

Università degli Studi di Perugia
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea Specialistica in Informatica

Seminario di Sicurezza Informatica



Docente: Stefano Bistarelli

Studente: Eno Pleqi

- 1. INTRODUCTION TO OPENID**
- 2. OpenID Demo**
- 3. AUTHENTICATION AND AUTHORIZATION**
- 4. OPENID PROTOCOL AND MESSAGES**
- 5. OPENID Scenario**

Introduction to OpenID

Identity Mangement

- Uno dei campi più importanti nella tecnologia dell'informazione
- Meccanismo primario per il controllo degli accessi
- Bisogno di un'identità per accedere a
 - Siti web
 - Banca online
 - Social Netwok
 - ...

Introduction to OpenID

Molti modi per creare e gestire le identità digitali

- A livello di sistema operativo
- A livello di applicazione
- Altri modi ...

A livello di sistema operativo

- UNIX/Linux: **LDAP** Lightweight Directory Access Protocol, **NIS** Network Information Service, **Kerberos**, ...
- Windows: Active Directory
- Mainframe: **RACF** Resource Access Control Facility.

Introduction to OpenID

- Prodotti commerciali e open source disponibili per questo scopo.
- Forniscono strutture per gestire l'identità degli utenti su più piattaforme e servizi:
 - Single Sign On (SSO),
 - Cross Company Authentication (CCA), etc.
- Aziende come RSA, Novell, Sun e altre forniscono prodotti commerciali per la gestione dell'identità.

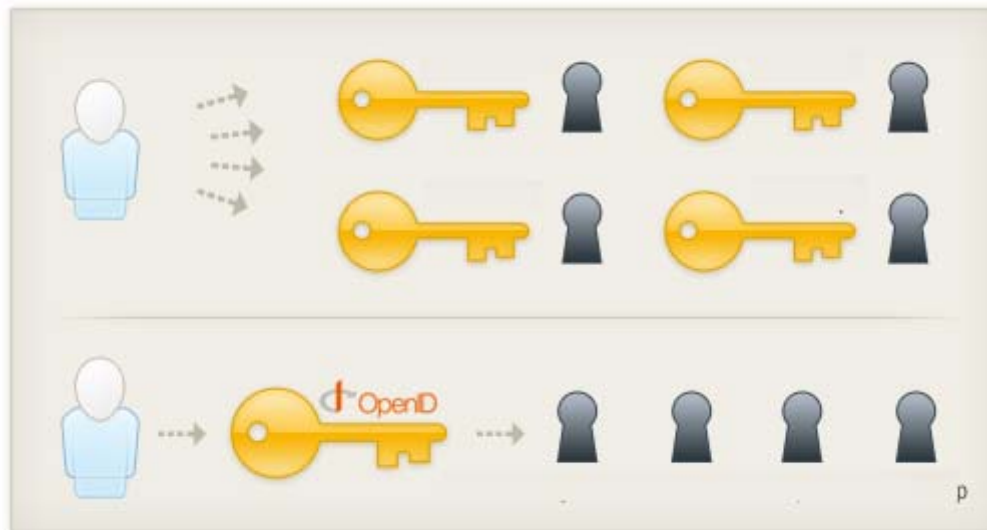
Introduction to OpenID

- Ok per sistemi centralizzati ...
- Utenti con molti account presso diversi siti web
 - Nuova identità per ogni sito
 - Ricordare login e password per ogni sito
 - Problemi:
 - Frustrante
 - Poca sicurezza (stessa password)
 - Poca affidabilità (molte password)

Introduction to OpenID

“Come gestire le molte identità in molti siti web con i quali l’utente deve interagire ? ”

Soluzione possibile “OpenID”



Introduction to OpenID – What Is ?

- OpenID è
 - Uno standard aperto e decentralizzato
 - Controllo dell'accesso e autenticazione del utente
 - Uso dell'URL come identità
 - Diversi servizi con la stessa identità digitale.
 - Sostituisce il processo di login comune
 - Il controllo dell'identità nelle mani dell'utente

Introduction to OpenID – Enable user to . . .

- Mette l'utente è in grado di
 - Avere una sola “identità”
 - Effettuare login senza username e password
 - Scegliere il profilo da utilizzare
 - Semplificare l'esperienza online

OpenID - Terminologia

- **End-user:** la persona che possiede un identità OpenID e che vuole affermare tale identità in un sito.
- **Identity provider** or **OpenID provider** (OP): provider di servizi che offre il servizio di registrazione dell'identificatore OpenID e provvede alla sua autenticazione. È un server di autenticazione OpenID in cui un Relying Party si basa per un'affermazione che l'utente finale possiede un identificatore.
- **OP Endpoint URL:** L'URL che accetta i messaggi di autenticazione del protocollo OpenID, ottenuti effettuando un controllo sull'identificatore fornito dall'utente. Questo valore deve essere un HTTP o HTTPS URL.
- **RP (Relying party):** il sito, chiamato anche provider di servizi, che intende verificare l'identificatore dell'utente finale. Un'applicazione Web che vuole prova che l'utente finale possiede un identificatore.

OpenID - Terminologia

- **User Agent:** il programma (il browser) che l'utente (end-user) sta usando per accedere ad un identity provider o ad un relying party.
- **Identifier:** Un identificatore è un URL "http" o "https". Si definiscono diversi tipi di identificatori, progettati per essere utilizzati in diversi contesti.
- **OP Identifier:** Un identificatore per il provider OpenID.
- **User-Supplied Identifier:** Identificatore che viene presentato dall'utente finale al "Relying Party", o selezionato dall'utente presso il provider OpenID.
 - Durante la fase di apertura del protocollo, l'utente finale può immettere il proprio identificatore oppure un identificatore di OP. Se si utilizza un identificatore di OP, l'OP può quindi assistere l'utente finale nella scelta dell'identificatore per condividere con Relying Party.

