object - oggetto richiesta non valido
- request_not_supported – richiesta non supportata
- request_uri_not_supported - uri della richiesta non supportato
- registration_not_supported - registrazione non supportata

I parametri di risposta d'errore sono i seguenti: errore RICHIESTO. Codice di errore. error_description FACOLTATIVO. Testo ASCII codificato leggibile dell'errore. error_uri FACOLTATIVO. URI di una pagina web che contiene ulteriori informazioni sull'errore.

OpenID Connect Discovery

OpenID Connect definisce un meccanismo di scoperta, chiamato **OpenID Connect Discovery** , in cui un server OpenID pubblica i suoi metadati su un URL
Questo URL restituisce un elenco (JSON) degli endpoint OpenID/OAuth, ambiti e attestazioni supportati, chiavi pubbliche utilizzate per firmare i token e altri dettagli.
I client possono utilizzare queste informazioni per costruire una richiesta al server OpenID.
I nomi e i valori dei campi sono definiti nella specifica di rilevamento di OpenID Connect .

Il documento Class Discovery contiene le seguenti proprietà dei metadati del provider OpenID

Proprietà	Valore	Descrizione
emittente	URI	Identificativo dell'emittente della classe.
endpoint_autorizzazione	URI	L'URI per effettuare richieste di autorizzazione al server di autorizzazione della classe come parte del flusso del codice di autorizzazione.
token_endpoint	URI	L'URI per effettuare richieste di token al server di autorizzazione della classe come parte del flusso del codice di autorizzazione .
utenteinfo_endpoint	URI	L'URI per effettuare richieste UserInfo per ottenere informazioni sull'utente.
concedere_tipi_supportati	Matrice di stringhe	I tipi di concessione OAuth 2.0 supportati dal server di autorizzazione della classe.

Linee guida per OpenID Connect in SPID

Sono disponibili sul sito docs.italia.it le nuove regole tecniche relative a Open ID Connect (OIDC) per SPID e CIE.

In base alle linee guida, redatte ai sensi del Codice dell'Amministrazione Digitale (CAD) e adottate da AgID con la Determinazione n. 616/2021, i gestori dell'identità digitale dovranno obbligatoriamente utilizzare **OpenID Connect** a partire dal 1 maggio 2022. La novità riguarda anche i fornitori pubblici e privati che vogliono erogare i propri servizi online.

OpenID Connect è la terza generazione dello standard open che permette di effettuare l'**autenticazione** su diversi siti attraverso un "identity provider" di terze parti, utilizzando le stesse credenziali.

La tecnologia è oggi integrata in quasi tutte le app mobile, tra cui quelle di Google, Microsoft e PayPal.

Rispetto allo standard **SAML** (Security Assertion Markup Language) attualmente usato per lo SPID, AgID evidenzia tre principali vantaggi:

- maggiore sicurezza
- maggiore facilità di integrazione in sistemi eterogenei (single-page app, web, backend, mobile, IoT)
- migliore integrazione di componenti di terze parti in modalità sicura, interoperabile e scalabile

OpenID Connect prevede inoltre vari **controlli di sicurezza obbligatori**, tra cui quelli che consentono di evitare ai malintenzionati di intercettare le comunicazioni, soprattutto nel caso di applicazioni per dispositivi mobile.

Lo standard permette anche di usare **sessioni lunghe revocabili** per evitare l'inserimento frequente della password e la possibilità per gli utenti di bloccare un'autenticazione precedentemente effettuata.

Tutte le amministrazioni – centrali, locali, enti pubblici e agenzie – devono rendere accessibili i propri servizi online tramite SPID e CIE.

Anche gli enti privati possono abilitare l'accesso con SPID ai propri servizi.

