LXI Security
Extended Function

Revision 1.1

January 26, 2023

Notices

Notice of Rights All rights reserved. This document is the property of the LXI Consortium. It may be reproduced, unaltered, in whole or in part, provided the LXI copyright notice is retained on every document page.

Notice of Liability The information contained in this document is subject to change without notice. "Preliminary" releases are for specification development and proof-of-concept testing and may not reflect the final "Released" specification.

The LXI Consortium, Inc. makes no warranty of any kind with regard to this material, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The LXI Consortium, Inc. shall not be liable for errors or omissions contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

LXI Standards Documents are developed within the LXI Consortium and LXI Technical Working Groups sponsored by the LXI Consortium Board of Directors. The LXI Consortium develops its standards through a consensus development process modeled after the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Consortium and serve without compensation. While the LXI Consortium administers the process and establishes rules to promote fairness in the consensus development process, the LXI Consortium does not exhaustively evaluate, test, or verify the accuracy of any of the information contained in its standards.

Use of an LXI Consortium Standard is wholly voluntary. The LXI Consortium and its members disclaim liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other LXI Consortium Standard document.

The LXI Consortium does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. LXI Consortium Standards documents are supplied "as is". The existence of an LXI Consortium Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the LXI Consortium Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every LXI Consortium Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any LXI Consortium Standard.

In publishing and making this document available, the LXI Consortium is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the LXI Consortium undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other LXI Consortium Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

This specification is the property of the LXI Consortium, a Delaware 501c3 corporation, for the use of its members.

Interpretations Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of LXI Consortium, the Consortium will initiate action to prepare appropriate responses. Since LXI Consortium

Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, LXI Consortium and the members of its working groups are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. Requests for interpretations of this standard must be sent to interpretations@lxistandard.org using the form "*Request for Interpretation of an LXI Standard Document*". This document plus a list of interpretations to this standard are found on the LXI Consortium's Web site: http://www.lxistandard.org

Trademarks Product and company names listed are trademarks or trade names of their respective companies. No investigation has been made of common-law trademark rights in any work.

LXI is a registered trademark of the LXI Consortium

Patents: Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. A holder of such patent rights has filed a copy of the document "*Patent Statement and Licensing Declaration"* with the Consortium. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. Other patent rights may exist for which the LXI Consortium has not received a declaration in the form of the document "*Patent Statement and Licensing Declaration*". The LXI Consortium shall not be held responsible for identifying any or all such patent rights, for conducting inquiries into the legal validity or scope of patent rights, or determining whether any licensing terms or conditions are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility.

Conformance The LXI Consortium draws attention to the document "*LXI Consortium Policy for Certifying Conformance to LXI Consortium Standards*". This document specifies the procedures that must be followed to claim conformance with this standard.

Legal Issues Attention is drawn to the document "*LXI Consortium Trademark and Patent Policies*". This document specifies the requirements that must be met in order to use registered trademarks of the LXI Consortium.

Revision history

Revision	***Description***
1.0 2022-05-10	Initial Version
1.0 2022-05-24	This revision updates the term ‘insecure’ to ‘unsecure’ throughout the document.
1.1 2023-01-26	Added rules regarding NIST 800-52 (TLS version and cipher suites)

22 LXI Security Extended Function

The LXI Security Extended Function adds support for securing the Command-and-Control Interface to the device, making secure connections and authentication with the device Web Server, and adding a REST API for configuring security settings

22.1 Purpose and Scope of this Document

This document is an extension of the LXI Device Specification 2021. Numbering for Section, **RULES,** and **RECOMMENDATIONS** is consistent with the hierarchy of the LXI Device Specification 2021.