OpenId - Demo

- **OpenID provider**

- <https://www.myopenid.com/>



- ***Relying Party***

- <http://www.livejournal.com/>



OpenId - Demo

- Step 1: create I'URL OpenId (<https://myopenid.com>)

SIGN UP FOR YOUR OPENID

Get your own OpenID and start using the last username and password you'll ever need. Signing up with myOpenID gets you:

- Secure control of your digital identity
- Easy sign-in on enabled sites
- Account activity reports
- And a whole lot more!

[SIGN UP FOR AN OPENID](#)

– Step 1.1: Scegliere lo username

1. CHOOSE YOUR USERNAME

Your OpenID URL is how [sites that accept OpenID](#) know you. You can use your name or anything that you want to be known by.

Username
John Doe, jdoe123

OpenID URL  Enter a user name

OpenId - Demo

– Step 1.2: scegliere la password

2. CHOOSE A PASSWORD

You'll use this password to sign in to myOpenID, but you won't have to give it to any other site.

Password

Password (confirm)

Strength

Status

– Step 1.3: inserire la mail

3. ENTER YOUR E-MAIL ADDRESS

Your e-mail address is optional, but providing it will let you recover your account if your sign-in information is lost or forgotten. We will never sell your e-mail address or send you spam.

Please configure your e-mail client to allow messages from support@myopenid.com, so you can see and respond to our confirmation message.

E-mail

☒ Keep me updated with news about myOpenID

OpenId - Demo

– Step 1.4: effettuare la registrazione

4. "THE FINE PRINT"

Enter the text from the image below.



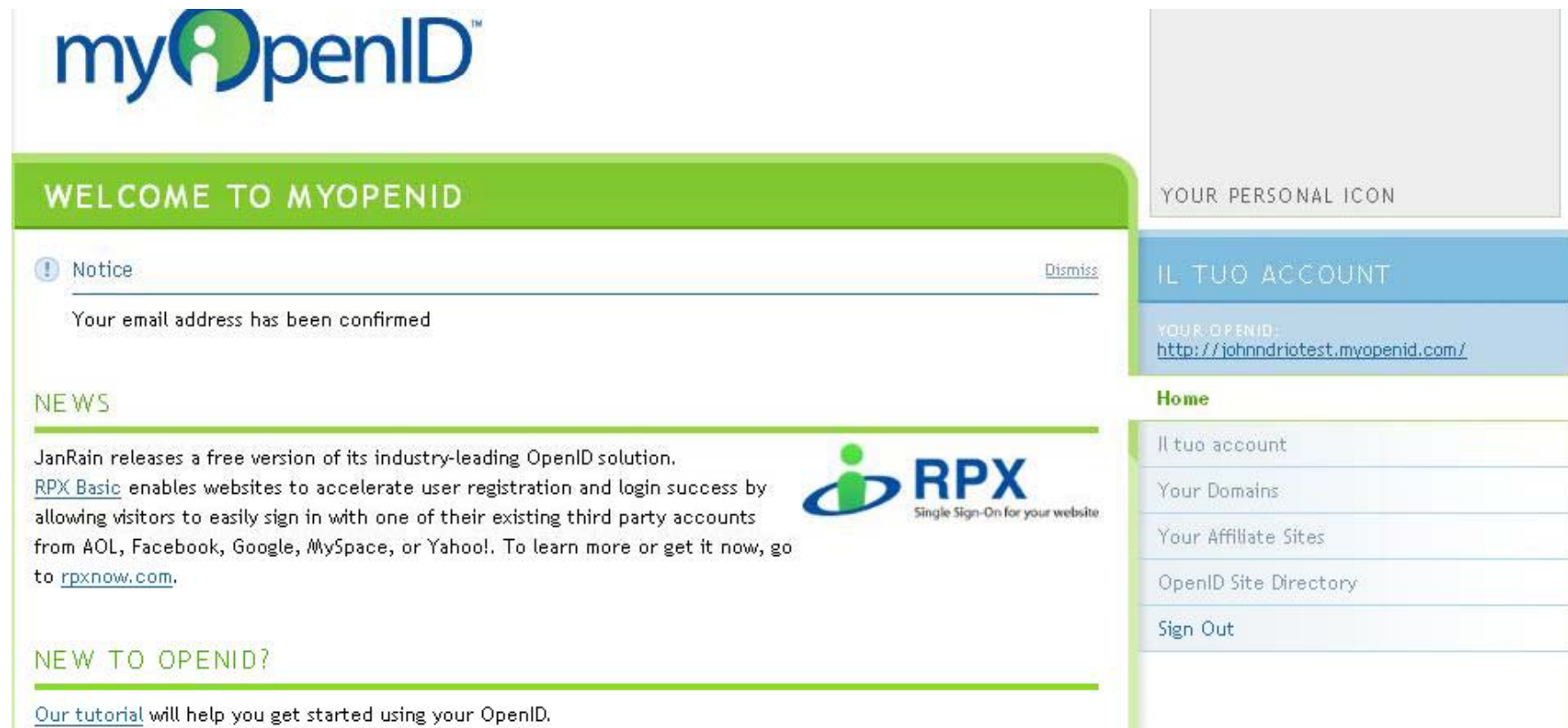
Please read the [myOpenID terms of service](#), and check the box below.