Il processo di adesione a SPID prevede una serie di step tecnico amministrativi che portano alla conclusione del processo di onboarding

1. seguire le regole tecniche di AgID per attivare SPID e le indicazioni per rendere riconoscibile l'accesso agli utenti; effettua i test necessari di implementazione della piattaforma e individua un referente tecnico per le interlocuzioni con AgID;
2. predispore e rendere disponibili per i controlli di AgID il metadata che consentirà ai gestori di identità (identity provider - IDP) di configurare l'accesso ai servizi con SPID. Dopo i controlli, il collaudo del servizio e la firma della convenzione, AgID comunica il metadata ai gestori;
3. se l'accesso con SPID prevede il secondo o il terzo livello di sicurezza, devi implementare anche il nodo italiano eIDAS che consente l'accesso ai servizi pubblici italiani dei cittadini dell'UE;
4. terminati i processi tecnici, dopo il riscontro positivo di AgID, si puo sottoscrivere la convenzione SPID tramite un referente amministrativo. Firmata la convenzione, AgID informa i gestori e successivamente i servizi diventeranno accessibili con SPID.

Per gestire l'accesso ai servizi pubblici e privati che utilizzano il sistema SPID, si rende necessario, sia per una questione di user experience che di immagine del sistema, la standardizzazione delle interfacce, della comunicazione e dell'utilizzo del logo spid.

Gli ambiti di analisi sono i seguenti:

1. Strutturazione pagina informativa (identity provider)
2. Strutturazione pagina di registrazione (identity provider)
3. Interfaccia di accesso all'autenticazione (service provider)
4. Interfaccia di autenticazione (identity provider)
5. Utilizzo del logo e componenti grafici
6. Json di standardizzazione testi, stringhe e implementazione multilingua

Strutturazione pagina informativa

La pagina informativa dell'identity provider deve:

- Definire cos'è SPID
- Indicare quali sono le caratteristiche
- Indicare come ottenere l'identità Digitale
- Indicare Come usare l'identità Digitale
- Indicare i servizi accessibili attraverso SPID

- Nella pagina deve essere presente e visibile il logo SPID (Per le regole da seguire nell'utilizzazione del logo SPID si rimanda alla sezione "Logo e componenti grafiche")
- Nel definire "cos'è SPID" deve essere specificato che i servizi offerti dall'identity provider sono strumenti che consentono di accedere ai servizi online di pubbliche amministrazioni e privati che sono parte del sistema SPID.
- Nella sezione dedicata alle caratteristiche dell'identità digitale SPID devono essere chiaramente indicati i tre livelli di identità e le differenti caratteristiche in maniera chiara e definita.
- Nella sezione dedicata a "come ottenere l'identità digitale" devono essere chiaramente indicate le modalità di riconoscimento dell'utente utilizzate dal gestore per il rilascio dell'identità digitale SPID.
- Nella sezione dedicata a "come ottenere l'identità digitale" devono essere chiaramente indicate le diverse modalità previste dall'identity provider per il rilascio di identità SPID di livelli differenti.
- Nella sezione dedicata ai "servizi" devono essere indicati i servizi online di Pubbliche amministrazioni e privati accessibili tramite SPID sulla base del percorso di implementazione comunicato dall'Agenzia per l'Italia Digitale.

Strutturazione pagina di registrazione

La pagina di registrazione dovrà essere strutturata in modo da informare in maniera puntuale l'utente sulle varie modalità di ottenimento dell'identità digitale e sulle strumentazioni da utilizzare.
Dovrà, inoltre, essere ben distinta la parte di dati/clausole per l'ottenimento di SPID da quella commerciale.

1. Per le varie modalità di ottenimento dell'identità digitale dovrà essere specificato, prima della procedura di iscrizione:
    a. Descrizione per ogni modalità di ottenimento dell'identità digitale di:
        i. Strumenti necessari all'ottenimento dell'identità digitale
        ii. Tempistiche medie di ottenimento con la modalità scelta iii. Eventuali costi accessori (ben evidenziando che non si tratta del pagamento dell'identità ma di una facilitazione commerciale a supporto della)
    b. Dopo aver scelto la modalità di erogazione dell'identità dettagliare i vari passaggi evidenziando:
        i. Step x: "Titolo fase di registrazione
        ii. Step x: "Descrizione delle informazioni che verranno richieste dividento tra informazioni per l'ottenimento di SPID e informazioni di natura commerciale"
        iii. Step x: "Tempistiche medie di compilazione"
        iv. Step x: "Attività tecniche diverse dall'immissione dati (scannerizzazione, attivazione webcam, firma pades/cades)
        v. Step x: "Tempistiche medie per passaggio a step successivo"

