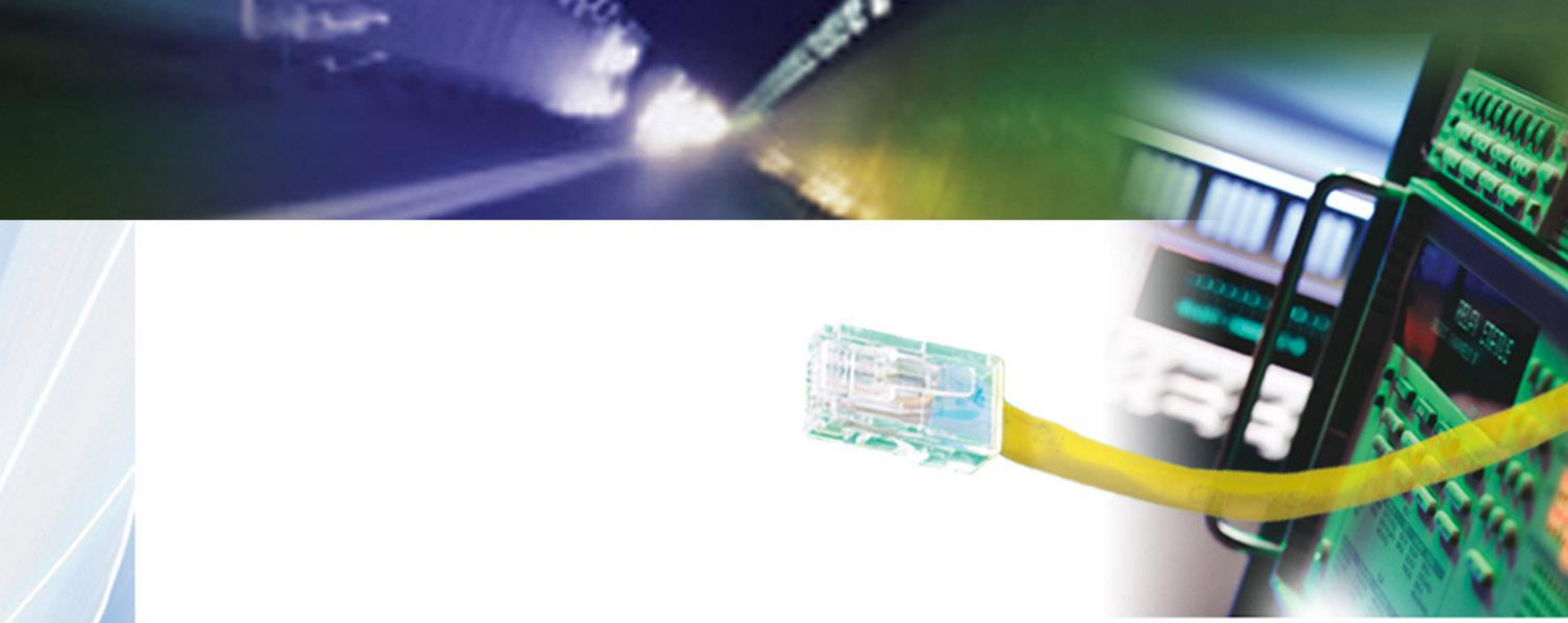


LXI Security

Overview

February 2019

Rev 1.91

www.lxistandard.org

Use the connection you already know!

Agenda

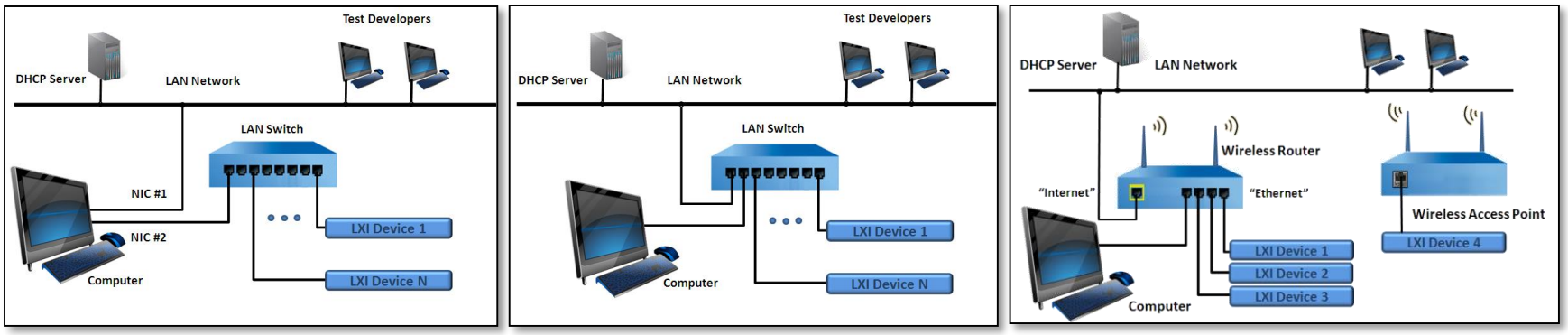
- Introduction & Overview Security Standards
- LXI Communication Channels
  - Remote Control (HiSLIP)
  - Web Browser Interface
  - Encryption
- PKI – Public Key Infrastructure
  - Certificates / Public & Private Keys / Encryption
  - Certificate Authorities (CAs)
  - Public Trust / Private Trust
- LXI Security WG Proposals for Secure Communication
- Questions & Feedback

Introduction – LXI Security

- Security is a critical attribute of industrial networks
- Industry is giving a growing amount of attention to cybersecurity issues
- LXI instruments are connected to company networks
- This presentation gives a summary of the current state of the LXI Security Working Group discussions and proposals for
  - Test Engineers setting up LXI based test systems
  - IT departments supervising the company network
- We are soliciting feedback and proposals to make sure the LXI Security WG covers all requirements

