2015

Federated Account System For Accelerated Development of Internal Systems

Javan Cohen
Virginia Commonwealth University

Nandu Radhakrishnan
Virginia Commonwealth University

Brian Seal
Virginia Commonwealth University

Team Members: Javan Cohen, Nandu Radhakrishnan, Brian Seal

Faculty Advisor: Pretam Ghosh

Sponsor: Massey Cancer Center

Sponsor Advisor: David Fenstermacher

COMPUTER SCIENCE

Federated Account System

For Accelerated Development of Internal Systems

CAPSTONE DESIGN EXPO 2015

Abstract

Applications need to get validated claims about an authenticated party to know the level of access to grant to the authenticated party. The application will not authenticate the user, a third party will do this. All claims that the application receives about the authenticated party will come from a specific trusted security token service that packages up all the claims the application needs in order to properly authorize the user.

An application's domain of trust will be termed "application local", meaning it will trust only a custom relying party STS (**RP-STS**) that issues claims about authenticated identities. This RP-STS can trust any number of Identity Provider Security Token Services (**IP-STS**). For purposes of these requirements, these can all be considered to be in another domain (relative to the application) as it doesn't matter if the IP- STS is VCU CAS or some third party IP.

The application designed takes in valid login information from a circle of trust, and produces identity tokens from these, which are then used as valid login credentials for gated services based upon the claims contained within.

Implementation

Actors

- **User -** the person attempting to access the secured application.
- **Secured Application** – the software system the User needs to interact with.
- **RP-STS**– the Domain Local RP-STS Claims Provider software system "trusted" by the Secured
- **Application** that is allowed to issue claims that the Secured Application can use.
- **IP-STS** –the identity provider "trusted" by the RP-STS that will authenticate the user and supply basic claims that the RP-STS can use to build a full set of claims.

- A user needs to access a secured application. The user will be required to authenticate against a trusted authority that has that capability (IP-STS) and a set claims about the user will be built by the RP-STS and supplied to the secured application. The secured application will then allow the user the appropriate level of access (including denying access) depending on the relevant claims supplied.
- In order to achieve this implementation, a number of preexisting technologies were leveraged, namely the currently existing VCU Central Authentication System, the Open-Source **Thinktecture IdentityServer**, and as a proof of concept, various sites which use **OpenID** tokens, such as Google.

Algorithm Visualization