Smart OpenID

October 2010

InterDigital / Novalyst IT

Smart OpenID

- Web2.0 Identity Federation
- OpenID in a Mobile Scenario
- Leverages SCWS Technology
- Identity Management Enabler for Operators
- Strong Smartcard Security
- Reduced Signalling and Computing Burden for OpenID Providers

Overview:

Smarter Identity Management using OpenID and SCWS

Federated Identity management (IdM) has great potential for application on small footprint mobile devices and is attracting much attention in industry and standards fora.

OpenID has been adopted by major industry players as a preferred IdM protocol and 3GPP has begun looking at OpenID. However, the wide range of use case scenarios that can emerge if key OpenID functions are smartly distributed across the mobile network infrastructure, devices, and smart cards, has so far not been explored.

Distributed implementation of OpenID entities enables security to be scaled with improved network efficiencies. We focus on the concept of partial representation of OpenID authentication server functions on a Smartcard or a UICC or other secure element. This has immediate benefits to mobile operators, service providers, and users, and presents a compelling use case for the SCWS in truly mobile scenarios.

Operators can address new business opportunities by exploiting their existing infrastructure for accounting and charging with minimum CAPEX for deployment.

Service providers benefit from enhanced trust and a large user base without catering for special 'mobile network' access capabilities.

The user gets a seamless and secure federated log-in experience for mobile services, with control over the smart card and device located credentials – providing greater incentives to participate in the rich mobile Internet experience. An OpenID Provider on the SCWS yields persistence to Identities across mobile and fixed networks, while minimizing the computing and communication burdens on device and network resources.

The security of Smart OpenID scales from Web-style authentication to corporate networks, payment systems, and e-Government applications.

With Smart OpenID, we provide an OpenID solution on a SCWS architecture, enabling rich and flexible mobile IdM.

What is OpenID?

OpenID is an open, community based IdM protocol and has large support from major industry players. The wide scale industry adoption of OpenID is demonstrated by the Open-Government initiative to enable OpenID login to US federal websites.

As a de-facto standard, OpenID is lightweight, easy to implement, distributed, deployed widely, and has great potential for large scale user adoption, especially for mobile applications.

OpenID has been endorsed by many industry forums and organizations, including the Open Identity Exchange forum which intends to build trust in the exchange of online identity credentials across public and private sectors and is backed by Google, PayPal, Equifax, VeriSign, Verizon, and CA, as well as the Kantara Initiative which seeks to assure interoperability for major IdM technologies including OpenID, Liberty AP and Infocard.

Single-Sign-On across networks enabled by Mobile Network Operators

Smart OpenID provides distributed Single-Sign-On access with reduced traffic and increased security

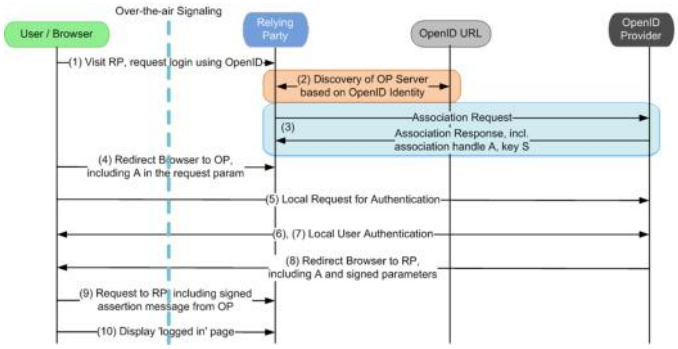
Using the Smartcard Webserver, we build on existing and standardised technology

Protocol and Technology

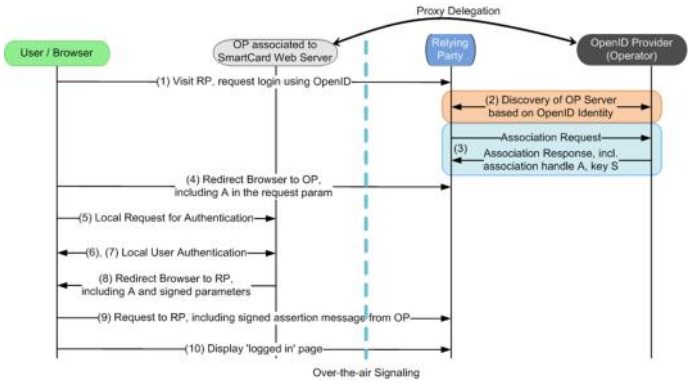
The standard OpenID protocol incurs a lot of over-the-air traffic when used in a mobile scenario. The client communicates with an OpenID provider (OP) which performs the authentication for a relying party (RP) providing a service.

