Abstract

Service Oriented Architectures are an abstract concept which exposes capabilities in distributed, domain-spanning environments as services. These modern systems have three characteristics: They are heterogeneous, distributed and loose Coupling. With increasing popularity of Service Oriented Architecture (SOA), this is no longer possible since interacting systems are generally not located within a single security domain anymore. Using SOA without extra attention to security issues leads to various problems. Federated Identification is one of the most important security issues in collaborative systems which are not in the same security domain. To deal with this security issue, several Federated Identity Architecture initiatives have appeared recently. Federated identity architecture lets users dynamically distribute identity information across security domains, increasing the portability of their digital identities. All Federated Identity Architectures keep user’s distributed mapping and/or centralized mapping of user’s identifiers for federated identity. Saving the mappings for each user and updating them when changes happen will bring a Heavy Overload for the architecture. In this paper Federated Identification Architecture is presented which provides a Centralized Identity Provider (CIP). The architecture presented is highly beneficial in SOA and distributed environments. All security domains can integrate with this architecture using very few adjustments. Advantage of using CIP model is that users can accesses a service by using any of the identifiers which they prefer.
The chosen identifier is not always the identifier recognized by the requested service.

References


Index Terms

Computer Science Communications
Keywords
Identification  SOA  Federated Identity