Unified Automation

Partner Solution

OPC UA Security Extension powered by Wibu-Systems

Stronger Security and Versatile Software Licensing for Modern M2M Communications

Background

The OPC UA standard is a platform-independent communication framework that rapidly emerges into all types of industry. Security is most essential when exchanging information between systems. Therefore a sophisticated security-in-depth concept was built into the core of OPC UA. OPC UA defines application level and transport level security, built into layers on top of the TCP/IP stack. OPC UA introduces the UA-Secure-Conversation layer in addition to the SSL (Secure Sockets Layer) and TLS (Transport Layer Security) used in HTTPS standards of today's web applications. OPC UA provides intrinsic security features and establishes a secured end-to-end channel between client and server. At a communication layer level, the identification of applications and users is handled with X.509 certificates and trust management processes, like trust lists and certificate revocation lists known in PKI. Thereby confidentiality and integrity are preserved and application authentication is ensured.

Unified Automation's OPC UA SDK/Toolkits fully support the defined Security Profiles and configurations and provide APIs to create, store, and validate certificates and trust stores. However, the application specific handling and management of certificates and trusts is outside the OPC UA standard and hence must be solved outside of the SDK/Toolkit. It is specific to the use case of the device and the available infrastructure; therefore the issue has to be addressed by the manufacturer of the equipment.

Wibu-Systems and Unified Automation initiated a joint project to develop a solution that combines the OPC UA security requirements with an easy to use PKI management and safe storage of secrets. Device manufactures can easily integrate a multi-platform protection, licensing, and security solution with the SDK to inherently boost OPC UA-native features and give vendors better access to broader capabilities.

Manufacturers that develop their automation software based on the OPC UA standard need to raise the security bar and protect their machines, their business, and the safety of machine operators from illicit actions or inadvertent manipulation. Additionally, in a time when intellectual property is shifting in the value chain from hardware to software, manufacturers have new opportunities to capitalize on their software and offer feature-based, time-based, version-based, or pay-per-use models to scale up their offerings, expand their market share, and produce recurrent revenues.

Challenges

The generic storage of cryptographic keys and sensitive configuration files, e.g. RSA private keys or trust lists, in the file system, exposes them to theft and tampering. Especially in a world of cyber-physical systems that are connected to open networks. Amongst several ways for compromising a system, attackers use vulnerabilities in operating systems to inject Trojans and get file system access. Protecting the secrets and simplifying the configuration of trust relations and certificate roll out scenarios are the major challenges and crucial aspects for a high level of protection.

Wibu-Systems' CodeMeter Embedded, a modular runtime environment for embedded systems, e.g. Linux Embedded, VxWorks, QNX, and Android, was the ideal candidate for integration with Unified Automation's ANSI C based OPC UA SDK. The Wibu-Systems' security solutions were integrated into the SDK without changing or complicating the user experience for the customer.

Solution

Developers can choose between a pure software solution using OpenSSL or the combined hardware solution using seamlessly integrated CodeMeter Embedded via the internal APIs and abstractions of the ANSI C based SDK. Wibu-Systems OPC UA Security Extensions consists of a software library, the engine of CodeMeter Embedded, and hardware secure elements. While the software components are accessible to vendors directly through the OPC UA SDK, the secure elements, typically USB dongles (but also ASICs or secure memory cards in an SD, microSD, CF, or CFast cards form factor), are associated with the OPC UA applications of the end user. They become the safe repository for encryption keys and software license entitlement details. In addition to secure storage, Wibu-Systems adds simplified configuration and management functionality.

Unified Automation GmbH

O'Brien Str. 2 • 91126 Schwabach • Germany

Tel: +49 911 495 25000 • Fax: +49 911 495 25009

info@unifiedautomation.com • www.unifiedautomation.com

OPC UA Background

CodeMeter adds secure key storage in a Common Criteria EAL5+ certified security controller; symmetric and asymmetric cryptography is executed inside this secure hardware element, which leaves encryption keys and license information fully protected. Containers that embed a smart card chip and rely on its additional encryption and certification properties can withstand side channel and Differential Power Analysis (DPA) attacks. This proprietary technology operates automatically without any need for intervention by the user and is fully transparent for OPC UA interfaces. With an additional software component to be integrated in the OPC UA server software, the content of the dongles can also be remotely managed: software updates and upgrades can be easily and securely deployed, and licenses can be extended, revoked, and transferred by the system administrator. The management and roll out of certificates but also the enabling of licensed product features can be done via the same existing WIBU infrastructure.

"Protecting device know-how in an OPC Unified Architecture has become easier, faster, and more secure with Unified Automation's SDK powered by Wibu-Systems' CodeMeter Embedded",

says Dr. Sören Finster, Senior Software Developer at Wibu-Systems.

Used Products of Unified Automation

"Investing in secure licensing means investing in business stability, good commercial standing, and new monetization opportunities", says Oliver Winzenried, CEO and co-founder of Wibu-Systems.

The OPC UA SDKs of Unified Automation come with abstract crypto and PKI interfaces. The standard delivery of the SDK expects the open source library OpenSSL to be integrated. Apart from this pure software solution, the WIBU Security Extension introduces a second option. The combined hardware dongle and crypto-on-chip option increases security and relieves the main CPU. Whenever a vendor purchases Unified Automation's OPC UA SDK, they automatically avail themselves of the fully integrated capabilities of Wibu-Systems' CodeMeter Embedded. Its set of security functionalities is available for the ANSI C based OPC UA SDK and the High Performance OPC UA SDK. The combination of secure key storage for the endpoint certificates, private keys and trust lists plus the versatile license lifecycle management opens an array of new business venues for automation vendors.

About WIBU-SYSTEMS AG

WIBU-SYSTEMS AG is an innovative security technology leader in the global software licensing market. In its mission to offer the most secure, unique, and highly versatile technology, Wibu-Systems has developed CodeMeter®, a comprehensive, award-winning suite of hardware and software-based solutions for computers, embedded systems, mobile devices, PLCs, and microcontrollers that incorporate internationally patented processes dedicated to protecting the integrity of digital assets. Software publishers and intelligent device manufacturers can safeguard the intellectual property of their applications against illicit and fraudulent use, reverse engineering, and tampering attacks, and generate new digital business models fully integrated with ERP, CRM, and e-commerce platforms.

About Unified Automation

As a leading supplier of OPC UA software Unified Automation provides UA enabled products, cross-platform toolkits and development frameworks in different programming languages (ANSI C, C++, JAVA and C# .NET) and for different platforms (Windows, Linux, VxWorks, QNX, RTOS, and many embedded operating systems). The target market of OPC UA products ranges from manufacturers of embedded devices to developers of enterprise applications.
Unified Automation sees itself as technology and software provider in the field of OPC based communication. The software development kits (SDKs) form the base of OPC UA products of nearly all large and small automation vendors worldwide.

Unified Automation GmbH
O'Brien Str. 2 • 91126 Schwabach • Germany
Tel: +49 911 495 25000 • Fax: +49 911 495 25009
info@unifiedautomation.com • www.unifiedautomation.com