The idea of Smart OpenID is to put part of the trusted functions of the OP on the smartcard. The result is:

- Reduced network traffic
- Smartcard security
- Distribution of Identity Management
- Local management of OpenID authentication



Standard OpenID protocol



Smart OpenID protocol

Standardisation

Smart OpenID is firmly rooted in well established standards:

- OMA SCWS v1.1,
- ETSI TS 102 221, TS 102 484 UICC-Terminal interface security
- ETSI TS 102 412 SCP requirements

Smart OpenID itself has great standardisation potential. Smart OpenID can be combined with a variety of existing bootstrapping mechanisms such as AKA, GBA, SIP-Digest or PKI. In 3GPP application layer identity management is increasingly being considered for binding with access security. In particular binding OpenID with the Operator GBA infra-structure has been considered in TR 33.924.

Smart OpenID has the potential to contribute protocol improvements in standards. We actively support standardisation efforts and drive the adoption of Mobile Network Operators (MNO) based identity management based on OpenID.

Benefits to Service Providers

Service providers are adopting OpenID to attract more customers in an easy way.

With Smart OpenID, Service providers can benefit from valuable customer data and a large user base enabled by the MNO.

Leveraging on the MNO infrastructure, service providers can minimize their efforts to implement their own identity management solutions. Service providers need less investment for infrastructure implementation and operation as well as fewer effort for customer support.

MNO provided identities provide for easy integration of payment options and payment assurance, especially for paid services.

Additional compliance to regulation can be assured by the MNO, protecting services from payment losses through minors.

Mobile Network Operator Business Value

MNOs today benefit from a large user base which recognizes the MNO as a trusted partner. For the MNOs, acting as an identity provider with Smart OpenID:

- Positions the MNO as an applications enabler at minimal risk and cost
- Increases customer loyalty and retention
- Attracts new customers
- Raises brand awareness

The MNO can leverage on existing and deployed smartcard security mechanisms to enable trusted and secure federated identities for consumers. The MNO can also provide additional Trust Framework services for business or government customers.

Using the common SCWS platform, implementation and deployment becomes easy, and the MNO can build upon established mechanisms for remote administration of the card content.

The MNO can also act as a gateway to accessing applications services, by positioning his brand image to the customer at initial login. Additional revenue may be generated by targeted mobile marketing, promotions, and selling banner ads on the SCWS identity provider webpage.

By leveraging on the inherent security of the smartcard, applications such as mobile banking and mobile commerce can benefit too.

Operator provided identities enable new business scenarios

Smartcard Industry

The Smartcard Web Server is a platform that enables smartcard manufacturers to provide added value to other stakeholders, by taking advantage of the proven security of smartcards.

Smart OpenID builds on the SCWS to enable novel applications and business models.

Smart OpenID is an entry point to the market for smartcard-based, user-centric identity management.

The technology is not restricted to mobile scenarios and can also be used for more expanded use cases, such as payment cards.

With Smart OpenID, the smartcard vendors can position themselves as a key player in the e-commerce value chain.

Smart OpenID requires minimum investment as it leverages standardized SCWS technologies.

Acting as an Identity provider positions the MNO as an applications service enabler, increases customer loyalty and attracts new customers

End User Benefits

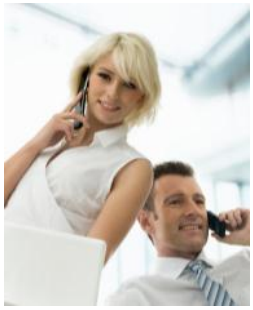
End users obtain an OpenID identity which can be used across a variety of different services and popular social networking sites. The identities can be used with any OpenID enabled service provider, minimizing end user efforts for service registration.

Enabling a secure SSO solution results in a decrease in the risk of identity theft.

Using Smart OpenID as a decentralised authentication method both enhances performance and lowers the risk of data misuse, through minimized external data exchanges for authentication.

Taking advantage of the strong security of smart cards, Smart OpenID also allows users to have higher trust in service providers for both security and privacy, compared to common OpenID implementations that use web-based authentication.

Seamless integration with the mobile browser provides a high level of usability and convenience to the end user.



Bring added value to customers

Interdigital Communications

781 Third Ave
King of Prussia, PA 19406
USA

p: +1 610 878 5758
m: Yogendra.Shah@InterDigital.com

InterDigital develops fundamental wireless technologies that are at the core of mobile devices, networks, and services worldwide.

We solve many of the industry's most critical and complex technical challenges, inventing solutions for more efficient broadband networks and a richer multimedia experience years ahead of market deployment.

InterDigital has licenses and partnerships with many of the world's leading wireless companies.

Visit our webpage at

www.InterDigital.com

Novalyst IT

Robert-Bosch-Str. 38
61184 Karben
Germany

p: +49 (0) 6039-9154-1501
m: Andreas.Schmidt@Novalyst.de
m: Andreas.Leicher@Novalyst.de

Novalyst IT is a private research entity for Information and Communication Technology.

Our know-how offers enterprises with innovative ideas access to funding, research and development resources. We help our clients throughout the process of knowledge and technology transfer — from creation of novel ideas to their commercialisation.

Moreover, we complement our clients' research and development with our competencies and services.

Visit our webpage at

www.novalyst.de