Entrust®
Securing Digital Identities
& Information

White Paper

Delivering Web Services Security:

The Entrust Secure Transaction Platform

September 2003

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. All other Entrust product names and service names are trademarks of Entrust. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATION AND/OR WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A SPECIFIC PURPOSE.

> "Web services present a new opportunity for enterprises to create value for their customers and business partners and strengthen existing relationships. With Web services, organizations can expose business processes and service requests in real time through interactions between application systems."
>
> Burton Group
> "Web Services Security"
> October 2002

1.0 Introduction

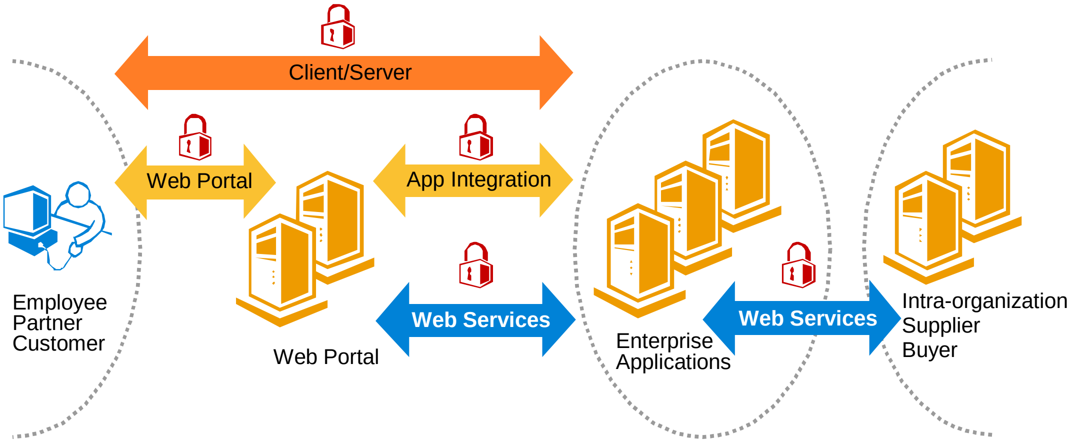
The wave of computing for the IT industry is focused on addressing the needs and challenges of business integration using Web service architectures and technology. Organizations that are able to leverage Web services to quickly integrate their business processes within their enterprises and with their business partners and customers will benefit from the efficiencies of automation and faster customer service.

Business integration is an evolution of previous computing models. Mainframe computing first introduced the ability to centralize and automate electronic processing of transactions. Client/server computing allowed for decisions and processing to be moved closer to the individual. E-business and the Internet made information and commerce readily available to employees, customers and suppliers. Web Portals have allowed companies to personalize the information based on each unique individual and role; essentially integration of information for the individual. Now, Web services will provide this same level of connectivity to business applications.

> "The **business benefits** of Web services can be erased in an instant if a customer's security is compromised or critical business intellectual property is exposed."
>
> Gartner
> "How to Be Leading Edge—
> And Safe—With Web Services"
> February 2002

A key enabler for extending access to information and business processes has been the level of security and trust organizations can implement in their systems. As organizations provide broader access to their sensitive information, the risk of serious damage due to malicious manipulation becomes a critical challenge. Now, as companies automate their sensitive business processes and transactions internally and with the outside world, security becomes essential, particularly because of the need to ensure that automated processes remain well-behaved and in control at all times.

In the past, Entrust's solutions and customers have been focused on enabling trusted transactions in client-server and Web portal applications. Entrust has now extended its product family to enable the trust and security required for broader and deeper transactions between customers and business partners.



The **Entrust Secure Transaction Platform** will help you to extend investments in secure client/server and Web portal solutions to **secure Web services**.

The paper discusses how Web services are the fundamental technology platform for business process integration and how Entrust can deliver a set of fundamental security capabilities for Web services based on a new security platform — the **Entrust Secure Transaction Platform**.

2.0 Web Services: Enabling Business Integration

The universal acceptance of two key standards — TCP/IP and XML — has created the technical foundation to enable companies to share information and deeply integrate business processes. Building upon these two standards, extensive industry effort has been initiated to develop a framework for interoperability between disparate business processes. This framework is known as Web services. IBM, Sun, BEA, and Microsoft have all announced major strategic investments and supporting product roadmaps that indicate wide-reaching support and adoption for these standards.

