LXI 1.6 Update

www.lxistandard.org

Use the connection you already know!

LXI 1.6 in Summary

- Updated Device Spec
  - Incorporated the Clarification Document
  - Rule to support HTTPS Web server
    - Permission to still support HTTP if required
  - New URL alias: <hostname>/lxi to get to LXI Welcome Page
  - Enable/disable mDNS
  - Permission to have a blank password is now deprecated
- New Extended Functions
  - Security (see slides later on)
  - API (see later slides)

Extended Functions – no changes

- No changes to these Extended functions
  - Eventlog
  - Event Messaging
  - Timestamped Data
  - Wired Trigger Bus
  - VXI-11
  - Clock Synchronization
    - Still requires at a minimum IEEE1588-2008(v2) and not IEEE1588-2019 (v2.1)

Extended Functions – minor changes

- HiSLIP
  - Implement IVI HiSLIP 2.0 instead of 1.1
    - IVI HiSLIP 2.0 added rules for TLS and authenticated connections, but they are optional
    - Therefore, LXI HiSLIP does not require them either
    - If you implement the Security Extended function, then you do need to support TLS and authenticated connections

Extended Functions - major Changes

- IPv6
  - LXI IPv6 written 10 years ago
    - greater adoption of IPv6 especially in US Gov
    - RFC's have changed numerous time
    - NIST maintains the NIST IPv6 Profile. A definitive list of all current RFC's pertaining to IPv6.
  - IPv6 compliance rules vs. LXI IPv6 rules
  - Recommendations Static IP and DHCPv6 are now rules
  - Added rule to be able to enable/disable IPv4 or IPv6
  - Enable/Disable Privacy Setting now becomes a rule
  - Added rule that if you support any extended functions on IPv6 then they have to work on IPv6 as well. This was a recommendation previously. E.g Clock Sync, Event messaging.

Other Specifications

- Guide to LXI Documentation
  - List of all LXI specs with dates and versions for LXI 1.6
- LXI Example and Reference Material
  - The example screenshots of web pages, to show support for LXI 1.6, will be updated when the Reference Design gets released

LXI 1.6 Schedule

- LXI 1.6 Standard Schedule
  - 2/28/22: LXI Board approval to start the 45-day formal review process
  - 3/4/22: Start formal 45-day review process
  - 4/25/22: Review process complete, conduct voting member LXI 1.6 Standard approval vote
  - 5/9/22: Member voting complete; LXI Board LXI 1.6 Standard approval vote

- LXI 1.6 Reference Design Schedule
  - 2/25/22: Updated LXI Reference Design alpha version
  - 3/31/22: Code complete LXI 1.6 Reference Design
  - 6/30/22: Final version with any updates identified with TSEP Kerberos testing – LXI 1.6 compliant implementation

- LXI 1.6 Conformance Testing Using TSEP Kerberos Schedule
  - April 22: Start licensing of initial Kerberos LXI 1.6 updates
  - 6/30/22: Full conformance tests complete / released (LXI 1.6 Device, HiSLIP, IPv6, Security, API, all existing Extended Functions (not WTB))

LXI SharePoint / Notebook

- All 1.6 specs are here
  - LXI Website
    - https://lxistandard.org/Specifications/Specification2022.aspx
  - LXI SharePoint:
    - https://lxistandard.sharepoint.com/:f:/r/Shared%20Documents/Technical%20Committee/Specifications/Under%20Construction/v1.6/Standard/Review/Specs?csf=1&web=1&e=yYirUh

- Detailed Summary of Spec Changes in LXI Notebook:
  - Changes from 1.5 to 1.6 (Web view)

LXI Security Overview

(with IVI)

Customer Updates 2021-10-14

www.lxistandard.org

Use the connection you already know!

