VORDEL White Paper
VordelSecure® Version 1.1

An in-depth description of Vordel's innovative VordelSecure, the XML security product

VORDEL® web services security

Executive summary

Web services introduce new security risks, which are not addressed by traditional security solutions that provide security at the network and transport layers. To ensure that your Web services are not compromised, they must be secured at the application layer. VordelSecure 1.1 provides full protection for your XML and Web services deployments against internal abuse and external attack. It enables security at the application layer by supporting the new and emerging XML and SOAP security standards.

VordelSecure offers broad security support that provides for content inspection as well as authentication, authorization, and accountability. It is deployed at the perimeter of your organization, intercepting incoming SOAP requests at the Web server and validating them against the security rules configured for the requested service. An intuitive management wizard is provided that allows you to easily apply security rules on a per-service basis. The following security rules can be enabled: -

- VordelSecure can examine the integrity, structure, and content of XML requests using industry standards - XML Signature, XML Schema, and XPath – to ensure that unwanted or malicious data does not reach your Web services.
- VordelSecure can verify the authenticity of X.509 certificates used, by integrating with PKI directories and local and global trust services to ensure that no invalid or revoked certificates are used.
- VordelSecure can delegate authorization of users to existing access control software using SAML to ensure that unauthorized requests are blocked. Alternatively for less fine-grained access control VordelSecure can authorize incoming requests using the issuing CA policy or the certificate profile.

VordelSecure also provides audit trails for all transactions processed to enable you to account for usage of your Web services. You can locate and view these signed audit trails using the VordelSecure report generator. A monitoring console is provided to track activity in real-time.

This paper presents the VordelSecure 1.1 product in more detail.

VordelSecure Version 1.0
White Paper

Table of Contents

1 Introduction

Web services represent a great opportunity for businesses, but they also introduce new security risks, which are not addressed by traditional Web security solutions. To ensure that your Web services are not compromised, they must be secured at the application layer. This is because Web services traffic bypasses firewalls by traveling through ports that are opened for HTTP traffic, and also because Web Services are independent of the security in the underlying session and transport security layers, including SSL and S/MIME. With your firewall and Web server securely configured and SSL enabled, you still need to be able to block unauthorized SOAP requests or malicious data from reaching your Web services and track who is using your web services. Security must be enabled at the message layer because SOAP messages may be routed through "chained" Web services. You need end-to-end security in this environment rather than the point-to-point security provided by session level solutions. Industry groups such as the W3C and OASIS are producing security standards, which put identification and entitlement information at the application layer, i.e. into the SOAP messages themselves. These standards include XML Signature, XML encryption and SAML.

The Web services model is designed to be easily deployed and to enable collaboration across organizations. Therefore, Web services security must be similarly convenient to deploy and must not be site-specific as Web services may be deployed across corporate boundaries and security domains. You may want to accept requests from users who are not set up in your internal security systems instead outsourcing identity and trust management to some third party.

VordelSecure provides the requisite solution to secure your Web services. It augments your existing security solutions, allowing you to protect your Web services by enabling security at the application layer. It uses XML security standards and provides a broad security platform from which you can choose appropriate security options to protect your Web services. VordelSecure simplifies security management, enabling you to quickly deploy security all for your Web services. It is also optimized to ensure that security does not become the bottleneck in your system.

VordelSecure is deployed at the perimeter of your organization, intercepting incoming Web services requests at the Web server and validating them against security rules configured for the requested service. Depending on the outcome of the rules, the XML messages are either routed to the service or blocked. It ensures that requests, containing unwanted data or received from unauthorized users, do not reach the business logic on an application server or interfere with internal systems.

VordelSecure supports both content filtering and access control (authentication, authorization, and accountability). It can examine the authenticity, structure, and content of requests. It integrates with PKI services and directories to establish identity, and access management software if fine-grained access control is required. VordelSecure also works with global security services if cross-site authentication and authorization is required. Using VordelSecure, you can accurately track usage of your Web services in real-time or according to archived transactions.

2 VordelSecure architecture

VordelSecure is deployed in a Web server that has Java Servlet support. It blocks unwanted SOAP messages at the Web server. A Servlet engine, Tomcat, is supplied with the product, which can be used as a plug-in to either the Apache Web server or IIS. Alternatively the product can be deployed in the iPlanet Web server, which has native Servlet support.