☐ I agree to the myOpenID terms of service

Sign Up

OpenId - Demo

– Step 1.5: confermare l'indirizzo mail



The screenshot displays the myOpenID website interface. At the top left is the myOpenID logo. Below it, a green banner reads "WELCOME TO MYOPENID". A notice box states "Your email address has been confirmed" with a "Dismiss" link. The "NEWS" section features a JanRain announcement and an RPX logo with the text "Single Sign-On for your website". The "NEW TO OPENID?" section includes a link to a tutorial. On the right, a sidebar shows "YOUR PERSONAL ICON" (a placeholder), "IL TUO ACCOUNT" with the user's OpenID URL, and a "Home" menu with links to account, domains, affiliate sites, directory, and sign out.

myOpenID™

WELCOME TO MYOPENID

Notice Dismiss

Your email address has been confirmed

NEWS

JanRain releases a free version of its industry-leading OpenID solution. [RPX Basic](#) enables websites to accelerate user registration and login success by allowing visitors to easily sign in with one of their existing third party accounts from AOL, Facebook, Google, MySpace, or Yahoo!. To learn more or get it now, go to [rpxnow.com](#).

RPX
Single Sign-On for your website

NEW TO OPENID?

[Our tutorial](#) will help you get started using your OpenID.

YOUR PERSONAL ICON

IL TUO ACCOUNT

YOUR OPENID:
<http://johnndriotest.myopenid.com/>

Home

- Il tuo account
- Your Domains
- Your Affiliate Sites
- OpenID Site Directory
- Sign Out

OpenId - Demo

- Step 2: test della nuova “identità” su LiveJournal

OpenID

What is OpenID?

LiveJournal.com supports the [OpenID](#) distributed identity system, letting you bring your LiveJournal.com identity to other sites, and letting non-LiveJournal.com users bring their identity here. After all, not everybody uses the same websites, but you should still be able to play together.

Using your OpenID here.

If you're not a member of LiveJournal.com but want to leave authenticated comments and let people add you as their friend, trust your comments, etc., then you can login either in the form below, or from any comment entry form. Once you're logged in, you'll also be able to read friends-only posts that LiveJournal.com users have indicated you're allowed to read.

Your OpenID URL:

For example: `melody.someblog.com` (if your host supports OpenID)

Using your OpenID on another site.

If another site says it supports OpenID and you want to use your LiveJournal.com identity there, just enter your journal URL. (you don't need the `http://` part either). For example, just enter **melody.livejournal.com**, or whatever your address is. After you do so, you'll be sent to LiveJournal briefly to ask if you want to trust that site to know who you are. You can either trust them once, or forever. You can change your [OpenID settings and trust](#) at any time.

BETA:
Our OpenID consumer support is very new. That is, external users logging in with their identity here will find some rough edges while we work on smoothing it all out.

Our server support is relatively complete, though.

OpenId - Demo

– Step 2.1 Reindirizzamento preso OpenID Provider



SIGN IN

 Notice [Dismiss](#)

You must sign in to authenticate to <http://www.livejournal.com/> as <http://johnndriotest.myopenid.com/>

Username <http://johnndriotest.myopenid.com/>

Password

☐ Stay signed in

[Sign In](#) [Cancel](#)

[Sign in with an SSL certificate](#)
[I cannot access my account](#)

YOUR PERSONAL ICON

OPZIONI

[Home](#)
[Recupera account](#)
[OpenID Site Directory](#)

OpenId - Demo

– Step 2.3: Ritorno a Relying Party

The screenshot shows the LiveJournal website interface. At the top, there is a dark blue header bar. On the left, a user profile icon is shown with the text "Carica un'Immagine Personale". To the right of the icon, the text "johnndriotest.myopenid.com" is displayed, followed by "Account" and a small upward arrow icon. Below this, there are links: "Aiuto | Esci", "Scrivi | Messaggi | Pagina Amici | Invita un Amico | Mobile". Further right, the "LIVEJOURNAL" logo is visible, accompanied by a birthday cake icon with the number "10" on it. Below the logo, there is a search bar with the text "Find", "Interesse", and "Vai".

Below the header bar, the text "Home : Accesso" is displayed. The main heading reads "Bentornato/a su LiveJournal!". Below this, a message states: "Hai effettuato l'accesso come [johnndriotest.myopenid.com](#). Buon divertimento. Ecco alcuni suggerimenti...".

A yellow box contains the text: "Please [set](#) and [validate](#) your email address to get started."

Below the yellow box, there are two suggestions:

- [Aggiorna il tuo Journal](#)
Sai che adesso puoi facilmente aggiungere delle foto?
- [Leggi la tua pagina amici](#)
Guarda gli ultimi aggiornamenti dei journal dei tuoi amici.

On the right side, there is a "Suggerimento" (Suggestion) box. It contains the text: "We're keeping an eye out for interesting communities! See the great ways people use LJ in [LJ spotlight](#)." Below this text, there are two links: "» Vedi Tutti" and "» Prossimo".

Authentication and Authorization

- Autenticazione : utilizzata per stabilire l'identità di qualcuno
- Autorizzazione: utilizzata per concedere o negare l'accesso a una risorsa dopo l'autenticazione.
- Sono molto baste sul sistema
- Si stanno muovendo verso l'utente

Authentication and Authorization

- Metodi di autenticazione/autorizzazione basate sull'utente
 - L'utente sceglie la card da inviare al sito.
 - Consentire richieste da siti web per ulteriori parametri
 - Consentire alla Identity Providers il rilascio delle identità digitali
 - Semplificare il processo di autenticazione per l'utente

Per soddisfare questi obiettivi, vengono sviluppati diversi tipi di sistemi.

