FORUM SYSTEMS™
THE LEADER IN API & CLOUD GATEWAY TECHNOLOGY

CONNECTING HEALTH AND CARE FOR THE NATION:
A SHARED NATIONWIDE INTEROPERABILITY ROADMAP

FORUM SYSTEMS
PUBLIC COMMENT

Legal Marks

Forum Systems, Inc.
199 Wells Ave, Suite 105
Newton, MA 02459

Forum Systems RFI Response for VA VistA.js Solicitation Number: VA11815Q0219, published March 2015.

RN-RFI-SE-00729

Company Information

Company Name:	Forum Systems, Inc.
Address:	199 Wells Ave, Suite 105, Newton, MA 02459
Type:	Corporation
DUNS	16-1346783
NAICS	334111
Point of Contact:	Randy Gardner
Telephone:	(703) 915-0371
Fax	(781) 791-7510
Email:	rgardner@forumsys.com

Executive Summary

The HHA Interoperability Vision requires a modern, secure and sustainable architecture. API Security Gateway technology is a fundamental component enabling the Vision by providing sophisticated centralized access control and data conformance across network boundaries. The value of perimeter cyber threat mitigation, identity and data validation across heterogeneous environments is key to normalizing disparate technologies and message patterns. It is far more secure and manageable to securely broker a trusted user/data at the perimeter than at the end-mile. API Security Gateway technology is widely deployed and gaining momentum as a key component of modern architecture design. Forum Systems and the Forum Sentry API Security Gateway is the market leader in this movement. This paper intends to raise awareness of this powerful technology to government and industry as it develops a best practice reference architecture supporting the HHA Interoperability Vision.

Mobile, Tele-health, B2B, Cloud and all message patterns are rooted in numerous identity and message standards. Through simple, point-and-click policy configuration, the API Security Gateway inspects and mediates the message/data between two points. The terminology of an API represents the points of communication among systems, and across data boundaries and integration points. APIs represent protocol and message formats that are used to present the integration points among systems. The term gateway means the ability to present an abstracted layer of logical connection to consolidate technologies and policies for the purpose of simplifying the overall architecture and using agile, repeatable, sustainable approaches to information sharing and consolidation. It therefore provides for secure interoperability layer that normalizes and validates heterogeneous access control and message patterns. The security term in this product type nomenclature speaks to the identity, access control, data privacy, and information assurance aspects of the communication exchanges.

API Security Gateways are as much about the richness of interoperability technology as they are about the principles of modern architecture design that enable a complex set of client and server technologies to seamlessly communicate by abstracting the complexities of vendor specific technologies to a vendor-agnostic approach.

The HHS challenges of interoperability are founded in the disparate set of technologies and messaging formats that exist in the computing landscapes. API Security Gateways provide the means to integrate those systems through simple, repeatable, and secure technology, purpose-built to do this. The combination of comprehensive interoperability-enabling technology together with integrated data security allows sensitive data exchanges to extend far beyond current boundaries and scope. The identity and access control aspect combines with this to enable dynamic agility and consistency for identification of users, devices, and actions.

The API Security Gateway technology and corresponding modernization design philosophies directly correlate with many aspects of the HHS Roadmap as detailed below.

FORUM SYSTEMS PUBLIC COMMENTS

ON

CONNECTING HEALTH AND CARE FOR THE NATION:

A Shared Nationwide Interoperability Roadmap

LHS Requirement

E. ***Ubiquitous, secure network infrastructure****:* Enabling an interoperable, learning health system requires a stable, secure, widely available network capability that supports vendor-neutral protocols and a wide variety of core services.

API Security Gateway technology is inherently vendor-neutral, supporting of a broad diversity of vendor specific formats so as to facilitate simplified brokering of system information without the overhead of tightly coupling disparate systems together. The secure portion aligns directly with the API Security Gateway capabilities to secure the protocol channels via SSL/TLS and the message-level information with PKI encryption, SSH encryption, and PGP encryption for data security in motion and at-rest. Network security is further ensured with API Security Gateway technology that has achieved FIPS 140-2 and NDPP certifications to ensure no ability to compromise the gateway systems themselves.

Cyberattacks are the additional consideration in this area, which is what the Security in API Security Gateway is comprised of. The API Security Gateway threat mitigation and deep-content inspection technology protects information flows from data breaches and cyberattack with unique content-specific attack vector analysis and detection technology.

LHS Requirement

F. ***Verifiable identity and authentication of all participants****:* Legal requirements and cultural norms dictate that participants be known, so that access to data and services is appropriate. This is a requirement for all participants in a learning health system regardless of role (individual/patient, provider, technician, etc.)