VordelSecure is made up of components that carry out specific tasks, such as signature verification and XML data validation. The use of XML and data security is processor-intensive, however, VordelSecure is optimized to perform XML and data security processing at speed. This is important not only for normal functioning, but also in the event of an automated attack on a Web service. Certain components of VordelSecure are implemented in C and accessed through JNI to remove potential security bottlenecks.

The deployment environment will typically be connected to the Internet through a firewall. VordelSecure requires no modification to this firewall since it processes SOAP messages received over HTTP or HTTPS. Industry standard SSL can be used to establish an encrypted channel between the Web server and external applications. SSL can also be used behind the firewall to create a secure communication channel between VordelSecure and the XML and Web services deployments it protects.

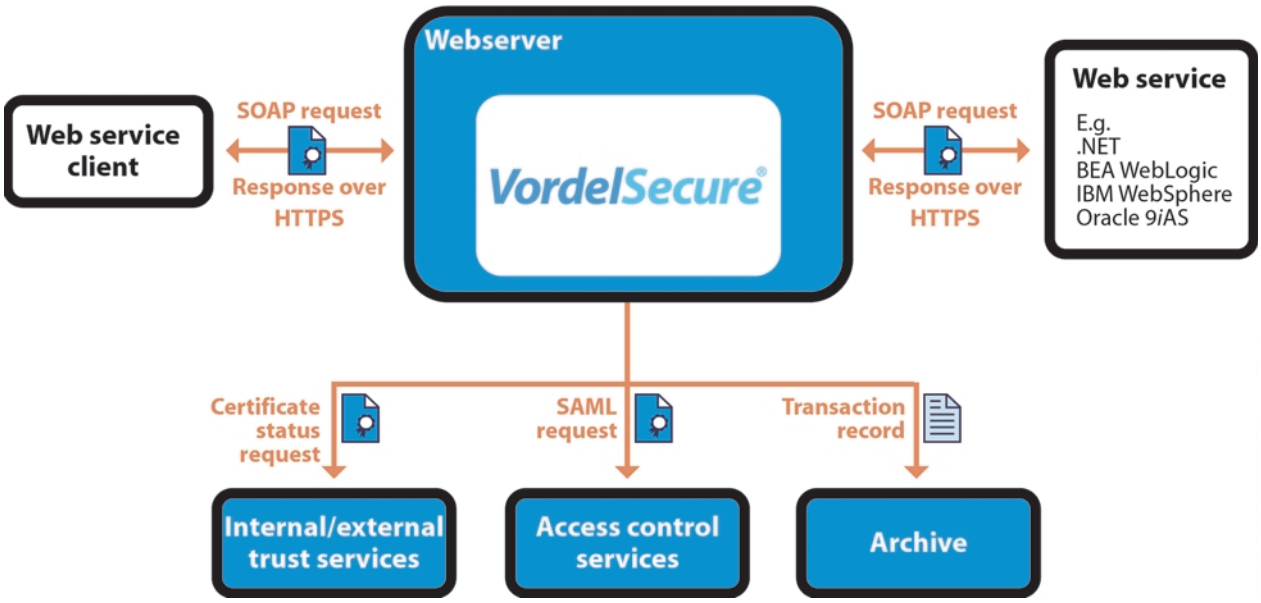

Figure 1 - Secure Web services deployment

Because VordelSecure supports open standards it can process requests received from various SOAP clients. XML security toolkits can be used on the client to generate the security credentials required to validate the incoming request. A number of available toolkits are listed in section 7, "Client Interfaces".

VordelSecure supports a broad range of security software and services for authentication and authorization, ensuring that security for Web services is flexible and is not limited to closed user groups. The full list of available security filters is described in section 3, "Security Filters". Some security filters involve internal processing only, while others involve interaction with third party authentication and authorization software and global trust services. Due to its componentized architecture, VordelSecure can be easily extended to support additional XML security standards as they emerge.

Security policies for your Web services are configured using the Security Management Wizard described in section 5, "Security Management" and stored in a database. VordelSecure includes the MySQL database, but as VordelSecure does not employ proprietary SQL extensions and features, any JDBC compliant SQL database, such as Oracle or SQLServer, can be used. A database is also used to store archived transaction logs used to account for usage of Web services.