Introduction – LXI Security (2)

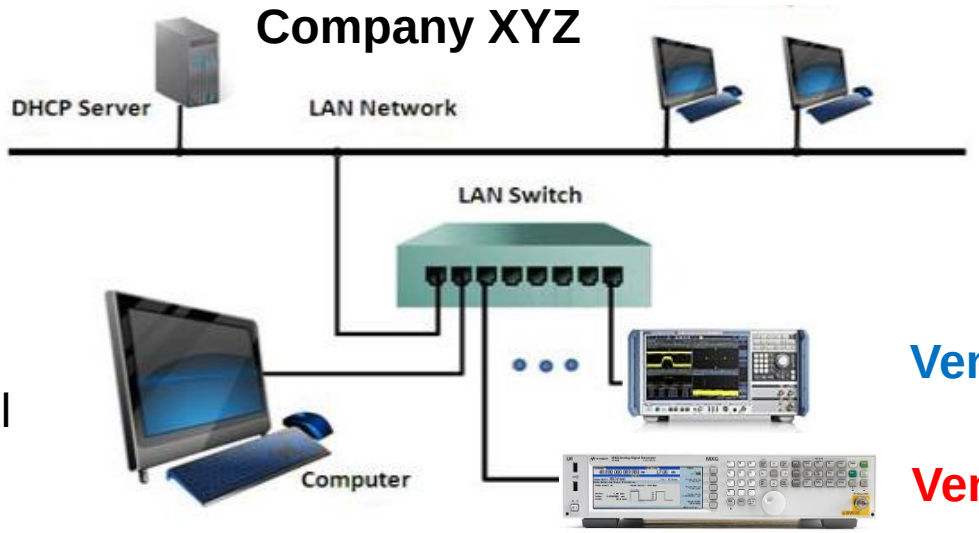
- Levels of Risk Introduction
  - LXI instruments are connected to company networks
  - Depending on the test setup for the LXI instruments there are different levels of risk introduction:
    - Benchtop (e.g. peer to peer connection) w/o connection to the company network
    - Test system setup with isolated subnet
    - Test system directly connected to company network
    - Test system with Internet connections (e.g. remote monitoring in the field)



Examples for test system configurations

Example

- Company XYZ using LXI instruments from LXI vendor A & B
- LXI instruments connected to the company network
- Test computer to control LXI instruments
- Test system developers may have access too

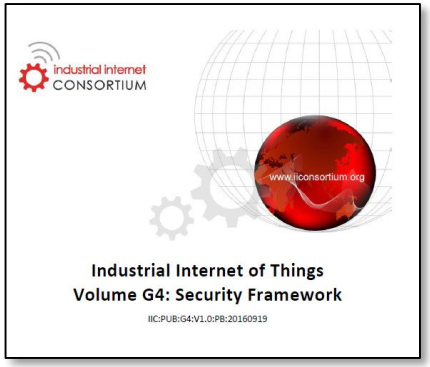


Importance of Network Security

- Primary goals for security within industrial networks are:
  - ***Confidentiality:***
    Data transported in the network cannot be read by anyone but the intended recipient
  - ***Integrity:***
    Any message received is confirmed to be exactly the message that was sent, w/o additions, deletions or modifications of the content
  - ***Authenticity:***
    A message that claims to be from a given source is, in fact, from that source.
    Authorization is another important aspect - both, authentication and authorization require a strong device identity

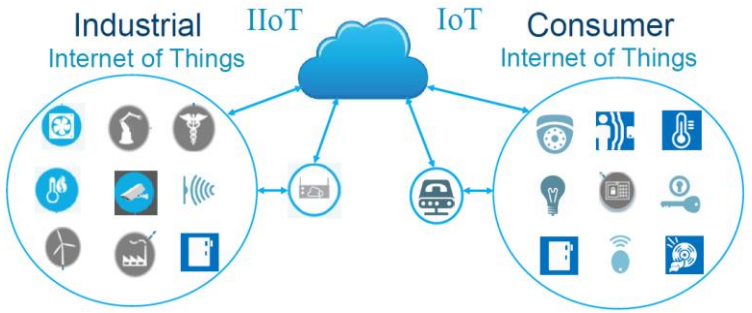
Overview Industrial Security Standards

- Aerospace & Defense:
  NIST: Framework for Improving Critical Infrastructure Cybersecurity
  NIST 800 SP Series
- Industrial Automation & Control:
  IEC 62443 standards (equivalent to ISA 99)
- UL CAP: Underwriters Laboratories Cybersecurity Assurance Program
  UL 2900 series of standards
- IIC Industrial Internet Consortium:
  Industrial Internet Security Framework IISF
- OWASP:
  Open Web Application Security Project – IoT:
  Top Ten Application Risks



LXI Security - Ecosystem

- Areas:
  - IoT (Consumer Internet of Things)
  - IIoT (Industrial Internet of Things)
  - IT (Information Technology)
- There are commonalities which LXI instruments share with IoT, IIoT, IT
- Observed commonalities:
  - Device security
  - Data security
  - Network security



