

Entrust Secure Identity Management Solution: Securing Web Services



Organizations are adopting Web Services for many reasons, including the simplification of communication between internal systems, as well as streamlining business processes beyond enterprise boundaries to suppliers and customers. Web Services may also drive down costs by using open and non-proprietary integration technology. Leveraging Web Services to build Service Oriented Architectures (SOAs), organizations are able to expose application logic as "services" and are able to easily chain together multiple applications, creating composite business processes without large-scale integration projects. As well, Web Services technologies are complimentary with those of Identity Federation, allowing additional efficiencies to be realized around identity and access management across organizational boundaries.



The Need for Secure Web Services

Deploying Web Services and SOAs has many benefits, but also introduces some challenges, as the architectures can quickly become very complex, with many systems talking to many other systems with potentially no human intervention in an entire transaction. Adding to the complexity are two key challenges: 1) Current perimeter-centric security alone is not appropriate for managing XML traffic; and 2) There are multiple entry points to the enterprise, including Wireless LANS (WLANs) and remote access VPNS, with no real controls in place to manage Web services traffic that enters through these access points.

The deployment of Web Services necessitates that organizations put in place mechanisms to ensure that only the right users or applications are able to access and execute transactions with the enterprise, regardless of where the transaction was initiated. Gaining the benefits of Service Oriented Architectures and Web Services opens up new attack paths that network firewalls do not block. Securing those Web Services requires the use of standards to authenticate and authorize XML transactions at the perimeter and inside the enterprise, enabling organizations to minimize the risk of deployment and maximize the benefits of distributed or federated Web Services.

Securing Web Services With Entrust

As part of the Entrust Secure Identity Management Solution, Entrust provides comprehensive content validation, threat detection, and centralized Authentication, Authorization and Audit (AAA) services for distributed or federated Web Services transactions. Made up of industry leading identity and access management products, the solution delivers key Web Services security services through:

- Entrust GetAccess
- Entrust Secure Transaction Platform
- Vordel XML Gateway

Solution Benefits:

- *Easily extend the extranet to support Web Services transactions.*
- *Centralized policy for internal, distributed or federated Web and Web Services applications to reduce administration costs*
- *Support for standards to ensure easy integration*

Solution Advantages:

- *Flexible deployment options to fit within organizational strategies for Web Services*
- *Easily secure Web Services transactions, allowing streamlined and secure integration between internal and external applications*
- *Decrease deployment costs with proven solution*

Entrust Secure Identity Management Solution: Securing Web Services

Entrust GetAccess is a high performance, scalable Web access control solution that can easily be extended to secure Web services applications through integration with the Entrust® Secure Transaction Platform, providing centralized authentication and authorization services for internal, distributed or federated Web and Web Services applications.

Vordel delivers XML and SOAP message security for SOAs. It leverages Entrust GetAccess for centralized policy definition and enforcement, performing authentication on incoming and outgoing XML traffic to ensure validity of SOAP messages. Authentication is complemented by a sequence of content filtering, transformation and routing operations performed on the XML data by Vordel, as well as the application of fine-grained authorization by Entrust GetAccess.

Regardless of how the Entrust solution is deployed, it addresses the security requirements of organizations that are seeking to protect business services exposed as Web Services - to external trading partners, customers and suppliers. Entrust's market-leading capabilities for securing Web Services also addresses the management of internal Web Services transactions, which may be accessing applications via wireless LANS or remote worker VPNs.

Features

Extend the Extranet

The integration between Entrust GetAccess and Vordel enables customers to extend their current Extranet policy infrastructure to support applications implemented as XML Web Services. Customers are not required to set up another silo of users, groups, roles, or policy data. Users need authenticate only once and use multiple local and third party Web Services, without a need to re-authenticate. Entrust GetAccess manages identity, authentication and authorization requests, as well as the security session, while Vordel enforces the security policies at each Web Service endpoint. Competing solutions force the customer to set up duplicate silos of user information and security policies at the XML Firewall level.