Once a request has been validated it can be routed on to the requested Web service.
There are three distinct usage models supported and these are described in detail in the next section. VordelSecure supports both Apache SOAP and WS SOAP routing and is interoperable with a range of Web services platforms, including .NET, IBM WebSphere, BEA WebLogic, iPlanet,

3 Deployment models

VordelSecure can be deployed in a number of scenarios, which are outlined below. In each deployment model, VordelSecure blocks unwanted SOAP messages at the Web server, ensuring that they cannot reach the business logic on an application server, or interfere with internal systems.

3.1 Gatekeeper

Some companies would initially prefer to deploy Web services internally, before exposing them to the Internet. In the gatekeeper deployment model, the only Web service being exposed to the Internet is VordelSecure. The name and interface of the Web service exposed by VordelSecure is configurable - meaning that the administrator can configure a Web service called, for example, 'SubmitInvoice', which is exposed by VordelSecure, while the internal fulfillment of the Web service is protected. The SOAP requester sends the request to VordelSecure, which carries out the security checks configured for the Web service exposed. If the request is successfully validated the data can be routed by VordelSecure to the internal system using routing information that is pre-configured for this service.

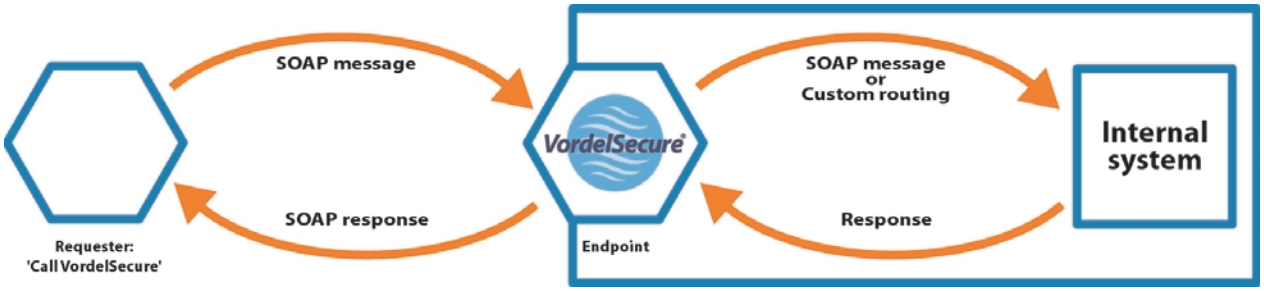

Figure 2 - Gatekeeper deployment model

By default, the SOAP request is routed on without modification over HTTP. However, if the internal system does not support the data format used by the requester then VordelSecure can convert the data using pre-defined mapping files before routing. This may involve changing from one XML vocabulary to another or converting XML data to or from another data format such as EDI or CSV. Stylesheets are used to convert from XML formats and Java classes can be implemented to convert from non-XML formats. Custom routing classes can be used to send data over protocols other than HTTP.

3.2 Interceptor

In the interceptor deployment model, an administrator can securely expose a Web service to the Internet, using VordelSecure to block unwanted traffic. In this scenario, the SOAP requester is unaware of the presence of VordelSecure and the request is addressed directly to the Web service. VordelSecure works within the Web server intercepting messages, bound for the Web service, through Web server filters (ISAPI, Apache and Netscape filters). It runs the security rules configured for that Web service to validate the request before returning control to the Web server. VordelSecure is not responsible for routing to the Web service; instead this task falls to a third party SOAP engine.

