



La federazione delle identità ed il suo valore dal punto di vista aziendale

Gennaio 2006

Indice

Introduzione	3
Federazione e valore aziendale	3
Sicurezza e federazione	3
Requisiti per la federazione	4
Casi d'uso della federazione	4
Scenari basati su browser	4
Federazione basata sul collegamento degli account	4
Federazione basata su ruoli	5
Scenari basati su documenti	5
Servizi web concatenati	5
Importanti questioni aziendali inerenti la federazione	6
Standard di federazione	7
Security Assertion Markup Language (SAML)	7
Liberty Alliance	7
ID-FF	7
WS-Federation	8
WS-Security	8
Conclusioni	8

Introduzione

Raggiungere un efficace coordinamento ed un elevato livello di integrazione dei processi aziendali con i partner commerciali in un panorama economico sempre più dinamico è una sfida complessa per molte grandi imprese. La federazione delle identità e gli standard su cui si basa sono stati ideati proprio per affrontare questa sfida cross-domain di interoperabilità delle applicazioni. Il presente documento introduce e definisce il concetto di federazione delle identità, i vantaggi che le aziende possono trarre dalla sua applicazione, alcuni casi d'uso resi possibili da tale sistema, i principali standard e specifiche che lo riguardano e le questioni aziendali che occorre risolvere per essere in grado di adottare la federazione delle identità su vasta scala.

Federazione e valore aziendale

La possibilità di disporre di un accesso di base alle applicazioni ed ai dati tramite Internet esiste da anni. Tuttavia la possibilità, per un utente, di accedere con facilità ed in sicurezza a servizi localizzati su molteplici domini di sicurezza all'interno di un'azienda oppure offerti da diverse organizzazioni, è rimasta una sfida. Vent'anni fa, molti guardavano con speranza allo scambio elettronico di dati (EDI, electronic data interchange), utilizzato con successo nell'industria automobilistica, manifatturiera e del commercio; tuttavia questo sistema non è riuscito a prendere piede in molte aziende, fondamentalmente a causa dei suoi costi, della scarsa flessibilità e della sua natura proprietaria. Inoltre, l'EDI non ha comportato alcun beneficio diretto ai consumatori né ad altre classi di utenti finali.

Oggi Internet, con le sue tecnologie ed i suoi standard, è maturata al punto che è divenuto possibile, ed anche economicamente sostenibile, ottenere un efficace coordinamento ed un elevato livello di integrazione tra partner commerciali. Inoltre, l'avvento degli standard sta rendendo possibile ampliare le aziende moderne eliminando le barriere che impediscono il collegamento di applicazioni aziendali diverse sia all'interno dell'ambito aziendale che tra organizzazioni differenti. In questo modo è possibile, per le aziende, abbattere i costi, creare nuove opportunità di guadagno e garantire più comodità, scelta e controllo ai propri utenti.

Mediante l'integrazione di applicazioni e processi tra aziende diverse, i partner commerciali, i clienti (sia interni che esterni) e gli outsourcer possono collegarsi automaticamente ai processi aziendali e prendere parte a transazioni tra molteplici entità eliminando non solo le interruzioni dovute ai metodi tradizionali di scambio di informazioni - come ad esempio il telefono, il fax e la posta elettronica - ma anche la necessità di implementare i tradizionali metodi di integrazione delle applicazioni. La "rete ubiqua" (Internet) e le applicazioni transazionali su vasta scala sono già presenti nella maggior parte delle aziende. Gli standard di federazione ed i sistemi di sicurezza che li implementano sono stati appositamente concepiti per collegare applicazioni distribuite mediante procedure sicure, in modo da rendere più scorrevoli i flussi di lavoro.

