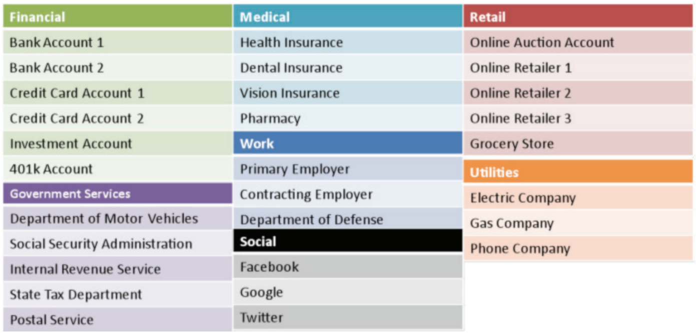
Whitepaper: Identity Federation Benefits and the Provisioning Challenges Ahead

In this whitepaper, we present a high level overview of the identity federation concept, and how it compares to traditional identity approaches. We highlight the benefits and drivers that have led TSCP to recommend the adoption of federated identity architectures, and to support identity federation via TSCP specifications. We also discuss some of the challenges that early adopters of identity federation faced, and what TSCP is doing to address these challenges, and how readers can participate.

By Steve Skordinski, TSCP

What are Legacy Silo Identity Architectures?

"Legacy silo identity architectures" are simply defined as architectures in which applications are accessed only by users with a local account issued by the organization owning the application. If a user outside the organization requires access, they are provided a local account and credential to log in. This architectural approach has led to a proliferation of credentials that users are familiar with, and shown in Figure 1.



Financial	Medical	Retail
Bank Account 1	Health Insurance	Online Auction Account
Bank Account 2	Dental Insurance	Online Retailer 1
Credit Card Account 1	Vision Insurance	Online Retailer 2
Credit Card Account 2	Pharmacy	Online Retailer 3
Investment Account	**Work**	Grocery Store
401k Account	Primary Employer	**Utilities**
Government Services	Contracting Employer	Electric Company
Department of Motor Vehicles	Department of Defense	Gas Company
Social Security Administration	**Social**	Phone Company
Internal Revenue Service	Facebook	
State Tax Department	Google	
Postal Service	Twitter	

Figure 1 - Typical Example of Identity Proliferation Resulting from Silo Identity Architecture

What is Identity Federation?

Identity Federation is an online means to authenticate and authorize users whose identities are managed by one organization, but who require access to information resources or services provided by another organization.

Acceptance of identity data that contains identity information as well as other attributes (claims) by a Relying Party (RP) depends on the RP having confidence in the policies and procedures utilized by the Identity Provider (IdP) who performed the initial identity proofing, issued the credential, and validates and binds that credential to additional attributes.

Figure 2 provides a high level overview of the services and steps required to log into an application in a federated environment.

What are the Benefits of Identity Federation over Silo Identity Architectures?

By deploying identity federation architecture, there are several advantages organizations can realize:

1. Reduced costs of credential management by reducing the number of credentials organizations are required to manage.
    - Every credential issued requires full lifecycle management by the issuing organization; all have tangible costs incurred by the provider:
        - Registration and issuance - user identity proofing and vetting
        - Token costs – smart cards, one-time-password (OTP) devices, even directory storage for username and password
        - Management processes – account lockouts, lost tokens, account disablement
2. Enablement of sharing information beyond organizational boundaries
    - By leveraging existing credentials, trusted IdPs and identity federation, RPs can rapidly deploy new services without incurring the costs associated with credentialing in identity silos. Reducing the barriers to building and enabling new services encourages organizations to make more data accessible online for collaboration with partners.
3. Reduced sign-on end user experience
    - Identity federation allows a single authentication session between the user and the IdP to enable access to any federated application that trusts the user's credential and IdP. From the end user standpoint, they are able to traverse from an application in organization 1 to application in organization 2 without the need to re-authenticate, or even having to be aware of the underlying identity architecture.
4. Increased identity assurance of end users
    - When reducing the number of credentials issued, organizations can focus on leveraging credentials distributed under robust registration processes, and using strong tokens such as smart cards and OTPs.
5. Increase accessibility of user attributes required for authorization
    - Applications require more than just the identity of the user to decide what information the user is authorized to see.

Identity alone cannot be used to determine user privileges; therefore it must be supplemented by complementary technologies to support the privilege management function within an application. User attributes are needed to support the authorization decision(s) at the applications.

