LXI Consortium integrates GlobalSign’s PKI-based IoT Device Identity Platform as an integral part of its security protocol

Standards-based organizations like LXI Consortium operate with a higher degree of excellence than stand-alone businesses, especially when it comes to developing, promoting and adhering to security protocols. When the LXI security working group reached out to GlobalSign to explore security choices, we knew we’d have to bring our best game forward to identify the challenge, collaborate to supply the best technology options, and deliver a security solution that was easily adopted by LXI Consortium members, all while properly securing the equipment according to best security standards. It was a tall order in the precise field of test, measurement and data acquisition industry.

> “As a standards organization, selecting the right security solution was critical in maintaining our ongoing reputation of excellence and reliability,” said Steve Schink, Keysight Technologies, Chair of the Board, LXI Consortium. “GlobalSign worked closely with our security working group to identify our challenges, propose solutions, then implement our vision in a way that works for, and protects, our membership.”

Project Summary

The challenge for LXI Consortium was to secure the supply chains of their members – to secure LXI certified devices/equipment and the WebServers (located on each device) from the manufacturing floor through end-customer deployment, confirming device authenticity and providing secure communication.

LXI members use in-house and/or third-party EMS manufacturing to produce their instrumentation equipment. Restricting the number of devices manufactured physically secures the supply chain by limiting overproduction and potential gray market sales of ‘extra’ units. Unique device identities (IDevIDs) for each piece of instrumentation equipment allows LXI vendors to authenticate each unit and deny unvalidated devices, thus enforcing the restricted number of units with precise accountability. Further, IDevIDs allow future OTA updates and other vendor specific communication or data collection. OCSP revocation services allow LXI to invalidate specific devices (using IDevIDs) in the event of lost or stolen instrumentation.

Once deployed, LXI customers remotely configure equipment/devices using the LXI standard through WebServers. Future work may include securing device identities for equipment already deployed in the field (brownfield application) but is not part of the scope at this time.

Greenfield Device Identity Provisioning, How We Did It

First, GlobalSign employed our IoT Identity Platform, a high volume, high value IoT certificate authority platform, based on best-in-class, Web-Trust audited, PKI Architecture. The GlobalSign IoT Identity Platform is secure, scalable, flexible and interoperable. It features RESTful APIs that facilitate integration and is backed by our trusted GlobalSign Certificate Authority (CA) Services.

Next, we established an LXI Private Root CA capable of creating and supporting multiple intermediate certificate authorities (ICAs) – one for each of its members as they elect to adopt the security standard. Each ICA is equipped with online certificate status protocol (OCSP) revocation services, allowing them to revoke individual digital certificates should they become compromised in any way.

The integration of the IoT Identity Platform with the Private LXI Root CA and LXI Member's Private ICAs uses our CA Direct application programming interface (API).

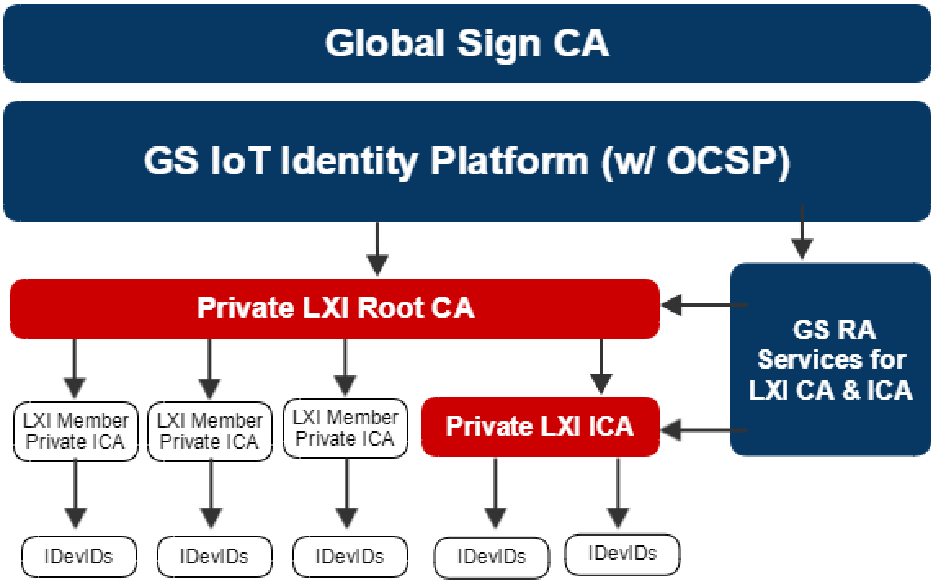
Most LXI members use electronics manufacturing services (EMS) firms to produce their equipment and instruments. Since most equipment do not have public URIs at the point of manufacture, they couldn't receive certificates from a Public CA, therefore a Private CA was needed. The private Root CA ecosystem provided the means to provision initial device identifiers, also known as IDevIDs for each newly manufactured (greenfield) piece of LXI certified equipment or instrumentation. With a proven IDevID, equipment/devices can later be validated upon deployment with a GlobalSign Public CA to obtain the LDevID (DV SSLs).