22.1.1 Purpose

The purpose of the LXI Extended function is:

- The LXI Security Extended Function specifies device behavior that enables clients to establish secure connections to devices. The required device capabilities include:
- Protocols and capabilities to support secure communication
- Requirements that devices permit more extensive configuration of protocols required by other LXI specifications
- APIs to configure the capabilities of interest to secure applications and provision certificates to devices
- The primary goals for security within industrial networks are following the key principles Confidentiality, Integrity and Authenticity. Confidentiality ensures that data transported in the network cannot be read by anyone but the intended recipient. Integrity means any message received is confirmed to be exactly the message that was sent and finally Authenticity ensures that a message that claims to be from a given source is, in fact, from that source.
- Secure communication between test computers and LXI devices requires encryption and authentication. The LXI Security Extended Function supports authenticated and encrypted communication to T&M instruments and also addresses security for LXI device hosted webpages, confirming device authenticity and providing secure communication.

22.1.2 Scope

This document defines a set of **RULES** and **RECOMMENDATIONS** for constructing a LXI Device conformant with the LXI Security Extension. Whenever possible these specifications use existing standards.

The standard specifies:

1. LXI Security Extended Function Operation Rules
2. LXI Security Extended Function Interface Requirements
3. LXI Security Extended Function PKI Requirements
4. LXI Security Extended Function Command-and-Control Requirements

5. LXI API Extended Function Requirements (this extended function is defined in an additional document)

22.2 Definition of Terms

This document contains both normative and informative material. Unless otherwise stated the material in this document shall be considered normative.

NORMATIVE: Normative material shall be considered in determining whether an LXI Device is conformant to this standard. Any section or subsection designated as a RULE or PERMISSION is normative.

INFORMATIVE: Informative material is explanatory and is not considered in determining the conformance of an LXI Device. Any section or subsection designated as RECOMMENDATION, SUGGESTION, or OBSERVATION is informative. Unless otherwise noted examples are informative.
RULE: Rules **SHALL** be followed to ensure compatibility for LAN-based devices. A rule is characterized by the use of the words **SHALL** and **SHALL NOT**. These words are not used for any other purpose other than stating rules.

RECOMMENDATION: Recommendations consist of advice to implementers that will affect the usability of the final device. Discussions of particular hardware to enhance throughput would fall under a recommendation. These should be followed to avoid problems and to obtain optimum performance.

SUGGESTION: A suggestion contains advice that is helpful but not vital. The reader is encouraged to consider the advice before discarding it. Suggestions are included to help the novice designer with areas of design that can be problematic.

PERMISSION: Permissions are included to clarify the areas of the specification that are not specifically prohibited. Permissions reassure the reader that a certain approach is acceptable and will cause no problems. The word **MAY** is reserved for indicating permissions.

OBSERVATION: Observations spell out implications of rules and bring attention to things that might otherwise be overlooked. They also give the rationale behind certain rules, so that the reader understands why the rule must be followed. Any text that appears without heading should be considered as description of the specification.

22.3 Relationship to other LXI Standards

This specification impacts several of the rules and recommendations in the LXI Device Specification and other LXI Extended Functions. In every case, the rules and recommendations in this specification supersede the other LXI standards. Devices that claim compliance to the LXI Security Extended Function shall follow all the rules specified in this document.

The LXI specifications with rules that are either extended or modified by this specification are:

LXI Device Specification

LXI HiSLIP Extended Function

LXI IPv6 Extended Function

22.4 References

This specification relies heavily on security standards created by other organizations such as the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronic Engineers (IEEE).

Several of these specifications are under continual improvements. Generally, where a referenced standard has a successor LXI devices should comply with the most recent version of the specification.

Several of the specifications noted below have extensions as well. Generally, LXI devices should be designed accounting for the complete specification and any extensions.

Some of the key references are:

IEEE802.1AR	Secure Device Identity Specification
RFC5280	Internet X.509 Public Key Infrastructure Certificate and CRL Profile
RFC 5246/8446	Transport Layer Security (TLS). Version 1.2 and 1.3
RFC 7235	HTTP Authentication Framework
RFC 7616	HTTP Digest Mechanism
RFC 7617	HTTP Basic Mechanism
TPM Specs	Trusted Computing Group Trusted Platform Module (TPM) specifications
HiSLIP	IVI Foundation HiSLIP specification (IVI-6.1)
SCPI	IVI Foundation SCPI specification
NIST 800-52	NIST Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

22.5 Terminology

The following terms are used throughout this specification.

