TRIDIUM®

WHITE PAPER

WP

NIAGARA AX 3.8 FRAMEWORK: SECURE COMPUTING FOR THE PROTECTED PREMISES

JANUARY 2014

Powered by Niagara AX FRAMEWORK®

TRIDIUM

SECURE COMPUTING FOR THE PROTECTED PREMISES

Niagara^{AX} 3.8 Framework: Secure Computing for the Protected Premises

Forward: This white paper has been created by Tridium to provide pertinent information to the end user, systems integrators, enterprise-level clients and other customers on the advantages of the Niagara^{AX} 3.8 FIPS 140-2 compliant mode for stations. For more information, contact your Niagara sales representative or visit www.tridium.com.

FIPS 140-2 option on Tridium software brings comprehensive levels of data security solutions to systems integrators and end user customers.

In every computing environment, including government, enterprise-level, corporate, healthcare, education and other vertical markets, data security is a critical, ever-present concern. Any network-based information that travels over the Internet needs to be protected from hackers and other anomalies that can attack the data, potentially compromising this information.

Data security continues to play a prominent role in media headlines in the U.S. and around the globe. Consider recent breaking news stories centering on the compromise of healthcare medical records and its HIPPA-mandated privacy requirements and other breaches as well. Case in point: Worried that computer hackers attacking bank and media companies could easily shift targets, the airline industry is engaging in steps to ensure it doesn't become the next victim. One major Chicago-based transportation company with an emphasis on aircraft safety is targeting computer security. Transportation cyber security experts are investigating ways they can develop thorough safeguards to limit the effects of hackers - in emails, tablet-based flight manuals and even the plane's hydraulics, where some fear a miscreant could inject malicious commands somewhere in the millions of lines of computer programming that power the transportation company's latest jets.

For physical security, data safety continues as a priority, as companies strive to make their protected premises as safe as possible, including the computer network and hardware and software residing on it. From access control to physical security information management (PSIM) to other edge and embedded devices now increasingly integrated together, data safety takes precedence and is a critical part of providing the highest level of secured computing environment.

Cryptography Protects User Data

Cryptography is the discipline which embodies principles, means and methods for the transformation of data to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. It deals with the transformation of ordinary text (plain text) into coded form (cipher text) by encryption and transformation of cipher text into plain text by decryption. Source: NIST

Powered by Niagara^{AX} FRAMEWORK®

Whether a direct attack from hackers or inadvertent breaches, data security is paramount to both the systems integrator providing contracted integrated solutions and the end-user, as it could mean the difference between a shored up computing environment protected from attacks and problems, or one that literally opens the door to data compromises.

FIPS, NIST and HSPD-12

Many of the standards behind data communications and computer security are rooted in the Federal Information Processing Standards or FIPS. FIPS publications are U.S. federal government security standardizations developed for use in computer systems by all non-military government agencies and government contractors. The purpose of FIPS is to ensure all federal government and agencies, as well as others, adhere to the same guidelines regarding security and communication. More specifically, they describe document processing, encryption algorithms, the production of associated cryptographic modules and other secure information technology protocols.

Computer System Data Security

FIPS 140-1 and its successor FIPS 140-2 are important government standards that focus specifically on providing a benchmark for implementing security requirements for cryptographic software. FIPS 140-1 became a mandatory standard for the protection of sensitive data in January 1994; FIPS 140-2, *Security Requirements for Cryptographic Modules*, superseded FIPS 140-1 in May 2001.

NIST issued the 140 Publication to coordinate the requirements and standards for cryptographic modules which include both hardware and software components.

FIPS 140-2 specifies best practices for implementing cryptographic algorithms, handling key material and data buffers and working with the operating system. Cryptographic modules encrypt network traffic packet data and file contents respectively if configured appropriately with the selections of FIPS compliant algorithms. Compliant cryptographic modules undergo a thorough certification process to ensure that all cryptographic algorithms adhere to and satisfy the government security guideline. The requirements cover not only the cryptographic modules but also their documentation and what information flows in and out of cryptographic module ports and interfaces and how it must be segregated.

Systems integrators who want to offer their end-user customers a higher level of security and a clear market differentiator should include the FIPS 140-2 option of Niagara^{AX} 3.8 in their proposals.

For systems integrators and their end-user customers, these security requirements are another building block in providing secured computing throughout the protected premises - for physical security as well as data networking. Standard 140-1 and now, 140-2, specify the exact security requirements that need to be satisfied by cryptographic modules used within a security system protecting sensitive but unclassified data.

FIPS 140-2 provides four qualitative tiers of security, Levels 1 through 4, with each level detailing requirements, range of potential applications and specific environments in which cryptographic modules may be deployed. These security requirements cover areas related to the secure design and implementation of a cryptographic module and include the following: module ports and interfaces, authentication, physical security, operational environment, key management, electromagnetic interference, self-tests and more - all intended to fortify the secured computing environment.