Partnering to Solve Instrumentation Technology Limitations

Some WebServers on the LXI certified devices did not have FDQNs, therefore we could not issue LDevID (DV SSL) certifications to the webservers on those devices. Beame Authentication Service, hosted on AWS, connects to the equipment/device using an API driven LXI Device Agent, located on LXI certified equipment/devices. It includes DNS mapping to tunnel back through HTTPS (incorporates device information from the IDevID) and assigns FDQNs to each server on LXI's behalf. GlobalSign, as the Public CA is then able to issue LDevIDs certifications (DV SSLs) to Beame for LXI's WebServer security.

GlobalSign functions as the Registration Authority (RA) for the LXI Private Root CA (and LXI member ICAs) for greenfield device identities (IDevIDs). Private RA duties for WebServers were split between GlobalSign and our technology partner Beame. GlobalSign confirmed whether members were in good standing and worthy of IDevIDs for their devices, while Beame issued the actual WebServer identities. WebServer device information (serial number, product family, vendor) were included in the WebServer IDevID for later use with the Beame Authentication Service for webserver security.

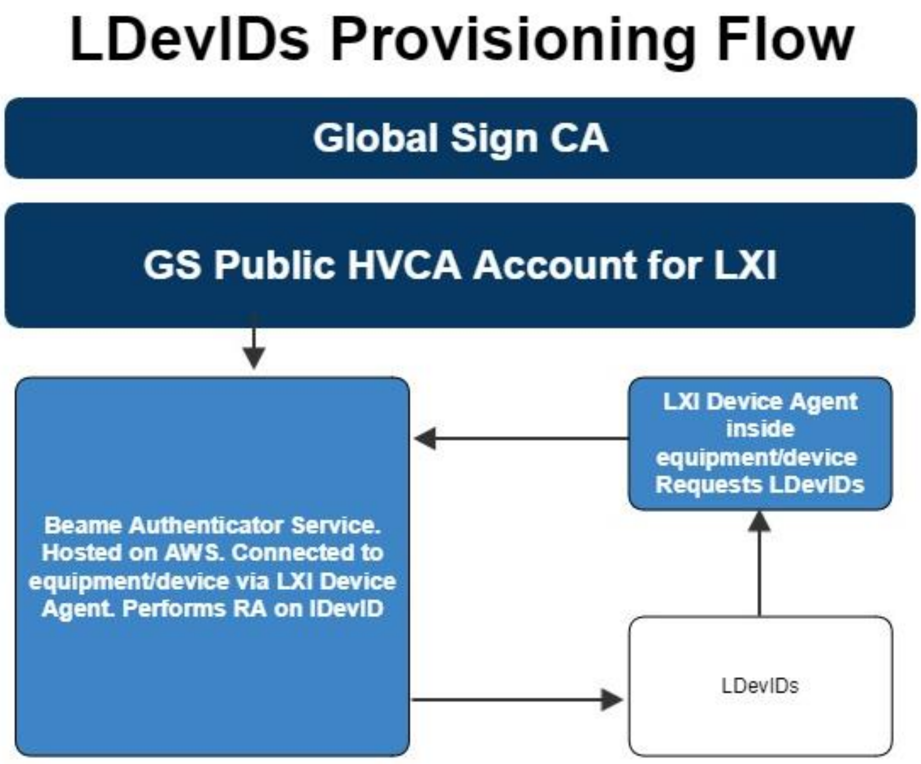
Greenfield Equipment/Device IDevIDs Provisioning Flow