- Key principles: C.I.A.
  - Confidentiality
  - Integrity
  - Authenticity

LXI Communication Channels

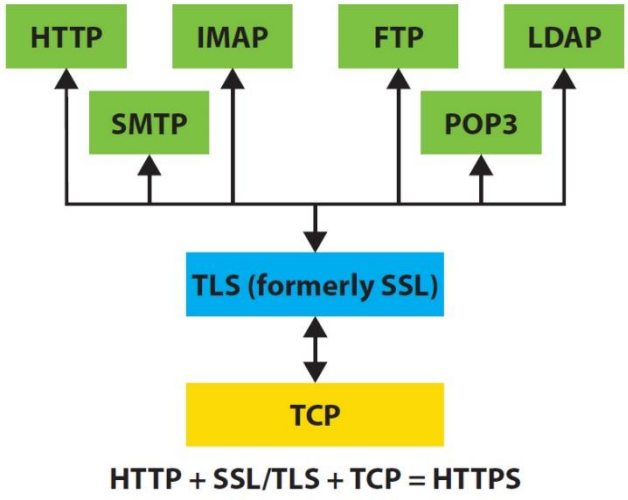
Currently we use within LXI the following communication channels

- Remote Control
  - SCPI based
  - TCP/IP: Socket / VXI-11 / HiSLIP
- Web Browser Interface
  - HTTP
- Ping, mDNS

- To ensure secure communication between test computers and LXI instruments encryption is required
  - TLS encryption
  - HTTPS (HTTP + TLS)

TLS – Transport Layer Security

- **Transport Layer Security (TLS)** is a protocol that provides privacy and data integrity between two communicating applications. It's the most widely deployed security protocol used today, and is used for Web browsers and other applications that require data to be securely exchanged over a network, such as file transfers, VPN connections, instant messaging and voice over IP.



TLS – Transport Layer Security

- TLS evolved from the Secure Sockets Layer (SSL) protocol and has largely superseded it. Key differences between SSL and TLS that make TLS a more secure and efficient protocol are message authentication, key material generation and the supported cipher suites, with TLS supporting newer and more secure algorithms.

- TLS is composed of two layers:
  - TLS Record Protocol
  - TLS Handshake Protocol
- The Record Protocol provides connection security, while the Handshake Protocol allows the server and client to authenticate each other and to negotiate encryption algorithms and cryptographic keys before any data is exchanged.

PKI – Public Key Infrastructure

- In the **Public Key Infrastructure** (PKI), digital certificates are based on public key cryptography. The PKI consists of a set of components, policies, protocols, and technologies that provide data authentication, integrity, and confidentiality through the use of certificates, and public and private keys.
- Data is protected by applying a hashing algorithm and signature algorithm to the original message. A hashing algorithm is an intricate mathematical algorithm which is applied to the message.
- With public key cryptography, the key that encrypts data is called a **public key**. The key that is used to decrypt data is called the **private key**. While the public key can be publicly distributed, the private key is kept secure.

Certificates

- **Digital certificates:**
  Certificates are the foundation of the PKI. The certificate contains the public key of the user. The public key can be used to encrypt and sign data before it is transmitted over the network. The digital certificate contains information such as the certificate version, serial number, signature, issuer, and validity period, among other information.

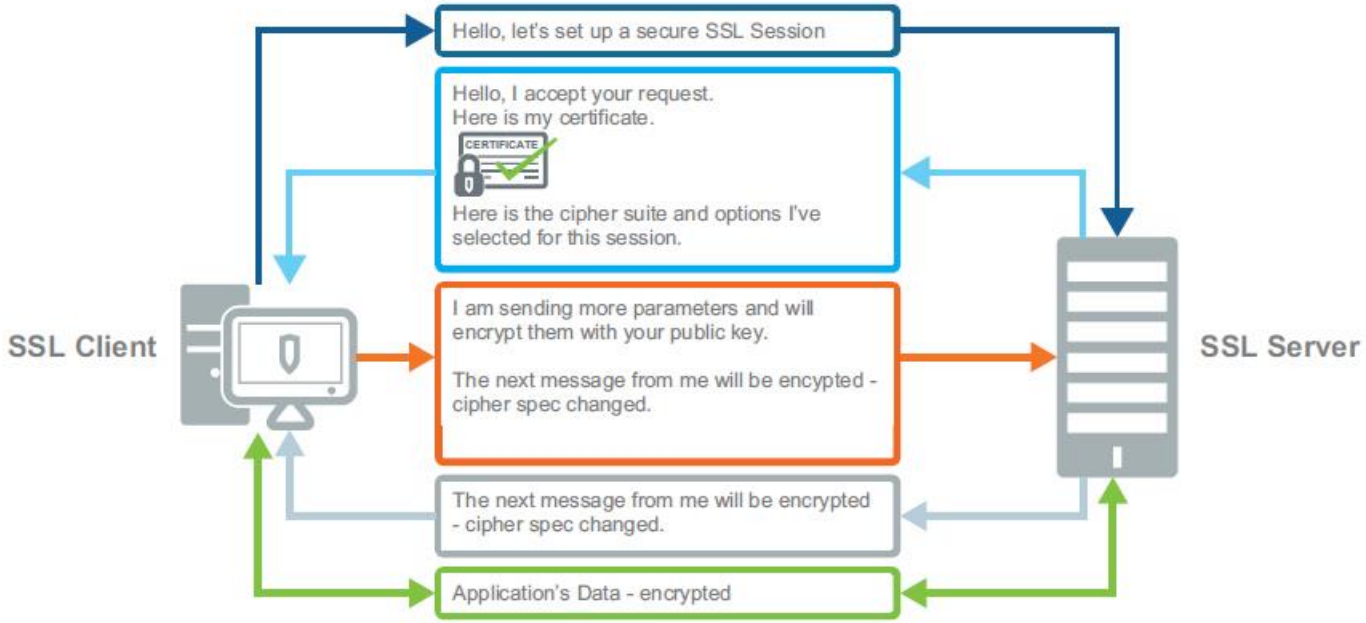
Certificate Authorities (CAs)

- **Certification Authorities (CAs):**
  A Certificate Authority (CA) is a trusted entity that generates and validates digital certificates to users, computers, applications, and services. The CA adds its own signature to the public key of the client. This essentially indicates that the public key can be considered valid, by those parties that trust the CA.