c. Il modulo di registrazione dovrà dividere i dati necessari all'ottenimento dell'identità digitale dalle informazioni che il gestore riterrà utili a fini commerciali/marketing e dovrà "nominare" due sezioni "Dati obbligatori per l'ottenimento dell'Identità Digitale SPID" e "Dati non obbligatori di natura commerciale e di marketing"; i dati per l'ottenimento dell'identità digitale (Art. 5 delle modalità attuative), ovvero:

i. Per le persone fisiche sono obbligatorie le seguenti informazioni:
    1. cognome e nome; 2. sesso 3. data 4. luogo di nascita 5. codice fiscale 6. estremi di un valido documento di identità, 7. numero di telefono 8. email 9. pec

ii. Per le persone giuridiche sono obbligatori
    1. denominazione/ragione sociale 2. codice fiscale o P.IVA (se uguale al codice fiscale 3. sede legale 4. visura camerale attestante lo stato di rappresentante legale del soggetto richiedente l'identità per conto della società5. estremi del documento di identità utilizzato dal rappresentante legale 6. numero di telefono 7. email 8. pec

iii. Tutti gli altri dati vanno inseriti nella sezione "Dati non obbligatori di natura commerciale e di marketing

d. La strutturazione dell'accettazione delle clausole, segue la linea dei moduli; dovranno essere infatti distinte le clausole di accettazione per l'utilizzo dell'identità digitale da quelle di natura commerciale e di marketing e dovranno essere nominate rispettivamente:

"Clausole di accettazione per l'ottenimento dell'Identità Digitale SPID" e "Altre clausole di natura commerciale e di marketing".

Interfaccia di accesso all'autenticazione (service provider)

I service provider dovranno creare una pagina di scelta Identity Provider a cui si accederà tramite il bottone SPID o direttamente dalla funzionalità di accesso all'applicazione per cui si richiede autenticazione.
Il bottone è presentato in 4 dimensioni (s / m / l / xl) ed in formato "get" (chiamata ad una pagina esterna con variabile) e "post" (form interna al pulsante).

Il bottone "Entra con SPID" non dovrà essere modificato nelle forme proposte o nei colori e potrà essere modificato, soltanto nel codice, se si verificasse un caso di incompatibilità con gli stili del portale web.

Le interfacce per gli Identity Provider sono rilasciate in formato html/css/javascript in modo da essere facilmente implementate nel sistema di autenticazione e sono già testate sotto il profilo di ***accessibilità, user experience e conformi alle linee guida di design dei siti della Pubblica Amministrazione.***

Il logo spid dovrà essere presente in ogni sito web, applicazione, documento, pubblicità che riguarda attività che gestiscono o utilizzano in maniera diretta o indiretta il sistema SPID ovvero: - Siti web informativi; - Applicativi e app desktop e mobile; - Ogni documento cartaceo - Ogni pubblicità o materiale informativo Il logo dovrà essere presente nell'header o comunque ben visibile nel contesto della layout

Nodo italiano eIDAS

Dal 29 settembre 2018 tutte le pubbliche amministrazioni che offrono servizi digitali tramite SPID o CIE rendono accessibili tali servizi ai cittadini europei dotati di identità digitale (eID) riconosciuta in ambito eIDAS.

Il nodo italiano eIDAS opera come un IDP SPID virtuale, pertanto l'impatto sulle attività di configurazione del service provider che aderisce al sistema SPID sono minime. Per attivare il login eIDAS:

1. Consultare le regole tecniche relative a SPID e l' Avviso eIDAS 01-2018.
2. Estendere l'attuale metadata SPID seguendo le specifiche riportate nell' Avviso eIDAS 01-2018
3. Dopo aver esteso il metadata, renderlo disponibile online e richiedi la federazione in ambiente di Quality Assurance
4. Una volta completata la federazione in ambiente di Quality Assurance è possibile richiedere la federazione in ambiente di Produzione

Convenzioni SPID

La federazione SPID prevede diverse convenzioni per entrare nel circuito.

SPID prevede i seguenti soggetti:
utenti, gestori di identità digitale, fornitori di servizi pubblici e privati, soggetti aggregatori e gestori di attributi qualificati.
Tali soggetti, ad eccezione degli utenti, devono sottoscrivere una convenzione con AgID per entrare nel circuito.