OpenID è uno degli sforzi leader nell'open source

Authentication and Authorization

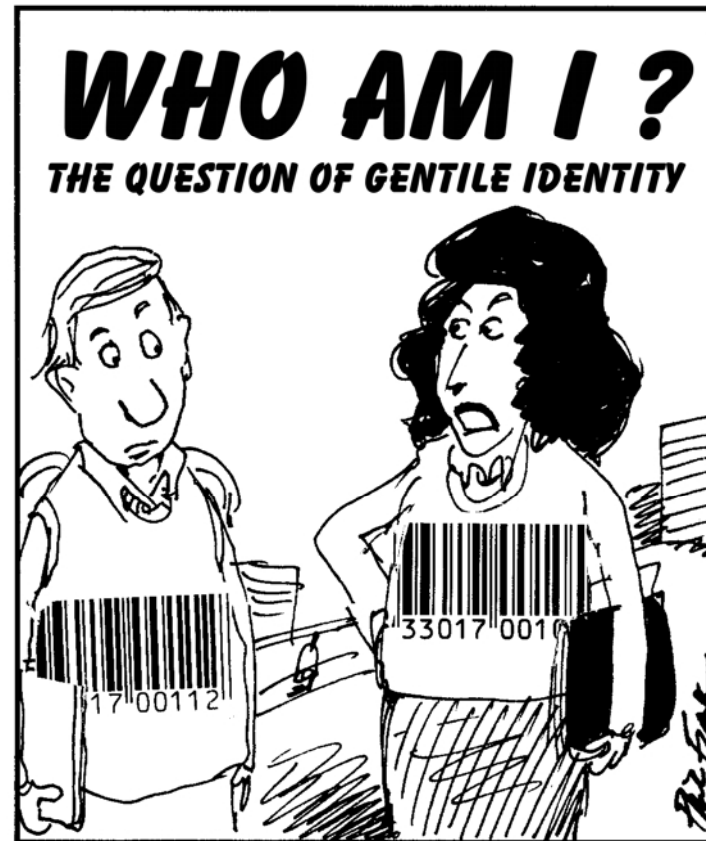
- Autenticazione:
 - processo che autentica qualcosa o qualcuno
 - è un processo con il quale un'entità (un utente, un'applicazione, un dispositivo, ecc.) accerta che esso è ciò che pretende di essere
 - Login / Password
- Autorizzazione
 - è il processo che in genere viene dopo l'autenticazione e viene utilizzato per concedere o negare l'accesso a un risorsa

Authentication and Authorization

- Autenticazione VS Autorizzazione
- L'autorizzazione può dipendere anche da:
 - la sensibilità e l'importanza della risorsa
 - Il metodo di autenticazione
 - il giorno e ora
 - la posizione dell'entità che deve accedere alla risorsa

What is An Identity?

- Who are you ?



Authentication Methods

- **Password Authentication**
- **PIN Authentication**
- **One Time Password (OTP) Authentication**
- **Smart Card Authentication**
- **Biometric Authentication**
- **USB Devices**

Weak and Strong Authentication

- Autenticazione debole
 - Username e password
- Autenticazione forte
 - Utilizzo di più metodi o fattori
 - *Something you know*
 - *Something you have*
 - *Something you are*

Two – Factor Authentication

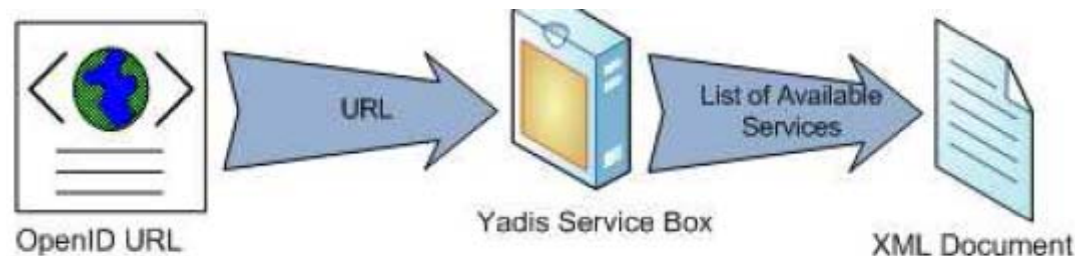
- Autenticazione con due fattori
 - Non appartenenti alla stessa categoria
 - Utilizzata per le informazioni più sensibili
 - Conti bancari
 - Cartelle mediche
 - Dati personali importanti

Single Sign-On (SSO)

- Login singolo per risorse multiple
 - Login per la prima risorsa
 - Stesso login per le successive
 - Gestito tutto in background
 - SSO oppure simplified sign ?
 - Meglio con two-factor authentication
 - Esempio: Kerberos
 - OpenID può simulare SSO

New Authentication Mechanisms - Yadis

- meccanismo per scoprire i servizi disponibili in un determinato URL
- un semplice protocollo basato su XML
- un documento XML viene restituito in un formato noto come eXtensible Resource Descriptor o XRD



