TSEP

Technical
Software
Engineering
Plazotta

# TSEP Kerberos
# –
# Self-Certification Tool and More

## Introduction

TSEP Kerberos is a hardware and software solution which was created to verify the functionality of a measuring device. This currently applies in particular to the LXI components of a device, because this was the initial spark to create such a test tool. The previous software solution for testing the LXI functionality required additional hardware, especially the choice of a suitable router that provided all the necessary parameters to configure, put many LXI testers in front of a great challenge. To solve this problem, TSEP has come up with a general hardware solution that not only solves the problems of finding individual hardware components, but also uses them to increase the level of automated testing for LXI functionality. Already during the development of the hardware, it was ensured that the components used can not only be used with regard to LXI tests but can also assume a general function in a test environment.

## Kerberos Concept

First, you should take a closer look at the hardware of the TSEP Kerberos. The hardware includes all necessary components for testing. It contains several network interfaces. Two of which are routed to the outside, they serve to connect the client PC and the device-under-test (DUT). Another interface is only used internally to simulate another device in the test network. This is necessary, for example, when testing the 1588 protocol to determine whether a device can cope with multiple devices in the network.

These network interfaces are internally switched to achieve the appropriate combination for the selected test. This could be a peer-to-peer connection or a connection through a switch. In this context, it should also be mentioned that the hardware of the TSEP Kerberos is also able to independently disconnect the DUT from the network or to connect it to the network. This greatly increases the automation of tests. The built-in router also automates many tests, as any changes in router settings can be handled by the software.

This hardware represents the server in a client-server concept. All actions are performed on the server, the client, however, is just a tool that reflects the current state of the server and provides the ability to configure the server and start tests. The display on the hardware shows only a small statistic of how many tests are included in the scope of testing and how many of them were successful and unsuccessful, as well as a detailed log of all actions performed by the server. This log can be displayed in more or less detail.
In the client software, the individual logs are assigned to the appropriate tests, so each test has a detailed log so it can easily be tracked as to how an error occurred. A test always consists of preconditions, the actual test and post conditions.

Preconditions are the settings that have to be made to have a suitable setup to run a test. These could be router settings or even whether the DUT is connected to the network at the beginning of the test. This is to ensure that the same conditions always exist when a test starts. Then come the defined test-specific steps and finally the post-conditions are checked. This could be a validation of the obtained IP address of the DUT or that it was also entered in the mDNS.

Once you have completed all necessary tests, you also want to have a summary of the results. These can be obtained via the client as a PDF. This PDF is created on the server and also signed by the server, so it cannot be manipulated without the loss of the signature.

To control the server, it is also irrelevant whether the TSEP Kerberos is connected via a peer-to-peer connection to the client or simply connected to the local network, because the client searches and lists all available Kerberos servers. You can connect to any in this list, but it should be noted that each server only allows a single client. Thus, an existing connection must be closed before you can access it from a second PC in the network.

### Comparison of Kerberos - LXI Conformance Test Suite

With the hardware components mentioned, Kerberos is a complete test environment and requires no additional hardware compared to the LXI Conformance Test Suite. The only requirement is a PC on which the Kerberos client is installed.

TSEP Kerberos ensures that the results obtained are compatible with the LXI Conformance Test Suite. This means the results are the same as if you ran the tests with the LXI Conformance Test Suite. If there are changes to the way an LXI Rule is tested, the test will be adjusted in Kerberos. Therefore, the informational data on the server indicates the compatible LXI Conformance Test Suite.

Currently, many of the LXI components are already supported by Kerberos, such as the "LXI Device Specification 2016" and the extended features "LXI HiSLIP", "LXI IPv6" and "LXI VXI-11 Discovery and Identification". These components are fully supported.
The modern user interface of the client allows an easy and fast configuration of the tests. This is important to ensure the possibility of self-certification. TSEP Kerberos minimizes the knowledge required to perform tests due to the step-by-step guidance which is especially noticeable with manual tests. That's why TSEP Kerberos is the only tool that allows self-certification of the LXI functionality of a measuring device.

## Self-Certification with TSEP Kerberos Test Suite

The LXI Consortium recently extended the LXI Conformance Policy with Self-Certification for LXI vendor companies. This is a new additional and improved LXI conformance testing process to reduce conformance testing efforts for LXI devices and streamline the LXI conformance process.

The TSEP Kerberos Test Suite for conformance testing is mandatory for self-certification.
Self-Certification is applicable for the LXI Device Specification 2016 and the following LXI Extended Functions:

- LXI VXI-11 Discovery and Identification
- LXI HiSLIP
- LXI IPv6

Self-Certification is restricted to LXI Consortium member companies in good standing using the TSEP Kerberos Test Suite for conformance testing and have at least one certified LXI device prior to the first application for Self-Certification. Training for LXI Self-Certification is planned at LXI Plug Fests. For the training, a separate registration at the LXI Consortium is necessary in advance.

If an LXI member company fulfills these requirements and wants to apply for LXI Self-Certification, then the company representative attends the next available LXI Plug Fest to demonstrate the LXI Self-Certification testing capabilities.

Once approved, the process for LXI Self-Certification is easy:

- Run the LXI Conformance Test with the TSEP Kerberos Test Suite within the company
- Submit the Test results to the LXI Conformance Committee

### More than just an LXI Test Suite

TSEP Kerberos is more than just an LXI Test Suite. With the help of the command line tool, Kerberos can also be used by programs or scripts, making it suitable for regression tests. This is very useful for continuously checking the LXI functionality of a device during its development. With the console client you can also create and configure test sessions as well as find all Kerberos hardware on the network. Basically, all options of the interface client are also available to the console client. Only manual tests cannot be performed with the console variant, because this requires an interaction of the user and this is only possible via the client.

Also, the already mentioned logging of the tests is an obvious added value of the Kerberos system. Here, individual steps are closely tracked and documented to allow easy debugging of the problem. How detailed the recording becomes, one can adjust over the client.

Another benefit of Kerberos is its modular structure, so it is possible to purchase customized modules to test core functionalities of your own devices. This provides a very compact and above all mobile test environment.

### Future extensions

A few topics are very high in the course for the Kerberos system, on the one hand the "LXI Clock Synchronization" is a big topic but also the "LXI LAN Event Messaging" tests shall be added in the near future. The LXI Security, where the LXI Consortium is making great progress, is also being followed and will certainly find its way into the Kerberos system. Such updates can easily be made via a prepared USB stick.