CORRISPETTIVI SERVIZIO DI AUTENTICAZIONE SPID
DEFINIZIONI Autenticazione - il processo con cui il Fornitore di Servizi chiede di ricevere dal Gestore dell'Identità digitale l'ID SPID e/o uno o tutti gli attributi dell'anagrafica (Codice Fiscale, Nome, Cognome, Sesso, Data di Nascita, Luogo di Nascita). Registrazione - il processo con cui il Fornitore di Servizi chiede di ricevere dal Gestore dell'Identità digitale l'ID SPID e/o uno o tutti gli attributi extra-anagrafica. La richiesta diregistrazione dà diritto di ricevere anche tutti gli attributi dell'anagrafica. Tipicamente il Fornitore di Servizi che fa una richiesta di registrazione richiede tutta l'anagrafica e tutti gli attributi extra-anagrafica. Utente unico - la persona fisica o giuridica che utilizza la propria identità digitale SPID per accedere una o più volte ad un servizio in rete.
MODELLO DI PRICING Il presente modello definisce le logiche di calcolo dei corrispettivi che i Fornitori di Servizi privati devono corrispondere ai Gestori dell'Identità digitale, individuando una logica di tipo 'pay per user'. All'interno di ciascun periodo di fatturazione, gli accessi effettuati da un utente unico, saranno fatturati dal singolo Gestore dell'Identità una sola volta per ogni Fornitore di Servizi, indipendentemente dalla numerosità degli accessi. Al fine di valorizzare in modo congruo le transazioni di accesso con SPID, il modello di pricing individua due differenti scenari, legando il prezzo degli accessi al numero e alla tipologia di attributi richiesti dal Fornitore di Servizi: - Accessi in modalità 'Autenticazione': autenticazioni SPID con richiesta dei soli attributi dell'anagrafica del Titolare (cfr. Definizioni) - Accessi in modalità 'Registrazione': autenticazioni SPID con richiesta di attributi non legati all'anagrafica del Titolare (cfr. Definizioni) ed eventuale richiesta di attributi dell'anagrafica del Titolare.

Sulla base delle logiche indicate, quindi, il corrispettivo che i Fornitori di Servizi dovranno pagare annualmente ai Gestori dell'Identità digitale sarà così calcolato:

Utenti per anno	Login Autenticazione liv 1 o 2	Login Registrazione liv 1 o 2	Login Autenticazione liv 3	Login Registrazione liv 3
0 - 1000	Gratuito	€ 3.5	Gratuito	€ 7
> 1000	€ 0.4	€ 3.5	€ 7	€ 7

Gestore	Data
Aruba PEC S.p.A.	8 novembre 2017
Etna Hitech S.C.p.A.	11 gennaio 2023
InfoCamere S.C.p.A.	04 marzo 2023
InfoCert S.c.p.A.	22 novembre 2017
Intesi Group S.p.A.	19 dicembre 2022
Lepida S.c.p.A.	31 ottobre 2018
Namirial S.p.A.	7 novembre 2017
Poste Italiane S.p.A.	18 dicembre 2017
Register S.p.A.	8 ottobre 2017
Sielte S.p.A.	8 novembre 2017
TeamSystem S.p.A.	29 giugno 2022
TI Trust Technologies S.r.l.	8 novembre 2017

Carta di Identità Elettronica

Vediamo adesso le modalità operative per l'adozione della Carta di Identità Elettronica (CIE) come strumento di accesso ai servizi erogati in rete dalle Pubbliche Amministrazioni e dalle organizzazioni private come previsto dall"art. 64 del CAD), così come modificato dall" art. 24, comma 1 – lett. e) nn. 3) e 6) - del Decreto Legge 16 luglio 2020, n. 76 recante "Misure urgenti per la semplificazione e l'innovazione digitale" ("Decreto Semplificazioni"), convertito, con modificazioni, dalla L. 11 settembre 2020, n.120.