22.5.1 LXI Security

The full reference to this specification is the LXI Security Extended Function. For clarity and brevity, it is generally referred to as *LXI Security* in this document.

22.5.2 Command-and-Control Interface

LXI devices usually provide a mechanism for remote clients to programmatically control, read data from or write data to the device to perform LXI device functions. Popular approaches include:

Instrument command interfaces (such as SCPI) via TCP, HiSLIP, or VXI-11

REST interfaces via HTTP or HTTPS

In this specification, these mechanisms are referred to as Command-and-Control interfaces. Command-and-Control interfaces include SCPI, REST, and other interfaces that provide the end user programmatic access to the LXI device.

When the term is used in this document, it refers to Ethernet-based communication. Devices frequently implement other communication interfaces such as USB and GPIB.

22.6 Acronyms

The following acronyms are used in this specification:

API	Application Program Interface
CA	Certificate Authority
CMS	Cryptographic Message Syntax, as defined by RFC 5652 or its successors
CSR	Certificate Signing Request
DevID	Device Identifier as defined by IEEE 802.1AR. When used in this document, the clarifications in section 22.12.1, *RULE – IEEE 802.1AR Compliance,* are assumed.
EST	Enrolment over Secure Transport (RFC 7030)
HiSLIP	High-speed LAN Instrument Protocol
HTTP	Hyper-text transfer protocol
HTTPS	Hyper-text transfer protocol performed over a TLS connection
IDevID	Initial Device Identifier as defined by IEEE 802. 1AR. When used in this document, the clarifications in section 22.12.1, *RULE – IEEE 802.1AR Compliance,* are assumed.
IVI	IVI Foundation (responsible for various standards referenced here)
LCI	LAN Connection Initialize
LDevID	A locally significant Device Identifier, as defined by IEEE 802.1AR, this is a DevID provisioned to the instrument by the end-customer. When used in this document, the clarifications in section 22.12.1, *RULE – IEEE 802.1AR Compliance,* are assumed.
LXI	LAN Extensions for Instruments
PEM	Stands for Privacy Enhanced Mail, although the use in this specification is to refer to the conventional PEM File format for representing X.509 certificates.
PKI	Public Key Infrastructure
REST	Refers to an HTTP API. Stylistically, an API organized as a Representational State Transfer API.
SCPI	Standard Commands for Programmable Instruments
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPM	Trusted platform module
XML	Extensible Mark-up Language

22.7 Compliance Requirements

For a device to comply with this specification the device is required to comply with:

- LXI Device specification version 1.6 or later
- LXI API Extended Function methods listed in 22.14, *RULE – LXI API Security Methods.*
- The rules called out in this specification

This includes requirements explicitly called out as rules and any behavior or requirement that states that devices *shall* behave in a certain fashion or provide a certain capability.

22.8 RULE – LXI Security Web Interface

Devices implementing the LXI Security Extended Function shall include 'LXI Security' in the 'LXI Extended Functions' display item of the welcome web page.

22.8.1 RULE – LXI Security Web Page Unsecure Mode Indication

LXI Secure devices shall provide an indication on the LXI welcome web page if they are currently operating in the *Unsecure Mode*.

Observation

> The LXI welcome page is not necessarily the instrument welcome page nor the instrument landing page. See the LXI Device specification for details.

22.9 RULE – LXI Security XML Identification Document

Devices implementing LXI Security extended function shall include *Function* elements for the LXI Security Extended Function. The *Function* element are contained in the XML *Device* element. With the *FunctionName* attribute of "LXI Security" and a *Version* attribute containing the version number of this document.