> "The Web services ecosystem—built around organizational service-oriented architectures (SOA), standardized transactional methods based on XML applications and accessible directories based on UDDI—is likely to be the most important technology deployment through 2008."
>
> Gartner
> "Web Services Key Issues for 2003"
> March, 2003

The result of these initiatives and investments is a technology base that allows organizations to integrate their key business processes within their enterprise networks and across the Internet with their suppliers and customers.

2.1. Securing Web Services

By building on widely accepted standards that enable easier connectivity between applications, Web services simplifies the development of business-to-business applications, reducing time-to-market and greatly improving the ability to change these applications over time. At the same time, the security mechanisms required for these applications must be sufficient to protect the sensitive and valuable transactions that will use Web services. Consequently, Web services will require security technologies that go well beyond the basic Secure Sockets Layer (SSL) of the browser-driven Web.

> “Web services will be the next wave of attack by those trying to subvert enterprise security policies.”
>
> Gartner
> "Security Strategies for Enterprises Using Web Services",
> May 2003

While a key enabler for browser-based e-commerce transactions, SSL has two fundamental issues that limit its applicability to high-value business transactions. First, SSL provides security only for the duration of the session set up between a browser and Web server. While this is important, the need for securing the transaction does not end at the point the connection is broken — for many business transactions, it is often critical for the security to persist beyond this limited session. Second, the technical details of SSL dictate that it is unable to digitally sign transactions to support “non-repudiation”, the concept of preventing participants from later denying that valid transactions did indeed take place — again, a key requirement for many business transactions.

A security solution for Web services must address the fundamental security issues of:

- Authentication – how can the service provider be confident that the requestor is who they claim to be, and vice versa? And, how can a service provider easily support the multiple types of identification methods (for example, digital certificates, userIDs and passwords, and more…) that exist today and will continue to exist for the foreseeable future?
- Authorization – how can the application determine whether the requestor is approved to use the service?
- Encryption – how can Web services transactions be protected from unauthorized access during end-to-end transmission and storage?
- Digital Signatures – how can an auditable record be created to help bind each party to the transaction?

In addition, a security solution for Web services cannot be considered as a standalone technology issue. Organizations require consistent security implementations that can be used across their enterprise, Web portal and Web services applications. Consequently, organizations need to consider how their security solution for Web services leverages and interoperates with their security solutions for enterprise desktop and Web portal applications.

To illustrate why this is important, consider an organization that is in the process of deploying Web services-based applications, but which also currently operates a Web portal to protect resources that are accessed by the same user group (this group could include employees, suppliers, citizens, or even other computer applications). To achieve a greater return on investment, it is important to maintain centralized control over the administration of these user identities so that the security is applied consistently and at the lowest total cost.

3.0 Entrust Secure Transaction Platform

The Entrust Secure Transaction Platform is a new product portfolio that delivers the fundamental security that will enable Web services transactions. It builds upon the expertise and solutions developed by Entrust over the past 10 years.

The Entrust Secure Transaction Platform consists of a set of Foundation Security Services that provide essential security capabilities to enable secure transactions. These services provide the building blocks for integrating authentication, authorization, digital signatures, and encryption into transactions. These fundamental security services are provided through Web services interfaces that allow for easier integration and deployment.

Foundation security services include the following:

- Identification and Entitlements Service for authentication and authorization
- Verification Service for digital signatures
- Privacy Service for end-to-end encryption

The following sections describe the purpose of each of these services.

3.2. Identification and Entitlements Service

The Identification and Entitlements Service allows Web services application developers to avoid having to understand the complexities of identifying other Web services and users. Through handling multiple types of identification methods (for example, userIDs and passwords, digital certificates, …) on behalf of Web services applications, the Identification Service provides a centralized capability for managing the different types of authentication methods that organizations have to deal with internally among different systems and externally when integrating business processes with customers and partners. For simplicity, the remainder of this document will refer to the Identification and Entitlements Service as separate services to clearly communicate the capabilities provided.

The Identification Service also provides an administrative interface for organizations to define the community of users (and the type of identities that will be accepted) that are to be trusted across the variety of authentication methods handled by the service. For example, organizations can specify the set of userIDs and passwords that are trusted for executing transactions. Similarly, organizations can easily specify — with flexibility and fine-grained controls — the community of digital certificates that are trusted.

From userIDs and passwords all the way up to strong identification through digital certificates (with and without smart cards), the **Identification Service** understands identification methods and knows which identities the organization trusts.