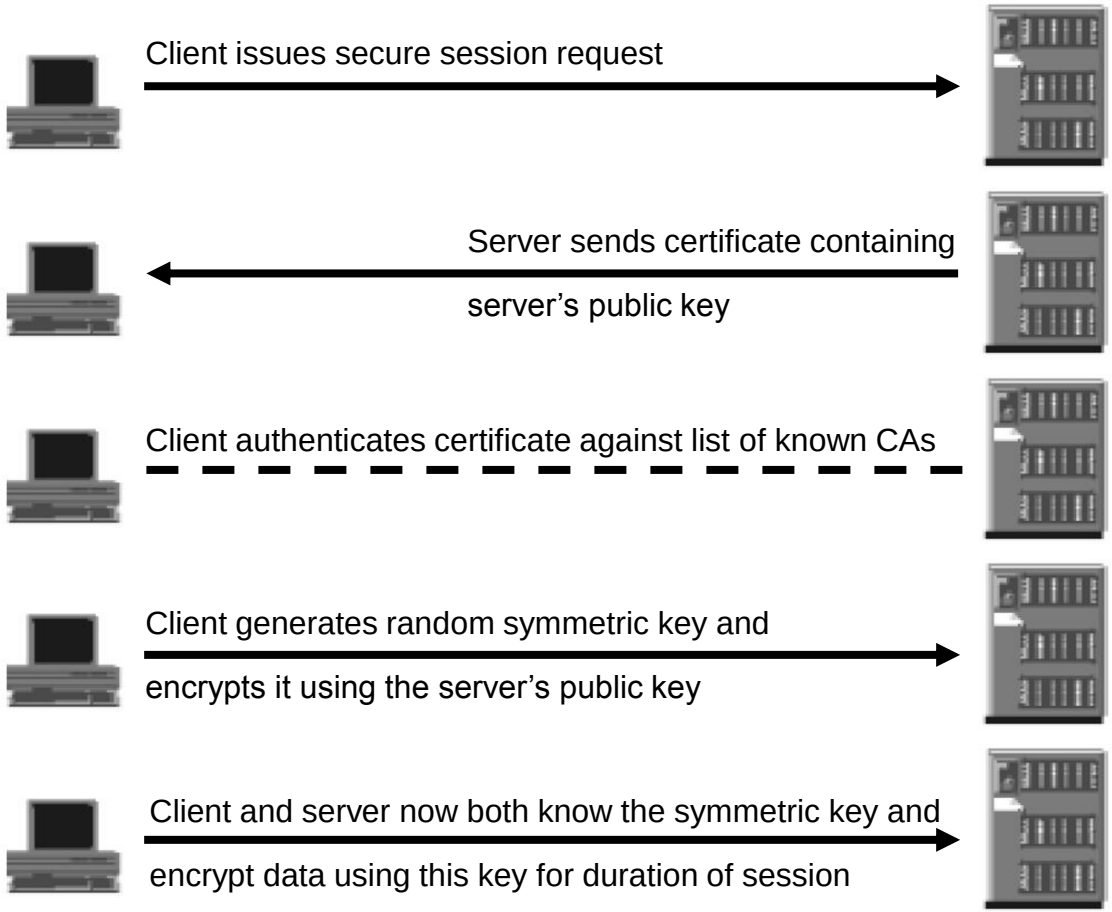
- CAs can be setup in a hierarchical structure, and define a CA trust model. In the CA hierarchy, you would define root CAs, intermediate CAs and leaf CAs. Users that trust the root CA would automatically trust all subordinate CAs beneath the root CA, which received certificates from the particular root CA.

Authentication & Encryption

- Client – Server Authentication
  - Client verifies server identify via certificate
- Exchanging keys for encryption



TLS – Secure Communication



TLS Encryption using PKI

- In order to prevent man-in-the-middle attacks, the public keys exchanged in the TLS handshake must be *certified*
- Usually, this is achieved by using X.509 certificates (SSL certificates) where 3rd party trust authorities (CAs) cryptographically bind *identities* to *public keys*

X.509 Certificates

- In TLS with X.509 certificates, the communication peer is identified via its DNS name (e.g. oscilloscope3.company-net.com) and/or its IP address (e.g. 192.168.0.4).

- For LXI devices, the IP address can change if the device is connected to a different network.
  This requires an update of the DNS entries.

Authorization

- Encryption of the communication channel is only the first step.
- Users authorized for using SCPI remote commands must identify themselves by providing a username and password or other authentication mechanisms.

IEEE 802.1AR Secure Device Identity

- IEEE 802.1AR provides cryptographically bound, unique identifiers for devices (DevIDs), which are composed of a secure device identifier secret and a secure device identifier credential.
- This standard uses options provided by X.509 specifications.
- IEEE802.1AR addresses the management and use of a single IDevID (**IDevID**, an Initial Device Identifier) and multiple LDevIDs certificates (**LDevID**, a subsequent Locally Significant Device Identifier derived from the IDevID).
- LDevIDs are bound to the IDevID in a way that makes it impossible for them to be transferred to a device with a different IDevID without knowledge of the private key used to effect the cryptographic binding.

