

VORDEL SECURITY TOKEN SERVICE

Cloud, SOA, mobile, and B2B all rely on web services. Most services need to authenticate the clients and the users that request access. Cross-domain authentication requires additional management of trust relationships and a secured method of federating identity. Vordel Security Token Service (STS) is an authentication broker that handles security token generation, exchange, transmission, and validation across different technologies and standards. Vordel STS offers a simple, reliable, and scalable way to control user and service access across Cloud, SOA, mobile, and B2B domains.

Secure Identity with Signed Security Tokens

Userid + password is still the mostly popular authentication method. Transmitting userid and password, especially across security domains, raises security, compliance, and operational issues. Best practice recommends using signed security tokens such as SAML and Kerberos to encapsulate identity claims and attributes for secured transmission and caching.

Mediate Tokens From Different Platforms

With new mobile and Cloud clients and existing SOA and B2B clients, the task of authenticating clients is ever more complex, involving different technologies and standards. Using Vordel STS to convert different client tokens to a standard based token such as SAML relieves web services the burden of handling multiple token types.

Broker Trust Relationships Across Domains

Trust of an identity provider is fundamental to authentication. Browser-to-service interactions rely on user inputted credentials to establish trust. Service-to-service interactions, including Cloud integrations, rely on PKI based mechanisms to establish trust. Using Vordel STS with standards like WS-Trust to broker trust relationships between clients and services is more scalable and reliable than managing direct relationships.

Feature Highlights

Vordel Access Gateway secures, audits, controls, and mediates access to enterprise applications and SOA infrastructure.

Token Management

Comprehensive security token management

- Generation of security tokens of any variety
- Token caching
- Token exchange between standard, proprietary, and custom types
- Enrichment of claim and attribute data in token
- Appending of converted token to request
- Token validation

Audit and Monitoring

Monitor, log, and report on token transactions

- Monitoring across all clients and services
- Monitoring and logging of all token transactions: authentication, issuance, exchange, and validation
- Real-time monitoring and time based reporting
- Automated report delivery
- Transaction tracking, alerting, and debugging

Trust Management

Broker trust relationships between clients and services

- Negotiation of token exchange
- Brokering of PKI between clients and services
- Policy enforcement point (PEP) for identity and access management platforms
- Works with WS-Trust enabled clients and agents

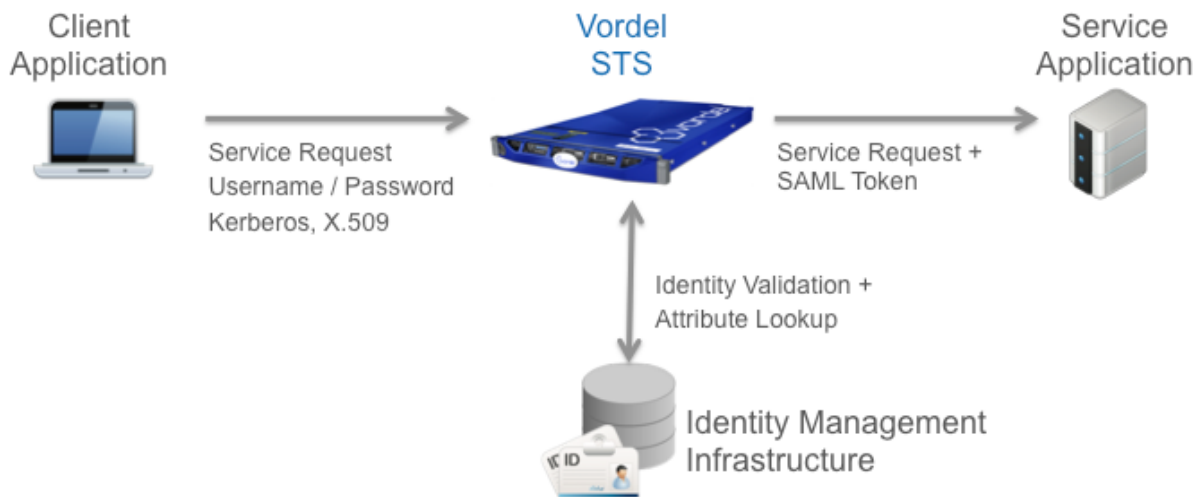
Standards Support

Support a broad range of open standards

- SAML 1.1 and 2.0
- Kerberos
- OAuth 1.0 and 2.0
- HTTP Basic and Digest
- WS-Username
- X.509
- WS-Trust & WS-Federation

See vordel.com for the full list of supported standards

Vordel Security Token Service Solution



 vordel® “Applications Anywhere”

Copyright © 2011, Vordel Inc. and/or its affiliates. All rights reserved.