Purpose of IVI/LXI Security

- Establish response to strong customer request for security
  - Including practical requirement for interoperability
- Establish a security baseline that customers can reference
- Setup an LXI CA to sign IDevIDs
- Companies working together to understand customer needs

- Security is Complex:
  - 213(API)+17(Security) RULES
  - Device spec: 75 rules

Status

- LXI has completed a “stable” draft of the LXI Security and LXI API extended functions
  - Will wait for completion of a trial implementation to ballot
  - Doing some rework of LXI IPv6 requirements, will impact the schema
- IVI has completed a first draft of VISA-C to support security
  - Impacts Drivers, since they only require secure address string
- IVI support for VISA.NET/VISA-COM drafts are ready for ballot

LXI Security Standard Provisions

- HTTPS (which will be required in LXI Device specification 1.6)
- SCPI must provide a secure connection
  - HiSLIP
  - Raw SCPI over TLS, Telnet in scope of specification
- Optional Client Authentication
- Flexible Configuration via REST API
  - Device configuration needed for security
  - Client credentials to the device
  - Manage the device credentials (certificates)

LXI Authentication

- Device authentication using IDevID or LDevID
  - IDevID
    - LXI has a CA and will sign certificates for members
    - Devices may self-sign, or use other CAs
  - LDevID
    - Standard provisioning and management of LDevID with REST API
- Client authentication using either:
  - Username and Password
  - Fingerprinted certificates
  - Certificates authenticated based on a root certificate

LXI Authorization

- Authorization only provided for the API
  - No concept of certain instrument users can access certain functions
  - Generally, users only need to be authenticated
- API KEY
  - Client provides a shared secret key with every API call
- Username/Password
  - The client user list includes a tag of API-authorized users
  - Utilizes HTTPS security scheme to pass username and password

LXI Configuration API

- The API is currently just for security, may be extended
- Common Configuration
  - Single document with:
    - Device configuration
    - Client credentials
  - Goal to permit same Common Configuration for all devices in a system
- Device-specific/Automatic Configuration
  - Basic network parameters (DNS,DHCP, addresses, SLAAC, etc)
- General read/write support
  - Get capability information on a read

Protocol Configuration

```
<Interface name="lxi" enabled="true" insecureMode="true" LXIConformant=""
        otherInsecureProtocolsEnabled="true">
    <Network>
        <IPv4 enabled="true" DHCPEnabled="true" autoIPEnabled="true" dynamicDNSEnabled="true" />
        <IPv6 enabled="true" DHCPEnabled="true" dynamicDNSEnabled="true"
                mDNSEnabled="true" pingEnabled="true" prefix="123"
                privacyModeEnabled="true" SLAACEnabled="true"  />
    </Network>
    <HTTP  operation="enable" port="80" />
    <HTTPS clientAuthenticationRequired="true" port="443">
        <Basic enabled="false" />
        <Digest enabled="true"/>
        <Service name="LXIAPI" enabled="true" />
    </HTTPS>
    <SCPIRaw enabled="true" port="5025" />
    <Telnet enabled="true" clientAuthenticationRequired="false" port="5024" TLSRequired="true"/>
    <SCPITLS port="5026" capability="99" clientAuthenticationRequired="true" enabled="true" />
    <HiSLIP enabled="true" port="4880" encryptionMandatory="true"  mustStartEncrypted="true">
        <ClientAuthenticationMechanisms>
            <PLAIN enabled="true"></PLAIN>
            <SCRAM enabled="true"></SCRAM>
            <MTLS enabled="true"></MTLS>
        </ClientAuthenticationMechanisms>
    </HiSLIP>
    <VXI11 enabled="true" />
</Interface>
```