IEEE 802.1AR – LXI Adoption

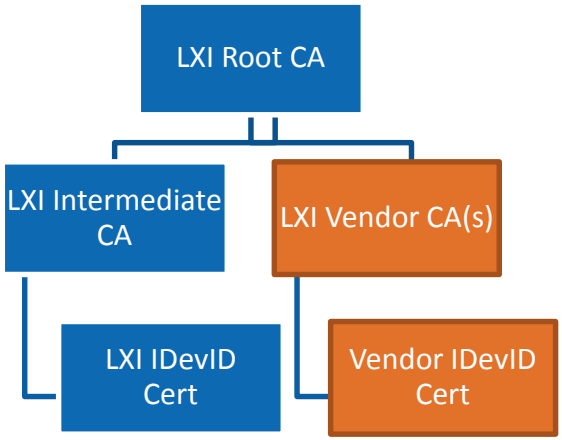
- DevIDs can be controlled by the vendor of the LXI device (IDevID) during the manufacturing process or by the end-user (LDevIDs) via a provisioning server.
- The IDevID certificate is also known as the “birth certificate” - used to identify the LXI device (serial #, model, vendor). This is typically the first certificate on the LXI device and generated during manufacturing.
- LDevIDs can incorporate, and fully protect, additional information like hostname and IP address of the LXI device for the DNS entries.
- Both, IDevIDs and LDevIDs are X.509 based certificates.
- IDevIDs are based on private root (“LXI Root CA”), LDevIDs are based on public root (Public CA).

Certificates for LXI Devices

- Certs used for Remote Control (SCPI):
  - IDevID (“LXI Root CA”) certificates with identity attributes such as: *Serial Number, Product Family, LXI Vendor*, *LXIDeviceDomain*
  - Standardized by LXI Consortium
  - Root of Trust: Root CA - LXI Device Vendor - Instrument
  - Deployment: Installation by LXI vendor (factory)
  - “Infinite” lifetime
- Certs for Web Browser Interface:
  - LDevID (X.509 certificate) derived from the IDevID of the LXI device
  - Problem: IP address of the LXI device may change
  - Solution: Update the DNS entries (IP address) via provisioning server

Private / Public Trust

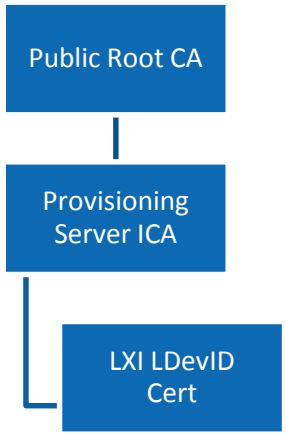
Private Trust: Secure Communications



Optional: Private Vendor ICA for companies that require one

- Cert format based on IEEE802.1AR / X.509
- IDevID
- Cert validity unlimited
- Metadata included in cert:
  Device serial #, Model, Vendor

Public Trust: Secure Web Servers



- Cert format X.509
- LDevID
- Maximum cert validity: 12 month

LXI Security WG Proposals

- Remote Control (SCPI):
  - Private trust model based on IDevIDs (LXI certs)
  - HiSLIP 2.0 which supports secure communication with TLS
  - Allows identification, authorization and encryption

- Web Browser Interface
  - Public trust model based on LDevIDs (X.509 certs)
  - Whenever the LXI device needs a LDevID for secure web server access (either nor present as in the initial state or the current LDevID is expired or revoked) it gets a new LDevID from the provisioning server
  - Whenever the LXI device gets a new IP address it has to assign and re-configure the host name (FQDN) to the new IP address and update the DNS entries via the provisioning server
  - Allows secure web server access

Remote Control with HiSLIP 2.0

- HiSLIP 2.0 supports secure communication with TLS 1.2 (and future protocol versions e.g. TLS 1.3)
- HiSLIP 2.0 uses still IANA port 4880
- Still using VISA resource string “tcpip::<hostname>::hislip<server>” to meet compatibility
- Introduce new security levels configured on the LXI device:

		Encryption (implies server authentication)	
		Optional	*Mandatory*
Client authentication required	*On*	Not supported	Mutual authentication
	Off	Permissive, allows fallback to HiSLIP 1	Not authenticated secure connection

HiSLIP Security Levels
Permissive

On level “Permissive” (Encryption is optional, client authentication is not required) the instrument supports both HiSLIP 1.0 and HiSLIP 2.0 clients and doesn’t require a TLS connection.

The user of the instrument may choose this mode for the following reasons:

- The client application or VISA application does not support HiSLIP 2.0.
- The user wants to inspect/debug the connection traffic with tools e.g. Wireshark
- The user wants to avoid performance loss by encryption
- By switching off encryption the user may accept the vulnerability of man-in-the-middle attacks
- A client can switch off encryption after successful authentication by `VI_ATTR_HISLIP_SECURITY=(NONE, ENCRYPTED)`

HiSLIP Security Levels

Server Authentication Only

In this level the encryption is mandatory, client authentication is not required. The purpose of this is to authenticate the server, encrypt the connection when any client is allowed to access.

The instrument only accepts HiSLIP connections with protocol versions >= V 2.0.

- Version negotiation (< 2.0) with legacy VISA client is blocked
- VISA client and instrument always use a TLS connection
- This level is implemented with an anonymous authentication

HiSLIP Security Levels

Mutual Authentication

The owner of the device may choose this mode within an untrustworthy environment:

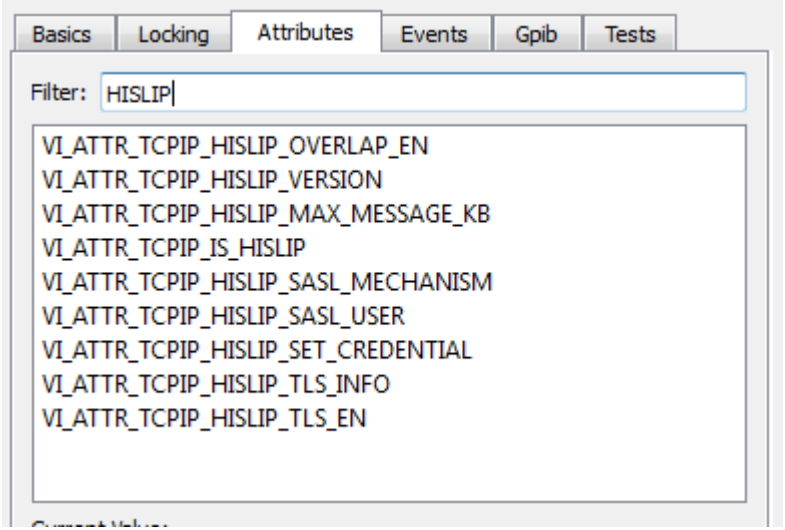
- Authentication of the server is required
- Only authorized clients are allowed to connect
- Only encrypted conversation is allowed
- Clients are not allowed to switch off encryption

This level is available for peer-to-peer secure communication between LXI devices

HiSLIP Authentication
Credential Management

- Authentication Mechanisms supported:
  - ANONYMOUS
  - GSSAPI (Kerberos)
  - NTLM (Windows Login)
  - PLAIN (Username/Password)

- VISA Security Extensions
  - New security attributes
  - Credential management from OS

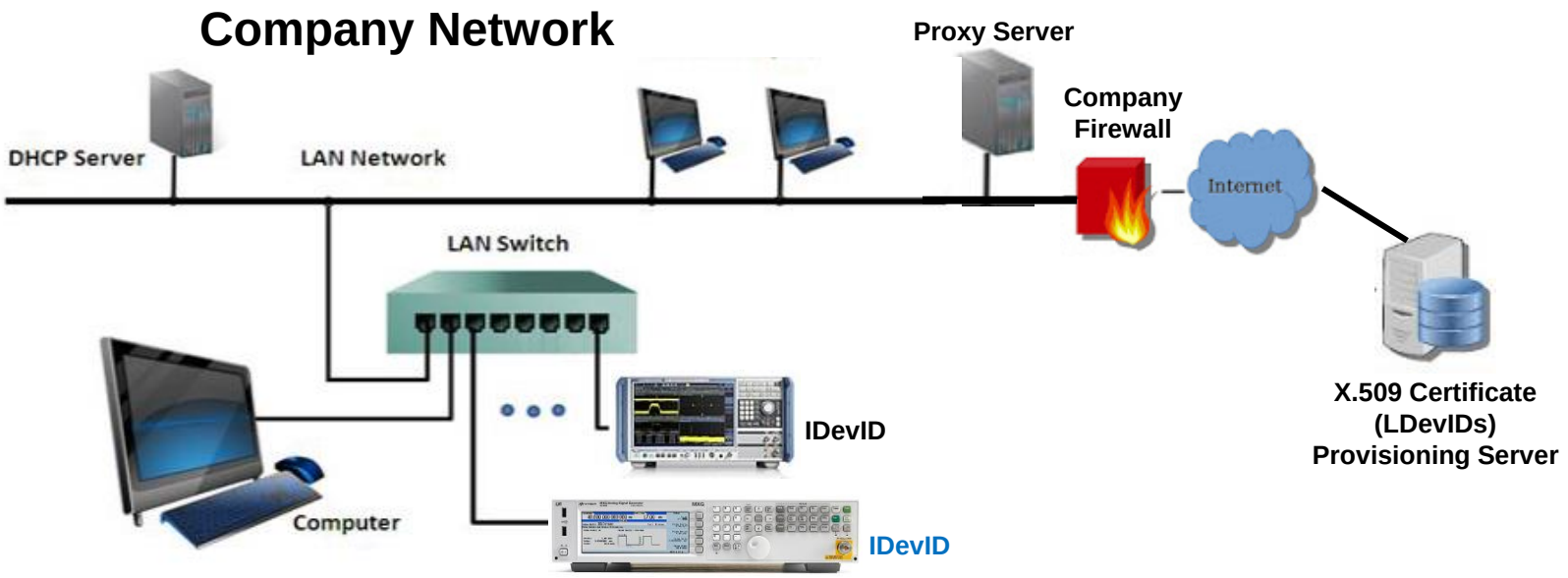


Web Browser Interface

Secure Web Browser Interface

- Secure web server access is based on HTTPS connections
- Public trust model – LDevIDs (X.509 certs)
- Whenever the LXI device needs a LDevID for secure web browser access (either nor present as in the initial state or the current LDevID is expired or revoked) it requests a LDevID via the provisioning server (Internet access required)
- Whenever the LXI device gets a new IP address it has to assign and re-configure the host name (FQDN) to the new IP address and update the DNS entries via the provisioning server (Internet access required)

X.509 Provisioning Server



Secure Web Browser Connection (1)

Pre-requisites:

- LXI Vendor:
  IDevID (LXI Cert) installed on the LXI device

- Customer/User:
  Proxy settings for company network ⇨ Internet access

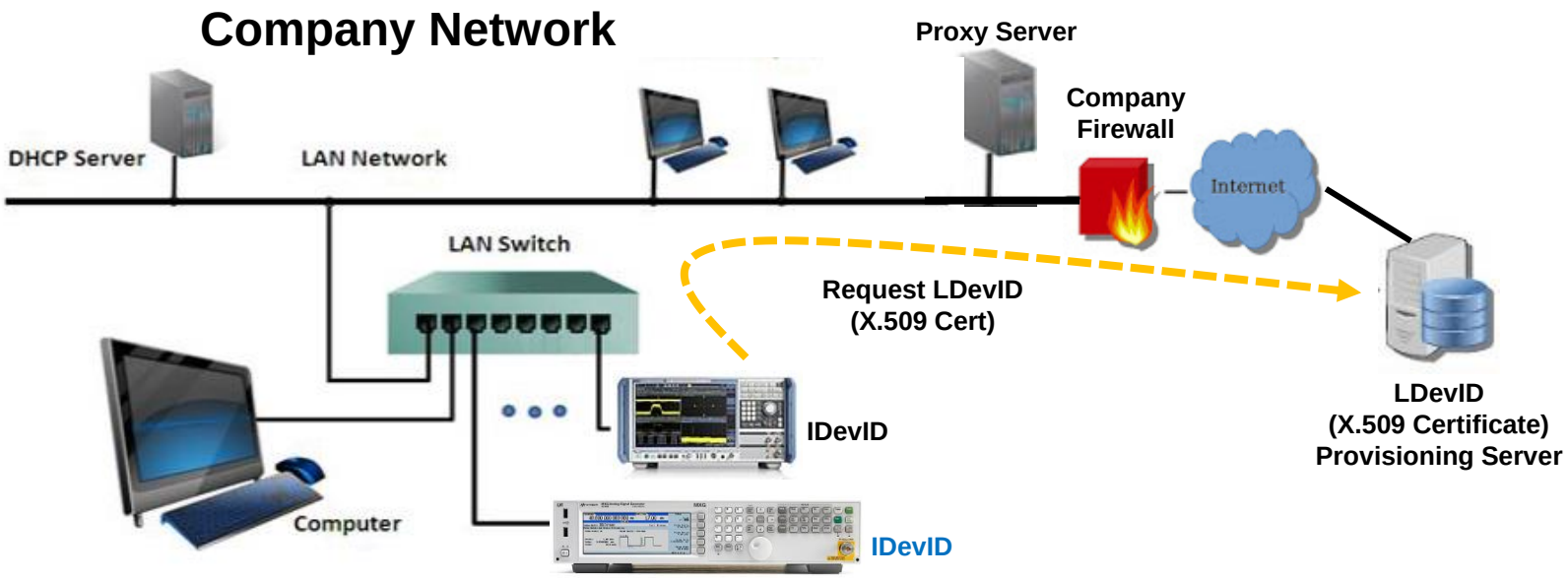
Secure Web Browser Connection (2)

Sequence (Step 1):

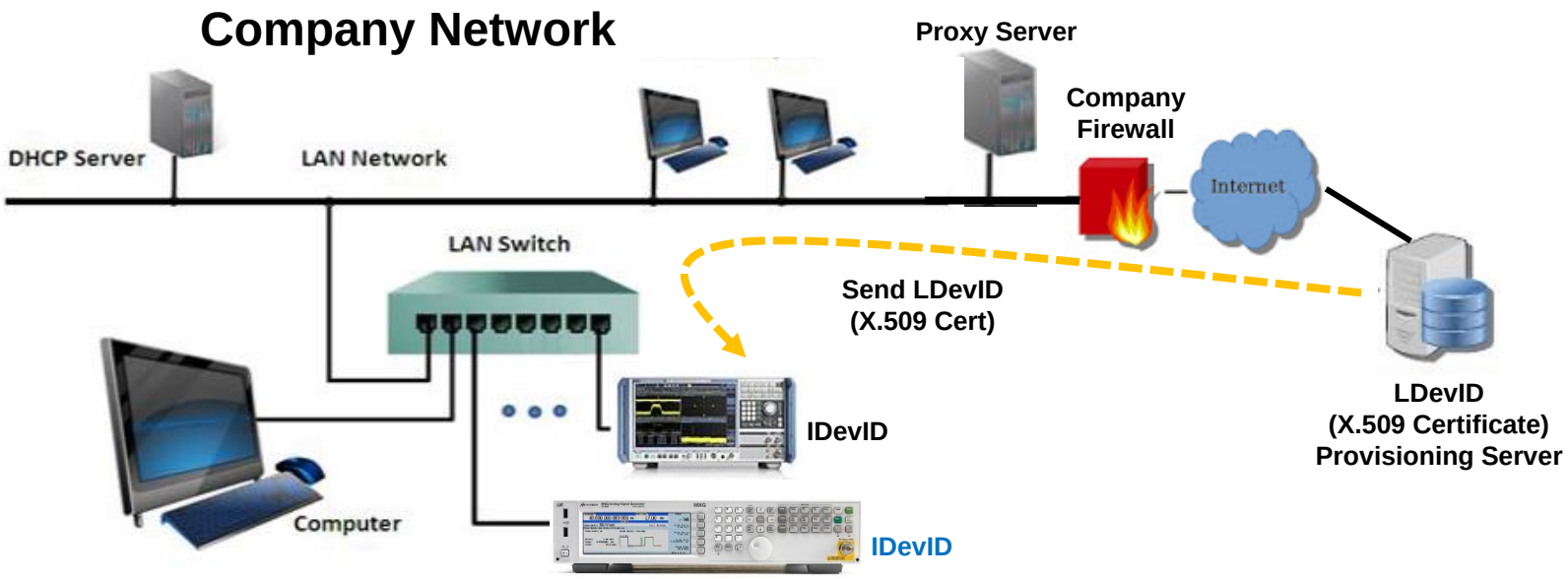
- LXI device:
  - Generate RSA key
  - Request X.509 certificate for the new key via company proxy server – Internet from the Provisioning Server using the IDevID (LXI Cert) for authentication/authorization
  - Communication to Provisioning Server encrypted (TLS) using the IDevID (LXI Cert)

- Provisioning server:
  - Authorize request from LXI device based on IDevID (LXI Cert)
  - Communication to LXI device encrypted
  - Provide signed LDevID (X.509 certificate) to LXI device

X.509 Provisioning Server



X.509 Provisioning Server



Secure Web Browser Connection (3)