For more information or sales enquiries, contact sales@vordel.com
USA +1 866-460-0987 | Rest of World +44 203-427-5082

Generate Security Tokens

With web services becoming more federated, credentials are being handled by more intermediaries than before. Every intermediate middleware and application that handles and caches the credential introduces an additional security and compliance risk. Security best practice calls for using signed tokens to encapsulate identity and attributes. Vordel STS is integrated with all the leading identity management platforms to handle authentication, token issuance and validation.

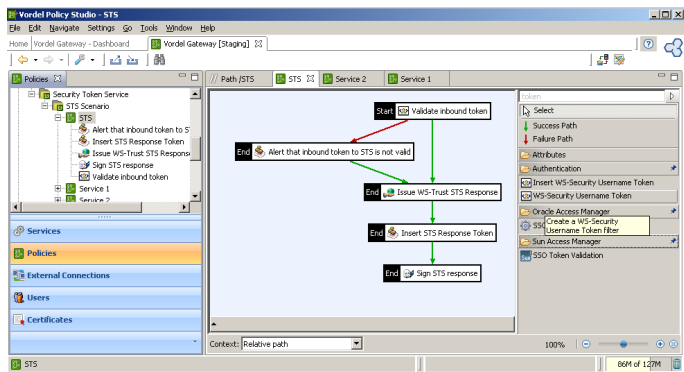


Enrich Token with Claim and Attribute Data

Web services often perform authorization, audit, and custom authentication tasks based on the claim and attribute data in the security token, but some tokens may contain insufficient or outdated data. This is often the case when a client, such as a Cloud based service, generates tokens based on a local copy of the identity data that is updated only periodically. Vordel STS can append or replace a token's claim and attribute data with up-to-date information from a trusted identity provider such as the enterprise directory.

Exchange Token Types

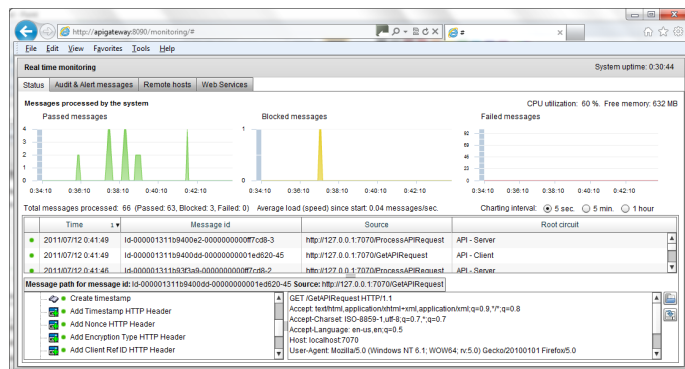
While SAML (Security Assertion Markup Language) has become the most popular security token standard and has been adopted by major Cloud service providers such as Salesforce.com and Google, there are numerous other token standards in use. Kerberos is the standard in Microsoft environments and there are other proprietary tokens used by leading identity management products. Even SAML 1.1 and 2.0 tokens are not compatible. Vordel STS exchanges tokens across standard, proprietary, and custom formats based on configurable policy.



Drag-and-Drop To Insert Token Into Message

Capture Full Audit Trail of Token Transactions

Auditing access across services and clients is tough; auditing in a federated environment where different tokens are used and exchanged is even tougher. Vordel STS provides comprehensive auditing of all token transactions, including authentication, issuance, exchange, and validation. When the STS is used with other gateway solutions from Vordel, Vordel provides end-to-end auditing of web service transactions and security.



Advanced Reporting and Real-Time Monitoring

Broker Trust Relationships

For a service to validate the authenticity and integrity of a client's credential, it must have a trust relationship with the client either directly or through a broker. Managing direct trust relationships for a large number of endpoints is simply not scalable, especially for cross-domain relationships. Vordel STS brokers PKI based trust relationships between clients and services and automates token negotiating using WS-Trust and WS-Federation standards.

Enable Single Sign-on (SSO) Across Services

An application may call several web services within a session or to complete a single transaction. To prompt for a credential every time a web service requests authentication is inefficient and/or an unacceptable user experience. Vordel STS caches security tokens to enable seamless SSO across web services built on disparate technologies. The STS supports configurable token retention and expiration policies, so caching can be controlled precisely to balance user convenience vs. security best practices.

Maximize Interoperability With Open Standards

Vordel STS leverages open standards to maximize interoperability with leading application, SOA, and identity management products. WS-Trust is the key Web Service specification for managing trust relationships. It defines protocols for issuance, exchange, and validation of security tokens based on token format, namespace, or trust boundaries. SAML is the most popular means of exchanging identity claim and attribute information between clients and services that do not reside within a single security domain.