The Identification Service enables organizations to centrally control which identities are trusted for automated Web services transactions — even though the administration of this information may be distributed across the organization — so that each Web services application does not have to manage these issues independently.

Digital certificates are expected to be the primary mechanism used by Web services to identify other services and users. Through its long history and experience in providing digital certificate solutions, Entrust already has the software base required for a comprehensive digital certificate capability. Similarly, Entrust GetAccess™, A leading Web Access Control solution already knows how to manage many different types of authentication methods, including digital certificates. Consequently, Entrust is leveraging existing, industry-leading technology, knowledge, and experience to create a flexible, reliable, and scalable Identification Service.

Through its continuing commitment to implementing standards for Web services, Entrust has built the Identification Service with standard identification mechanisms, including the proposed SAML (Security Assertion Markup Language) standard for authentication. More information on SAML can be found on the Entrust Web site at: www.entrust.com/resources/standards/saml.htm

After the originator of a Web services transaction (typically in the form of a SOAP message) has been identified— and a determination made as to whether or not to trust them— a decision must be made as to whether or not the requested action should be performed.

The purpose of the Entitlements Service is to confirm that the entity trying to access a Web service (and other types of resources, also) has the right to do so. Like the Identification Service, the Entitlements Service makes it possible for Web services applications to focus on business logic and rely on fundamental security operations occurring centrally in Foundation Security Services by “outsourcing” the authorization decision.

Because Web services applications will drive automated business process, organizations running these services need to know that entities attempting to access their Web services are authorized to do so … and that specification of these authorization and access control policies can be done in an easy-to-manage, centrally controlled administrative system.

Organizations must centrally specify Authorization and Web Access Control to Web services interfaces so that business processes automated through Web services can be secure and well-controlled.

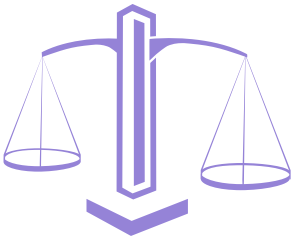
The **Entitlements Service** drives both the centralized administration of Authorization to Web services interfaces and interfaces that allow applications to check those access rights.

Today, the Entrust GetAccess product provides Authorization and Web Access Control capabilities for Web portal applications exactly in this manner. Through a centralized administrative capability, organizations administer the resources (for example, Web pages and applications) that identities can access through single sign-on to the portal. Authorization is verified in a way that is transparent to the Web portal application. This solution makes it possible for application developers to focus on business logic rather than worrying about security.

The Entitlements Service leverages and extends the capabilities that Entrust GetAccess provides today to a Web services environment.

As a further demonstration of Entrust's commitment to implementing standards for Web services, Entrust has built the Entitlements Service using the SAML (Security Assertion Markup Language) standard for authorization assertions. More information on SAML can be found at the Entrust Web site.

3.3. Verification Service



The Verification Service is designed to deliver integrity and accountability capabilities for Web services transactions through centralized digital signatures, timestamping and certificate validation. These services provide critical functions for business-to-business transactions because those transactions typically involve some or all of the following elements:

- Digital signatures to represent approval of the transaction by the organizations involved in the transaction
- Evidence that the transaction occurred at a particular moment in time
- Verification that the transaction has not been altered since it was signed
- And, to deliver auditable records, all of the above must be maintained with the transaction itself for a significant period of time after the transaction occurred

The **Verification Service** confirms the integrity and accountability of transactions through centralized digital signature and timestamping services.

The digital signature capability of the Verification Service provides "organizational signatures" on transactions (rather than the signatures of individuals), a concept which is analogous to the concept of a "corporate seal of approval" on paper transactions. These digital signatures, which conform to the XML Digital Signature standard, verify the organization(s) that signed the transaction and assess whether the transaction has been altered in any way since it was signed.

The timestamping capability of the Verification Service allows a transaction to be ‘notarized’ as having occurred at a particular moment of time.

The XKMS certificate validation capability of the Verification Service enables the digital signatures and timestamps associated with transactions to be validated. You can check the validity of both Entrust certificates and non-Entrust X.509 certificates. This enables you to verify the digital signatures and timestamps produced by Verification Server.

Entrust is chairing the OASIS Digital Signature Services Technical Committee which is responsible for developing the techniques to support the processing of digital signatures. For more information on the Digital Signature Services, refer to the OASIS site at www.oasis-open.org/committees/dss/

For more information on the XML Digital Signature standard, refer to the W3C site at www.w3c.org.

