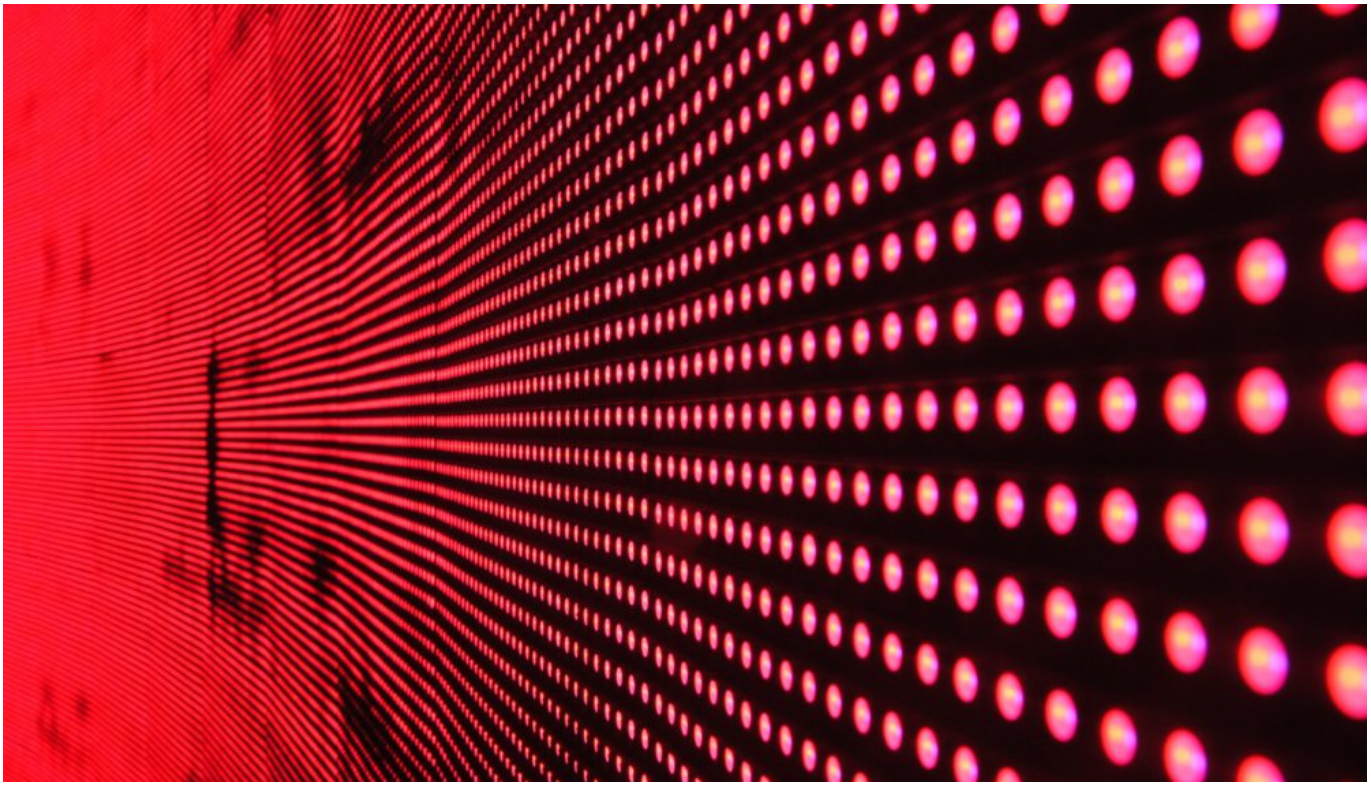
OPENID CONNCET

Identità digitali: la ricerca e la PA insieme verso nuovi standard

OpenID Connect è uno standard di autenticazione per web e mobile usato da Google, Microsoft e tanti altri attori di primo piano del mondo digitale. E i settori della ricerca e dell'istruzione, così come l'e-Government si stanno mostrando interessati, anche per normarlo nel sistema SPID. Facciamo il punto

1 giorno fa

Davide Vaghetti
GARR, Coordinatore del Servizio IDEM



OpenID Connect è uno standard attualmente utilizzato per l'autenticazione e l'autorizzazione dalla quasi totalità delle moderne applicazioni web e mobile per uso personale.

