DATA SHEET

CA Mobile API Gateway

At a Glance

The mobile app has become the central focus for new revenue opportunities, improving employee productivity and innovative business strategies. Central to these objectives is the need to externalize enterprise information assets in mobile-ready formats that can be easily consumed by both mobile developers and the apps they create. CA Mobile API Gateway simplifies the process of adapting internal data, application and security infrastructure for mobile and Internet of Things (IoT) uses.

Key Benefits/Results

- **Accelerate app development** – Adapt backend services into mobile-ready APIs while externalizing to developer communities
- **End-to-end security** – Protect the mobile app through transmission to the backend
- **Convenient access** – Authenticate once and gain access to multiple apps with single sign-on and social login
- **Backend protection** – Granular risk-based user, app and device polices with API threat protection
- **Optimized performance** – Maximize performance and scale with app caching cloud integration and notification services

Key Features

- **Adaptation** – Externalize services and data as modern and RESTful mobile APIs
- **Identity and access** – OAuth and OpenID delivers mobile app authentication, social login and single sign-on
- **Mutual SSL** – Cryptography-based security for API consumption
- **API security** – Protect REST, SOAP and OData APIs against DoS and API attacks
- **Optimization** – Cache calls to backend applications, minimize bandwidth and improve user experience
- **Integration** – Centralize connectivity between social networks, cloud, IoT and notification services

Business Challenges

Enterprises are facing an increasing array of mobile challenges when attempting to accelerate mobile innovation and drive business forward. Here are the common mobile app challenges that must be overcome:

Inaccessible data. Legacy systems and data are often difficult to externalize in a safe and reliable way.

App development barriers. Applying security within the development process can add significant time to the release cycle.

Security impacting UX. Security can often inhibit business process and app consumer adoption.

Managing and securing a broad range of app types. Whether leveraging existing Web applications, developing new native mobile apps or partnering with third–party app provider like Salesforce.com, each app type will require different management and security solutions.

Solution Overview

Adapt, optimize and integrate with ease—CA Mobile API Gateway is a premium level application program interface (API) gateway that supports mobile app architecture and development initiatives. This lightweight, low-latency gateway comes with integrated security and management controls designed to help enterprises safely and reliably expose internal assets as mobile APIs while solving critical identity, security, adaptation, optimization and integration challenges.

Secure the client to the backend ensuring seamless access for authorized users—The Gateway comes with a mobile software development kit (SDK) for enterprise app developers, which enables:

- Secure consumption of backend APIs through configuration of mutual Secure Sockets Layer (SSL) between the gateway and the mobile device
- Single sign-on (SSO) across mobile apps and devices via enterprise identity and access management (IAM) systems or social login to maintain a seamless end-user experience
- Mobile SSO Reference App organizes applications in a single console while integrating with existing IAM infrastructure to deliver SSO across app types
- Secure session sharing via QR code (QRC), near field communication (NFC) and Bluetooth low energy (BLE)
- Multi-user support allows users to access provisioned apps without deregistering the device
- Samsung KNOX integration delivers SSO with the mobile SDK while allowing customers to create policy assertions requiring device integrity and app containerization checks as a condition to accessing APIs

Identity	
Mobile SDK	▪ Client-side libraries, code examples and documentation to help developers simplify implementation of SSO and mutual SSL ▪ Ability to leverage device OS security to create a secure SSO container ▪ Standards-based security flows based on OAuth 2.0, OpenID Connect and PKI ▪ Single API call to leverage cryptographic security (mutual SSL) ▪ Secure transfer, storage and pinning of certificates, adding additional trust to authentication ▪ Geolocation access control applies GPS, geolocation aggregators and carrier coordinates to context variables ▪ Mobile social login enables users to gain access to mobile apps through social credentials such as Facebook, LinkedIn, Salesforce ▪ Samsung KNOX Authenticator for CA Mobile SSO is an Android Service through Samsung's KNOX SDK ▪ Multiuser support & session sharing (QRC, NFC, BLE)
Access Control	▪ Support for OAuth, OpenID Connect, SAML, X.509 certificates, LDAP, etc. ▪ Support for HTTP basic, digest, SSL client-side certificate authorization, etc. ▪ Samsung KNOX for APIs: Policy Assertion (requires Attestation) to force Samsung Knox Attestation Service as API access condition ▪ KNOX container management and integrity validation ▪ Supports phone unlocking using fingerprint recognition, supports one-time passwords for critical APIs ▪ Share user credentials (SSO) between apps with no coding and transfer user session between devices and platforms ▪ Advanced Auto Risk Evaluation integration ▪ Uses SCIM 2.0 endpoints on gateway to abstract identity backends
Identity Integration	▪ Integration with enterprise identity, access, SSO and federation systems, including CA Single Sign-On and SOA CA Security Manager, LDAP, Microsoft Active Directory®/Federated Services, Oracle® Access Manager, IBM Tivoli® (TAM and TFIM), RSA ClearTrust, Sun Java™ Access Manager and Novell Access Manager ▪ Mapping between Web Access Tokens and mobile token exchange mechanisms, as well as SAML-to-OAuth enablement ▪ Cassandra token store for better performance and improved scalability for B2C use cases
Mobile Application Data Security	
Threat Protection	▪ Validate HTTP parameters, REST query/POST parameters, JSON data structures, XML schemas, etc. ▪ Protect against cross-site scripting (XSS), SQL injection and DoS attacks ▪ Track failed authentications and/or policy violations to identify patterns and potential threats
Data Streaming Proxy	▪ Proxy mobile streaming protocols like WebSocket and XMPP
Privacy and Digital Certificates	▪ Onboard PKI and certificate management with optional hardware security module (HSM) ▪ Fast elliptic curve cryptography (conforms to NSA's Suite B algorithms and FIPS 140-2 support in both hardware and software)
Adaptation and Orchestration	
API Orchestration	▪ Compose and orchestrate REST and OData APIs from any legacy backend API
SLA Controls	▪ Control API usage: throttle to ensure backend services are not overwhelmed; limit by user, time of day, location, etc.; quota manage (e.g., number of uses/user per day)
Optimization	
Compression	▪ JSON conversion and dynamic message compression
Message Caching	▪ Cache responses to common API requests, decreasing backend service load ▪ Pre-fetch hypermedia API content
Request Aggregation	▪ Aggregate responses to mobile devices to save on-device processing and latency
Integration	
Cloud Services SSO	▪ Enable and manage SSO from enterprise identities to cloud services, such as Salesforce
Social Networks	▪ Proxy and manage mobile application access to social networks and services like Facebook and Twitter ▪ Detect and filter for sensitive/confidential content with subsequent scrubbing, rejection or redaction of messages
Notification Services	▪ Send messages across multiple mobile platforms
Collaboration	▪ Create groups on the fly for collaborative apps ▪ Create real-time IoT friendly apps using an MQTT-based pub/sub infrastructure ▪ Seamlessly integrate your app with an existing enterprise user directory ▪ Create collaborative apps with secure, reliable messaging

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**.

CS200-267848_0417