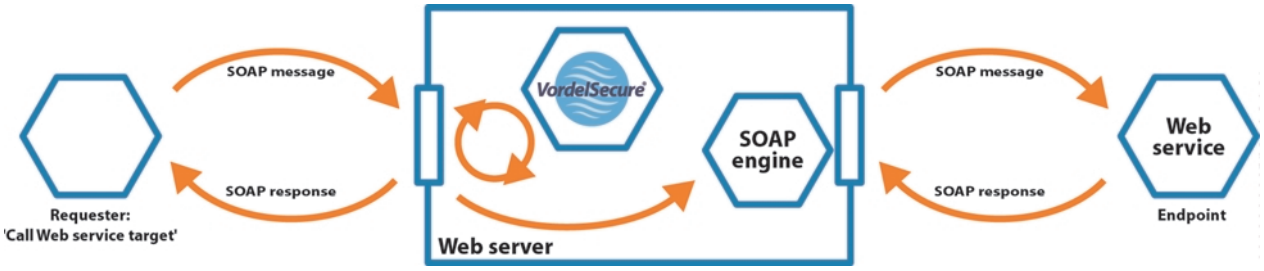

Figure 3 - Interceptor deployment model

3.3 Intermediary

The intermediary deployment model is possible because VordelSecure is fully SOAP-enabled. VordelSecure can act as a SOAP "intermediary", enabling security functionality to be deployed as a Web service itself. In this scenario, the SOAP requester calls VordelSecure and then a subsequent Web service. When VordelSecure receives the request, it determines which security checks to perform based on the security rules configured for the subsequent Web service. If the request is successfully validated VordelSecure will route it on to the subsequent Web service using information contained within the SOAP request. VordelSecure supports both Apache SOAP and WS SOAP routing formats.

Figure 4 - Intermediary deployment model

4 Security filters

VordelSecure augments your existing security solutions, to protect your Web services in deployment, by enabling security at the message layer. VordelSecure is highly configurable and allows you to define a policy for each Web service that determines which security rules to run on incoming requests for that service. If any of the security checks fail for a given request, a SOAP fault will be returned to the requester. The SOAP fault does not include internal detail about which security failure occurred, so the client remains unaware of the security rules configured for the Web service. The security options available are described below.

4.1 Signature verification to ensure data integrity and accountability

VordelSecure can verify an XML Signature[1], contained in an incoming request ensuring the authenticity of the data. If VordelSecure detects that changes have been made to the data since it was signed then the request will not be routed to your Web service.

The signature can also be used to associate the signatory with the data. Since the enactment of digital signature laws[2] the signatory can be held legally accountable for the data submitted, because the signature is said to guarantee the contracting will of the signatory.
To ensure that signature verification does not become a bottleneck, this component is implemented in C for high-speed processing.

4.2 Certificate validation for identity and trust

VordelSecure can check the status of the certificate, contained in the signature, to ensure that it has not timed out or been revoked. If the certificate is no longer valid then it cannot be used to hold the user accountable for their actions. Signatures contain a timestamp so that it can be determined if the certificate used was valid at the time of signing.

Using VordelSecure you can choose the method you want to use to validate the certificates contained in requests to a particular Web service. VordelSecure leverages investment in PKI and directories. VordelSecure can do a lookup on an LDAP directory where a CRL (Certificate Revocation List) from a particular Certificate Authority (CA) is published. Alternatively it can issue a certificate status request to an OCSP (Online Certificate Status Protocol) responder.
VordelSecure can also use global trust or identity services that support XKMS[3] (XML Key Management Specification) from vendors such as VeriSign and Entrust.

XKMS is the emerging standard for key management in a Web services environment. It enables applications to make use of certificates without using complex security toolkits, and bypasses firewall restrictions that have hindered PKI usage in the past. Users can register, retrieve, or revoke their certificate with an XKMS Web service. It is then possible for VordelSecure to query the trustworthiness of the user's certificate over the Internet by issuing a certificate status request to the XKMS service.

For each of your Web services it is necessary to configure information about the location of the LDAP directory, OCSP responder or XKMS service to use and other parameters required to access these directories or services.

---

1 The XML-DSig charter – a joint IETF/W3C charter, developed XML Signature technology.

2 Passed into US law in June 2000 in the "Electronic Signatures in Global and National Commerce Act" – commonly called the "E-Sign Act". Passed into EU law in Directive 1999/93/EC.

3 The XKMS specification was originally defined by Verisign, Microsoft and webMethods, and has been submitted to the W3C.

4.3 SAML support to achieve fine-grained access control

VordelSecure can authorize incoming requests by verifying the requester using SAML[4] (Security Assertions Mark-up Language). SAML provides a standard way for exchanging authentication and authorization information about users over the Internet using XML messages called assertions. Using SAML you can leverage corporate investment in access management tools. These tools store user profiles and permissions and can act as SAML PDPs (Policy Decision Points), to which VordelSecure can interface using SAML. There are a large number of use cases to be considered with SAML and the scenarios supported by VordelSecure are described below.