There is a physical and logical component to this item. API Security Gateway technology handles the logical component of identity token variant consolidation and unification of identity from the myriad of technologies across the on-premise and cloud landscapes to mobile, desktop, and smart-devices. The ability for the API Security Gateway to unify identity ensures that the concepts of role-based, attribute-based, and content-based access control can be applied. This is essential in the realm of HHS where participant sensitivity to data access and information is paramount. The API Security Gateway combines modern technologies of single-factor, mutli-factor, PKI-based, SAML-Based, and OAuth-based authentication as core aspects of the unification abilities.

LHS Requirement

G. ***Consistent representation of permission to collect, share and use identifiable health information****:* Though legal requirements differ across the states, nationwide interoperability requires a consistent way to represent an individual's permission to collect, share and use their individually identifiable health information, including with whom and for what purpose(s).

Achievement of this area is known in the logical access world as ABAC, attribute-based access control. This is an extensible means to aggregate the types of permissions and roles that an identified subject, device, or system is entitled to which then is used to build the policies of enablement and sharing. API Security Gateway technology is an ABAC engine allowing interoperability to also be a guiding factor to achieving a common representation of permissions even if the disparate systems are not prepared, or technically capable of achieving this on their own.

LHS Requirement

H. ***Consistent representation of authorization to access health information****:* When coupled with identity verification, this allows consistent decisions to be made by systems about access to information.

Achievement of this area is known in the logical access world as ABAC, attribute-based access control. This is an extensible means to aggregate the types of permissions and roles that an identified subject, device, or system is entitled to which then is used to build the policies of enablement and sharing. API Security Gateway technology is an ABAC engine allowing interoperability to also be a guiding factor to achieving a common representation of permissions even if the disparate systems are not prepared, or technically capable of achieving this on their own.

LHS Requirement

I. ***Stakeholder assurance that health IT is interoperable:*** Stakeholders that purchase and use health IT must have a reasonable assurance that what they are purchasing can interoperate with other systems.

A principled approach of adoption of API Security Gateways gives this assurance as the founding principles of this technology and the modernization capabilities achieve a posture of vendor-agnostic standards-based integration optimization, reduction of vendor-lock and proprietary solutions, and decouples the complexities of identity, access-control, and data security from the applications layers and builds this into an interoperability-layer (the gateway itself) whereby these patterns and principles are repeatable and agile.

LHS Requirement

J. ***Consistent Data Formats and Semantics****:* Common formats (as few as necessary to meet the needs of learning health system participants) are the bedrock of successful interoperability. Systems that send and receive information generate these common formats themselves or with the assistance of interface engines or intermediaries (e.g., HIOs, clearinghouses, third-party services.) The meaning of information must be maintained and consistently understood as it travels from participant to participant. Systems that send and receive information may or may not store standard values natively and therefore may rely on translation services provided at various points along the way.

Defining standards and driving adherence is one strategy to achieve higher consistency, but often systems are gated by their own limitations, either technical or cost-prohibitive. This is where the capabilities of data mediation and data conversions of API Security Gateway technology enable presentation of APIs that are defined, standard, and modern while in-turn converting those data streams and formats for vintage systems to align with the new common formats.

LHS Requirement

K. ***Standard, secure services****:* Services should be modular, secure and standards-based wherever possible.

This is the precise concept of Secure API Agility. Services are communicated with via their APIs. These APIs should be extensible, agile, and secure. It should not solely be the role of the service provider to try and build all these concepts and design principles into the end-mile service layer. Rather, the approach is the build these principles in the API layer that exposes these services. This enables much more streamlined agility in the development and maintenance of the services, while still maintaining the security posture and diverse interoperability concepts at the API layer where the consumers access the service. This is the fundamental principle of the API Security Gateway.

L. *Consistent, secure transport technique(s)*: Interoperability requires transport techniques that are vendor-neutral, easy to configure and widely and consistently used. The fewest number of protocols necessary to fulfill the needs of learning health system participants is most desirable.

Driving adherence is one strategy to achieve higher consistency, but often these systems are limited by technology and cost to try and alter the underlying technology baselines to achieve modern secure formats. A great example of this is Heartbleed and OpenSSL. Over 2/3 of the entire internet remains exposed to vulnerabilities imposed by these c-based security library approaches to transport security. API Security Technology is not based on OpenSLL or C-based libraries and can thus expose the communication point to these services through consistent, secure transport, and then translate the protocol what the back-end systems can consume and understand.