The *Function* element shall have a child element, *CryptoSuites,* which indicates the cryptographic suites supported by the device in a comma-separated list.

Example:

```
<Function FunctionName="LXI Security" Version="1.0">
   <CryptoSuites>name,name<CryptoSuites/>
<Function/>
```

Observation

> The names of the listed crypto suites may be sent to the instrument using the LXI API extended function to specify the crypto suite to use for a certificate.

22.10 Operation

This section contains rules and recommendations related to general device operation.

22.10.1 RULE – Unsecure Mode

An LXI Secure device is regarded as operating unsecurely if its configuration enables protocols or behaviors that are known to be unsecure. If any part of a device configuration is known to explicitly enable unsecure operation, the device is operating in the *Unsecure Mode*.

If any device setting is in an unsecure configuration, the device is operating unsecurely. The LXI API Extended function identifies LXI-specific device configuration settings that are unsecure. In addition, devices shall determine if device-specific settings put the instrument into an unsecure mode. Generally:

> *A device is operating in a known unsecure mode if a client can change the device measurement/stimulus/routing configuration or measurement results over an ethernet connection that does not authenticate the device (server) and provide encryption.*

Devices provide an API that interrogates if the device's current configuration is in an *Unsecure Mode*. See the LXI API Extended Function.

Observation

> The LXI API Extended Function reports if individual Ethernet interfaces are operating in Unsecure Mode. The Device unsecure state is the logical OR of each interfaces unsecure mode. Devices presumably will report the Device unsecure state from the human interface.

Observation

> LXI does not make the assertion that a device is in a secure operating mode if it is NOT in the Unsecure Mode. Such an assertion cannot be made without qualifications that are beyond the scope of LXI. Therefore, LXI assertions are limited to asserting that the device is not in a known unsecure mode however, that may not meet all the customers' needs for security.

22.10.1.1 RULE – Vendors Shall Indicate Unsecure for non-LXI device Settings

Devices shall also indicate they are operating in an Unsecure Mode if settings beyond the scope of LXI Security are considered by the device manufacturer to be unsecure.

22.10.2 RULE – Multiple LAN Interfaces supporting LXI Security

If multiple LAN network interface cards (NICs) are present in an LXI Secure device, those that are LXI compliant shall support the LXI Security Extended Function.

Observation

> The security settings may be independently configured for each LXI compliant NIC.

22.11 Interface Requirements

22.11.1 RULE – Support IPv4 Secure Configuration

All LXI Devices implement IPv4. LXI Secure devices shall implement the secure requirements for IPv4 in this section and the required security methods of the LXI API Extended Function specification.

22.11.2 RULE – Support IPv6 Secure Configuration

Devices that implement IPv6 capability and LXI Security shall implement the secure requirements for IPv6 in this section and the required security methods of the LXI API Extended Function specification. This requirement shall be followed regardless of if a device complies with the LXI IPv6 extended function.

22.11.3 RULE – Ignore mDNS Unicast Queries From Outside the Local Link

Since it is possible for an mDNS unicast query to be received from a machine outside the local link, LXI Secure devices shall check that the source address in the mDNS query packet matches the local subnet for that link (or, in the case of IPv6, the source address has an on-link prefix) and silently ignore the packet if not. This behavior is as recommended in RFC6762.

22.11.4 HTTPS Changes from Device Specification

The LXI Device specification rev 1.6 or later requires that devices provide an HTTP and HTTPS server (HTTP over TLS) and that certain privileged operations be forwarded to HTTPS and protected using the LXI password. However, devices that also comply with LXI Security differ in that they do not have the LXI password defined in the LXI Device specification. Instead, they use the username/password pairs managed by the LXI Security API. For details, see the LXI Common Configuration API as referenced in 22.14, *RULE – LXI API Security Methods*.

22.11.5 RULE – Use TLS Version Specified by NIST 800-52

Device TLS implementations shall be able to restrict the TLS version to those permitted by the TLS version guidelines for TLS servers in the version of NIST 800-52 that is current at the time the device goes through LXI compliance testing.