If a Web service request contains a SAML assertion, VordelSecure can use this assertion to determine if the requester is a valid user of the Web service. An assertion may contain only authentication information or it may contain information about the resources that the user has permission to access. VordelSecure can process both authentication and authorization assertions.

If the request contains an authorization assertion, VordelSecure will examine it to see if the Web service requested is listed as a resource. Since a SAML Authority will typically sign the SAML assertions it issues, VordelSecure can validate the assertion by verifying the signature to ensure the assertion has not been modified since it was issued. VordelSecure can also verify that the SAML Authority is trusted to issue assertions for your Web service. The certificates for the SAML Authorities you want to trust must be imported into the VordelSecure certificate store and then assigned to the Web service.

If the request contains an authentication assertion, VordelSecure will use this assertion to create an authorization request. It then issues the request to a trusted SAML PDP configured for the requested Web service. The response returned from the PDP is used to determine whether the user should be allowed access the requested service.

If, however, the request contains no assertion, VordelSecure can issue an authorization request to a trusted SAML PDP using the user's certificate. The response returned will again be used to determine whether the requester is a valid user of the Web service.

4.4 Examination of certificate characteristics for access control

As it may not be suitable to configure all users of your Web services in advance VordelSecure provides a means of restricting access on a less fine-grained basis.

VordelSecure can restrict access to users who hold certificates issued by particular CAs. When VordelSecure receives a request for a particular Web service the signatory's certificate can be examined and the issuer can be compared to the list of trusted issuers, configured for that Web service. For example, you could decide to trust only users with VeriSign class 1 certificates to access your service.

The certificates for the Certificate Authorities you want to trust must be imported into the VordelSecure certificate store and then assigned to the Web service.

VordelSecure can also examine the X.509 attributes in the signatory's certificate to ensure that they match a profile configured for your Web service. In this way, it is possible to restrict access to your Web service based on certificate attributes. For example, you could decide to trust only US employees of Vordel to access your service by configuring a profile of "C=US", "O=Vordel".

4 The security services technical committee of OASIS has developed SAML.

4.5 Schema checking and XPath content queries for data validation

Your Web services are potentially vulnerable to the same security problems as your Web servers, such as buffer overflow attacks. VordelSecure can prevent unwanted data from reaching corporate business logic on application servers or internal systems by enforcing XML Schema and XPath-based rules at the web server.

VordelSecure can validate incoming data against an XML Schema to ensure that the structure of the request conforms to that expected by the Web service. This means that your Web services do not receive messages they will be unable to process and are protected from buffer overflow attacks, where a user sends unexpected data to methods exposed by your Web services. For example, a user could send a 15,000-character string to a method that expects a 15-character string. To improve performance, the required Schemas can be imported into the VordelSecure database in advance. Alternatively, if the Schema is not available locally and the incoming request contains a URL that indicates the location of the Schema then VordelSecure will attempt to download the Schema into the database. You can define XPath expressions that VordelSecure uses to identify which sections in the request need to be verified against the XML Schema.

VordelSecure can also examine the content of an incoming message to see if it meets specified criteria. An XPath expression can be defined and used to locate and verify particular content in the message, before it will be routed to your Web service. For example, you may want to specify that a request should not be routed to your 'SubmitInvoice' service unless the total field in the payload is greater than zero.

5 Security management

VordelSecure enables you to deploy security for all your Web services quickly. By adopting the VordelSecure security solution, you can avoid the complexities and costs associated with integrating security toolkits into your applications. If a toolkit approach is taken you may need to use several toolkits to build sufficient security functionality into your applications as no one toolkit provides the broad range of security options offered in VordelSecure. VordelSecure includes an intuitive security management wizard that allows an administrator to easily configure security rules for each of their Web services.

The security management wizard can parse a WSDL file to display a list of deployed Web services. Alternatively the administrator can manually enter a Web service description. Once a Web service has been selected, the wizard walks the administrator through the available security options allowing him/her to configure a policy for each service. The administrator can create a new policy or may choose to customize an existing policy.

Configuration information is stored in a JDBC compliant database. When the administrator logs in to the Security Management Wizard he/she must supply the location of the database, which may be deployed on another machine, and the username and password required to access the database.