Section 3 - Forum Sentry API Security Gateway Description

Forum Sentry™ is a government certified API Security Gateway that functions as a trusted intermediary for exchanging secure messages within an API-based RESTful solution architecture. Sentry enables agencies and enterprises to achieve a modern approach to cybersecurity protection and contextual policy-based access control for FHIR externalization and modernization initiatives. The Forum Sentry API Gateway is the industry's only patented API Security Gateway and also the industry's only gateway with combined NIST FIPS 140-2, NIAP NDPP, and DoD PKI certifications. These qualifications uniquely provide an edge-based security approach to enable secure API communications and seamless, secure integration with internal and external partners.

3.1 Forum Sentry - Security Certifications

Forum Sentry API Security Gateway technology has the following security certifications and components

- FIPS 140-2 Level II Certified Hardware Chassis
- EAL 4+ Certified Integrated Hardened Security Module
- US Department of Defense Certified PKI Component
- FIPS 140-2 Level II Certified Administration APIs
- FIPS 140-2 Level II Certified Policy Storage and Key Management
- NIAP NDPP v1.1 Certified Hardware and Software

3.2 Forum Sentry - Key Features

Forum Sentry API Security Gateway technology is a security device ensuring there is no ability to compromise the system itself, and thus grants the ability to deploy the product technology at any information border where data and access control scenarios are desired. The API gateway is an integral part of securing environments where the border of information exchange is continually extended through APIs and challenged by information sensitivity, interoperability, performance, and cryptography.