Centralize identity management, authentication and authorization with distributed security enforcement.

Entrust GetAccess enables authentication and authorization services to be leveraged across both Extranet and Web Services environments. Vordel provides the ability to enforce security policies across multiple XML systems, with each XML system capable of having specific authentication, and content filtering policies.

Support for standards.

The solution supports the leading Web Services standards, including SAML, WS-Security, and WS-Trust to secure Web Services. The use of non-proprietary, standards based technologies ensures that customers avoid the use of tightly-coupled APIs and therefore future proof their environments.

Benefits

Improve customer service levels and increase competitive advantage

Extend customer and partner reach with deeper access to information. Secure the extension of business processes

across the firewall, based on Federated and Web Services integration technologies and conduct transactions 24x7 over open networks with customers, partners and suppliers.

Decrease development and integration costs for secure Web Services applications

By employing a centralized approach to authentication and authorization enforcement, organizations can ensure a consistent application of security policy across internal, distributed or federated Web and Web Services applications. Entrust's approach to securing Web Services applications makes it highly deployable, reducing the cost of application development and accelerating application time-to-market.

By using a security platform to secure Web Services, which can be deployed as an XML Firewall or enterprise-wide as security services, the customer avoids the need to develop and maintain custom code for XML security enforcement. Similarly, the ongoing management of security policies is GUI-driven

with the option of batch-updates via XML configuration files, rather than involving programming.

Ensure Regulatory Compliance

The solution delivers the appropriate levels of audit and risk management controls (for both internal and external communications), and provides access to the required level of security transaction archives and reporting.

Leverage investment in security infrastructure.

Organizations can leverage the investment they have made in Entrust GetAccess by extending its functionality to secure their Web Services transactions. In addition, the components used to secure Web Services are also tightly integrated with other key security capabilities delivered by the broader Entrust Secure Identity Management Solution, providing organizations with an extensible investment for securing internal, distributed or federated Web and Web Services applications and client-server environments.

