BUILDING BLOCK

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

PRIVACY-ENHANCED IDENTITY FEDERATION

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of enhancing identity federations with privacy protecting capabilities through collaborative efforts with industry and the information technology (IT) community, including vendors of cybersecurity solutions. This sheet provides an overview of the background and challenge, goals, and potential solution. For more information about the project, see the *Privacy-Enhanced Identity Brokers* white paper on the NCCoE website. The solution we propose is not meant to be authoritative; there may be other solutions in this fast-moving cybersecurity technology market. If you would like to propose an alternative architecture or know of products that might be applicable to this challenge, please contact us at petid-nccoe@nist.gov.

BACKGROUND

Many organizations allow online customers to use third-party credentials to create and manage accounts and services. For example, your social media account login can be used to access your fitness tracker account. In effect, the social media company is authenticating your identity for the fitness company.

Allowing third-party credentials saves businesses time and resources in managing identities. It is convenient for people as well. Yet, especially for credentials that need higher levels of assurance—such as a bank, which may require liability and fee negotiations, a growing number of organizations are laboring to manage—and integrate—each third-party relationship. The current primary solution is to establish an identity broker to manage and contract for multiple third-party credentialing options on an organization's behalf, versus managing each credentialing option in-house.

THE CHALLENGE

While the benefits of federated identity management are significant for both organizations and individuals, these connections can create new cybersecurity and privacy concerns. For example, they could create additional opportunities for an organizational data breach, exposure of business or personal information, or leave openings for new ways to track online user activity. In addition, the broker could gain insight into user data it does not need while performing operations to facilitate identity authentication. Both organizations and users must be able to trust that the federated identity management service is not going to reveal sensitive information in order for them to participate.

GOALS

The primary goal of the privacy-enhanced identity federation project is to demonstrate how federated identity services, leveraging market dominant standards, can include privacy enhancements directly in the solution. More specifically, this project seeks innovative ways to encrypt user attributes in order to prevent intermediaries in federated identity transactions from gaining access to personal information. Additionally, it seeks to retain an architecture in which organizations and identity brokers do not know each other's organizational identities, so that neither entity can track or link user activities beyond what is known from their direct relationship with the user. Any approach used to achieve this goal must be able to mitigate common online attacks.

BENEFITS

Benefits of privacy-enhanced identity federation for businesses include:

- Reduced risk of exposure of personal and organizational information (e.g. customer lists) to participant organizations that have no operational need for the information
- Reduced risk of unauthorized access to personal information

The National Cybersecurity Center of Excellence at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic, and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable.

LEARN MORE ABOUT NCCOE
Visit http://nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

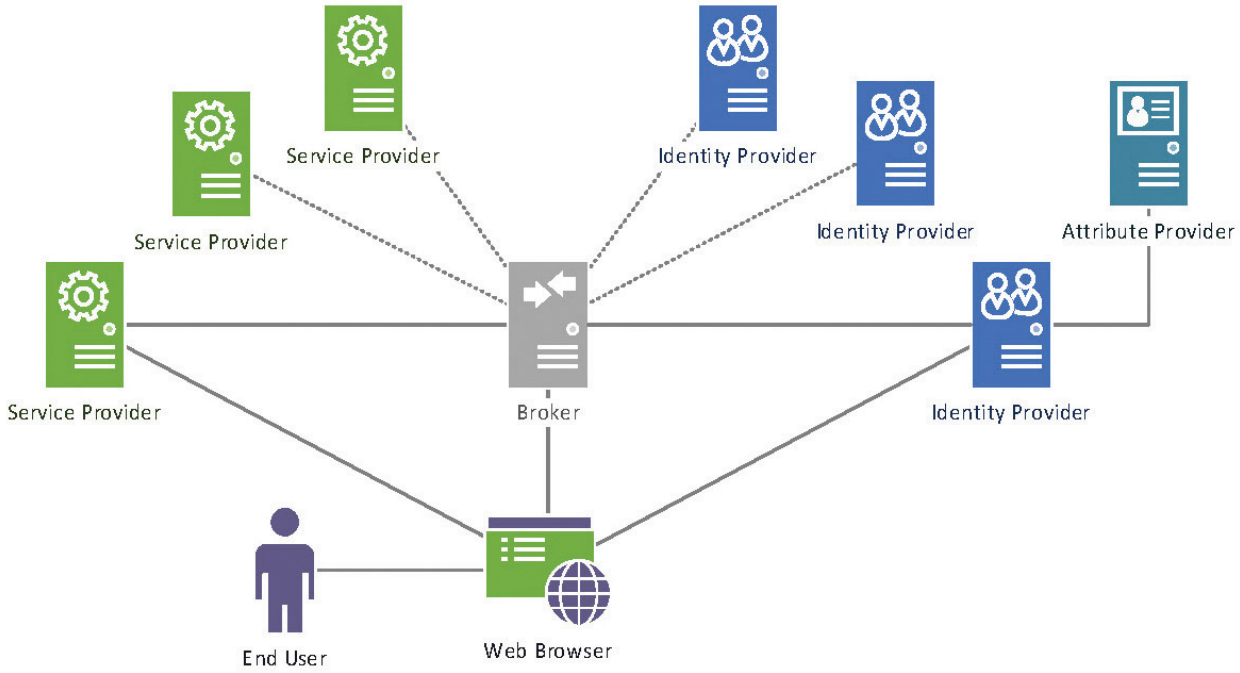
- Streamlined compliance as a result of collecting and storing less personal information
- Market differentiation by building privacy protection into software and hardware solutions
- Operational and cost efficiencies due to the reduction of identity management requirements

Benefits of privacy-enhanced identity federation for consumers include:

- Reduced exposure to online tracking and profiling
- Reduction in the amount of personal information necessary to obtain access to online services
- Convenience and security by having fewer identity credentials to manage

ARCHITECTURE

The proposed privacy-enhanced identity federation architecture captures the various actors at a system of systems level; each relying party (RP) and identity provider (IdP) could compromise a variety of additional components. It is important to note that there could be multiple solutions and that some solutions may require other components and/or standards in addition to those already identified.



COMPONENTS

The following list is an example of the components that might comprise a final privacy-enhanced identity federation solution. This list is only a starting point; specific components will be identified through future vendor collaborations.

- RP hosts (physical or virtual) and instances
- IdP hosts (physical or virtual) and instances
- Optional Identity Federation host(s) (physical or virtual) and instances
- Attribute provider hosts (physical or virtual) and instance(s) (optional)
- User agent/host with web browser

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking collaborators, insights, and expertise from businesses, the public, and technology vendors. If you are interested in contributing or collaborating on this project to enhance identity brokers with privacy technologies, please contact us at petid-nccoe@nist.gov.
For more information about this project https://nccoe.nist.gov/projects/building_blocks/privacy-enhanced-identity-brokers.