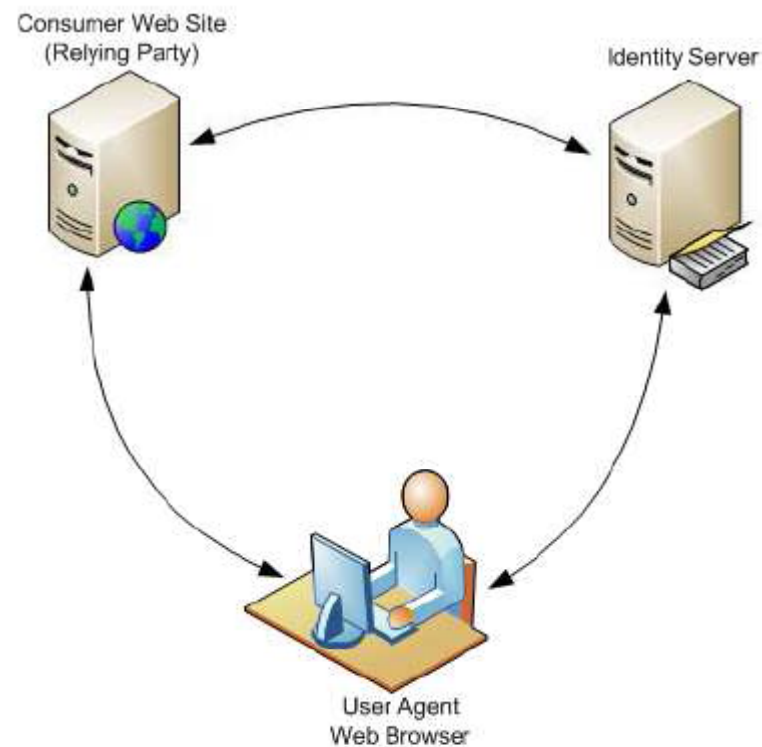
OpenID - Terminologia

- **End-user:** la persona che possiede un identità OpenID e che vuole affermare tale identità in un sito.
- **Identity provider** or **OpenID provider** (OP): provider di servizi che offre il servizio di registrazione dell'identificatore OpenID e provvede alla sua autenticazione. È un server di autenticazione OpenID in cui un Relying Party si basa per un'affermazione che l'utente finale possiede un identificatore.
- **OP Endpoint URL:** L'URL che accetta i messaggi di autenticazione del protocollo OpenID, ottenuti effettuando un controllo sull'identificatore fornito dall'utente. Questo valore deve essere un HTTP o HTTPS URL.
- **RP (Relying party):** il sito, chiamato anche provider di servizi, che intende verificare l'identificatore dell'utente finale. Un'applicazione Web che vuole prova che l'utente finale possiede un identificatore.

OpenID - Terminologia

- **User Agent:** il programma (il browser) che l'utente (end-user) sta usando per accedere ad un identity provider o ad un relying party.
- **Identifier:** Un identificatore è un URL "http" o "https". Si definiscono diversi tipi di identificatori, progettati per essere utilizzato in diversi contesti.
- **OP Identifier:** Un identificatore per il provider OpenID.
- **User-Supplied Identifier:** Identificatore che viene presentato dall'utente finale al "Relying Party", o selezionato dall'utente presso il provider OpenID.
 - Durante la fase di apertura del protocollo, l'utente finale può immettere il proprio identificatore oppure un identificatore di OP. Se si utilizza un identificatore di OP, l'OP può quindi assistere l'utente finale nella scelta dell'identificatore per condividere con Relying Party.

Communication among OpenID System Components



Direct and Indirect Communication

Esistono due metodi di comunicazione base tra le entità diverse in un sistema OpenID:

- comunicazione diretta
 - Le entità parlano direttamente usando metodi HTTP POST
- comunicazione indiretta
 - le entità si parlano tramite una terza entità (user agent) utilizzando il metodo HTTP GET

OpenID Modes of Operation

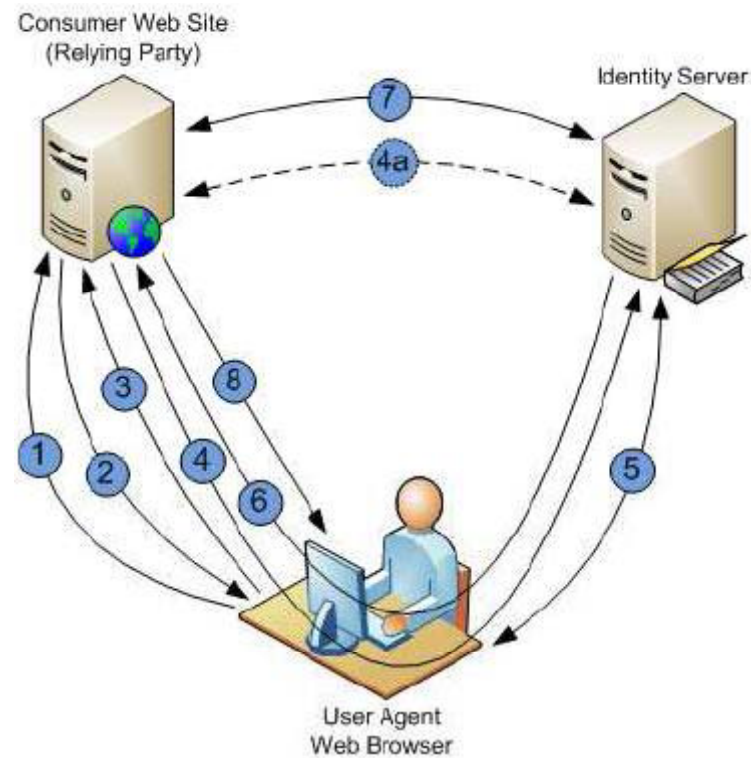
OpenID ha due modalità principali di operare:

- Dump mode
 - Passaggi aggiuntivi per l'autenticazione
 - Il Consumer non tiene traccia dello stato
- Smart mode
 - Consumer “intelligente”

