"Geneva"
Claims Based Access Platform

Beta 1 Datasheet

Microsoft Identity and Access solutions are a set of platform technologies and products designed to help organizations manage user identities and associated access privileges. With a focus on low total cost of ownership, security, ease of use, and open interoperability, these solutions help improve developer productivity, reduce IT costs, and efficiently achieve business goals.

Users need an efficient and intuitive way to collaborate – to interact with other people, resources and information through tools such as email and portals. At the same time, businesses and governments need to ensure people collaborate within the bounds of internal security policies and external regulations.

Microsoft addresses these needs with identity and access infrastructure and solutions that manage users, devices, access privileges, and credentials.

Microsoft "Geneva"

Claims Based Access Platform

Geneva" is Microsoft's open platform for simplified user access based on claims.

Claims describe identity attributes and can be used to drive application and other system behaviors with an open architecture that implements the industry's shared Identity Metasystem vision.

Business Needs

There are two major challenges "Geneva" claims based access can help organizations solve:

- Businesses and governments need to enable collaboration within the enterprise, across organizational boundaries, and on the Web while satisfying cost cutting and security requirements.

- Organizations must react to changing needs more quickly and economically by enabling existing systems to interoperate with new systems such as cloud services and service-oriented architecture (SOA).

Today's Challenges

The complexity of implementing and managing identity-based user access to applications and other resources makes it difficult for developers and IT to satisfy these business needs. There are several problems with today's application access solutions:

- Too many different identity technologies for developers to choose from

- Expensive and complex to implement and manage user access

- Difficult to interoperate heterogeneous applications and systems, and hard to adapt applications to new scenarios

- Emerging cloud services and SOA trends could amplify these challenges

Identity Metasystem: A Shared Industry Vision

The Identity Metasystem is a shared industry vision that defines a single identity model for the enterprise, federation, and the consumer and citizen Web. Claims issued by security token services (STS) are used in the Identity Metasystem to help applications make user access decisions across applications and systems regardless of location or architecture. Claims are delivered inside security tokens produced by an STS, and can disclose identity information selectively.

Microsoft Solution Overview

"Geneva" implements the Identity Metasystem vision for open identity interoperability including a single simplified user access model that works across different applications and systems to enable security-enhanced collaboration. "Geneva" is open and adaptable to enable user identities to interoperate seamlessly.

"Geneva" improves application developer productivity by simplifying and externalizing access logic from applications. It also reduces development effort with pre-built security logic and .NET tools.

"Geneva" helps IT efficiently deploy and manage new applications by reducing custom implementation work, consolidating access management in the hands of IT, helping establish a consistent security model, and facilitating seamless collaboration between organizations with automated federation tools.

Consumers and information workers can benefit from help navigating logins, managing different personas, and controlling how personal information is shared.

In addition to claims-based architecture, "Geneva" supports industry standards including WS-* and SAML 2.0 for open and interoperable identity. "Geneva" also enables claims-based and non-claims systems to interoperate by translating between claims and non-claims token formats.
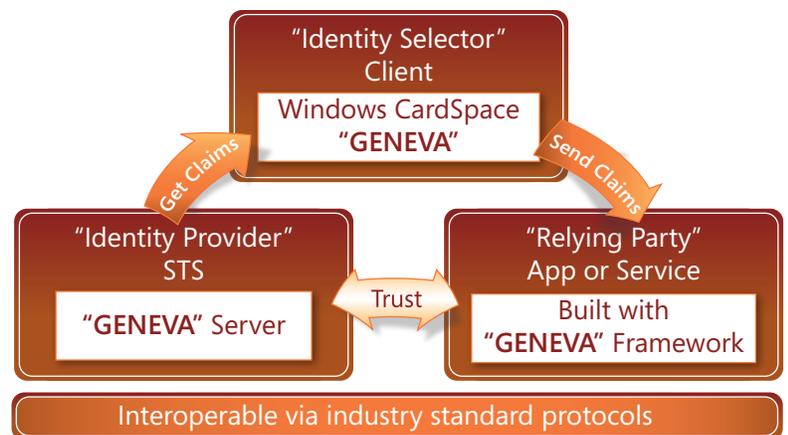
Product Components

"Geneva" includes three platform components for enabling claims-based access. Beta 1 of the following components are now available for public evaluation:

- **"Geneva" Framework** for helping developers build claims aware .NET applications that externalize user authentication from the application, plus custom security token services (STS).

- **"Geneva" Server**, an STS for IT that issues and transforms claims and other tokens, manages user access, and enables easy federation.

- **Windows® CardSpace "Geneva"** for helping users navigate access decisions.

Key Features

- .NET developer tools including pre-built user access logic based on one common identity model that externalizes authentication from applications

- Ability to change user authentication methods with minimal application re-work

- Federation provider STS with simple administration tools to quickly set up federations

- Federation between on-premises directories and cloud services for seamless SSO

- Identity provider STS to issue and transform claims

- STS transformation between claims and non-claims token formats to enable interoperability and SSO between claims-aware and non-claims applications

- Ability to issue managed CardSpace identity cards

- Next generation CardSpace identity selector client to help users navigate between multiple identities

- User control and transparency for how personal information is shared

- Streamlined download and installation for efficient user experiences on the client and Web

- Support for both WS-* and SAML 2.0 protocols, plus updated token format support for SAML 2.0

"Identity Selector" Client
Windows CardSpace **"GENEVA"**

Get Claims · Send Claims

"Identity Provider" STS
"GENEVA" Server

Trust

"Relying Party" App or Service
Built with **"GENEVA"** Framework

Interoperable via industry standard protocols

Get "Geneva" Betas

Download Download Beta 1 of all three "Geneva" components: http://go.microsoft.com/fwlink/?LinkId=122266

Get the "Geneva" whitepaper: http://www.microsoft.com/geneva

Microsoft®