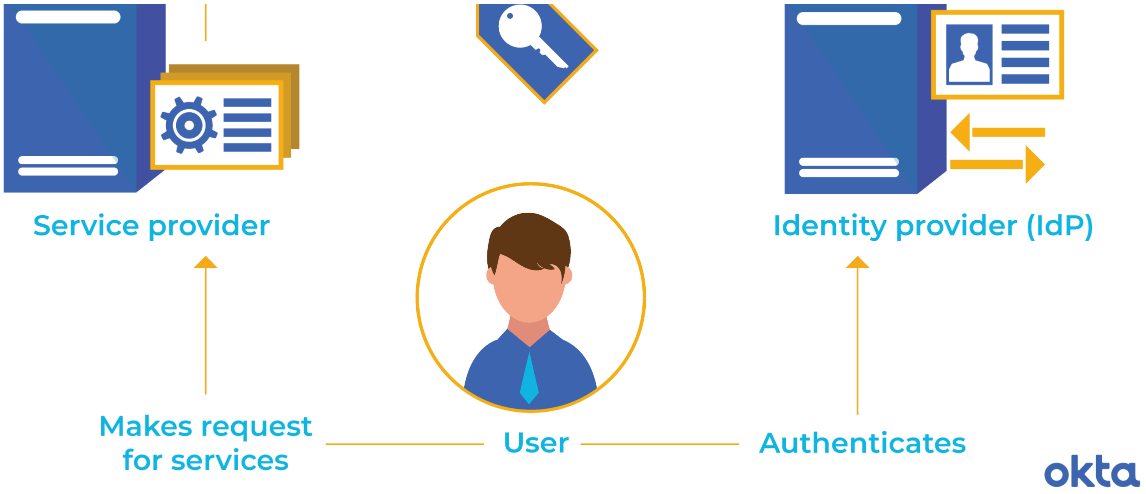
Building on SSO Techniques

The average employee has **191 passwords to track, perfect, and update**. Those same employees have crucial work to do, families to run, and finances to protect. Reusing passwords seem harmless or even helpful. But doing so can lead to immense security risks.

Enter single sign-on (SSO) techniques. With one form of identity verified, the user can move from system to system without logging in to each one.

Federated identity management supports SSO, but it takes the concept of signing a bit further.

Companies that invest in federated identity solutions agree on a set of shared principals. That ensures quick movement between systems without compromising security.



Federated Identity & Authentication

Your digital identity is made up of attributes that define you as a unique person moving through the landscape. Federated identity is an agreement between entities about the definition and use of those attributes. Agreements allow you to sign on in one place and then jump to another asset without signing in again.

Identity federation is a generic term, and it can apply to many different types of companies, platforms, and protocols. But those that offer identity federation products agree to use technology others understand and can access. That way, different platforms can communicate and share without requiring another login.

Seven so-called "**laws of identity**" sit beneath federated identity systems.

1. User control and consent: Users give permission to share data, and they have at least some say in how shares happen.

2. Minimal disclosure: The smallest amount of identifying information is shared, and it's stored securely and deleted quickly.

5. Competition: Many identity providers should be supported, as competition breeds better performance.

6. Human integration: A real person has a place in the process, reducing the risk of computer-to-computer hacks.

7. Consistency: The users have a simple, consistent experience among platforms.

Read through these concepts carefully, and a picture of federated identity begins to form. And chances are, every modern user has encountered the process at least once. If you've logged into Google and then dashed to another website for protected info without another login, you've encountered federated identity concepts.

How Does Federated Authentication Work?

Federated identity management relies on **strong agreements**. Identity providers and service providers develop an understanding of what attributes (such as your location or phone number) are representative of who you are online. Once those credentials are verified, you're authenticated across multiple platforms.

Common technologies used in federated identity management include:

- Security Assertion Markup Language (SAML)
- OAuth
- OpenID

Companies might use security tokens, such as JWT (JSON Web Token) tokens and SAML assertions, to pass permissions from one platform to another.

Consider Google's federated identity process with OAuth. To use this system, **developers must**:

1. Pull OAuth credentials from Google's API. Choose data, such as a client ID and client secret, that both Google and your company know.

4. Send the token to an API. Users are ready to gain access, as long as the token is included in an HTTP authorization request header.

To a user, the process is almost invisible. They come to a website they'd like to enter, and they're shown a screen asking them to log in via other credentials. They hit a button or two, and access magically appears.

The Government's Role in Identity Federation

Computer developers think of themselves as autonomous entities, free of politics and interference. In reality, the government is deeply interested in how federated identity works and who is in charge of it.

That interest stems from **Homeland Security Presidential Directive 12**, issued in 2004. Here, experts required secure credentials to access government assets, and teams were encouraged to build systems that allowed for quick movement between platforms and programs. Speed was crucial, but safety was needed.

Since 2004, plenty of companies have developed agreements, protocols, and programs for federated identity. But more work is required.

Currently, the National Cybersecurity Center of Excellence and the National Strategy for Trusted Identities in Cyberspace National Program Office are collaborating on a **Privacy-Enhanced Identity Federation project**. When complete, the team will release a set of standards companies can use for federated identity. No release date is available quite yet.

Benefits of Federated Access

Some companies allow secure sign-on without touching federated identity concepts at all. Others wouldn't dream of running a product this way. Which side is right?

The benefits of federated identity include:

protection and security. And since each login is a **point of vulnerability** for companies, streamlining the process could reduce hacking risks.

Misconceptions About Federated Access

There aren't significant drawbacks to using federated access, but there are some common misconceptions about it. These include:

- **Less control.** Federated identity management solutions follow a specific set of rules and agreements. Some people fear this means less control, but this isn't the case. SSO vendors usually provide various configuration options so systems can behave as needed.
- **Potential security risks.** No authentication protocol is entirely secure, and some federated programs come with **known vulnerabilities**. Generally, a federated program built to typical standards is more secure than almost any other program.

Plenty of companies consumers know and trust use federated identity concepts, including Google, Microsoft, Facebook, and Yahoo. If these organizations lean on the concepts, it's realistic to assume that they're safe and trusted. But every company must do its own assessment of risk and benefit.

Discover how Okta can help you decide if federated authentication or single sign-on authentication is the more secure solution for your organization.

References

Average Business User Has 191 Passwords. (November 2017). *Security.*

Federated Identity Management. (2009). David W. Chadwick.

Understanding Federated Identity. (August 2007). Network World.