Tridium, an independent wholly-owned Honeywell company, continues to perform at the forefront of global leadership in open platforms, application software frameworks, automation infrastructure technology, energy management and device-to-enterprise integration solutions. The latest update to its Niagara Framework® software platform - which integrates diverse systems and devices and is manufacturer agnostic - is Niagara^{AX} 3.8, which provides a comprehensive option for FIPS 140-2 compliance.

Safe Solutions for Integrated Network Devices

The Niagara Framework is a unified software platform easily managed and controlled in real time over the Internet using a standard Web browser. Niagara^{AX} 3.8 is scalable and based on an open API, integrating and providing interoperability between diverse systems and devices. Niagara^{AX} 3.8 increases the functionality and value of "smart devices and systems" by connecting real-time operational data to the people and systems that manage business enterprises and creates a common environment that connects to almost any embedded device imaginable. It models the data and behavior of the devices into normalized software components, providing a seamless, uniform view of device data to the enterprise via a wide variety of IP-based protocols, XML-based connectivity options, and open APIs. By transforming the data from diverse external systems into normalized components, Niagara^{AX} 3.8 creates architecture that provides substantial benefits over gateway-based integration.

Tip for Specification

Explain the benefits of encrypted software modules to your customer and the inherent, updated safety it provides to the integrated communications environment. Be a true solutions provider and strive to bring the best in secured data and computing specifications to your customers.

Now, this latest version also has the option of the highest level of communications security in the marketplace. A new safety feature introduced in Niagara^{AX} 3.8 software is a FIPS140-2 compliant mode for stations. When running in FIPS mode, stations will only use cryptographic algorithms supplied by a FIPS-certified module. Niagara^{AX} 3.8 software provides encryption algorithms that ensure secure transmission and storage of sensitive data throughout a Niagara system. And today, that's as critical as ever for a wide range of customers and corporate campuses, in addition to government customers.

Internet Brings the Need for Additional Security

Any organization that uses the Internet for data communications can benefit from FIPS 140-2. As devices and systems continue to integrate and interoperate, the inherent benefits of FIPS 140-2 compliant stations are more apparent than ever. For the end user, they provide an additional layer of security because their system's use Web platform for communications. In fact, if the system is going to be accessible via the Internet, systems integrators will serve their end-user customers well if they offer the enhanced security options that FIPS 140-2 and Niagara^{AX} 3.8 provide.

David Daxenbichler is the President and Chief Executive Officer of Network Harbor Inc., Bartonville, Ill., and has provided consultancy and PSIM OEM software to a host of high-level clients in the access control industry who require strict data communications security, many in the federal procurement contracting space. He understands the importance of specifying and designing FIPS 140-2 compliant software to the integrated systems industry and end-users.

"The importance of a secure platform for integrated computing solutions can't be understated," Daxenbichler said. "But the nature of access control and APIs or SDKs used in communications could literally leave the door open to

compromise, and that's why there needs to be an authenticated connection between the server and the edge reader or device. That's where FIPS 140-2 comes in. If you don't secure the connection with cryptographic modules and compliant stations meeting this standard, someone can obtain the API and then hackers have the 'keys' to open the door. Authentication helps secure the communication and stops the middle man in rogue attacks," he said.

End users who want to deploy market-leading specifications should include the FIPS 140-2 option offered by Niagara^{AX} 3.8 in their Requests for Proposals.

Daxenbichler said the industry has been focused on the more commonly understood and known FIPS 201, but that doesn't lessen the importance of FIPS 140-2. "If you don't have the FIPS 140-2 secured connection and authentication, then what's the sense of having 201? Because in essence, you don't have complete security," he added.

Companies like Tridium that offer 140-2 options and adhere to encrypted algorithm standards published by NIST are authorized to display the standard-body's logo, which indicates their compliance. End users and systems integrators should look for this logo to determine standards compliance and to ascertain their communications have the highest level of security. (FIPS 140-2 is a software option to the Niagara^{AX} 3.8 Framework or later versions and is licensed separately, similar to Tridium drivers. Users will not be able to install it on earlier versions.)

Systems integrators should offer the Niagara^{AX} 3.8 FIPS 140-2 option to end-user customers as an important and available benefit promoting secure computing. End users should also seek this level of compliance to increase the data security of their systems and network communications.

The Niagara^{AX} 3.8 Framework is a clear market leader and differentiator for both systems integrators and end users. Systems integrators would be well-positioned to include the FIPS 140-2 option in their proposals as a market differentiator and as a leadership qualifier of their companies. In addition, end users should strive to include it in their Request for Proposals to be assured of having availability to the latest, most up-to-date levels of computer communications security. For more information, contact your Niagara sales representative.