Sicurezza e federazione

Tuttavia, i vantaggi appena menzionati potrebbero non verificarsi se lo scambio di informazioni a livello di sistemi avvenisse in condizioni non sicure. Ad esempio, una perdita di informazioni private dei cittadini potrebbe essere un serio problema per un ente pubblico. Un'istituzione finanziaria potrebbe andare incontro a pene pecuniarie o potrebbe essere pubblicamente screditata se si verificassero transazioni o prelievi non autorizzati. Un ente sanitario potrebbe essere condotto in tribunale se le informazioni personali riguardanti la salute dei pazienti finissero nelle mani sbagliate. Inoltre una falla nella sicurezza potrebbe mettere determinate organizzazioni in condizioni di mancata conformità rispetto a regolamenti di vario genere inerenti la confidenzialità dei dati od il controllo informatico, rischiando quindi di incorrere in sanzioni od azioni legali. Con la federazione, così come con la maggior parte delle risorse IT, le aziende non devono mai perdere di vista la sicurezza. È comunque vero che occorre trovare un equilibrio tra l'apertura alle opportunità di business ed il rifiuto del rischio.

In un contesto di federazione, il modo di affrontare le sfide della sicurezza consiste nell'integrare i sistemi di security delle aziende partner in modo che le informazioni riguardanti gli utenti, la sicurezza ed i privilegi di accesso possano essere condivise in maniera ben definita e controllata, nel quadro di un rapporto di affari basato sulla fiducia tra le parti. La "federazione delle identità" consiste nel condividere le identità digitali affinché diverse applicazioni, in diversi domini di sicurezza, possano lavorare insieme in modo completamente sicuro. Grazie alla federazione, gli utenti e le applicazioni possono muoversi attraverso business unit interne autonome, partner commerciali esterni ed altri soggetti diversi in maniera fluida, esattamente come se si trovassero all'interno dello stesso dominio di sicurezza, anche se tali domini restano in effetti largamente indipendenti.

Se la federazione attraverso aziende diverse è il fine ultimo, l'unica maniera di ottenerlo è mediante lo sviluppo e l'utilizzo di standard aperti. Fortunatamente in passato sono stati sviluppati (e vengono tuttora sviluppati) molti standard e specifiche per affrontare svariati aspetti della federazione delle identità: autenticazione unica (single sign-on), condivisione degli attributi, autorizzazioni, sicurezza dei servizi Web, privacy ecc. Se combinati insieme, questi standard costituiscono la base della federazione delle identità, necessitano di diversi requisiti e consentono molteplici casi d'uso.

Requisiti per la federazione

A causa di aspetti fondamentali come la privacy, il controllo delle identità digitali, le infrastrutture di gestione delle identità che le aziende di oggi possiedono e l'elevato valore delle informazioni relative ai clienti che esse spesso detengono, è virtualmente impossibile immaginare che le imprese possano collaborare alla creazione ed alla gestione di un unico punto in cui condividere tutte le informazioni sulle identità. Richiedere alle organizzazioni di fondere insieme e successivamente gestire a livello centrale le identità digitali dei loro utenti, come prerequisito per realizzare la federazione delle loro applicazioni e permetterne l'utilizzo ai medesimi utenti, non è la maniera più adatta di affrontare il problema. Questo è uno dei requisiti fondamentali alla base degli standard di federazione, ed è anche all'origine dell'adozione del termine stesso (federazione in quanto cooperazione tra aziende indipendenti e debolmente collegate).

Le aziende che fanno parte di federazioni delle identità stabiliscono tra loro relazioni di fiducia e consentono ai rispettivi utenti o sistemi di accedere a risorse gestite dai partner. A tale scopo, le imprese coinvolte rilasciano ai propri utenti dei "ticket di sicurezza" che vengono elaborati dai partner commerciali che si avvalgono di questo sistema. In termini semplicistici, gli standard di federazione definiscono questi ticket di sicurezza, ne illustrano la struttura ed il contenuto, stabiliscono come vengono trasmessi, gestiti, validati ed a quale tipo di servizi possono o devono dare accesso.

Casi d'uso della federazione

La federazione delle identità può trovare innumerevoli applicazioni. I casi d'uso illustrati nel presente documento non intendono essere esaustivi, ma descrivono in termini generali alcuni utilizzi tipici della federazione, con l'obiettivo di far riflettere i lettori su questo sistema e sul modo in cui le aziende potrebbero sfruttarlo appieno.