Using Local Device Identifiers (LDevIDs) and Public Roots

We set up an IoT Identify Platform (HVCA) account for LXI under the GlobalSign Public Root to authenticate each LXI certified equipment/device as well as the WebServer that lives on each device at deployment. Since each device had been issued an IDevID through the LXI Private CA at manufacture, this could then be verified during deployment and issued an LDevID (DV SSL cert) via the GlobalSign Public CA.

Using Beame's Authentication Service to generate FDQNs and IDevIDs for each equipment/device WebServer, GlobalSign was able to issue LDevIDs certifications (DV SSLs) to Beame (on behalf of LXI) for WebServer security.



LDevIDs Provisioning Flow

Global Sign CA

GS Public HVCA Account for LXI

Beame Authenticator Service. Hosted on AWS. Connected to equipment/device via LXI Device Agent. Performs RA on IDevID

LXI Device Agent inside equipment/device Requests LDevIDs

LDevIDs

About the IoT Identity Platform

GlobalSign's next-generation IoT Identity Platform delivers exceptional device identity security. It is flexible and scalable enough to issue and manage billions of identities for IoT devices of all types and integrates simply with developer friendly, RESTful APIs.

Using PKI as the core identity mechanism, the IoT Identify Platform can serve the varied security use-cases of the IoT across all verticals, including manufacturing, agriculture, smart grid, payments, IoT gateways, healthcare, other industrial ecosystems and more. The Platform supports the full device identity lifecycle, from initial certificate provisioning (both greenfield birth certificates during manufacturing and local, brownfield identity deployments) to certificate lifecycle management and final sunsetting, including decommissioning or transfer of ownership. Giving each device or endpoint a unique identity allows them to get authenticated when they come online and then throughout their lifetime, prove their integrity, and securely communicate with other devices, services and users.

Benefits of PKI-based Device Identity Provisioning

PKI has become the de facto standard for IoT device identity. It easily accommodates a wide diversity of devices, includingLXI devices. It is built on a strong trust model based on tried and tested cryptography, standardized by IETF and backed by third party certificate authorities like GlobalSign whose sole purpose is one of establishing trust for device identities in order to authorize, authenticate and ensure privacy. The PKI system binds public keys with identities of devices or endpoints to create a solid trust model. Moving Forward as a Team

GlobalSign engages with the LXI consortium and its members throughout three different phases.

Phase 1: Setup of PKI Root of Trust

GlobalSign has worked with the LXI Security Working Group to define the PKI root hierarchy for LXI. This included modeling the PKI architecture, a custom solution proposal for enrollment and specification of the Root CA, ICA and device certificate details. This is now operational and created according to the best in class regulatory and security practices. GlobalSign also maintains certificate revocation and inventory system for all certificates issued by it. Members can now move onto Phase 2.

Phase 2: Device enrollment using IDevIDs

GlobalSign will now work with individual LXI member companies to provision IDevIDs directly from GlobalSign's IoT Identity Platform, into each manufacturer's assembly line/programming process. GlobalSign offers a range of integration options with its Cloud CA-as-a-service and also offers custom solutions that work directly with a manufacturer's end of line tools. At this time, the LXI Device Agent by Beame.io is also integrated into the device software/firmware.

Phase 3: Provisioning of LDevIDs

Once each device has an IDevID, and has been deployed in the field at the customer's location, it reaches out automatically (via the LXI Device Agent) to the Beame Authenticator Service. The IDevID certificate is required to authenticate to the service, and several checks are performed to verify the authenticity of the LXI device – proof of certificate private key possession, certificate revocation status, and verification of certificate contents. The IDevID certificate fields are used to formulate the certificate request for the LDevID ensuring that the device can only request a certificate it is supposed to.

This workflow and rigorous process ensures that the LXI devices are verified to be authentic on a periodic basis, protects and encrypts the communication between LXI members' servers and the devices and finally ensures that the root of trust and the device identity is maintained throughout the device's lifecycle.