Dumb Mode Communications Flow

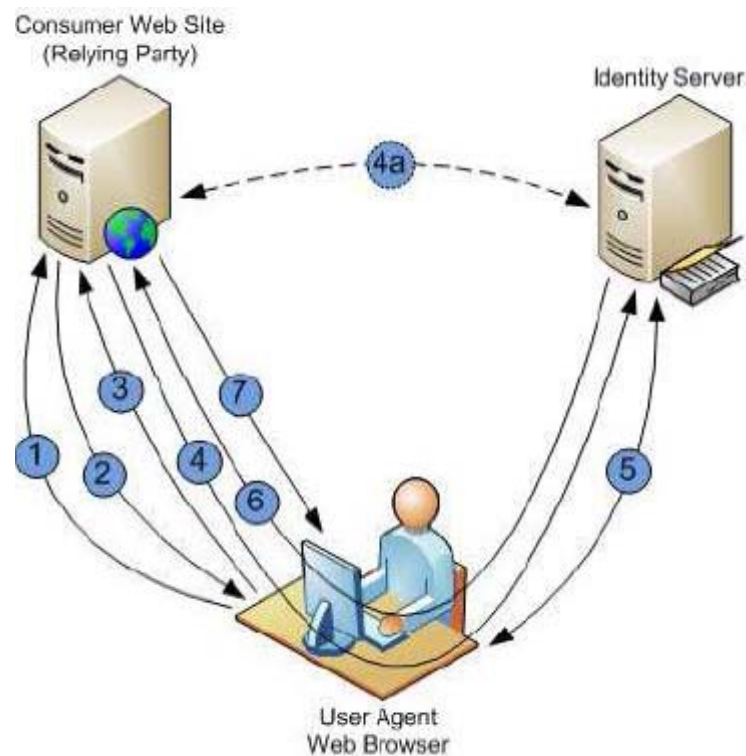
1. Accesso alla pagina web del consumer
2. Inseriamo l'identifier
3. Recupero della posizione del provider
4. Discovery del servizio e reindirizzamento del browser verso il provider
 - 4.a Connessione diretta con il provider
5. Login dell'utente preso l'identity provider
6. Browser redirect preso il consumer
7. Connessione consumer - identity provider
8. Accesso dell'utente preso il consumer

Dump mode flow



Smart mode

- Simile alla modalità “dump”
- Al passo 7 utilizza la chiave condivisa al step 4.a



OpenID Identity URL Page

Il documento HTML avrà l'informazione riguardante il server OpenId (il provider) nella sessione HEAD della pagina

```
<html>
<head>
  <link rel="openid.server" href="http://idp.conformix.com/index.php/serve">
  <link rel="openid.delegate" href="http://idp.conformix.com/?user=test">
</head>
</html>
```

OpenID Messages

- *associate* message
- *checkid_immediate* message
- *checkid_setup* message
- *check_authentication* message

The associate Request Message

- Inviato dal Consumer (Relying Party o RP) all'Identity Provider (OP)
- Per stabilire un “segreto condiviso”
- Comunicazione diretta, quindi HTTP POST
- Associate message parameters:
 - **openid.ns**: versione del protocollo
 - **openid.mode** : tipo di messaggio (associate)
 - **openid.assoc_type** : l'algoritmo utilizzato per la firma(HMAC)
 - **openid.session_type** : il tipo di crittografia (Diffie-Hellman)
 - **openid.dh_modulus** - **openid.dh_gen** - **openid.dh_consumer_public** (se usato Diffie-Hellman)

The associate Response Message

- Inviato dall'Identity Provider al Consumer
- Risposta positiva (success) o negativa (failure)
 - Success: handle con un ttl
 - Failure: error message
- associate Response Message parameters
 - **openid.ns**
 - **openid.assoc_handle**
 - **openid.session_type**
 - **openid.assoc_type**
 - **openid.expires_in**
 - **openid.mac_key**
 - **openid.server_public**
 - **openid.enc_mac_key**

The checkid_setup and checkid_immediate Request Messages

- informazioni di affermazione dal server OpenID
- vengono avviati dal Consumer
- utilizzata la comunicazione indiretta (HTTP - GET)
 - **openid.ns**
 - **openid.mode**
 - **openid.claimed_id**
 - **openid.identity**: opzionale
 - **openid.assoc_handle**
 - **openid.return_to**
 - **openid.realm**

The checkid_setup and checkid_immediate Request Messages



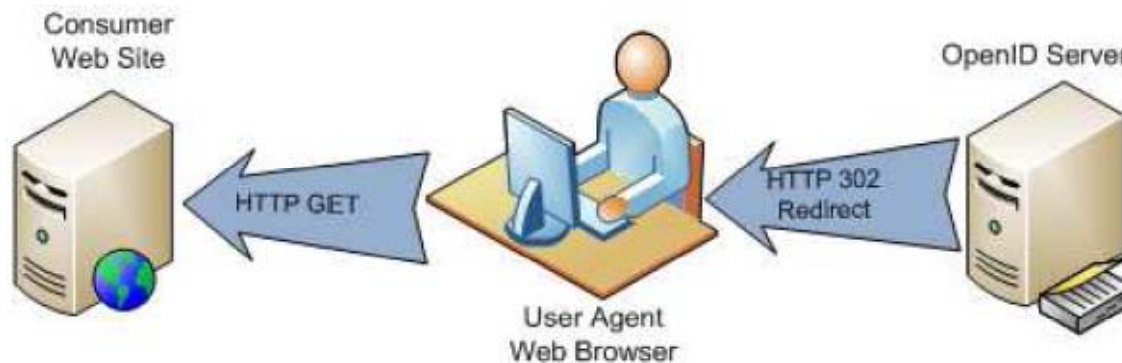
Figure 3-6: The flow for the checkid_setup request message.