La federazione delle identità può essere realizzata attraverso due modalità fondamentali e strettamente correlate: **basata su browser** oppure **basata su documenti**. La modalità di federazione basata su browser si concentra sul supporto fornito agli utenti che utilizzano applicazioni Web alle quali accedono mediante normali browser Internet. In questo caso la federazione consente ad un utente autenticato di passare da un dominio di sicurezza ad un altro senza dover fornire nuovamente le sue credenziali. Le federazioni basate su browser forniscono all'utente un'unica autenticazione per due insiemi di applicazioni o portali localizzati su due domini di sicurezza diversi, senza richiedere la sincronizzazione delle identità digitali dell'utente nei due domini. Fondamentalmente, l'utente viene autenticato su un dominio e può utilizzare le applicazioni di un altro dominio senza doversi registrare nuovamente.

Invece, la federazione basata su documenti si basa sull'uso di documenti XML trasportati attraverso due domini di sicurezza sfruttando gli standard del servizio Web. In questa modalità l'attività è guidata da un utente che utilizza un'applicazione "client" oppure da un'applicazione client che agisce senza alcun coinvolgimento umano diretto. Le federazioni basate su documenti prevedono la definizione delle strutture dei documenti XML, della dislocazione delle informazioni sulle credenziali, nonché altri fattori necessari per richiedere ed ottenere determinati servizi Web resi disponibili da una organizzazione partner.

In ogni caso, entrambe le modalità di federazione (basata su browser e basata su documenti) sono rese possibili dallo sviluppo e dall'utilizzo di standard, che consentono a due diverse applicazioni, residenti in due domini di sicurezza indipendenti, di lavorare insieme a vantaggio di un utente comune o di processi aziendali condivisi.

Scenari basati su browser

I seguenti casi d'uso illustrano maniere diverse di utilizzare le identità per fornire agli utenti finali, collegati tramite browser, un'unica autenticazione con cui operare all'interno di un determinato numero di entità coinvolte in una partnership.

Federazione basata sul collegamento degli account

Nel presente caso d'uso, l'azienda Lavoro.com subappalta la gestione dei benefit sanitari dei propri dipendenti alla società partner Sanità.com. Per accedere al proprio account, una dipendente di Lavoro.com viene autenticata sul portale dedicato ai dipendenti (www.lavoro.com) e clicca su un link per visualizzare i propri benefit sanitari su www.sanita.com. La dipendente viene indirizzata sul sito Internet di Sanità.com e visualizza tutte le informazioni riguardanti i propri benefit sanitari senza doversi registrare sul sito di Sanità.com. I suoi account vengono automaticamente trasmessi nel momento in cui la dipendente viene reindirizzata dal browser.

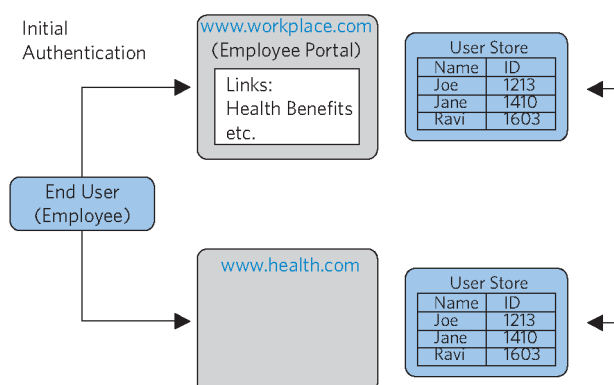


Figura 1: Federazione basata sul collegamento degli account

Sanità.com detiene tutte le informazioni sanitarie dei dipendenti di Lavoro.com. Sanità.com quindi possiede a priori le identità utente di ciascun dipendente di Lavoro.com. Quando un dipendente di Lavoro.com accede tramite la federazione al sito di Sanità.com, Lavoro.com trasmette (mediante procedure sicure) un identificatore del dipendente a Sanità.com. Tale identificatore consente a Sanità.com di determinare l'identità dell'utente e quindi, indirettamente, di fornire il tipo specifico di accesso che gli/le compete. I sistemi di sicurezza di Lavoro.com e Sanità.com sono debolmente collegati (federati) in modo da garantire agli utenti comuni ai due sistemi un'unica autenticazione.