Lo schema di identificazione basato sulla CIE, dettagliato nel presente documento, è compatibile con il Level of Assurance 4 (HIGH) del regolamento UE 910/2014 eIDAS (GUUE C309 del 13 settembre 2019) e consente ai cittadini di fruire dei servizi offerti online dalle Pubbliche Amministrazioni e dei soggetti privati utilizzando gli elementi di sicurezza presenti sulla propria CIE (chiavi crittografiche protette da PIN e Certificati) come credenziali per la propria identificazione.

La Carta d'identità elettronica (CIE) è il documento di identità rilasciato dai Comuni italiani su richiesta dei cittadini che ne certifica l'identità fisica e digitale.
È considerata una piattaforma abilitante ai sensi del Piano Triennale per l'informatica nella Pubblica Amministrazione dal momento che consente l'attivazione di servizi basati sull'utilizzo del microprocessore a radio frequenza di cui è dotata. Nello specifico, per il tramite della CIE e del PIN che ciascun cittadino riceve, metà alla richiesta, metà con la carta, è possibile accedere ai servizi erogati in rete dalle PP.AA. e dai soggetti privati con i massimi livelli di sicurezza.
Lo schema di autenticazione con CIE si basa su un modello diverso da quello utilizzato per l'accesso in rete mediante la Carta Nazionale dei Servizi "CNS".
Con la CNS, infatti, l'utente utilizza la carta come contenitore della coppia di chiavi di autenticazione TLS.
Il middleware CNS consente l'autenticazione verso il sito dell'erogatore del servizio, sul quale ricade interamente l'onere della verifica della validità della catena di certificati della CA Autenticazione del Ministero dell'Interno.
Lo schema di autenticazione "***Entra con CIE***" è, invece, basato su un sistema di *Single Sign-On* (SSO) che consente a chi rilascia l'identitá digitale (Identity provider) di inviare le credenziali di autorizzazione dell'utilizzatore finale al fornitore di servizi (Service Provider), sollevando quest'ultimo dall'onere di gestione delle identità digitali.
Il vantaggio da parte dell'utilizzatore che fa richiesta di autenticazione è altrettanto tangibile, in quanto tale schema di identificazione consente di avere un'unica chiave di accesso superando, in questo modo, il modello tradizionale di autenticazione basato su password specifiche per ogni servizio.

Schema di autenticazione

1. il cittadino richiede a un Service Provider la fruizione di un servizio digitale;
2. il Service Provider invia all'Identity Provider una richiesta di autenticazione del cittadino;
3. l'Identity Provider richiede al cittadino di utilizzare la sua CIE per autenticarsi avvicinandola a un lettore RF collegato a un PC o direttamente al proprio dispositivo mobile dotato di interfaccia NFC e inserendo il PIN. Viene, inoltre, verificata, la validità del certificato digitale associato al cittadino;
4. l'Identity Provider reindirizza l'utente verso il Service Provider inviando a quest'ultimo l'esito di avvenuta autenticazione e gli attributi identificativi dell'utente;
5. il Service Provider, in caso di esito positivo, concede l'accesso al servizio richiesto.

Il set di dati che vengono inviati al Service Provider sono i seguenti:

•nome; cognome; data di nascita; codice fiscale.

Il processo di autenticazione è garantito mediante la verifica di validità (autenticità e scadenza) del certificato digitale presente nella CIE che viene letto dal microprocessore della carta ed inviato presso la CA Autenticazione (DM del 23/12/2015 "Modalità tecniche di emissione della Carta d'Identità elettronica").

La procedura garantisce la correttezza delle informazioni sia al Ministero dell'Interno - cui è riservata l'emissione della Carta di identità elettronica – che alle pubbliche amministrazioni e ai soggetti erogatori di servizi pubblici e privati che consentono l'accesso tramite CIE.

La CIE, inoltre, è stata riconosciuta dal Cooperation Network eIDAS (electronic IDentification Authentication and Signature) come strumento di identificazione digitale e di accesso ai servizi online erogati nei paesi dell'Unione Europea compatibile con il Level of Assurance 4 (high), in conformità con quanto previsto dal Regolamento UE n° 910/2014 sull'identità digitale.

