



Position Paper

Federated Identity

Problem

The majority of user authentication schemes today still use userid and password. The burden to users of managing large numbers of userids and passwords has led to proposals for *Federated Identity* systems, where a single set of credentials can be used to authenticate with several organisations, which have agreed to work together as a federation. (An additional problem is the ease of capturing userid/password credentials, but this will not be further considered in this paper.)

The Federated Identity approach has been proposed for business-to-business service provision for employees, where one organisation manages the user credentials and authorisation to systems run by the other organisation.

However, several Federated Identity approaches require one organisation, the Identity Provider, to be in a privileged position in control of the issuance and/or validation of credentials. This approach limits the application of federated identity, as naturally most businesses do not wish to pass control of a major asset – their customers – to another entity. It may also imply an asymmetric relationship, where users show their credentials to the identity provider, without necessarily being able to easily mutually verify its credentials. It is frequently difficult to mix different credential verification services within an organisation; the implementation assumes the same technology will be used throughout.

Additionally, several Federated Identity approaches combine user credentials (proof of identity) with user attributes (such as personal data). This leads to potential privacy issues, which may also cause legal problems, especially if the credentials and attributes are passed across national borders. Complex proposals have been made to allow the user to control which attributes may be passed between organisations.

Most approaches have been limited to authenticating human users. As raised in other Jericho Forum position papers, devices, applications and resources also need to be able to authenticate themselves.

Why should I care

To fully develop the potential of boundary-less electronic business, users need simpler and stronger ways to authenticate to organisations and between organisations (JFC#8)¹. These must also meet the business requirements for different and changing degrees of trust between organisations, and allow for equal partnerships.

Privacy concerns must be visibly met, with the data under control of the data owner, normally the end user, and disclosure should be limited to the least amount necessary.

¹ The term JFC#n refers to the relevant Jericho Forum Commandment number. See www.jerichoforum.org

Jericho Forum response

Many Federated Identity technologies do not directly match the key business needs and trust relationships required in a de-perimeterized environment.

To support business-to-business service provision, a person granted one or more credentials in one authentication/authorisation domain should be able to use these credentials with another organisation. This implies the second organisation must be able to check credentials with the first organisation, and also that each organisation must be able to supply authorisation information, which are combined to define the final authorisation permissions. (JFC#8)

There should be no requirement for a privileged Identity Provider; instead peer-to-peer authentication should be supported. Business models using a separate identity provider may also be supported.

Systems should support the use of several different credentials and authentication technologies referring to the same individual. Different credentials may be used in different contexts (JFC#3), for example to distinguish different roles taken by the same individual, and may also affect the trust level to be used (JFC#6). There should be no requirement for homogenous credential technology; any system should be flexible and extensible.

Clearly distinguishing between credentials and attributes will clarify use of data, help meet privacy legislation, and also ease the introduction of new authentication techniques to replace passwords. In general, shared secret credentials should not be transferred to other organisations, due to the increased risk of compromise. Instead, identity assertions or seamless pass-through authentication should be used. This applies whether the identity information is being transferred between organisations, or between component layers of an application (JFC#8 – systems must be able to pass on security credentials/assertions)

In most cases data attributes should be held by the end user, rather than centrally stored by a third party. For browser-based applications, a standardised data form schema would make it simple to pass the same data to different organisations completely under user control. Individuals should be able to choose which sets of attributes are used for a given transaction (work/home address, credit card selection). (JFC#8)

Challenges to the industry

The numbering here provides for ease of reference and does not imply any priority.

1. Create common schemas for the majority of transaction data attributes requested, including name, address and payment details, to remove the need for centralised attribute storage.
2. Mutual authentication should be used by default.
3. Peer-to-peer authentication should be permitted, without the need of a privileged identity provider.
4. The currently assumed role of an individual should be made explicit to systems.
5. Subject attributes should not be used as credentials.
6. Credentials and authorisation information should be able to be transferred between organisations using open protocols and standards, and be simple to manage the equivalence relationships.
7. It should be possible to support a multiplicity of credentials and technologies for an individual.

The way forward

The Jericho Forum believes that development of heterogeneous federated peer-to-peer identity systems will allow simpler and stronger authentication schemes meeting the corporate requirements of a de-perimeterized world.