Il collegamento di account è il più tipico esempio di federazione browser-based. Tuttavia, vi è un altro scenario di federazione basata su browser che potrebbe rivelarsi utile in determinate situazioni.

Federazione basata su ruoli

In questo caso d'uso, Lavoro.com acquista componenti dalla società partner FornitorediComponenti.com. Un ingegnere di Lavoro.com viene autenticato sul portale dedicato ai dipendenti (www.lavoro.com) e clicca su un link per accedere alle informazioni di FornitorediComponenti.com.

Visto che l'utente è un ingegnere (questo è il ruolo che ricopre) di Lavoro.com, viene indirizzato automaticamente alla documentazione tecnica ed alle pagine dedicate alla risoluzione dei problemi del sito Internet di FornitorediComponenti.com senza doversi autenticare nuovamente.

Quando invece è un dipendente del reparto acquisti di Lavoro.com ad autenticarsi sul portale di Lavoro.com ed a cliccare su un link per accedere alle informazioni di FornitorediComponenti.com, le pagine visualizzate dal sito di FornitorediComponenti.com (senza doversi registrare di nuovo) saranno quelle dedicate agli ordini. In entrambi i casi, le pagine di FornitorediComponenti.com possono essere personalizzate con informazioni quali, ad esempio, il nome dell'utente; ciò è possibile utilizzando i dati contenuti nel ticket di sicurezza inviato da Lavoro.com.

In questo scenario basato sui ruoli, FornitorediComponenti.com non è tenuto a possedere tutte le identità dei dipendenti di Lavoro.com. Tuttavia, da parte di FornitorediComponenti.com, è comunque necessario mettere in atto un controllo degli accessi ad aree sensibili del proprio sito. Per consentire tale controllo, FornitorediComponenti.com mantiene un numero limitato di identità di profilo (associate a ruoli o mansioni aziendali) per gli utenti di Lavoro.com.

Nel caso appena illustrato, viene mantenuta un'identità di profilo per gli ingegneri ed una per i dipendenti del reparto acquisti. Quando un dipendente di Lavoro.com accede al sito di FornitorediComponenti.com, Lavoro.com comunica a FornitorediComponenti.com gli attributi dell'utente mediante procedure sicure, sulla base degli standard di federazione. Tali attributi definiscono il ruolo dell'utente e determinano l'identità di profilo utilizzata per il controllo degli accessi da parte di FornitorediComponenti.com.

Ovviamente il numero di casi d'uso potenziali della federazione basata su browser è molto più elevato e potrebbero essere sviluppati infiniti scenari specifici per diversi settori od aziende, tuttavia i due casi presentati dovrebbero essere sufficienti ad illustrare esaurientemente le potenzialità di questo sistema.

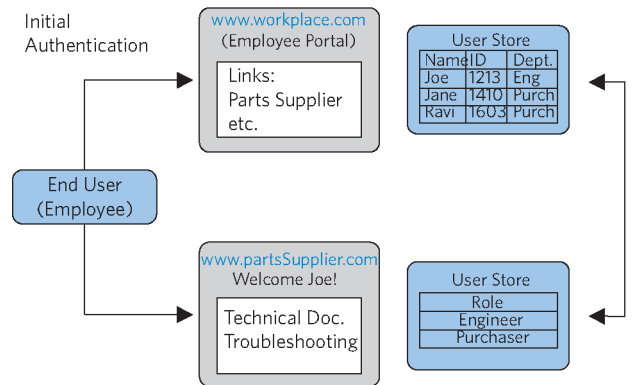


Figura 2: Federazione basata su ruoli

Scenari basati su documenti

Le federazioni basate su documenti vengono realizzate utilizzando i flussi di servizi web. Esattamente come nel caso delle federazioni browser-based, esistono diversi possibili scenari d'uso. Nel presente documento verrà presentato un caso tipico per illustrare i concetti basilari di questo tipo di federazione.

