Microsoft

Windows Server 2008

Microsoft Code Name "Geneva"

A Simpler Identity and Access Management Platform

Microsoft's Identity and Access Management solutions are a set of platform components 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 information technology (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"

Simplified Access and Single Sign-On. "Geneva" is Microsoft's next generation identity and access management platform built on Active Directory® directory services. "Geneva" provides claims-based access and single sign-on for on-premises and cloud-based applications in the enterprise, across organizations, and on the Web.

"Geneva" leverages claims which 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" can help organizations solve:

1. Businesses and governments need to enable collaboration and simplified single sign-on within the enterprise, across organizational boundaries, and on the Web while satisfying cost cutting and security requirements.
2. Organizations must also react to changing needs more quickly and economically by enabling existing systems to interoperate with new systems such as hosted 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 hosted 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. 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.

Windows Server 2008

Product Components

"Geneva" includes three platform components for enabling claims-based access management. The following "Geneva" components are now available for public evaluation:

- **The "Geneva Framework"** provides .NET development tools, which includes pre-built, user-access logic that externalizes authentication from applications. The "Geneva Framework" helps developers build claims-aware .NET applications that externalize user authentication from the application, plus build custom security token services (STS).
- **"Geneva Server,"** an STS for IT that issues and transforms claims and other tokens, manages user access and enables federation and access management for simplified single sign-on.
- **"CardSpace Geneva"** for helping users navigate between multiple logons for simplified single sign-on while providing complete user control and transparency for how personal information is shared.

Scenarios Enabled

Cross-organization and Federated Single Sign-on

Organizations want to connect their people and their applications with those of other business units, customers, and partners. Managing the interconnected relationships between people, organizations, and federations typically increases IT costs, lowers security, and ultimately acts as a roadblock to effective collaboration. "Geneva" enables organizations to provide single sign-on by securely connecting users to applications both inside and outside their security infrastructure.

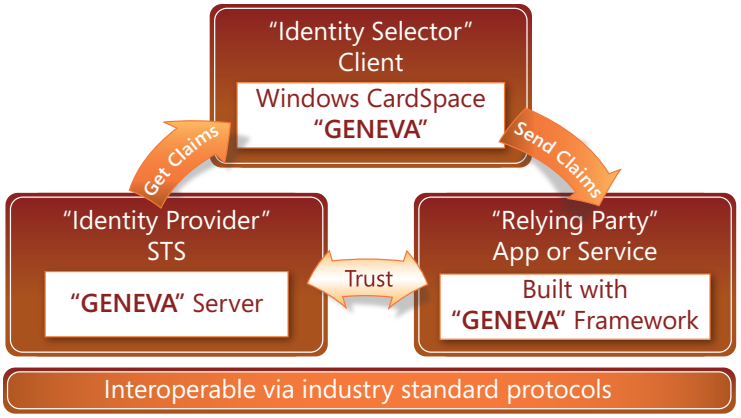
"Geneva" gives customers choice based on functionality and business need by allowing them to mix and match "Geneva" with third-party, claims-based STSes, frameworks, and clients. Support for open standards and tested interoperability allows organizations to easily collaborate without having to manage extra user accounts and passwords or compromise security.

Accessing Hosted Services

Organizations are looking to take advantage of cloud-based application offerings to reduce cost on data center management as well as increase flexibility. Challenges in access management, including increased IT costs, security risks, and end-user hurdles threaten the benefits achieved by moving to cloud-based services. "Geneva" enables simple identity federation and single sign-on to cloud-based services, whether hosted by Microsoft or others, so organizations gain flexibility and cost savings while avoiding the access-management challenges of managing extra user accounts and passwords.

Enable Simplified and Flexible Access Management

IT professionals increasingly have more applications to manage, running on more platforms, using more complex forms of security, and targeted at more people. All this management complexity makes the implementation of security policy much more difficult to do consistently. "Geneva" allows developers to decouple authentication and access management by using the "Geneva" Framework to build richer, more secure applications built to easily evolve with changing security and access-management requirements with minimal application re-work. Using "Geneva," IT professionals can simply manage access to applications of various types, with varied security requirements, in order to more efficiently apply security policy in a standard way across the enterprise.



Learn More About "Geneva" Today

Download "Geneva," the next generation identity and access management platform from Microsoft:
http://go.microsoft.com/fwlink/?LinkId=122266

Get "Geneva" whitepapers and other materials:
http://www.microsoft.com/geneva

Learn about the Microsoft vision for Identity:
http://www.microsoft.com/mscorp/twc/endtoendtrust/

Microsoft

For more information about Microsoft Identity and Access (IDA), visit www.microsoft.com/ida. For the latest developer news and more information on the broad range of Microsoft resources for developers, including support programs, events, training, and the MSDN® Library Online, visit MSDN Online at http://msdn.microsoft.com/.