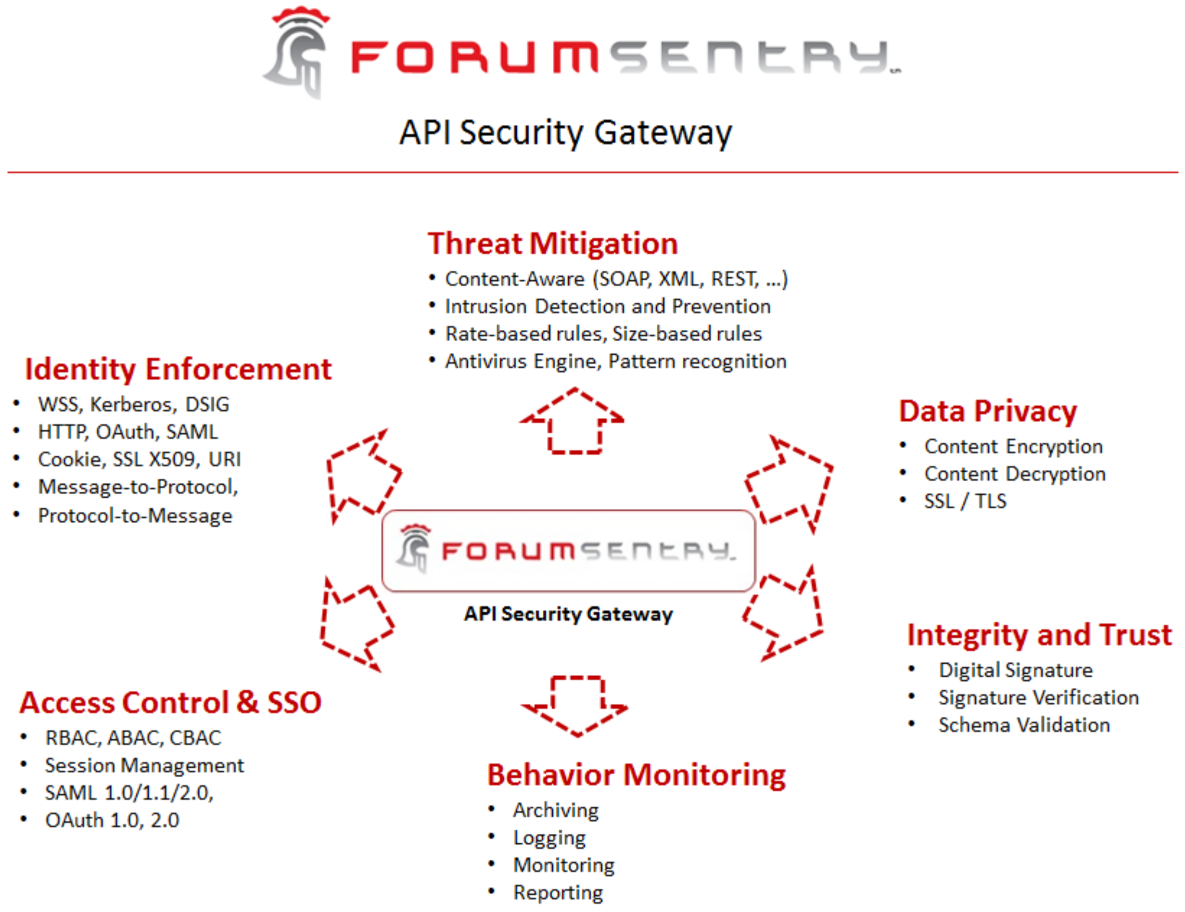

Figure 2: Forum Sentry API Gateway Features

3.4 Forum Sentry - Product Technology Overview

Forum Sentry API Gateway product is designed for enterprise-class scalability for deployment of solutions that address expose data and services to external entities requiring a risk mitigation to ensure Security, Identity, and Interoperability requirements.

3.4.1 Modern Information Security

Forum Systems holds the industry's only cryptographic security acceleration patent for a hardware device. This architecture design aspect enables enterprise-class speed and performance of PKI related security processing. The API Security Gateway is designed to provide a combined approach to both threat and trust based security for data in motion and data at rest. The Forum

Sentry API Gateway architecture consists of FIPS 140-2 Level III ASIC Crypto Acceleration module, a DoD certified PKI Infrastructure, and an NDPP certified Security Architecture and management layer. The security features enabled on our secure architecture include:

Transaction Privacy
- Encryption, Decryption
- SSL

Transaction Integrity
- Digital Signature, Signature Verification, Schema Validation

Transaction Accountability
- Archiving, Logging, Reporting, and Monitoring

Transaction Threat Mitigation
- Intrusion Detection and Prevention
- Rate-based rules, Size-based rules, Antivirus detection, Pattern recognition
- Structural integrity, Protocol adherence, Authorization attempts

3.4.2 Identity Enforcement and Access Control

The Forum Sentry API Gateway fills the void left by other security infrastructure components that are unable to combine policy enforcement across all 3 primary areas of access control (role, attribute, and content). This capability is the hallmark of an API Security Gateway which by intent must be able to understand different protocols and message formats in order to facilitate information exchange. Layered on this is the identity and access control that enables a centralized approach to unifying access control, SSO, and security at the information borders.

The identify features of the Forum Sentry API Gateway include

Identity Mediation
- Message and Protocol Based credential consumption
- Message and Protocol-based credential generation
- Credential Translation – Message-to-Protocol, Protocol-to-Message

Identity Management
- Identity Management integration with all modern IdM systems
- Built-in PKI with X.509 lifecycle management

Access Control
- Role based access control (RBAC)
- Attribute based access control (ABAC)
- Content based access control (CBAC)
- Authorization acceleration via decision caching engines

Federation
- Federation and SSO
- Cookies
- WS-Trust, XACML, OAuth, and SAML
- Custom authentication schemes

3.4.3 Mediation and Centralized Integration

One key aspect of the Forum Sentry API Gateway is the ability to intercept and broker information on behalf of the consumers to the services and services back to the consumers. This is the fundamental concept of a gateway. Deployment of API Gateway architecture becomes the central point for integrating disparate mobile technologies by leveraging the message and protocol processing features built-in to the gateway. Common interoperability features used on the Sentry API Gateway include

Protocol and Data Mediation

- Native Protocol Mixing (HTTP, SFTP, SMTP, JMS)
- Comprehensive Support of W3C and OASIS standards
- XML, SOAP, REST, and JSON content-aware

Data Conversion

- Attribute Mapping into protocol headers
- Attribute Mapping into message document
- SOAP to XML conversion
- XML to REST conversion
- XML to JSON conversion
- XSLT transformation
- External environment attribute enrichment

Database Connectivity

- Oracle, Oracle RAC, DB2, SQL Server, MySQL

API Security Gateway Support for Mobility and Telehealth

Forum Systems is the industry leader in API Security Gateway technology for on premise and cloud deployments of API security for role-based access control (RBAC), attribute based access control (ABAC), and content-based access control (CBAC). Forum Systems' flagship product Forum Sentry is the industry's only FIPS 140-2 and NIAP NDPP certified API Security Gateway product for combining cyber security threat prevention and data security for mobile Apps.

MDM solutions provide device-centric authentication controls and integrated authentication and access control, as well as lifecycle control of app development and usage monitoring. What MDM does not provide is edge-hardened security at the information border where security gateway technology provides mobile threat vector protection, universal token authentication, role-based, attribute-based, and content-based access control, request and response threat correlation, information assurance and content-validation, and centralized event monitoring and logging. It is not enough to have trusted users and trusted services; the information exchange itself must be analyzed and vetted by API security gateway technology to ensure a secure architecture and threat mitigation posture.

