Research on OpenID and its integration within the GravityZoo framework

Jarno van de Moosdijk

Research questions

- How does OpenID work?
- What are the requirements for integrating OpenID into the GravityZoo framework?
- How mobile phone friendly are the most popular OpenID Providers?

GravityZoo: What?

- Cloud that handles application delivery to devices (SaaS)
- ConTaX, MediaZoo

NUzakelijk

Voorpagina

Algemeen
Beurs
e-Business
Ondernemen
HRM
Personal Finance
Lifestyle
Groenzakelijk
De Koffiecorner

Dinsdag 3 Februari 2009, Nieuws voor professionals

NUzakelijk video > Bedrijven van NU

GravityZoo lanceert adressenboek in de cloud

Uitgegeven: 23 januari 2009 15:01
Laatst gewijzigd: 26 januari 2009 9:55

AMSTERDAM - Het Nederlandse internetbedrijf GravityZoo lanceert voor het einde van het eerste kwartaal ConTaX, een sociaal adressenboek in de 'cloud'.

Dit is een nieuwe aflevering in de serie Bedrijven van NU , waarin vernieuwende bedrijven onder de loep genomen worden

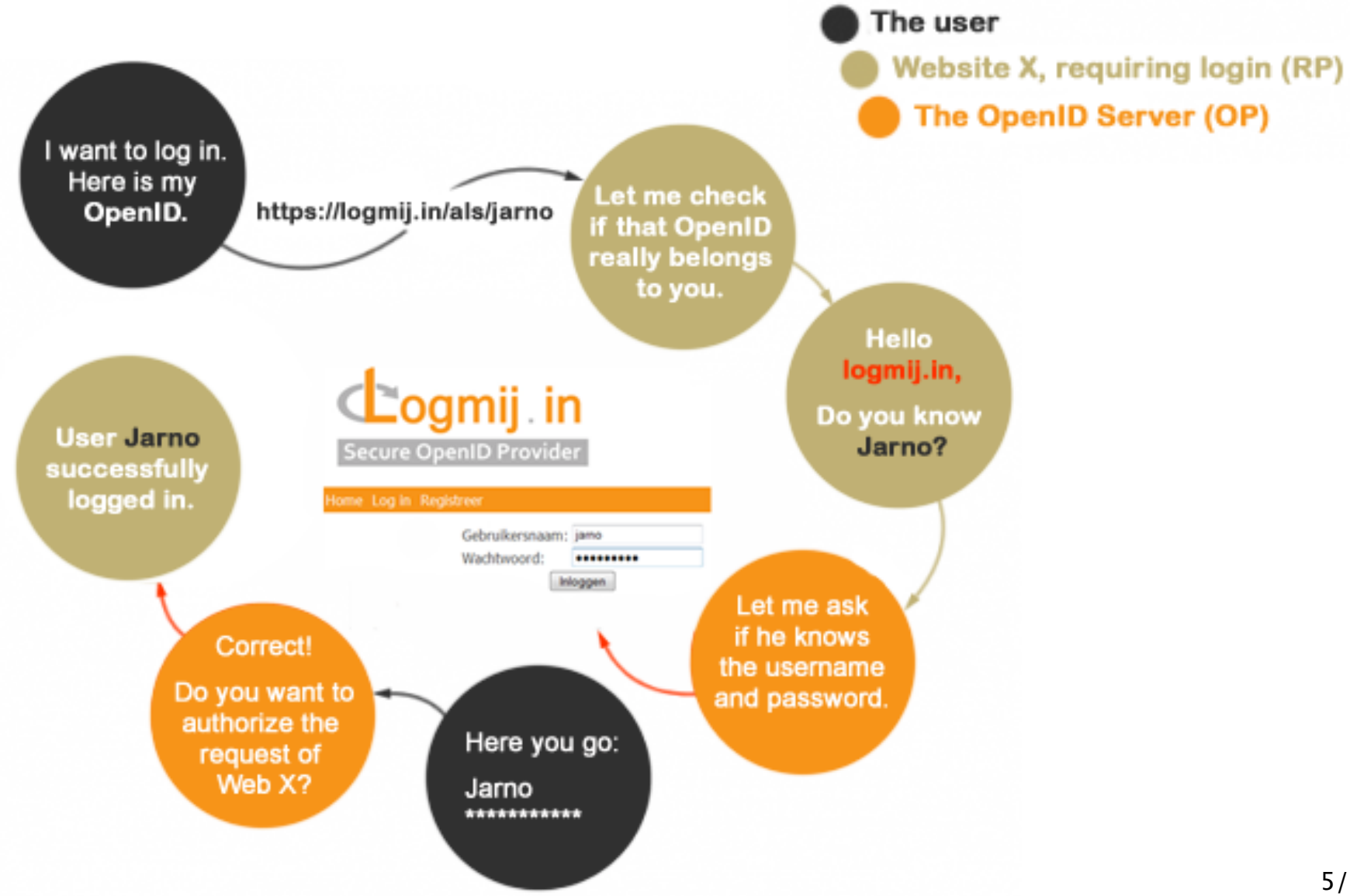
ConTaX moet naast bellen ook instant messaging, bestanden delen en meer toepassingen gaan bieden. CEO Marc Vrijhof noemt het een "unieke" online service. "Als je je telefoon of je simkaart verliest, blijven je contacten bestaan".