Servizi web concatenati

Nel presente caso d'uso, Lavoro.com e FornitorediPin.com sono vincolate da un contratto di acquisto; a sua volta, FornitorediPin.com ha rapporti commerciali con SpedizioniElettroniche.com.

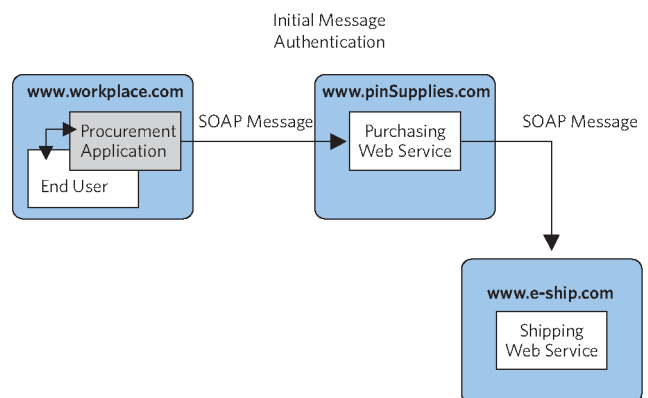


Figura 3: Servizi web concatenati

L'utente finale si registra sulla propria applicazione di approvvigionamento aziendale inserendo username e password. L'applicazione visualizza un elenco di fornitori di Lavoro.com. L'utente finale clicca sul tasto di FornitorediPin.com e viene indirizzato su un buono d'ordine in formato HTML. L'utente compila il buono d'ordine e clicca sul tasto Invia del modulo HTML.

L'applicazione di approvvigionamento converte il modulo HTML in un documento XML/SOAP che viene inserito nel corpo di un messaggio basato su XML. L'applicazione quindi inserisce le credenziali dell'utente finale e l'identità aziendale di Lavoro.com nell'intestazione del messaggio.

L'applicazione invia quindi il messaggio al servizio "acquisti on-line" di FornitorediPin.com. Il servizio di acquisti on-line (oppure un'applicazione di sicurezza che agisce in sua vece: la soluzione più scalabile e facile da gestire) autentica il messaggio in arrivo ed elabora la richiesta. Una volta completato il procedimento di acquisto, il servizio "acquisti on-line" invia una richiesta a SpedizioniElettroniche.com utilizzando un altro messaggio XML/SOAP. Il messaggio contiene un token di sicurezza di FornitorediPin.com nell'intestazione, mentre il corpo del messaggio include l'elenco di articoli da inviare e le informazioni di spedizione. Il servizio "spedizioni on-line" (oppure un'applicazione di sicurezza che agisce in sua vece) autentica la richiesta ed elabora l'ordine di spedizione.

Uno dei nodi centrali della creazione di applicazioni federate (ma il discorso può essere generalizzato a qualsiasi tipo di applicazione) è pensare in termini di utente finale, immaginare il tipo di esperienza che si desidera fornirgli e come ottenerla al meglio utilizzando le infrastrutture disponibili. Quando si considerano le potenziali applicazioni federate, è importante ragionare in termini di federazione browser-based oppure document-based.

Importanti questioni aziendali inerenti la federazione

La federazione delle identità promette vantaggi sostanziali tanto agli utenti quanto alle aziende; tuttavia, la verità è che gli standard e le specifiche del settore, quali SAML, Liberty Alliance ed altri (che verranno trattati brevemente in seguito) si rivelano utili solo quando due o più aziende tentano di integrare i propri sistemi e processi aziendali. Gli standard che verranno brevemente illustrati nei paragrafi successivi contribuiscono enormemente al funzionamento congiunto delle infrastrutture di sicurezza delle aziende, ma da soli non bastano a risolvere le questioni aziendali relative alla federazione. Coloro che intendono avvalersi di una federazione dovranno risolvere le seguenti questioni (e non solo) in una maniera che sia soddisfacente per tutti i partner coinvolti, prima di inaugurare i propri progetti di federazione e di applicarli su vasta scala.

