Simplify OAuth Deployments with CA API Gateway OAuth Toolkit

Authentication and Authorization for Web and Mobile APIs

OAuth is fast becoming a key standard for access management with RESTful APIs. OAuth advantages include the ability to be lightweight for over-the-air mobile applications and open—to prevent vendor lock-in or insecure integration. It can also be optimized for enabling a Single Sign-On (SSO) user experience with Web properties integrated using RESTful APIs. Unfortunately, OAuth can also be complex to set up, given the number of actors, token formats, transports and security mechanisms required.

An all-in-one solution for implementing OAuth to secure services and APIs

CA API Gateway OAuth Toolkit simplifies OAuth implementation for Web and mobile APIs by delivering a central point for implementing OAuth. This highly-scalable solution delivers:

- An OAuth authorization server for issuing access tokens in both two- and three-legged OAuth scenarios
- An OAuth resource server for API access control and policy enforcement
- 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 has algorithms and RSA signature algorithms
- Configurable runtime policy and logic that allows users users to tailor behavior to each service
- A token format-agnostic solution that can work with any XML (SAML) or REST-based tokens (OAuth)
- The ability to use OAuth in a developer-focused API Portal

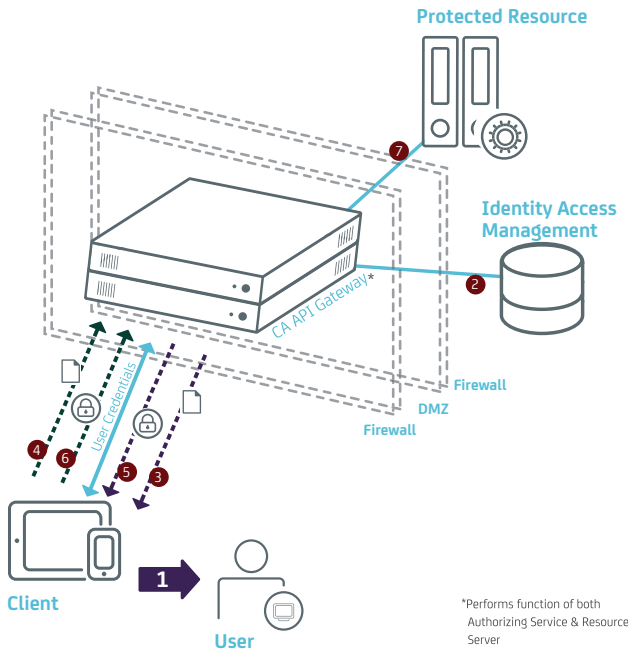
Using the OAuth Toolkit, organizations can implement policy and identity STS controls to handle a wide range of OAuth token operations and credentials types, including:

- HMAC-SHA1/SHA2 (SHA-256) or RSA-SHA1/SHA2 (SHA-256) signature methods and SAML
- Mix and match how they implement OAuth with SAML in order 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 their APIs
- Customize OAuth implementations to bridge between specification versions and differing partner implementations

The CA Technologies solution:

A three-legged OAuth is made easy with CA API Gateway OAuth Toolkit with these steps:

1. Client requires access to protected resource and redirects to user
2. User enters credentials, which CA API Gateway validates against any identity and access management (IAM)
3. If valid, CA API Gateway redirects user back to client, with OAuth code
4. Client uses OAuth code and API key to request OAuth token from CA API Gateway
5. CA API Gateway issues signed and encrypted OAuth access token to client
6. Client sends OAuth access token to protected resource



Key Features

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, administrative token management ▪ Support for a variety of token hashing algorithms and grant types, including implicit, authorization code, SAML etc. ▪ 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 request tokens and access 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 & Integration	▪ Automated integration with CA Layer 7 API Portal for mapping generated API keys to OAuth tokens ▪ Simple integration with popular public OAuth implementations such as Salesforce.com, LinkedIn, Twitter, Google etc. ▪ OAuth integration with onboard SAML STS issuer featuring support for SAML 1.1/2.0 authentication, authorization and attribute-based policies and security context tokens

Identity & Message-Level Security Enforcement	
Security Management for Cross-Domain & B2B Relationships	▪ Credential chaining, credential remapping and support for federated identity ▪ Support for HTTP basic, digest, SSL client-side certificate authorization, Microsoft SPNEGO etc. ▪ Integrated PKI CA for automated deployment and management of client-side certificates and integrated RA for external CAs ▪ Support for SAML, X.509 certificates, LDAP etc.
Security for REST, WSDL & 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 requestors ▪ 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/arbitrary signatures, with subsequent scrubbing/rejection/redaction ▪ Identifies and suppresses leakage of sensitive information (SSNs, credit card numbers etc.) ▪ Support for REST, XML, POX and other XML-based services
Intrusion & 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 and/or policy violations to identify patterns and potential threats ▪ Validates HTTP parameters, REST query/POST parameters, JSON data structures, XML schemas etc.
Form Factors	
Hardware	▪ Active-active clusterable, mirrored hot-swappable drives, multi-core 1U server
Software	▪ Solaris 10 for x86 and Niagara, SUSE Linux, Red Hat Linux 4.0/5.0
Virtual Appliance	▪ VMware/ESX (VMware Ready certified)
Cloud	▪ Amazon EC2 AMI
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 information, please visit **ca.com/api**

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

CS200-87756-1014