La fase di onboarding costituisce il prerequisito fondamentale per il processo di integrazione dello schema di autenticazione «Entra con CIE». Tale fase è eseguita mediante il portale di federazione erogatori di sevizi, messo a disposizione dall'Identity Provider e gestito e sviluppato dal Poligrafico che, in qualità di partner tecnologico del Ministero dell'Interno, ne cura tutti gli aspetti tecnici. Il portale di federazione erogatori di sevizi consente al Service Provider di:

- registrarsi ed effettuare facilmente la richiesta di adesione
- federare i metadata e ricevere l'esito della federazione
- verificare in ogni istante lo stato delle attività

I principali vantaggi che derivano dall'utilizzo del portale di federazione sono:

- gestione e controllo dell'intero ciclo: federazione, sviluppo, test, produzione, esercizio e conduzione operativa;
- Snellimento delle procedure amministrative e tecniche di onboarding;
- processo di federazione e configurazione più efficiente.

Il processo di onboarding puó essere suddiviso in quattro sottofasi distinte:

1. Registrazione al portale e richiesta formale di adesione;
2. Autorizzazione alla federazione
3. Inserimento dei dati tecnici di federazione;
4. Federazione.

Conservazione Logs

Ai fini della tracciatura l'Identity Provider dovrà mantenere un Registro delle transazioni contenente i tracciati delle richieste di autenticazione servite negli ultimi 24 mesi. L'unità di memorizzazione di tale registro dovrà rendere persistente per ogni transazione la tripla composta dell'identificativo dell'identità digitale (spidCode) interessata dalla transazione, dalla <AuthnRequest> e della relativa <Response>.

Al fine di consentire una facile ricerca e consultazione dei dati di tracciature potrebbe essere opportuno memorizzare in ogni record informazioni direttamente estratte dai suddetti messaggi in formato SAML.

Il regolamento recante le modalità attuative per la realizzazione dello SPID (articolo 4, comma 2, DPCM 24 ottobre 2014) riporta l'obbligo dei fornitori di servizi alla conservazione per ventiquattro mesi delle informazioni necessarie a imputare alle singole identità digitali le operazioni effettuate sui propri sistemi.
Le informazioni saranno costituite da registrazioni composte dal messaggio SAML di richiesta di autenticazione e della relativa asserzione emessa dal gestore delle identità.
I messaggi riportano identificativi e date di emissione e sono firmati, rispettivamente, dallo stesso fornitore di servizi e dal gestore dell'identità digitale; quest'ultima caratteristica fornisce le necessarie garanzie di integrità e non ripudio.

L'insieme delle Registrazioni costituisce il Registro delle transazioni del fornitore del servizio. Le tracciature devono avere caratteristiche di ***riservatezza, inalterabilità e integrità*** e sono conservate adottando idonee misure di sicurezza ai sensi dell'articolo 31 del decreto legislativo 30/06/2003, n. 196 , sotto la responsabilità del titolare del trattamento; l'accesso ai dati è riservato a personale espressamente autorizzato e incaricato del trattamento dei dati personali. Devono essere utilizzati meccanismi di cifratura.

I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Analogo registro dovrà essere tenuto dal gestore delle identità digitali, secondo modalità definite nelle regole tecniche di cui all'articolo 4, comma 3 del DPCM.

Gli accessi al servizio sono registrati sotto forma di log certificato. Il log certificato è composto da un file di testo prodotto dall'applicativo che gestisce il processo di autenticazione e dialogo con i Service Provider, il quale viene firmato e marcato temporalmente prima della conservazione nel sistema di conservazione InfoCert. È garantita l'integrità nonché la disponibilità secondo quanto previsto dal DPCM.
Contiene, le seguenti informazioni corrispondenti a quanto richiesto nonché consigliato nelle regole tecniche:

- lo SPID code (come chiave del tracciato)
- la richiesta del SP
- la risposta del IdP
- ID della richiesta
- timestamp della richiesta
- SP richiedente autenticazione (issuer richiesta)
- ID della risposta
- timestamp della risposta
- IdP autenticante (issuer risposta)
- ID dell'asserzione di risposta
- soggetto dell'asserzione di risposta (subject)

Il che fornisce una chiara informazione dei campi da conservare anche se indicano che il log "contiene tra l'altro" quindi non si sa cosa altro viene salvato.