GravityZoo is sinds 2005 bezig met de ontwikkeling van een nieuwe technologie waardoor gebruikers van een telefoon of pc geen applicaties meer hoeven te downloaden. Deze applicaties zijn dan via de telefoon of de pc te gebruiken als een

OpenID: Basic terminology

- End user
- Identifier
- OpenID Provider (OP)
- Relying Party (RP)

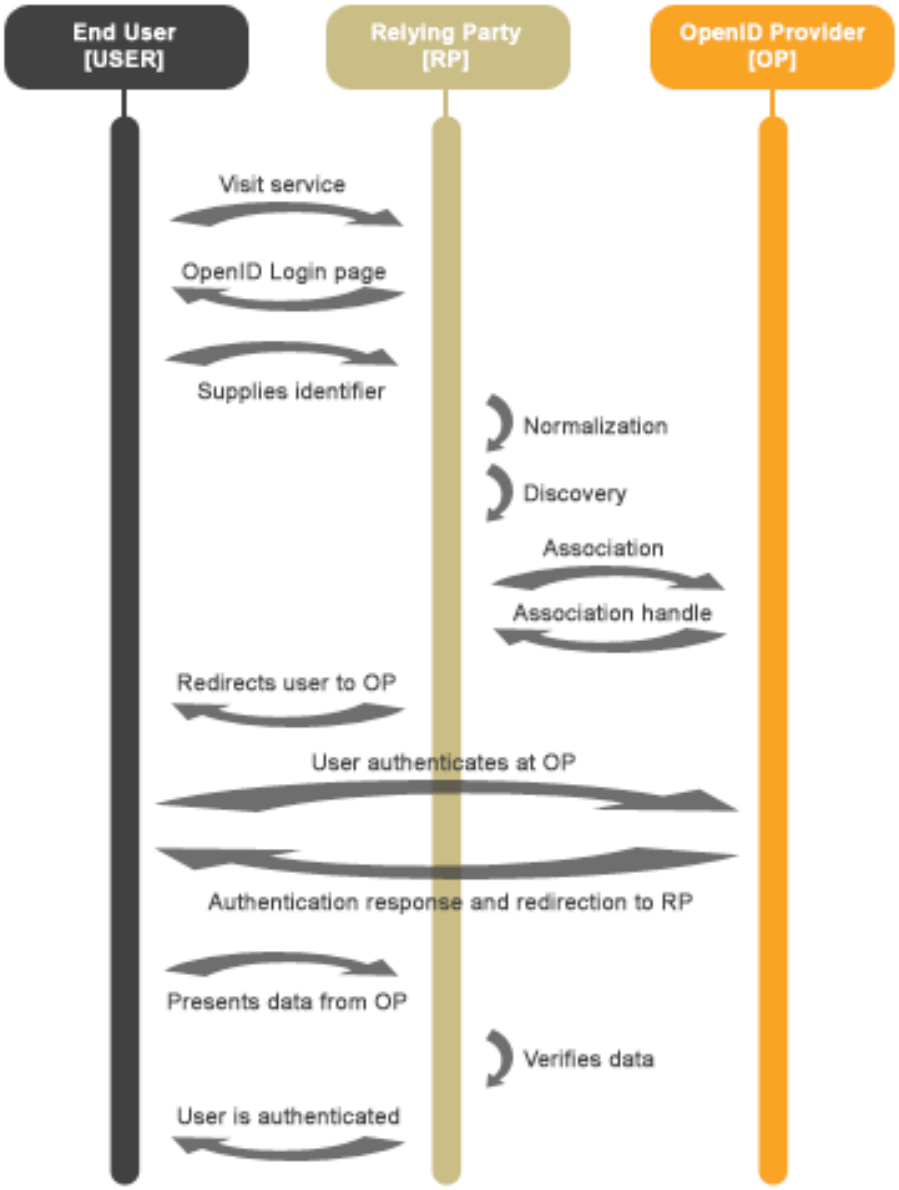
OpenID: end user experience



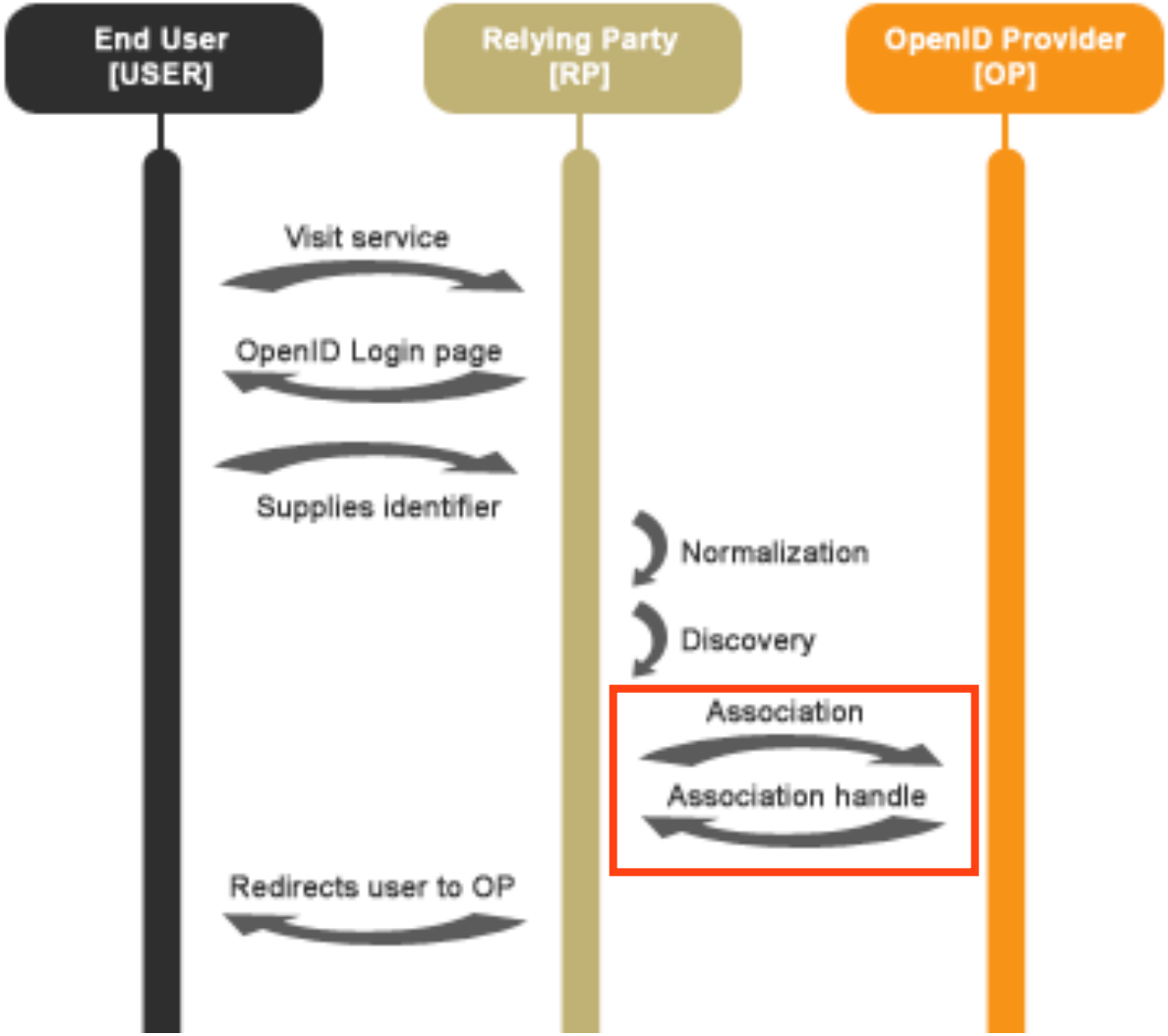
OpenID: Redirection

- No authentication data is transfered directly between RP and OP
- Authentication data is transfered through keys appended to the redirect URL
- RP never sees the password of the user, only the OP response
- https://logmij.in/index.php/serve?**openid.assoc_handle**=%7BHMAC-SHA1%7D%7B49744372%7D%7BMEOX0w%3D%3D%7D&**openid.identity**=https%3A%2F%2Flogmij.in%2Fals%2Fjarno&**openid.mode**=checkid_setup&**openid.return_to**=http%3A%2F%2Fopenidenabled.com%2Fresources%2Fopenid-test%2Fdiagnose-server%2FTestCheckidSetup%2F%3Faction%3Dresponse%26attempt%3D1%26nonce%3DPIX42n6G&**openid.trust_root**=http%3A%2F%2Fopenidenabled.com%2Fresources%2Fopenid-test%2Fdiagnose-server%2FTestCheckidSetup%2F