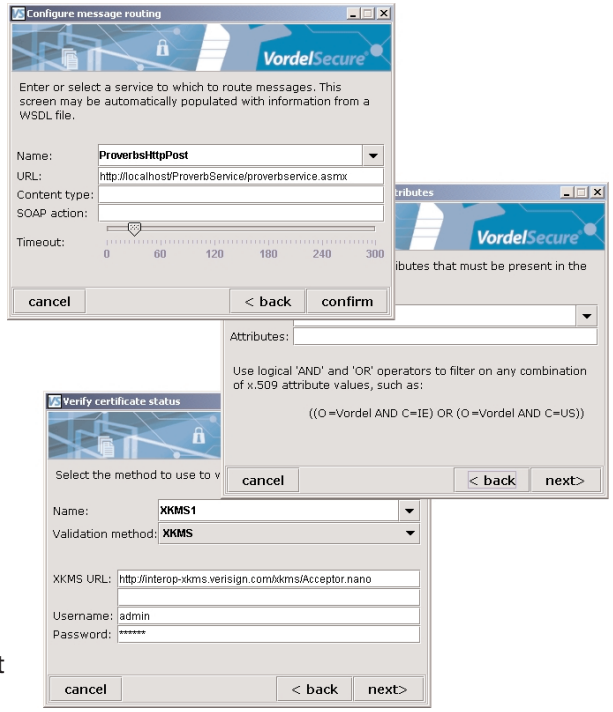

Figure 5 - Security Management Wizard

6 Monitoring

VordelSecure reduces transaction risks by allowing you to easily track the usage of your Web services and account for all transactions processed in real-time or based on transactions archived.

The detail of the information available is determined by the logging level configured. If the level is set to DETAIL then the content of the request, including the XML payload and the security credentials, and the response returned will be logged. In addition, all processing steps that were performed to validate the request will be output, for example signature verification failed or SAML authorization passed.

For real-time monitoring of activity, logging information can be output to the VordelSecure monitoring console. This allows an administrator to track detect malicious activity in real-time and take precautionary actions if they feel a service is under attack. The monitoring console can be run locally or remotely.