Sequence (Step 2):

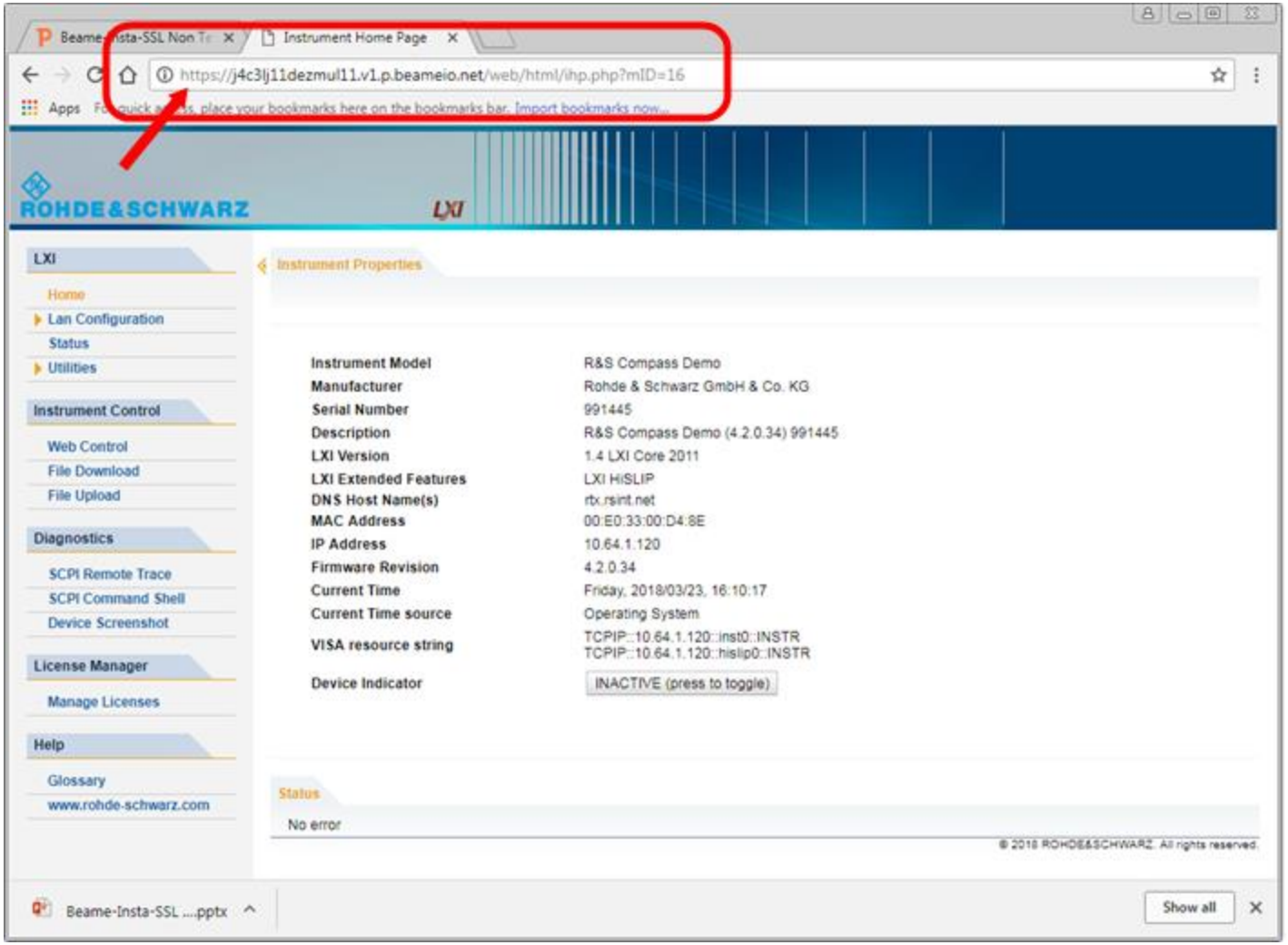
- LXI device:
  - Store signed LDevID (X.509 certificate) and install it on internal web server
  - Update DNS entries: Hostname (FQDN) and new IP address

Sequence (Step 3):

- Test computer:
  - Connect to LXI device via web browser (using host name)
  - Request https connection / encryption

- LXI device:
  - Setup encrypted (https) web server connection to test computer

Screenshots



IP Address Change

IP Address change:

- Whenever the LXI device gets a new IP address it has to assign and re-configure the host name (FQDN) to the new IP address and update the DNS entries via the provisioning server (Internet access required)

DNS Settings & Revocation Check

DNS settings:

- Host name (FQDN) is a LXI vendor specific custom domain name (Device serial #, model, vendor, LXIDeviceDomain)
  "LXIDeviceDomain" is common to all LXI devices:
  lxidevices.org

Revocation / Renewal Checks:

- IDevID revocation will be checked each time the LXI device connects to the provisioning server (OCSP)
- LDevID revocation will be checked by the web browser based on web browser policy

Local Network w/o Internet Access

Certificates issued by company internal CA (private root):

- Certificate is issued by customer PKI
- Install the certificate on the LXI device(s):
  Certificate (plus private key) is uploaded to the LXI device (REST, SCEP (Simple Certificate Enrollment Protocol) or CMP (Certificate Management Protocol) and user authentication/authorization)
- Install the root CA certificate on client systems (web browser(s) of the test computer)

Self-signed certificates:

- LXI Device creates self-signed certificate on demand
- Download certificate from device and install it manually in web browser(s) of the test computer

LXI Security – Questions

We are soliciting feedback and proposals to make sure the LXI Security WG covers all requirements

Send you comments and questions to the following email address: **LXI Security WG**