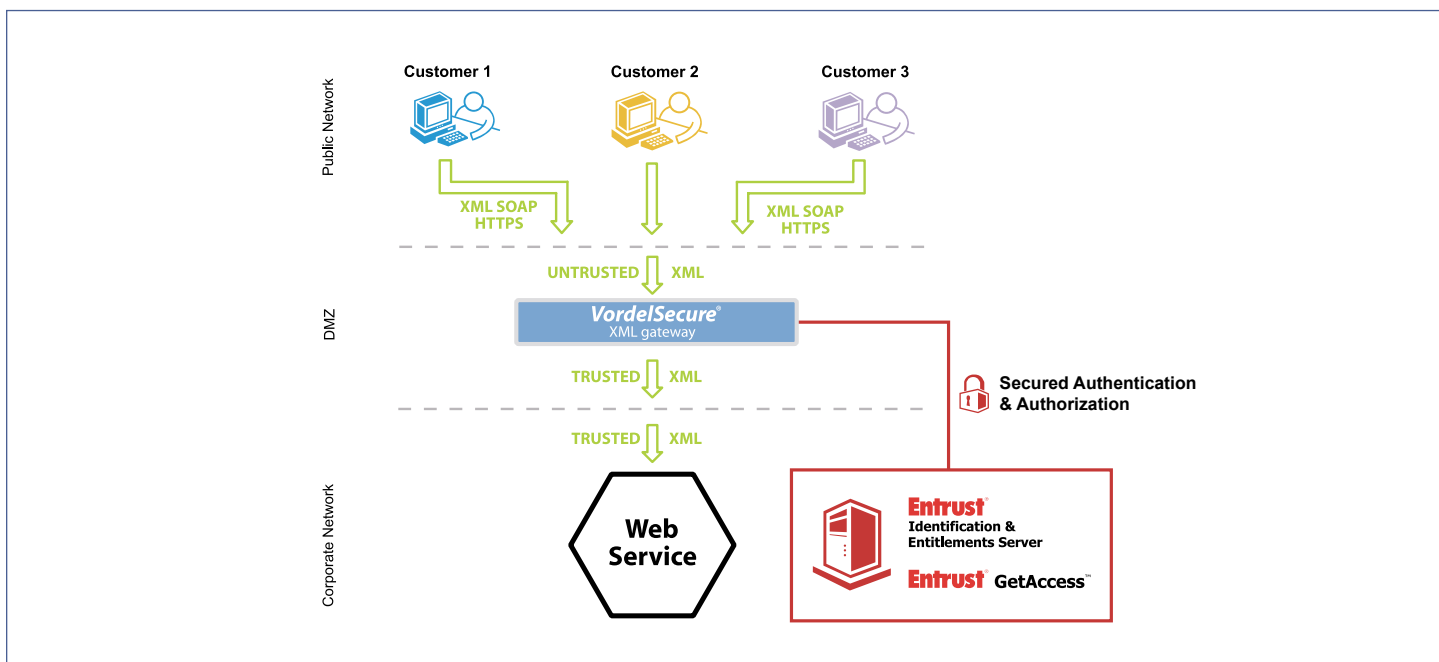






Figure 1: VordelSecure Gateway in the DMZ communicating with Entrust GetAccess and Entrust Secure Transaction Platform

Entrust Secure Identity Management Solution: Securing Web Services

The Solution Portfolio

The Entrust Secure Identity Management Solution is built upon market leading, best-of-breed products delivered and supported by Entrust. Solution capabilities are tightly integrated to help reduce deployment cost and risk through modularity and interoperability, allowing for phased deployments in any customer environment.

	Client-server	Web	Web Services
Strong Authentication	<p>Entrust® Entelligence™</p> <p>Delivers a single security layer to enterprise desktop applications, including strong authentication, authorization, digital signatures and encryption, for greater accountability and privacy.</p> <p>Entrust USB Token Securely stores an individual's digital ID, which can be used for strong authentication, digital signatures and encryption.</p> 	<p>Entrust® TruePass™</p> <p>Provides end-to-end Web security, including strong authentication, digital signatures and encryption with unmatched ease of deployment and user transparency.</p> <p>Entrust USB Token Securely stores an individual's digital ID, which can be used for strong authentication, digital signatures and encryption.</p> 	<p>Entrust® Secure Transaction Platform</p> <p>Delivers a comprehensive set of Web Services security capabilities for integrating authentication, authorization, and digital signatures into Web Services applications.</p>
Authorization & SSO	<p>passlogix®</p> <p>Enables enterprise single sign-on by seamlessly connecting to any mainframe, Windows, Web or "homegrown" application.</p>	<p>Entrust® GetAccess™</p> <p>Provides high performance, scalable Web access control and single sign-on to Web applications. Centrally manages access to single or federated portals and can be easily extended to support Web Services environments.</p>	<p>Entrust® Secure Transaction Platform</p> <p>Delivers a comprehensive set of Web Services security capabilities for integrating authentication, authorization, and digital signatures into Web Services applications.</p>
Provisioning	<p> Identity Manager</p> <p>Provides identity provisioning across a broad range of applications and platforms.</p>	<p> Identity Manager</p> <p>Provides identity provisioning across a broad range of applications and platforms.</p>	<p>Entrust® Certificate Services</p> <p>Makes it easier and more cost effective to manage the lifecycle of SSL certificates on Web servers through automated provisioning. Can be extended to manage digital identities for Web services applications and network devices.</p>

About Entrust

Entrust, Inc. [Nasdaq: ENTU] is a world-leading provider of Identity and Access Management solutions. Entrust solutions for secure identity management, secure messaging and secure data enable enterprises and governments to extend their business reach to customers, partners and employees by transforming the way transactions are done online.

For More Information

Please call us at 888-690-2424, or send an e-mail to: entrust@entrust.com
Visit us on the Web at: www.entrust.com