The checkid_setup and checkid_immediate Response Messages

- a “checked_setup” ricevuto il server OpenID effettua alcune operazioni ed invia la risposta indietro al Consumer via browser
- può chiedere all’End User di autenticarsi
- checkid_setup and checkid_immediate parameters:
 - openid.ns
 - openid.mode
 - openid.op_endpoint
 - openid.claimed_id
 - openid.identity

The checkid_setup and checkid_immediate Response Messages

- openid.assoc_handle
- openid.return_to
- openid.response_nonce
- openid.invalidate_handle
- openid.signed



The check_authentication Request Message

I messaggi di check_authentication request:

1. non vengono inviati se esiste già un'associazione tra il sito web del consumer e il server OpenID
2. “openid.assoc_handle ” nella richiesta e il Server OpenID invierà lo stesso handle nella risposta, se esiste un'associazione.
3. “openid.invalidate_handle ” per handle non valido
4. Sempre nel caso della comunicazione dumb

Comunicazione diretta tra il consumer e il server di OpenID utilizzando il metodo POST HTTP.

The check_authentication Response Message

- **openid.ns**
- **is_valid**: parametro che ha un valore “true ” o “false ”
- **invalidate_handle**: parametro facoltativo e in caso che il parametro “is_valid” è true, il consumer rimuoverà l'handle dal elenco delle handle salvate.

Scenario One: First Time Login to a Web Site Using OpenID in Dumb Mode

1. Inseriamo il nostro OpenID URL nella pagina del consumer cliccando il pulsante Login.
2. Il sito web del consumer identifica la locazione del OpenID server, e può usare Yadis per scoprire i servizi che l'URL offre. Il consumer reindirizza il browser (lo user agent) al server OpenID per ottenere le credenziali.
3. Poiché questa è la prima volta che l'utente va presso questo sito web, il server OpenID non sa se questo sito web è attendibile o no. Così il server OpenID visualizzerà una schermata di login (login al server OpenID).
4. L'utente indica questo sito web (del consumer) come sito fidato al server OpenID.
5. Il server OpenID reindirizza il browser nella pagina del consumer.
6. Il consumer controlla l'autenticazione direttamente con il server OpenID e l'autenticazione è finita.

Scenario Two: Login to a Trusted Web Site Using OpenID in Smart Mode

1. Inseriamo il nostro OpenID URL nella pagina del consumer cliccando il pulsante Login.
 2. Il consumer stabilisce un'associazione con l'OpenID server, se una tale associazione non esiste.
 3. Il sito web localizza l'OpenID server e reindirizza il browser presso il server per ottenere le credenziali. In questo passo può utilizzare anche Yadis.
 4. Il server OpenID sa che questo è un consumer fidato e sa quali parametri passargli. Se l'utente è già autenticato presso il server OpenID, il server invierà al consumer le credenziali richieste.
- L'utente verrà loggato presso il consumer senza ulteriori passaggi.

Problems Solved by OpenID

OpenID risolve una serie di questioni riguardante l'Identity Management.

Alcuni di questi sono i seguenti:

- gli utenti hanno il controllo su quali dati devono essere condivisi con il sito web del consumer.
- OpenID consente, l'utilizzo delle credenziali attraverso tutti i siti web abilitati per OpenID. Così non è necessario creare singolarmente username e password per ogni sito web.
- Ferma i replay attacks utilizzando la variabile nonce una sola volta. Un consumer può ignorare un'affermazione positiva, esaminando il timestamp nella variabile nonce. Se il timestamp è troppo lontano dal tempo corrente, il consumer può respingerla.

Altro scenario

- Attori
 - **Alice:** *End User*
 - **Operafox Explorer:** *User-Agent*
 - **Bob:** *Consumer*
 - **Carol:** *OpenID Server*
 - **<http://carol.example.com/Alice>:** *Identity*
 - **Ive:** *malicious attacker*

Altro scenario

- Scenario
 - Alice vuole autenticarsi presso Bob
 - Bob supporta l'utilizzo del protocollo Open ID
 - Alice è autenticata presso l'OpenID Provider Carol, è possiede un account
 - `http://carol.example.com/Alice`, è l'identifier di Alice presso Carol
 - Ivo vuole spacciarsi per Alice presso Bob

Altro scenario

- **Domande:**

- Cosa succedere quando Alice inserisce il suo identifier ?
- Come fa Bob ad essere sicuro che si tratta veramente di Alice e non di Ives ?
- Cosa deve fare Carol per assicurare Bob che si tratta di Alice?
- Come fa Carol a ottenere la fiducia di Bob ?