API Gateway technology is a seamless gateway intermediary that augments the security posture of MDM exposed solutions to facilitate agile deployments with privacy, trust, and threat based security enforced at the information border.

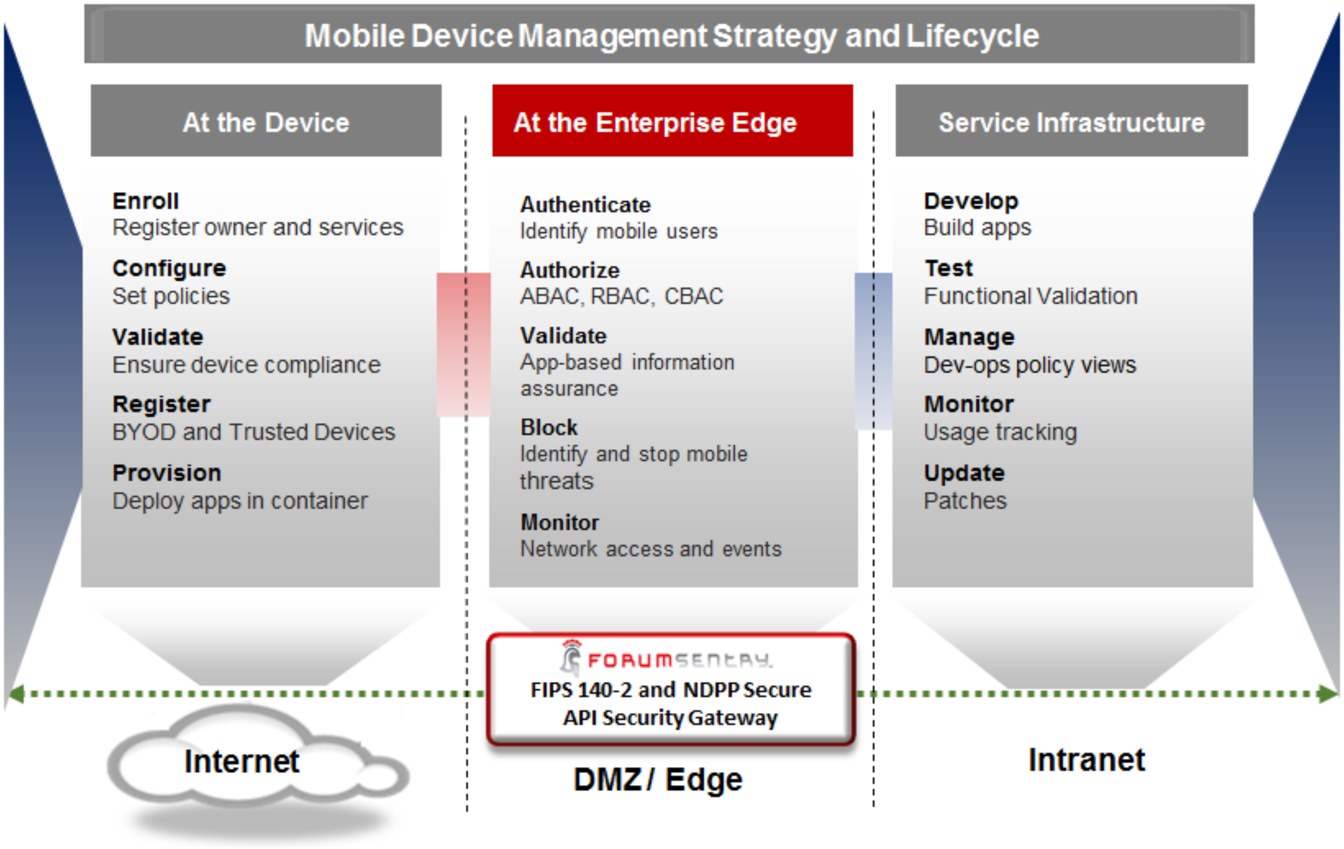

Figure 1 : MDM Strategy and Roles with API Gateway Enforcement

The Forum Sentry API Gateway is directly suitable to achieve the requirements set forth in this RFI, with specific adherence to security and multi-factor attribute-based identification of devices, users, services, apps, roles, and request and response data payload contents which are designed to adhere to MDM published standards, but require API Security Gateway technology to enforce and protect the data boundaries from attack and data breaches.   API Security Gateway technology is designed to provide information assurance and externalization of mobile services via MDM through a security architecture that combines data security with mobile identities.