- **Questioni legali e contrattuali relative alla fiducia.** La federazione implica che una parte dipenda almeno parzialmente dai sistemi di sicurezza e dalle pratiche dell'altra parte coinvolta; perciò, qualsiasi contratto stipulato deve definire chiaramente i requisiti, gli obiettivi, le responsabilità, i livelli di servizio garantiti, le conseguenze in caso di violazione della sicurezza, i tipi di controllo adottati dai partner nel momento in cui attribuiscono credenziali agli utenti, eccetera.
- **In caso di problemi, cosa succede e a chi deve rivolgersi l'utente?** Se per qualsiasi ragione un utente non riuscisse ad ottenere ciò che desidera, è necessario che vi sia un help desk od un servizio clienti che possa aiutarlo; in modo analogo deve esistere una procedura di risoluzione dei problemi che uno qualsiasi dei partner potrebbe riscontrare nell'ambito della federazione. Inoltre è imprescindibile un accordo sui livelli di servizio che ci si impegna a fornire.
- **Quali normative esistono in materia?** E come è possibile accertarsi che i partner le rispettino? A seconda del settore, dell'area geografica e del tipo di dati personali trattati, possono esserci in vigore normative diverse. Ogni federazione delle identità deve tenere in considerazione le regole vigenti e la maniera più adatta per rispettarle.
- **Chi sostiene i costi della federazione?** Dato che, per definizione, le applicazioni federate vengono condivise e consentono a tutte le parti coinvolte di trarne dei benefici, non è fuori luogo immaginare che tutte le parti coinvolte debbano concorrere alle spese sostenute per la realizzazione della federazione. La suddivisione delle spese dipenderà in larga parte dal tipo di relazione economica esistente tra le parti. Ovviamente è possibile che una delle parti coinvolte decida di sostenere tutti i costi della federazione, ma questa è una questione di natura non tecnica da risolvere prima di realizzare qualsiasi federazione.
- **Tutela della privacy.** In molti scenari, affinché possa esistere una federazione è necessaria la "condivisione", tra i partner coinvolti, di determinati dati personali relativi agli utenti. Tale condivisione deve essere non solo legale, ma anche eseguita nel rispetto delle politiche di tutela della privacy di tutte le società federate. Inoltre, ogni azienda deve verificare se è necessario o meno ottenere il consenso dell'utente.
- **Infrastrutture e competenze tecniche delle parti federate.** Affinché sia possibile la federazione tra due società, occorre che le loro infrastrutture di sicurezza siano integrate utilizzando uno standard a loro scelta. Ciò implica che entrambe le parti siano a conoscenza del significato di tale operazione e siano in grado di acquisire o realizzare i sistemi richiesti. Come con ogni nuova tecnologia, è consigliabile iniziare con i partner aziendali prioritari che abbiano le maggiori competenze in campo informatico e di sicurezza.