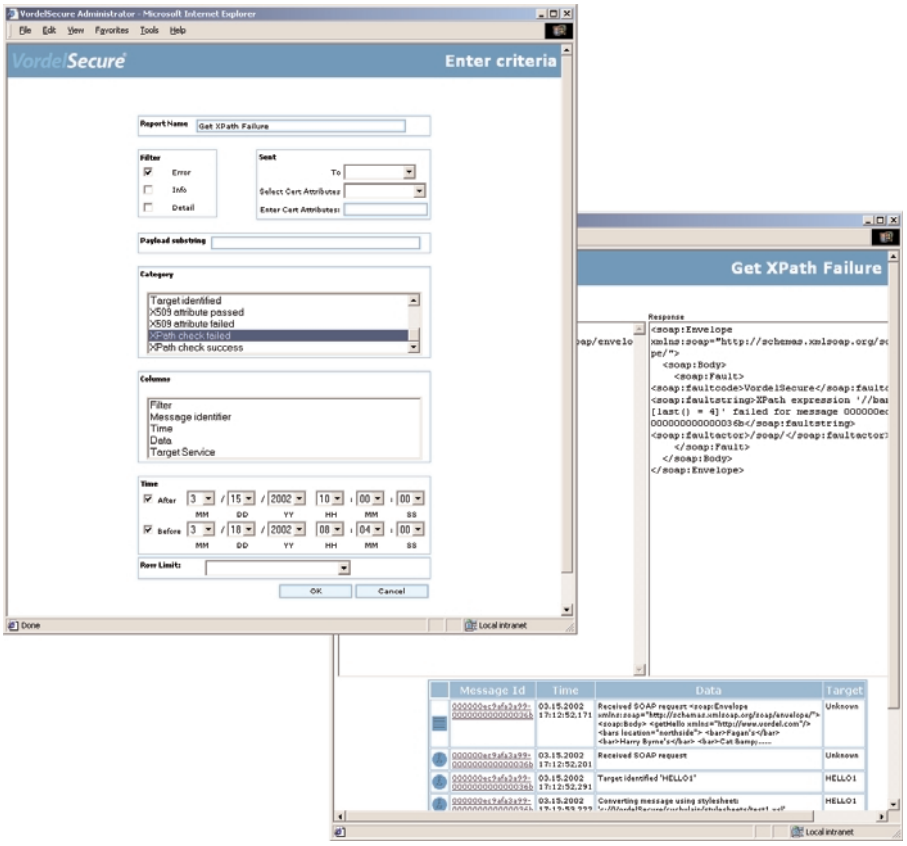

Figure 6 - Web reports

VordelSecure supports logging to a database or a file. It can sign information logged about a transaction to ensure data integrity over time for information archived. VordelSecure includes a Web based reporting tool, which can be used to locate and view archived transaction records. Reports can be generated according to a range of criteria, including date and time; Web service requested; characteristics of requester's certificate; transaction content; and particular security events. A number of transaction records can be returned as the result of a query. The VordelSecure reporting tool allows you to drill down into particular transactions and view detailed information. When generating a report, you can choose to create a new query or to run an existing query.

The reporting tool is accessed through the VordelSecure browser interface, described in section 7, "Client Interface". In order to run reports, you must be set up as a user of the VordelSecure reporting tool by the administrator of the system. You can then log in and select your signing key. All report requests must be signed using your key so that VordelSecure can verify the signature and certificate contained before generating and displaying the report.

7 Client interfaces

VordelSecure processes SOAP messages received over HTTP or HTTPS, allowing easy interoperability with clients that issue SOAP messages. The product supports new and emerging XML security standards. It can validate security credentials, created using a number of standards based XML security toolkits ensuring interoperability with SOAP clients that use these toolkits. Examples of available toolkits include the IBM XML Security Suite, the Apache-XML-Security Toolkit, VeriSign Trust Service Integration Kit (TSIK), and the IAIK XML Signature Library (IXSIL).

VordelSecure also includes a security API that can be integrated into your SOAP applications and an applet that enables end-users to issue signed requests to secured Web services. In the case of user access through a browser, the user's signing key can be stored in the browser keystore or on a smart card. Alternatively, if roaming usage is required the user can import their encrypted key in to the VordelSecure database and download that key to the browser on login. A user in VordelSecure equates to the signing key they use and details about that key must be imported into the VordelSecure database through a user import Web page.

8 System requirements

VordelSecure is available for the Microsoft Windows, Sun Solaris, and Linux platforms. This section provides an overview of the recommended system requirements on each of these platforms.

Microsoft

Windows NT 4.0 with SP6a
Windows 2000 version 5 with SP2
Windows XP version 5.1.2600
Minimum Intel Pentium II, 266 MHz or equivalent with 64 MB RAM
IBM JVM 1.3
Web server - IIS 5.0 or Apache 1.3.2 with Tomcat 3.2.2, iPlanet 6.0
JDBC compliant database

Solaris

Solaris 8.0
UltraSPARC-IIi, 360-MHz with 128 MB RAM
Sun JVM 1.3 on Solaris
Web server - Apache 1.3.2 with Tomcat 3.2.2, iPlanet 6.0
JDBC compliant database

Linux

Linux kernel version 2.2.13 or higher
glibc2 version 2.1.3 or higher
Minimum Intel Pentium II, 266 MHz or higher, with 64 MB RAM
IBM JVM 1.3 on Windows
Web server - Apache 1.3.2 with Tomcat 3.2.2, iPlanet 6.0
JDBC compliant database

Browser Requirements

Internet Explorer 5.5 or higher
Netscape 4.6 or higher
JVM 1.1 or higher

9 Further reading

To learn more about Web services security challenges and XML security standards, you can access the Vordel Knowledge Base for our latest tutorials and white papers.

http://www.vordel.com/knowledgebase/index.html

10 Contact details

Sales:	sales@vordel.com	**Support:**	support@vordel.com
General:	info@vordel.com	**Press:**	press-info@vordel.com

Vordel Ltd.
Cranford House
Cranford Court
Dublin 4
Ireland

T: +353 1 215 33 33
F: +353 1 215 33 34

Vordel USA
101 Federal St.
Suite 1900
Boston
MA 02110

T: +1 617 342-7127
F: +1 617 342-7080

Vordel UK
168 Westborne Park Road
London
W11 1BT

T: +44 207 727 4141
F: +44 207 243 6663

11 Glossary of terms

API - Application Programming Interface
An API is a series of functions that programmers can use to access the behavior and state of classes and objects.

CA - Certificate Authority
CAs are the digital world's equivalent of passport offices. They issue digital certificates and validate the holder's identity and authority. They also manage security credentials and public keys for message encryption.