- Attributes are often not readily available at the RP, and even when they are available they are not always, accurate or reliable. The relationship between the user and the IdP often makes the IdP a stronger candidate to manage attributes than the RP. An IdP with a strong attribute management process can more cost-effectively share the attributes with a dozen RPs, instead of 12 RPs all trying to maintain and update the same attributes in isolation.
- Identity federation provides a technical channel for IdPs to pass attributes about the user to the RP.

What Challenges Do Identity Federation Present Compared to Traditional Federation?

While we have noted the many benefits of identity federation, we must also acknowledge that this new paradigm creates new challenges as well. For instance, identity federation can often require RPs to provision information owned by the IdP in order for applications to function. Let's begin by exploring why that is:

Identity federation-enabled applications broadly fall into two categories:

1. Legacy Account Based Applications: Federation-enabled legacy applications feature access control list (ACL) and group policy to authorize user access to the application contents. In order for the ACL system to function, the application must maintain an account for the user in a local database or directory. In a federated implementation, the user will not be permitted to directly authenticate to this account. Instead, the user authenticates to the IdP, and the assertion sent on behalf of the user is then mapped by the RP to the local account. We typically refer to these local accounts without direct authentication support as shadow accounts.
2. Claims Aware Applications: Claims aware applications are able to make access control decisions to data based solely on the attributes available to the consuming application. The application does not map the incoming claims to an account managed by the RP.

It is the identity federation-enabled legacy account-based applications that pose a particular challenge to RPs and administrators. Some applications contain tens to hundreds of thousands of users. Before a user can successfully authenticate to the application, a shadow account must be created. This process is referred to as shadow account provisioning. Currently, thousands of accounts are provisioned bilaterally, agreed to by the IdP and RP. Unlike the authentication technologies and processes that have become ubiquitous across IdPs and RPs, there isn't yet a widely-adopted group of inter-organizational provisioning technologies, nor are there repeatable best practices and policies in place.

What is TSCP doing to address the Provisioning Challenge?

The TSCP Identity Federation Working Group is actively looking at the provisioning challenge. The goal of this work effort is to improve the provisioning process by identifying and documenting standards-based reusable method(s) for provisioning. This will allow IdPs and RPs to build provisioning services once, and reuse the service many times, just as identity federation services can be easily reused with additional partners once established.

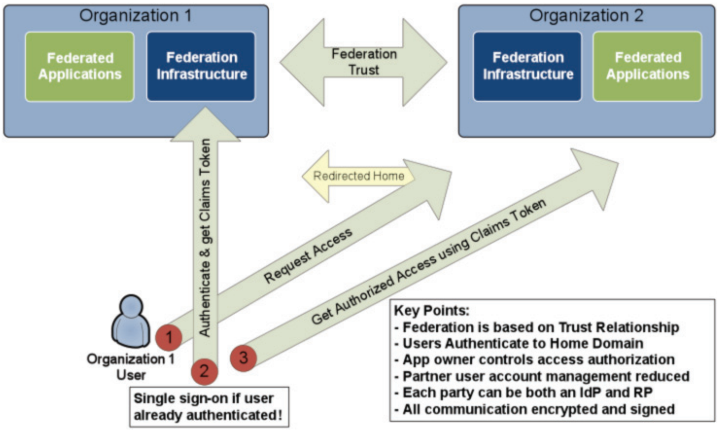

Organization 1
Federated Applications
Federation Infrastructure
Federation Trust
Organization 2
Federation Infrastructure
Federated Applications
Authenticate & get Claims Token
Redirected Home
Request Access
Get Authorized Access using Claims Token
1
2
3
Organization 1 User
Single sign-on if user already authenticated!
Key Points:
- Federation is based on Trust Relationship
- Users Authenticate to Home Domain
- App owner controls access authorization
- Partner user account management reduced
- Each party can be both an IdP and RP
- All communication encrypted and signed

Figure 2. Identity Federation Overview

To meet this objective, the working group will:

- Directly engagement with IdP and RP identity management architects and engineers to capture the real-world use cases and applications that require provisioning.
- Identify and analyze the protocols available to support provisioning.
- Work with COTS vendors to identify the current and planned support for provisioning protocols in their identity management product lines.
- Identify and document existing gaps in both existing standards and products; provide feedback to both the appropriate standards and vendor communities.
- Publish TSCP specifications that provide detailed implementation guidance for both IdPs and RPs, to encourage adoption of reusable provisioning approaches.