DATA SHEET

CA API Gateway With Common Criteria Certification

At a Glance

CA API Gateway enables organizations to selectively share data and applications with both internal and third-party developers across back-end applications, third-party systems, cloud applications and mobile devices by connecting disparate sets of information across a multitude of environments. To help ensure the highest level of security for apps developed using this API Gateway, CA has met the rigorous requirements of Common Criteria (CC), an independent security certification recognized by governments in more than 26 countries, including the United States.

Key Benefits/Results

- **Independent Certification.** Certified as meeting the rigorous requirements of Common Criteria (CC), an independent security certification
- **Security Assurance.** Applies military-grade security to data and services shared by partners, developers, mobile apps and cloud
- **Information Access.** Provides a flexible and secure SOA, XML, API and information sharing solution

Key Features

- **Connectivity.** Makes apps and data available across cloud, mobile and social platforms—the key to providing information to partners, developers and constituents when and where they need it
- **Securing Open Environments.** Enables agencies to open data and services to partners, developers and constituents while maintaining application and data security
- **Military Grade Security.** With Common Criteria certification, meets the top defense and intelligence community requirements for security and control capabilities
- **Access Management.** Integrates with CA Single Sign-On and numerous alternatives to provide secure and flexible access management to APIs, applications and Web services on-premises, in the cloud, from a mobile device or a partner's site by providing a common policy access layer

Business Challenges

The need to open data and apps to third parties across a variety of enterprise, cloud and mobile platforms raises a variety of manageability and security concerns. Providing a scalable network infrastructure that enables information to be openly accessed and used by interested constituents across a multitude of environments is key to ensuring that the business of government agencies is available for sharing to the widest array of users at any time, on any device.

In today's connected world, the biggest challenge has changed from sharing apps and data across multiple environments to protecting this array of systems and devices and the information they contain. With a vast array of APIs now available to make apps and data open to virtually any individual, agencies face a huge task as they work to deploy a security infrastructure that provides effective protection against evolving threats, such as intrusion and data breaches.

Solution Overview

CA API Gateway and CA Mobile API Gateway provide an agile, highly functional and secure infrastructure for controlling and securing information access. By providing CC-certified API solutions, CA enables agencies to link disparate sets of information, making it easy for users to run apps and get information when and where they need it.

As a SOA, XML, API and information sharing solution certified to meet National Information Assurance Partnership (NIAP) Common Criteria Protection Profile for policy management and access control, CA API Gateway meets an implementation-independent specification as defined by a combination of threats and security objectives, security functional requirements and security assurance requirements.

Certification was based on an extensive evaluation performed by an independent Common Criteria Testing Laboratory (CCTL) that examined product functionality, design, development environment and documentation. By achieving and maintaining this current security certification, CA is committed to providing API solutions that help government agencies work smarter, faster and more securely to meet mission goals.

Critical Differentiators

Certification: CA API Gateway received certification for the recently revised Common Criteria standard, an international standard (ISO/IEC 15408) for computer security that provides assurance that a security product has been evaluated in a rigorous, standard and repeatable manner to meet stringent security targets used in critical infrastructure, such as Federal Government agencies.

Security: Provides FIPS 140-2 compliance, threat detection, message content filtering and access management using industry standards and integration with third-party IAM systems.

Flexibility: Multiple form factors/deployment models with support for a wide range of platforms. Provides protocol bridging across legacy and new systems and includes content-based routing.

Enforcement: Detailed policies to help ensure robust access control is defined by the Policy Manager and enforced by CA API Gateway. Communication between the Policy Manager and the Gateway is protected from disclosure and modification over secure channel and the Gateway will continue policy enforcement in the event of a loss of connectivity with the Policy Manager.

For more information, please visit **ca.com/publicsector**

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**.

CS200-112944_0215