CRL - Certificate Revocation List
A CRL is a signed list issued by the CA identifying all revoked certificates by their serial numbers. This list is published to a directory and timestamped and signed by the CA that originally issued the certificates.

EDI - Electronic Data Interchange
EDI is used for the direct computer-to-computer transfer of business documents. These documents are in a structured, pre-defined standard format so processing can be automated without the need for human intervention.

HTML - Hypertext Markup Language
HTML is the set of markup symbols inserted into a file intended for publishing hypertext on the web. The markup tags tell the Web browser how to display the text and images on a Web page. It is based upon SGML, and can be created and processed by a wide range of tools, from simple plain text editors to sophisticated authoring tools.

HTTP - Hypertext Transfer Protocol
The Hypertext Transfer Protocol (HTTP) is an application-level protocol for requesting and transmitting files, especially Web pages and Web page components, over the Internet or other computer network.

HTTPS - Secure Hypertext Transfer Protocol
Secure HTTP is an extension of HTTP, which uses SSL as a sublayer under the regular HTTP application layering. This provides independently applicable security services for transaction confidentiality, authenticity/integrity and non-repudiation of origin.

JVM - Java Virtual Machine
A software execution engine designed to run compiled Java code. This includes stand-alone Java applications, as well as applets that are downloaded and run in Web browsers.

OASIS - Organization for the Advancement of Structured Information Standards
OASIS is a non-profit, international consortium that creates interoperable industry specifications based on XML.

OCSP - Online Certificate Status Protocol
The Online Certificate Status Protocol is a real-time mechanism for getting up-to-the-instant status information on digital certificates. It can be used to provide more timely revocation information than is possible with CRLs and can also provide additional status information.

PKI - Public Key Infrastructure
The most common functions of a PKI are issuing and revoking certificates, creating and publishing Certificate Revocation Lists (CRLs), storing and retrieving certificates and CRLs, and policy enforcement. Emerging PKI functions include time-stamping and policy-based certificate validation. Some companies host their own internal PKI, while others choose to outsource this to a Trusted Third Party (TTP).

SAML – Security Assertions Markup Language
The SAML specification has been developed by OASIS. It provides a standard way for exchanging authentication and authorization information over the Internet using XML.

SOAP - Simple Object Access Protocol
SOAP is an XML/HTTP-based protocol for accessing services, objects and servers in a platform-independent manner and has been established as the enveloping protocol of choice for Web services.

SSL - Secure Sockets Layer
SSL is a network protocol layer, located directly under the application layer with responsibility for the management of a secure (encrypted) communication channel between the client and server.

W3C - World Wide Web Consortium
The World Wide Web Consortium develops interoperable technologies (specifications, guidelines, software, and tools) for communication over the Internet.

for formatting XML documents for display.

XKMS - XML Key Management Specification
This specification was proposed originally by VeriSign, Microsoft and webMethods and has now been submitted to the W3C. XKMS reduces the complexity involved in developing XML applications that make use of digital certificates. It deals purely with the key management aspects of PKI such as key generation, registration, certification and revocation, rather than cryptography functions such as signing.

XML - Extensible Markup Language
XML is defined by the W3C and IETF and is based on SGML. It is designed especially for Web documents and is human-readable as well as machine-readable. Customized tags can be created, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations. XML is more than a markup language; it is a family of technologies including XSLT and XPath.

XML-DSig - XML Signature
The XML Signature recommendation is defined by W3C and IETF. XML signatures provide integrity, message authentication, and/or signatory authentication services for data of any type. The use of XML Signatures is not limited to XML data - XML Signatures can be applied to all types of electronic data. An XML Signature can be applied to sections of a document, so that multiple signatures may be contained in a single document.

XPath - XML Path Language
XPath is a language used to identify specific patterns in XML data and is designed to be used by both XSLT and XPointer.

XML Schemas - XSD
XML Schemas are defined by W3C and provide a means for defining the structure, content and semantics of XML documents. XSD provides application developers with a lightweight means to check element and attribute structures without needing to figure out parameter entities, external inclusions, and the other power tools, which make processing a DTD, more complex.

XSL - Extensible Stylesheet Language
XSL is a stylesheet language for XML. It consists of two parts: a method for transforming XML documents and a method