Altro scenario

- Act 1
 - Alice inserisce la sua identità OpenID
 - Lo User Agent di Alice processa la form e la invia ad un CGI implementato presso Bob
 - Il CGI di Bob normalizza l'url inserito da Alice ed analizza il documento che li viene restituito da tale Url
 - “<link rel=”opened.server” href=<http://carol.example.com/openid-server.cgi>”>”

Altro scenario - checkid_setup / checkid_immediate
Request (get)

- Nella modalità “dumb” Bob reindirizza l’End User di Alice a tale URL aggiungendo alcune informazioni (HTTP GET):
 - **openid.mode** = checkid_setup
 - **openid.identity**=<http://carol.example.com/Alice>
 - **openid.return_to** =
http://bob.example.com/comment.cgi?session_id=Alice&nonce=123456
 - ... e lve ... nonce

Altro scenario - checkid_setup / checkid_immediate
Carol Risponde

- <http://bob.example.com/comment.cgi?session\ id=Alice&nonce=123456>
- **openid.mode** = id_res: affermazione o cancel
- **openid.return_to**: lo stesso di prima
- **openid.identity** = <http://carol.example.com/Alice>
- **openid.signed** = mode,identity,return_to: lista di parametri da firmare da Carol
- **openid.assoc_handle** = *opaque handle*
- **openid.sig** = *base 64 encoded HMAC signature*

Altro scenario - **check_authentication**

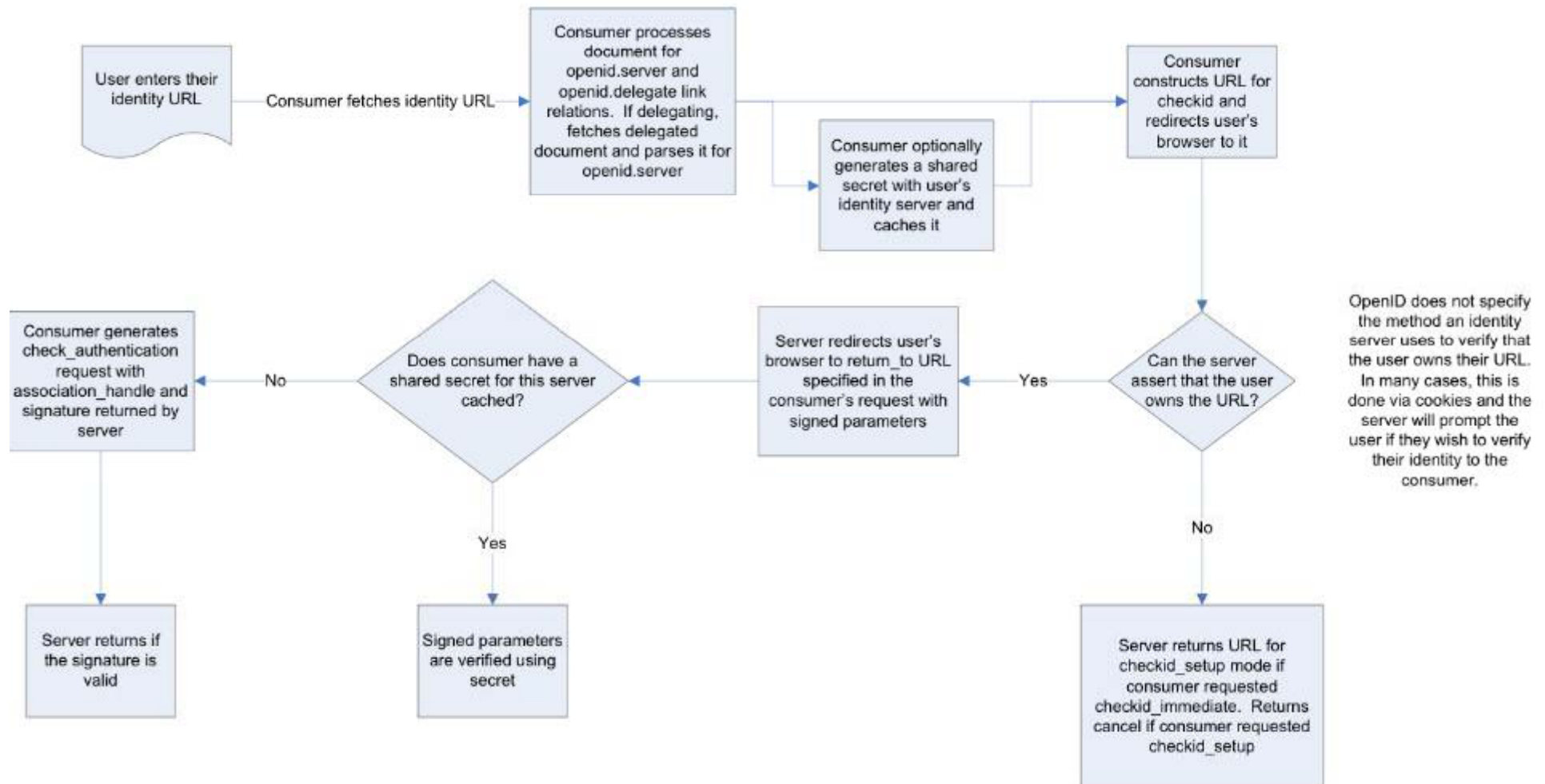
Request (post)

- **openid.mode** = check_authentication: dicendo a Carol che intende confermare quanto Carol ha detto di Alice.
- **openid.signed** = mode,identity,return_to: firmati come prima
- **openid.assoc_handle** = *opaque handle*:
- **openid.sig** = *base 64 encoded HMAC signature*
- Quando Carol riceve questa richiesta andrà a fare tutto il lavoro che ha già fatto in precedenza.
- is_valid: true / is_valid:false

Altro scenario – smart mode
associate request

- <http://carol.example.com/openid-server.cgi>
- **openid.mode** = associate Questo indica a Carol che vuole condividere una chiave segreta con lei.
- **openid.assoc_type** =
 - HMAC-SHA 1
 - HMAC-SHA 256
- **openid.session_type** = *blank* Indica come il segreto deve essere stabilito, un valore vuoto significa in chiaro. "DH-SHA1" indica che verrà usato il protocollo Diffie – Hellman per lo scambio delle chiavi.

OpenId flow



Fine