Considerato il successo dello standard e delle sue varianti, non stupisce che anche i settori della ricerca e dell'istruzione, così come l'e-Government si stiano muovendo verso OpenID Connect. In tale contesto vanno inserite le **Linee Guida OpenID Connect in SPID** elaborate da AgID e presentate al Workshop GARR 2019 da Antonio Florio e Michele D'Amico durante il panel su OpenID Connect.

Vediamo quali sono le principali caratteristiche dello standard e come si sta muovendo il mondo italiano della ricerca per sostenere una maggiore diffusione delle identità digitali federate.

Indice degli argomenti

Integrazione dei sistemi di gestione delle identità digitale

In Italia, il mondo dell'università e della ricerca, ma anche quello della pubblica amministrazione, stanno perseguendo l'obiettivo di facilitare l'integrazione dei sistemi di gestione delle identità con un numero sempre maggiore di applicazioni basate su diverse piattaforme (app, web, mobile, IoT) e con componenti di terze parti in modalità sicura, interoperabile e scalabile.

Per discutere di queste novità tra gli esperti del settore, in occasione di Net Makers, il Workshop GARR 2019 che si è svolto a Roma dall'8 al 10 ottobre, è stato organizzato un panel dedicato allo standard di autenticazione OpenID Connect che rappresenta la soluzione che più di tutte sta riscontrando successo e la cui filosofia di design è «rendi semplici le cose semplici e rendi possibili le cose complicate».

OpenID Connect è uno standard di autenticazione per web e mobile usato da Google, Microsoft e tanti altri attori di primo piano del mondo digitale. La quantità di applicazioni disponibili e la sua diffusione presso gli sviluppatori ha reso imperativo il supporto da parte dei sistemi di eGov-ID come SPID e delle federazioni di identità della ricerca e dell'istruzione come IDEM, gestita da GARR. Non a caso AgID ha da qualche mese pubblicato una bozza di linee guida per l'uso di OpenID Connect in SPID. Allo stesso tempo nel mondo della ricerca si stanno sperimentando sistemi di autenticazione OpenID Connect da affiancare a quelli già esistenti.

Un protocollo di autenticazione robusto e flessibile

OpenID Connect permette alle applicazioni web e mobile di **fornire servizi senza dover registrare ed autenticare gli utenti per conto loro**. In pratica, quando un utente tenta di accedere ad un'applicazione, viene rediretto verso un sistema di autenticazione presso il quale ha precedentemente registrato la propria identità. Una volta autenticato con successo, l'utente viene riportato sull'applicazione web o mobile e può immediatamente utilizzarne i servizi. Se avete utilizzato almeno una volta uno dei tanti servizi che si appoggiano alla vostra identità Google, Facebook, Microsoft, ecc., avete già usato OpenID Connect, o una sua variante.

OpenID Connect è comunemente definito come un semplice strato di identità al di sopra del protocollo di autorizzazione OAuth 2.0. Difatti, è proprio avvalendosi per intero dell'estesa superficie di specifiche di OAuth 2.0 che gli autori di OpenID Connect sono riusciti a limitare il loro lavoro alla parte di identità. In particolare, per la definizione delle identità digitali OpenID Connect si avvale di **JSON Web Token** (JWT), uno standard di rappresentazione di dati compatto e sicuro fatto apposta per trasmettere affermazioni su specifici soggetti tramite il web. Non a caso JWT è stato scritto dagli stessi autori di OpenID Connect. Il connubio tra nuove specifiche, come JWT, e OAuth 2.0 ha creato un protocollo di autenticazione al contempo robusto e flessibile, vediamo come.