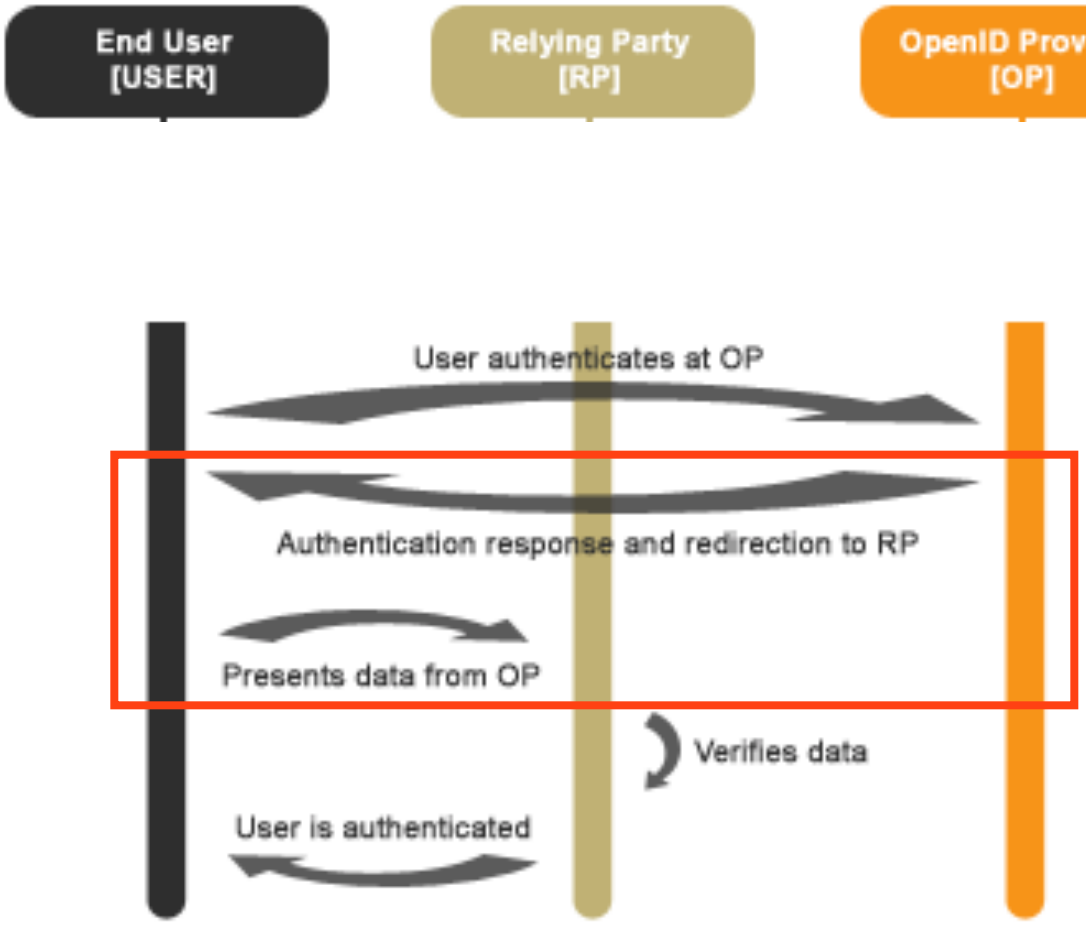
OpenID: In depth



OpenID: In depth



OpenID: In depth



GravityZoo: Authentication

- Currently only username/password login
- Handled by the Authentication and Licensing server role

OpenID: The requirements

- Requirements that have the biggest impact

- **1: Association**
  - Internet access needed to create association with the OP
  - Shared secret key and MAC key need trusted storage

- **2: Intercepting the response**
  - Webserver needed to intercept the response of the OP

- **3: Authorization**
  - Communication with the ALS needed to handle authorization

Three scenarios: 1/2

- **Everything on a new server role**
  - Secret Keys need to be stored in the trusted part of the cloud
  - Keys would need to be sent over the network to trusted part
  - Authorization requests would need to be sent to the ALS
  - The (web-)server has a direct link to the ALS

- **Integrate the whole RP role into the GravityZoo ALS**
  - No web-server allowed in the trusted part of the cloud

Three scenarios: 2/2

- **Best of both worlds:**

- **Separate web-server, rest on the GravityZoo ALS**
  - Shared secret keys can be stored in the trusted environment
  - Web-server act as a forwarder for the authentication response
  - Authorization can be handled by the ALS in the normal way

Future Work

- **Security of OpenID**