Client Credentials

```
<ClientAuthentication>
        <ClientCredential APIAccess="true" password="secret" user="Suzie"/>
        <ClientCredential APIAccess="false" password="supersecret" user="Billy"/>
        <ClientCertAuthentication>
            <RootCertPEM>
                -----BEGIN CERTIFICATE-----
                MIIEczCCA1ugAwIBAgIBADANBgkqhkiG9w0BAQQFAD..AkGA1UEBhMCR0Ix
                EzARBgNVBAgTClNvbWUtU3RhdGUxFDASBgNVBAoTC0..0EgTHRkMTcwNQYD
                VQQLEy5DbGFzcyAxIFB1YmxpYyBQcmltYXJ5IENlcn..XRpb24gQXV0aG9y
                aXR5MRQwEgYDVQQDEwtCZXN0IENBIEx0ZDAeFw0wMD..TUwMTZaFw0wMTAy
                MDQxOTUwMTZaMIGHMQswCQYDVQQGEwJHQjETMBEGA1..29tZS1TdGF0ZTEU
                MBIGA1UEChMLQmVzdCBDQSBMdGQxNzA1BgNVBAsTLk..DEgUHVibGljIFBy
                aW1hcnkgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxFD..AMTC0Jlc3QgQ0Eg
                THRkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCg..Tz2mr7SZiAMfQyu
                AQH/MA0GCSqGSIb3DQEBBAUAA4IBAQC1uYBcsSncwA..DCsQer772C2ucpX
                xQUE/C0pWWm6gDkwd5D0DSMDJRqV/weoZ4wC6B73f5..bLhGYHaXJeSD6Kr
                XcoOwLdSaGmJYslLKZB3ZIDEp0wYTGhgteb6JFiTtn..sf2xdrYfPCiIB7g
                BMAV7Gzdc4VspS6ljrAhbiiawdBiQlQmsBeFz9JkF4..b3l8BoGN+qMa56Y
                It8una2gY4l2O//on88r5IWJlm1L0oA8e4fR2yrBHX..adsGeFKkyNrwGi/
                7vQMfXdGsRrXNGRGnX+vWDZ3/zWI0joDtCkNnqEpVn..HoX
                -----END CERTIFICATE-----
            </RootCertPEM>
            <CertThumbprint hash="SHA-256" thumbPrint="4281B2V490b84a129weff08908fsdjfksljf" />
        </ClientCertAuthentication>
    </ClientAuthentication>
```

LXI Certificate Management API

- Several conventional REST APIs to:
  - List certs
  - Delete a cert
  - Get a cert
  - Get a Certificate Signing Request, then Put signed certificate
  - Request the device generate a self-signed certificate

- No LXI requirement for SCEP or EST
  - EST seems the ‘proper’ well-written secure standard, but limited support in IT infrastructures
  - SCEP is commonly used, but implementations are a little divergent
  - Configuration, debug, and scalability all concerns
  - The API makes it practical for a client to integrate into any system

IVI Address for Drivers and VISA

- The address string has decoration of “Credential Information”

  `TCPIP0::DevCredentials@192.168.1.0::INSTR`

  - Identifier includes how VISA:
    - Authenticates itself to the device
    - Authenticates the device
  - Vendor-specific configuration completed outside of VISA
- Optional syntax permits credentials directly in string (vendor specific)
  - ***Contentious***, some vendors refuse to implement (security concerns)
- Why do it this way?
  - Vendors utilize their own scheme to *secure* the credential information
  - Vendors create their own applications software to collect and store credentials (difficult for consortium)

IVI Extensions for Security

- VISA-C with Address string updates, completed early 2021
  - Additional APIs to acquire device certificate and various fields
  - Address strings per previous slide
- VISA-COM, VISA.NET, minor changes, ready for ballot
- No changes identified for drivers – only address strings needed

Future Priorities (Need Input!)

- Certificate Enrollment using standard protocols
  - Do we use EST, SCEP or something else?
  - What does a customer need to debug and configure?
- Port-based network access control
  - IEEE 802.1X and subsequent standards
  - How common is this in T&M systems? Is MAC registration adequate?
- More complete User Authorization solution
  - What users are allowed to do what?
- Participation in federated/SSO systems for user Authentication and Authorization
  - What systems to support? (MSFT Active Directory)
  - How to use information?