A Broadcom Company
technologies

Product Brief

Simplify OAuth Deployments with OAuth Toolkit

Key Benefits

- OAuth Toolkit simplifies OAuth implementation for Web and mobile APIs by delivering a central point for implementing OAuth. This highly scalable solution delivers the following key benefits:
  - An OAuth authorization server for issuing access tokens in both two-legged and three-legged OAuth scenarios .
  - An OAuth resource server for API access control and policy enforcement.
  - An OAuth Manager to input project scope, with support for extended scope limits.
  - Customizable templates for OAuth client and user implementations
  - Integration with all popular identity and access management (IAM) and SSO solutions.
  - The ability to bridge between OAuth and other access control standards such as XACML and WS-Trust.
  - Support for HMAC secure algorithms and RSA signature algorithms.
  - Configurable runtime policy and logic that allows users to tailor behavior to each service.
  - A token format-agnostic solution that can work with any XML (SAML) or REST-based tokens (OAuth) including JWT access tokens.

Overview

OAuth has become the key specification for authentication and authorization of Web and API data and application assets. OAuth enables delegation and consent for access management decisions, allowing the integration of distributed data into modern applications. The open standard approach of OAuth prevents vendor lock-in and has resulted in rapid adoption. Combined with OpenID Connect, OAuth enables a cohesive single sign-on (SSO) experience across properties that are integrated using RESTful APIs. Unfortunately, implementing OAuth can also be complex and error-prone because of the number of actors, token formats, transports, and security mechanisms that are required.

Solutions Overview

An all-in-one solution for implementing OAuth to secure services and APIs, OAuth Toolkit simplifies OAuth implementation for Web and mobile APIs by delivering a central point for implementing OAuth.

This highly-scalable solution includes the following features:

- An extensible, customizable, full-featured authorization server that supports all OAuth grant types and scenarios.
- An OAuth resource server for API access control and policy enforcement.
- An Admin UI for client and token management.
- Integration with most popular identity and access management (IAM) and SSO solutions.
- Support for algorithms defined in the JSON Web Algorithm (JWA) specification.
- Configurable runtime policy and logic that allows users to tailor behavior to each service.
- A token-format agnostic solution that can work with any XML (SAML) or REST-based tokens (OAuth), including JWT access tokens.
- OpenID certifications for basic, config, implicit, and hybrid profiles.

Key Benefits (cont.)

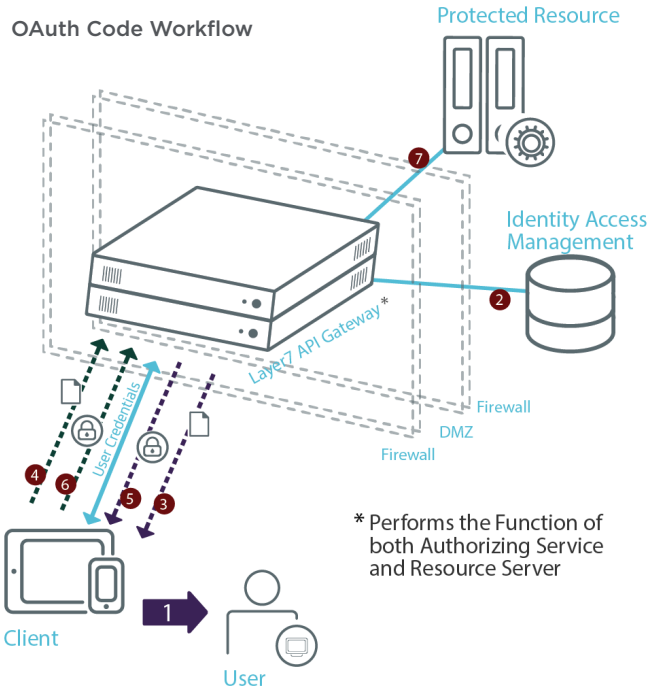
- The ability to use OAuth in a developer-focused API portal.
- OpenID Certifications for basic, config, implicit, and hybrid profiles.

- Using the OAuth Toolkit, organizations can implement policy and identity STS controls to handle a wide range of OAuth token operations and credentials types, enabling the following capabilities.
  - Use HMAC-SHA1/SHA2 (SHA-256) or RSA-SHA1/SHA2 (SHA-256) signature methods and SAML.
  - Validate JWT access tokens without needing to make a call to an authorization server.
  - Mix and match implementation of OAuth with SAML to address typical use cases such as user-delegated authorization for accessing APIs, or cross-domain federated SSO for website users.
  - Drop in new signature and credentials methods without changing APIs.
  - Customize OAuth implementations to bridge between specification versions and differing partner implementations.
  - Add strong but unobtrusive security to mobile apps that access backend enterprise resources with OpenID Connect.

Solutions Overview (cont.)

OAuth is made easy with OAuth Toolkit. The OAuth code workflow works in the following way.