Entrust delivered the first release of the Verification Service in Q4 2002 and has recently released another version Q3, 2003.

Privacy Service

Rather than each Web services application having to understand how to encrypt information, the Privacy Service takes care of the complexity of using cryptographic keys to provide data encryption in a centralized service. This service understands how to encrypt information so that only specific entities (for example, individuals or other computer processes) can access that information.

The same experience in providing digital certificate solutions applied to the Identification Service, is being leveraged to create a flexible, robust, and scalable Privacy Service.

With the availability of the Privacy Service, application developers can access a full range of encryption capabilities with minimal integration effort. Because the Privacy Service knows how to find, validate, and apply users’ digital certificates for end-to-end encryption, developers can focus on the business logic of their applications and let the Privacy Service focus on the details of data encryption.

For instance, if an enterprise specified a security policy that required that only certain portions of a Web services transaction be encrypted (for example, specific aspects of a SOAP message would be encrypted and the rest left in the clear to make it available for intermediate routing, logging or other activities) the Privacy Service would make it quicker and easier to conform to this policy.

The **Privacy Service** encrypts information so that only designated entities can access that information.

4.0 Integrating Web Services Security

There are four methods of integrating Web services security into applications and business processes. Entrust believes (along with many industry analysts) that organizations require a range of multiple integration methods to properly address their full suite of Web services security requirements. One of these integration methods has been available from Entrust for years and is already actively used for securing Web services by customers and other technology vendors.

The four methods of integrating security into Web services are the following, each of which is discussed in more detail in the following subsections:

- Security Toolkit integration
- Direct integration with Foundation Security Services
- “SOAP firewall” integration
- Application server plug-in (or “filter”) integration

4.1. Security Toolkit Integration

The traditional method of integrating security into applications through the use of embedded security toolkit functionality will continue to be used as a method of integrating security into Web services applications. With this integration method, developers include the security functionality they need directly into their applications.

Entrust has current customers and partners using the Entrust Authority™ Security Toolkit for Java for Web services security.

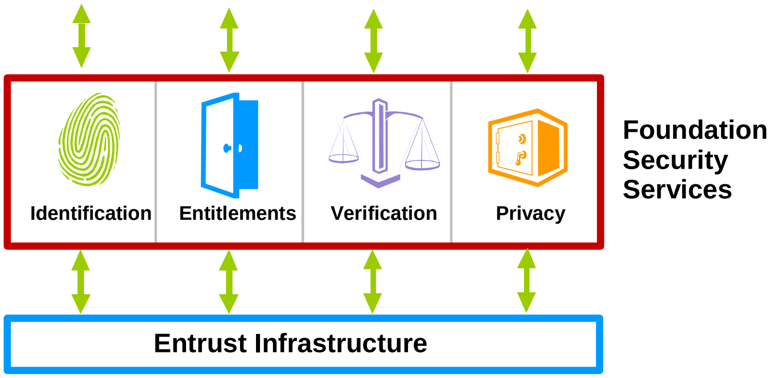
Among many features, the Entrust Authority Security Toolkit for Java includes the capability to create standards-compliant XML Digital Signatures and XML Encryption data objects, and to establish secure sessions through SSL. This Toolkit also includes Entrust’s advanced key and digital certificate management capabilities that make it easier for developers to integrate security into applications. (For more information on the Entrust Authority Security Toolkit for Java, visit: http://www.entrust.com/authority/java/index.htm)

While the use of security toolkits will continue to be a valuable method of integrating security into Web services applications, there are other interesting options for enabling security as well, including having applications directly call security services available as part of the Entrust Secure Transaction Platform.

4.2. Direct Integration with Foundation Security Services

Rather than embedding security functionality through a toolkit, Web services applications can directly call out to the Foundation Security Services delivered by the Entrust Secure Transaction Platform.

This platform offers Web services interfaces to application developers; consequently, applications can interface directly with the Foundation Security Services in a loosely coupled manner.