Uno standard a sviluppo continuo

Il 62% dei progetti di trasformazione digitale fallisce? Le idee ci sono, ma appena il 38% dei progetti ha successo.

Chiariamo un aspetto, OpenID Connect non nasce nel vuoto: oltre a basarsi su OAuth 2.0, molti dei concetti legati all'autenticazione e alla definizione delle identità digitali sono stati **mutuati dai protocolli esistenti** ed in particolare da SAML 2.0. Pubblicato nel 2005 da OASIS (Organization for the Advancement of Structured Information Standards), SAML 2.0 è diventato nel tempo lo standard di riferimento per l'autenticazione nel settore enterprise, in quello della ricerca e dell'educazione e per le soluzioni di e-Government. Su SAML 2.0 sono infatti basate la Federazione di identità delle università e degli enti di ricerca italiani **IDEM** (), l'inter-federazione mondiale **eduGAIN** e **SPID**, il Sistema Pubblico di Identità Digitale. SAML 2.0 è uno standard molto ampio che copre un numero elevato di casi d'uso e definisce dettagliatamente le possibili varianti di utilizzo a seconda delle esigenze. SAML 2.0 si basa su XML per la rappresentazione dei dati e delle entità in gioco, questo permette di definire e validare con precisione ogni parametro a patto di sacrificare brevità e, molto spesso, flessibilità.

Semplicità e flessibilità

OpenID Connect 1.0, pubblicato nel 2014, è invece uno standard che ha fatto di compattezza, semplicità e flessibilità le proprie bandiere. **Si basa su due principi di design: fare in modo semplice le cose semplici e rendere possibili le cose più complesse**. OpenID Connect, come SAML 2.0, distingue tre attori principali: l'utente, il servizio da autenticare o *client* ed il server di autenticazione. La semplicità è massima proprio nei requisiti e nelle tecnologie che il *client* è tenuto a rispettare ed implementare, ovvero il protocollo HTTP ed il formato dei dati JSON Web Token, almeno per le funzioni di base. Il supporto per i casi d'uso più complessi è offerto in modo modulare tramite estensioni e interazioni con altri standard.

OpenID Connect è attualmente supportato da Google, Microsoft, PayPal, Ping Identity, Verizon e molti altri. **Va inoltre considerato che altri grossi player, come Facebook e Linkedin, pur non supportando direttamente lo standard, utilizzano i suoi componenti fondamentali ovvero OAuth 2.0**

ed il formato JSON Web Token. Ne consegue che la quasi totalità delle moderne applicazioni web e mobile per uso personale utilizzano lo standard, o sue varianti, per l'autenticazione e l'autorizzazione. Moltissime sono anche le applicazioni in ambiente enterprise, dove fino a poco tempo fa dominava invece quasi unicamente SAML 2.0.

Ricerca, istruzione e PA verso lo standard

Le linee guida di AgID, che ad oggi sono ancora allo stato di bozza, definiscono l'utilizzo dello standard nell'ambito di SPID. Lo scopo dichiarato è avvalersi dei punti di forza di OpenID Connect (ovvero la semplicità, il supporto per il mobile, la diffusione, e così via) coniugandoli con il rispetto degli standard di sicurezza richiesti da SPID. Ma andiamo con ordine.

Le linee guida si basano sul profilo iGOV dello standard OpenID Connect 1.0. Il profilo iGOV, definito dal **gruppo di lavoro International Government Assurance Profile** della OpenID Foundation, stabilisce una serie di regole per l'uso sicuro dello standard proprio dedicato al settore del e-Government. Al profilo iGOV le linee guida aggiungono ulteriori requisiti, come ad esempio l'uso dello standard PKCE [PKCE] per le credenziali delle applicazioni, e limitazioni, come il supporto per il solo scope *openid*.