- **Dimensionamento della federazione.** La scalabilità del sistema è ovviamente una questione tecnica. Gli ingegneri incaricati di progettare e realizzare l'infrastruttura di federazione, da entrambe le parti, dovranno ricevere informazioni dettagliate riguardo al numero di controparti da supportare, al numero di transazioni stimate e ad una serie di altri fattori. Il fatto è che una federazione concepita per supportare un partner potrebbe essere radicalmente diversa dal tipo di federazione richiesta per supportare 100 partner allo stesso tempo. Durante la fase di progettazione della federazione, sarà quindi necessario affrontare la questione dell'aumento previsto del numero di servizi federati, in modo da realizzare un sistema scalabile che possa adattarsi alle esigenze di business attuali e future delle società coinvolte.
- **Amministrazione degli utenti federati.** Solitamente una federazione non elimina in toto la necessità di amministrare le identità digitali degli utenti delle varie parti coinvolte. Tale amministrazione non richiede solo una soluzione di tipo tecnico; occorre che le società sappiano identificare un processo comune che sia in grado di supportare la gestione dei dati relativi alle identità digitali. In altre parole, le aziende devono applicare procedure in grado di supportare l'intero ciclo di vita delle identità degli utenti, dalla loro creazione all'eliminazione definitiva passando per le varie modifiche - e questo per le applicazioni federate di tutte le parti coinvolte.
- **Diritti di auditing dei partner della federazione.** I sistemi di sicurezza e gli interventi di auditing sono solitamente due realtà strettamente correlate. Non è naturale supporre che lo stesso discorso si applichi anche ai sistemi di sicurezza federati? Tuttavia, dato che metà (o una parte inferiore) del sistema di sicurezza (e relativi processi quali convalida iniziale delle identità) di una soluzione federata si trova presso la sede di un partner, occorre negoziare anticipatamente condizioni e modalità di accesso agli eventuali dati di auditing informatico del partner stesso.

Il presente elenco di questioni aziendali non è stato introdotto con l'obiettivo di spaventare e far desistere i lettori dai loro progetti di federazione. Piuttosto è stato concepito con lo scopo di non generare aspettative sproporzionate. È fondamentale comprendere quali sono le questioni di natura tecnica ma anche di natura aziendale che devono essere affrontate nella realizzazione di una federazione delle identità. Lanciarsi in un progetto di federazione senza considerare le diverse questioni che potrebbero emergere sarebbe infatti estremamente rischioso.

Come nel caso della maggior parte delle iniziative in ambito informatico per le aziende, la realizzazione concreta del primo progetto è fondamentale per l'ampliamento del progetto stesso nel tempo. Un esito positivo comporta ulteriori richieste, fondi, attenzione ed auspicabilmente l'espansione dell'iniziativa nel tempo. Il consiglio migliore è iniziare con il partner più motivato e convinto. Con questo partner verranno impostate tutte le questioni economiche e tecniche della federazione; in seguito sarà più facile espandere il progetto se il tempo, le richieste e le risorse lo consentiranno.

Standard di federazione

Che si tratti di federazione basata su browser o su documenti, non esiste un unico standard in grado di soddisfare tutti i requisiti necessari. Come già accennato nel presente documento, una federazione comporta, tra le altre cose, la descrizione delle identità (ad es. token di sicurezza), protocolli di scambio di token di sicurezza e metodi per stabilire relazioni basate sulla fiducia.

In questa sezione verranno brevemente analizzati quattro standard tra i più importanti nelle iniziative di federazione delle identità:

- SAML
- Liberty Alliance
- WS-Federation
- WS-Security

Security Assertion Markup Language (SAML)

SAML è un framework aperto - a livello di applicazione - per la condivisione di informazioni di sicurezza via Internet mediante documenti XML. Nel gennaio del 2001 una divisione di CA, insieme ad altre società, ha dato vita alla Commissione Tecnica per i Servizi di Sicurezza (SSTC, Security Services Technical Committee) del consorzio OASIS, che è culminata con l'adozione dello standard SAML nel mese di novembre 2002. SAML 2.0, la versione attuale di SAML, è stata approvata dalla SSTC di OASIS nel mese di marzo 2005.

SAML è probabilmente lo standard singolo di federazione più importante, supportato ed adottato, che esista al momento. In particolare, la parte di standard denominata Assertion (ticket di sicurezza) è largamente supportata dagli altri standard di seguito descritti. SAML è utilizzato per realizzare federazioni browser-based.

Liberty Alliance

Il Liberty Alliance Project (conosciuto anche come Liberty Alliance o solo Liberty) è una organizzazione del settore nata nel settembre del 2001; ora annovera oltre 150 membri nel mondo, tra i quali figura anche CA. L'obiettivo di Liberty Alliance è creare un insieme di specifiche per la federazione delle identità.