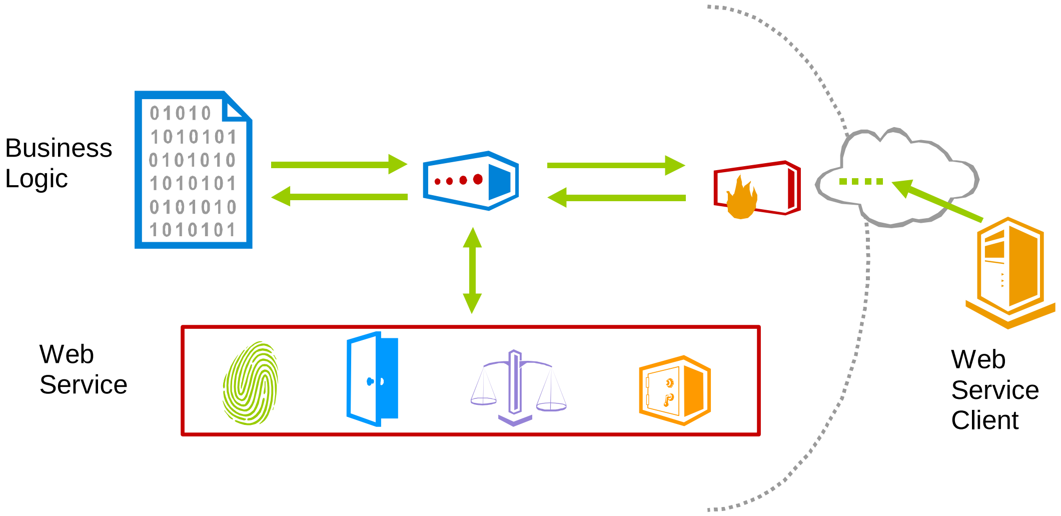


When integrating security in this manner, for example, an application would directly call out to the Identification Service to determine if it should accept a Web services transaction from another service. In this example, the application might receive a digitally signed SOAP message, where the digital signature on the message can be used to identify the originator of the message and also provide integrity on the message contents. In such a case, the application would pass the signer's digital certificate to the Identification Service to determine whether or not the signer is trusted by the organization. Once the signer's identity is known to be trusted, the application could then send that identity to the Entitlements Service to determine if the signer has the right to send a SOAP request to the Web service.

In a similar fashion, a Web services application could interface with the Verification Service to obtain a centralized digital signature and timestamp on a transaction.

4.3. "SOAP Firewall" Integration

Another interesting opportunity for Web services is the potential to deliver security transparently to applications — which means that application developers can focus on the business logic of their applications rather than security. "SOAP firewalls" provide one method to deliver this transparent security; the other method is through the use of



application server plug-ins (which are discussed further in the next section).

SOAP firewalls reflect the concept of application-level firewalls. These firewalls sit in the flow of information on a network and look for specific application-level messages and act upon those messages. In the case of SOAP firewalls, these products watch for SOAP messages and “transform” those messages as they pass through the firewall. In this type of architecture, the SOAP firewall can perform a wide variety of security actions on behalf of applications, including the following:

- Identifying the originator of an incoming SOAP message to validate that the identity is trusted by the organization
- Validating the entitlements of the originator of an incoming SOAP message to confirm they have a right to send a message to a particular Web service
- Verifying the XML Digital Signature on an incoming SOAP message to make certain that the signature is valid to prove that the message has not been altered since it was originally signed

Ideally, SOAP firewalls will use the foundation security services from the Secure Transaction Platform as the core of their security functionality. This type of architecture can help customers maintain a consistent security infrastructure across their applications and security integration methods.

4.4. Application Server Plug-In Integration

The concept of an application server plug-in providing security on behalf of Web services is very similar to that of a SOAP firewall. The most significant difference is that the application server plug-in runs directly on an application server that also executes the business logic of the Web services application, as opposed to the SOAP firewall that typically runs on a completely different network device. Like a SOAP firewall, application server plug-ins provide the significant benefit of keeping security transparent to the Web services application. And, like SOAP firewalls, application server plug-ins can use the foundation security services as the core of their security functionality.

5.0 Conclusions

The Entrust Secure Transaction Platform is a revolutionary new security framework for defining how to integrate foundation security services into Web services applications. This platform will allow companies and governments to more easily integrate and deploy security services that add authentication, authorization, digital signatures and end-to-end encryption to provide accountability and audit to their Web services transactions.

Through the Entrust Secure Transaction Platform, Entrust is expanding the ways in which organizations can integrate security into Web services applications. Historically, Entrust customers and partners have used the Entrust Authority™ Security Toolkit for Java to add security to Web services applications. The Entrust Secure Transaction Platform will enable organizations to directly call Foundation Security Services from their Web applications, or to alternatively integrate these services into SOAP firewalls and application server plug-ins that transparently provide security to applications.

To foster widespread adoption and interoperability of security and Web services, Entrust will continue to be an active participant in the security standards organizations.