Le linee guida definiscono poi la modalità con cui implementare i livelli di autenticazione corrispondenti ai livelli SPID, come richiedere e trasmettere i dati personali dell'utente e la funzione del Registro SPID per la distribuzione dei metadata dei server di autenticazione (chiamati OpenID Provider) e delle applicazioni. **Va notato che ad oggi non sembra essere molto chiaro come validare le informazioni contenute nel Registro SPID**, visto che le informazioni non sono firmate digitalmente, ma questo specifico aspetto potrà essere affrontato in futuro.

Infine le linee guida definiscono le cosiddette "sessioni lunghe revocabili" da utilizzare nell'ambito delle applicazioni mobile laddove non sia sempre necessario per l'utente inserire ogni volta le proprie credenziali. **Le sessioni lunghe revocabili si basano sui *refresh token* di OpenID Connec**t, ma limitano le funzionalità in assenza dell'utente alle sole notifiche e permettono di mantenere solo il livello base di autenticazione (SPID livello 1).

Da poco più di un mese è terminato il periodo di consultazione sulla bozza delle *Linee Guida OpenID Connect in SPID* elaborate da AgID, speriamo che il grande sforzo di elaborazione e di adattamento fatto dagli autori porti presto alla versione definitiva.

Cosa sta facendo la comunità dell'università e della ricerca

Anche nel settore della ricerca e dell'istruzione, come detto, cresce l'interesse ed il supporto per OpenID Connect. Sul tema, Enrico Maria Vincenzo Fasanelli dell'Istituto Nazionale di Fisica Nucleare (INFN) ha raccontato una prima implementazione dello standard OpenID Connect nell'infrastruttura di autenticazione e autorizzazione dell'INFN (INFN-AAI). INFN, come la quasi totalità delle università e degli enti di ricerca italiani, è membro della Federazione IDEM, gestita da **GARR,** ed ha una infrastruttura essenzialmente basata su SAML 2.0.

L'implementazione di OpenID Connect di INFN è basata su un software di gestione dell'identità e dell'accesso open source, Keycloak. Durante il suo intervento al al Workshop GARR 2019, Fasanelli ha mostrato come siano state utilizzate le funzionalità di proxy del software Keycloak per implementare OpenID Connect al di sopra dell'infrastruttura esistente. Inoltre **INFN ha implementato il servizio utilizzando la propria piattaforma per container basata su OpenShift**. Il riutilizzo dell'infrastruttura esistente e l'impiego dei container hanno permesso di mettere in piedi un servizio pronto per la produzione con tempi e risorse molto contenuti. Il servizio è in questo momento in una fase pilota e passerà in produzione nei prossimi mesi.

In molte altre università e centri di ricerca si implementano soluzioni locali per implementare OpenID Connect e poter beneficiare del vasto ecosistema di applicazioni, librerie e sviluppatori che si è creato attorno al protocollo. Allo stesso tempo, nella OpenID Foundation, nelle federazioni di identità e nella **comunità di eduGAIN** (il servizio di inter-federazione mondiale) sono allo studio soluzioni per utilizzare il protocollo anche nell'ambito delle federazioni multilaterali, in cui cioè vi sono servizi di identità e servizi di accesso alle risorse che dialogano in sicurezza tramite una terza parte fidata, la federazione appunto. Con tutta probabilità nel corso del 2020 emergerà finalmente uno standard per la creazione di federazioni di identità multilaterali per OpenID Connect 1.0 che possano affiancare le consolidate architetture basate su SAML 2.0.

Proprio per facilitare la ricerca, lo scambio di esperienze e l'evoluzione in questa direzione, nella Federazione IDEM è attivo un gruppo di lavoro aperto a chiunque, all'interno della comunità della ricerca, della pubblica amministrazione e dell'industria, voglia contribuire.

Il 62% dei progetti di trasformazione digitale fallisce? Le idee ci sono, ma appena il 38% dei progetti ha successo.