Il modulo ID-FF (Liberty Identity Federation Framework) costituisce la base dell'architettura Liberty ed è la parte di Liberty più ampiamente utilizzata.

ID-FF

Un normale ambiente ID-FF si compone di tre parti essenziali: un provider di identità (ad es. una società di telecomunicazioni), un provider di servizi (ad es. un negozio on-line, un ente creditizio, un ente statale) ed un agente utente. L'agente utente può essere un thin client (ad es. un normale browser) oppure un client o un proxy abilitato all'utilizzo di Liberty (LECP), ad esempio un telefono cellulare.

I casi d'uso di ID-FF ricadono nell'ambito della federazione basata su account descritta nel capitolo dedicato agli scenari browser-based.

Con ID-FF, una volta avvenuta con successo l'autenticazione del "principal", l'identity provider produce una assertion SAML che include una dichiarazione di autenticazione la quale, a sua volta, definisce il contesto di sicurezza del principal ed un identificatore di nome (un "handle"). È importante evidenziare che, con l'uscita della versione SAML 2.0, Liberty e la Commissione Tecnica di OASIS hanno accorpato ID-FF e SAML. Liberty, pertanto, non si baserà più sul modulo ID-FF della propria specifica in modo indipendente da SAML.

WS-Federation

Web Services Federation Language (WS-Federation) è una specifica sviluppata congiuntamente da IBM, Microsoft, BEA, Verisign e RSA Security. WS-Federation sarà un sistema di sicuro interesse per la maggior parte dei lettori, in quanto Microsoft ha recentemente realizzato un prodotto che supporta WS-Federation denominato Active Directory Federation Service (ADFS). Microsoft ha incluso ADFS come parte integrante di Windows Server 2003 R2. ADFS implementa la specifica Passive Requestor Profile di WS-Federation, pertanto consente di realizzare federazioni browser-based.

WS-Security

La specifica Web Services Security (WS-Security) è stata inizialmente sviluppata da IBM, Microsoft e Verisign. È divenuto uno standard ufficiale nel mese di marzo 2005 ed ora è gestito dalla Commissione Tecnica per la Sicurezza dei Servizi Web del consorzio OASIS (Web Services Security Technical Committee, WSS TC). La versione dello standard attualmente in circolazione è la 1.0.

WS-Security specifica le estensioni di sicurezza SOAP che garantiscono integrità e confidenzialità dei dati, pertanto è utile nell'ambito di scenari di federazione document-based. WS-Security definisce la maniera di allegare firme e intestazioni di crittazione ai messaggi XML. Inoltre definisce profili di inserimento di diverse tipologie di token di sicurezza XML e di tipo binario nelle intestazioni WS-Security.

Conclusioni

Nella ricerca di un difficile equilibrio tra la sicurezza e la crescente esigenza di garantire ad utenti sempre più numerosi e variegati un accesso fluido alle informazioni, le aziende si trovano ad affrontare sfide sempre più impegnative. Per integrare i vari partner tra loro, tenendo presenti i rispettivi eterogenei sistemi di sicurezza ed infrastrutture, occorrono soluzioni in grado di supportare una sicurezza scalabile e interaziendale, che possa estendersi a numerosi partner; solo così sarà possibile condividere ed amministrare le informazioni, i profili e le prerogative degli utenti utilizzando procedure sicure. Gli standard di federazione e i prodotti di sicurezza che li implementano sono stati appositamente concepiti per offrire questo tipo di servizi.

Oggi Internet, con le sue tecnologie ed i suoi standard, è maturata al punto da rendere praticabile, ed anche economicamente sostenibile, la possibilità di garantire un efficace coordinamento ed un elevato livello di integrazione tra partner commerciali. I vantaggi immediati di queste innovazioni sono appannaggio delle aziende in grado di capire e sfruttare le tecnologie disponibili. La domanda che poniamo ai lettori è: come lasciare aperte le porte alle opportunità, respingendo nel contempo i rischi? La federazione delle identità costituisce un meccanismo per ottenere questo difficile equilibrio in una maniera efficace, scalabile e basata su standard.