If a device is awarded LXI conformance based on technical justification, it shall be able to restrict the TLS versions to those required by this rule at the time that the new device is presented for conformance.

22.11.6 RULE – Use Cipher Suites Permitted by NIST 800-52

Devices shall have the ability the restrict the cipher suites to those permitted for TLS servers in the version of NIST 800-52 that is current at the time that the device goes through LXI compliance testing.

If a device is awarded LXI conformance based on technical justification, it shall be able to restrict accepted cipher suites to those required by this rule at the time the new device is presented for conformance.

22.12 PKI Requirements

This section has requirements associated with how a device participates in a public key infrastructure to authenticate its identity.

Note that central to these requirements are the LXI Security APIs which provide the capability to acquire a certificate signing request, provision a certificate, and manage certificates.

22.12.1 RULE – IEEE 802.1AR Compliance

Devices shall comply with the device requirements stated in IEEE 802.1AR with the following caveats:

1. IEEE 802.1AR has a detailed description of the DevID module. In general, LXI Secure device software has no such module externally visible, thus those requirements do not directly bear on an LXI device although the device implementation is expected to substantially follow those requirements. This may be ideally accomplished through either a physical or firmware TPM in conjunction with the LXI Security API.

   LXI Security does require an API that includes several certificate management features similar to the DevID Module requirements, see the LXI API Extended Function.

2. IEEE 802.1AR 6.4 implies that DevID certificates can be validated using a CA root certificate as the trust anchor. Although not clearly in conflict with IEEE 802.1AR, LXI Security explicitly permits devices to use self-signed certificates in their DevID, thus making the self-signed certificate itself the trust anchor.

3. IEEE 802.1AR section 5.5, *Supplier Requirements,* places several requirements on the supplier which are beyond the scope of LXI and are not placed on the device vendor by LXI.

22.12.2 RULE – Use the Most Recently Provisioned DevID

If any LDevID has been provisioned to the device, the IDevID shall not be used, regardless of the cryptographic suite of the LDevID.

Unless explicitly configured otherwise, devices shall use the most recently provisioned valid certificate for each cryptographic suite that the device supports to authenticate itself regardless of the protocol being used.

Observation

Note that 22.12.2, *RULE – Use the Most Recently Provisioned DevID*, requires that devices initially use the IDevID

Observation

Most browsers will warn about the IDevID. It potentially warns for the following reasons:

- The IDevID never expires
- Depending on how the IDevID is signed and the authorities in the browser's trust store, the browser may not trust the root authority.

Observation

There may be multiple ways to provision DevIDs to a device, including the LXI API and device-specific mechanism such as EST, SCEP, or physically copying to the device.

22.12.3 IDevID Requirements

This section has requirements related to the IDevID defined by IEEE 802.1AR.

The information for the **Subject DN** attributes must be provided by the LXI manufacturer for each LXI Device so unique IDevIDs can be installed during the manufacturing process on each LXI Device.

LXI permits multiple OUs.

22.12.3.1 RULE – Distinguished Name

Subject Distinguished Name (DN) – field shall have the following attributes:

Attribute Name	Description	Max Size	Example	Data Type	Notes
CN	Common Name	64	XYZ Oscilloscope 54321D – 123456	UTF8	LXI default mDNS description name (Alternative: Instrument serial number)
O	Organization Name	64	Keysight	UTF8	This is the LXI manufacturer Static field for each LXI manufacturer
OU	Organization Unit Name	64	MXA9020B,Opt U3	UTF8	Instrument model name

Attribute Name	Description	Max Size	Example	Data Type	Notes
Serial Number	Instrument Serial Number	64	CO0123456789	UTF8	This is the instrument serial number

22.12.3.2 RULE – Subject Alternate Name

Devices that have a hardware or firmware TPM shall have a SAN field that contains:

Name	Description	Max Size	Example	Data Type	Notes
SAN	HW Module Name (HMN)	NA (as required)	<hex encoded TPM identifier>	DER Encoded	This is a two field ASN.1 entry that identifies the TPM version and serial number. This is required for both hardware and firmware TPMs. This is an OID as specified in the Technical Computing Group and cited in IEEE 802.1AR. Note that there are versions for TPM 1.2 and 2.0.