1. The client requires access to protected resource and redirects to user.
2. The user enters credentials. Layer7 API Gateway then validates those against any identity and access management (IAM).
3. If the credentials are valid, the gateway redirects the user back to the client with an OAuth code.
4. The client uses the OAuth code and API key to request an OAuth token from the gateway.
5. The gateway issues a signed and encrypted OAuth token to the client.
6. The client sends an OAuth access token to a protected resource.
7. The gateway validates the access token. Policy logic allows or denies access to the resource.



Key Features

OAuth Toolkit is part of a complete portfolio from CA Technologies, A Broadcom Company, and it includes the key features that you see on the following pages.

Key Features (cont.)

OAuth Toolkit	
Scenario Support	• Support for two- and three-legged OAuth implementations. • Addresses every stage of the OAuth protocol flow: user, client, authorization server, runtime token validation, and administrative token management. • Support for a variety of token hashing algorithms and grant types defined in OAuth 2.0 specification, as well as the ability to customize grant types. • Support for OAuth access token session parameters, including scope, client ID, subscriber ID, grant type, associated refresh token, original credential, usage data, and user-defined fields.
Full OAuth Lifecycle	• OAuth authorization server for generation of access, refresh and id tokens. • Integration with leading identity, access, SSO, and federation systems from Oracle, Sun, Microsoft, CA, IBM Tivoli and Novell. • Runtime validation of access tokens for resource servers. • Customizable OAuth client templates for outbound OAuth integration and testing scenarios. • Customizable user templates for SSO to external OAuth clients. • Rich token management for viewing, monitoring, managing, and revoking generated OAuth tokens.
Federation and Integration	• Automated integration with the Layer7 API Portal for mapping generated API keys to OAuth tokens. • Simple integration with popular public OAuth implementations such as Layer7 API Management, Salesforce.com, LinkedIn, Twitter, and Google. • Integration with SiteMinder as a SAML STS issuer that features support for SAML 1.1, 2.0 authentication, authorization, and attribute-based policies and security context tokens.
Identity and Message-Level Security Enforcement	
Security Management for Cross-Domain and B2B Relationships	• Credential chaining, credential remapping, and support for federated identity. • Support for HTTP basic, digest, and JWT client authentication. • Integrated PKI CA for automated deployment and management of client-side certificates and integrated RA for external CAs. • Support for SAML, X.509 certificates, and LDAP.
Security for REST, WSDL and POX Interfaces	• Ability to selectively control access to interfaces, down to an operation level. • Out-of-the-box support for popular Cloud and SaaS interfaces from SFDC and Amazon. • Ability to create on-the-fly composite WSDL views tailored to specific requesters. • Service look-up and publication using WSIL and UDDI.
Transaction Auditing	• Logs message-level transaction information. • Ability to spool log data to off-board data stores and management systems.
Threat Protection	
Content Filtering	• Configurable validation and filtering of HTTP headers, parameters, and form data. • Detection of classified words or arbitrary signatures with subsequent scrubbing, rejection, or redaction. • Identifies and suppresses leakage of sensitive information (such as SSNs and credit card numbers). • Support for REST, XML, POX, and other XML-based services.
Intrusion and Attack Prevention	• Protects against cross-site scripting (XSS), SQL Injection, XML content, structural threats and viruses. • Ability to create custom threat profiles, extending filters for message structure and XML threats • Tracks failed authentications or policy violations to identify patterns and potential threats. • Validates HTTP parameters, REST query, POST parameters, JSON data structures, or XML schemas.
Form Factors	
Hardware	• Active-active and clusterable, mirrored hot-swappable drives, and multi-core 1U server.
Software	• Solaris 10 for x86 and Niagara, SUSE Linux, Red Hat Linux 6, 7, and 8.
Virtual Appliance	• VMware ESX (VMware Ready certified).
Cloud	• Amazon EC2 AMI.

Key Features (cont.)

Supported Standards
XML, SOAP, REST, PCI-DSS, AJAX, XPath, XSLT, WSDL, XML Schema, LDAP, SAML, XACML, OAuth 1.0a, OAuth 2.0, PKCS, FIPS 140-2, Kerberos, X.509 Certificates, XML Signature, XML Encryption, SSL/TLS, SNMP, SMTP, POP3, IMAP4, HTTP/HTTPS, FTP/FTPS, MQ Series, JMS, Raw TCP, Tibco EMS, WS-Security, WS-Trust, WS-Federation, WS-Addressing, WSSecureConversation, WS-I BSP, WS-MetadataExchange, WS-Policy, WS-SecurityPolicy, WS-PolicyAttachment, WS-SecureExchange, WS-I, WSIL, UDDI, WSRR, MTOM, IPv6, WCF.

For more product information, please visit broadcom.com/api.

Copyright © 2019 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. Broadcom, the pulse logo, Connecting everything, CA Technologies, and the CA technologies logo are among the trademarks of Broadcom.
CS200-370599-1219 December 10, 2019