Observation

> LXI does not require either OCSP or CRLs for IDevIDs. LDevIDs are more appropriate to ascribe a high degree of trust to a device, so complex revocation infrastructure for IDevIDs is only provided at the vendor's discretion.

22.13 Command-and-Control Requirements

This section has general rules regarding the device Command-and-Control interfaces.

22.13.1 RULE – Secure Command-and-Control Interface

Devices shall provide at least one secure Command-and-Control interface. That is, a protocol that provides encryption and server authentication (e.g., IVI HiSLIP rev2.0, HTTPS, etc.).

22.13.2 RULE – Client Authentication Configuration

At least one Command-and-Control protocol shall provide a configuration that requires client authentication.

22.13.3 RULE – Unsecure Command-and-Control Interfaces

Devices implementing unsecure Command-and-Control interfaces shall provide settings to control which of these protocols are enabled.

Observation

> Non-Ethernet unsecure interfaces like USBTMC and GPIB connections are permitted and do not require settings to disable them.

22.13.4 RULE – HiSLIP Devices Supported SASL Mechanisms

Devices that implement the HiSLIP extended function shall support client authentication using the SASL mechanisms of ANONYMOUS, PLAIN, and SCRAM.

Additional SASL mechanisms may be supported.

22.13.5 RULE – Devices Shall Support IVI 6.5, SASL Mechanism Specification

IVI 6.5, SASL Mechanism Specification contains requirements on usernames, passwords and SASL mechanism implementation. Devices shall follow these requirements for usernames and passwords. Devices that implement SCRAM shall comply with the SCRAM requirements.

22.14 RULE – LXI API Security Methods

Devices shall provide the following APIs as defined in the LXI API Extended Function:

URL	HTTP Method	Summary
/lxi/identification	GET	Returns identity information about the device (and connected devices). This is an unsecure API. Note compliant implementations might not include the Content-Type response header.
/lxi/api/common-configuration OR /lxi/common-configuration	GET	Returns the overall device LXI configuration and capabilities. This API is available both over secure and unsecure connections.
lxi/api/common-configuration	PUT	Configures the overall device LXI configuration The network settings managed by this API can usually be applied to all devices in a system.
/lxi/api/device-specific-configuration /lxi/device-specific-configuration	GET	Returns device-specific configuration and capabilities. This API is available over both secure and unsecure connections. The two endpoints behave identically.

/lxi/api/device-specific-configuration	PUT	Configures device-specific network settings. The network settings managed by this API are potentially unique to a particular device.
/lxi/api/certificates	GET	Returns a list of certificate GUIDs.
/lxi/api/certificates	POST	Places a PKCS#7 style certificate or certificate chain on the device to use with its LDevID. The certificate must be based on CSR acquired from the device. The response XML has the GUID that is used to identify this certificate.
/lxi/api/certificates/<GUID>	GET	Returns the PKCS#7 certificate, certificate chain, or PKCS#10 CSR identified by <GUID>
/lxi/api/certificates/<GUID>	DEL	Deletes the certificate, certificate chain or CSR identified by <GUID>
/lxi/api/get-csr	GET	Acquires a PKCS#10 CSR from the device based on the request parameters.
/lxi/api/create-certificate	PUT	Tell the device to create a self-signed certificate (also known as an LDevID) based on the request parameters.
lxi/api/certificates/<GUID>/enabled	PUT	Used to enable or disable a certificate identified by <GUID>
lxi/api/certificates/<GUID>/enabled	GET	Used to determine if a certificate identified by <GUID> is enabled or disabled.