

# SSL and Telemetry

From Engineering Wiki

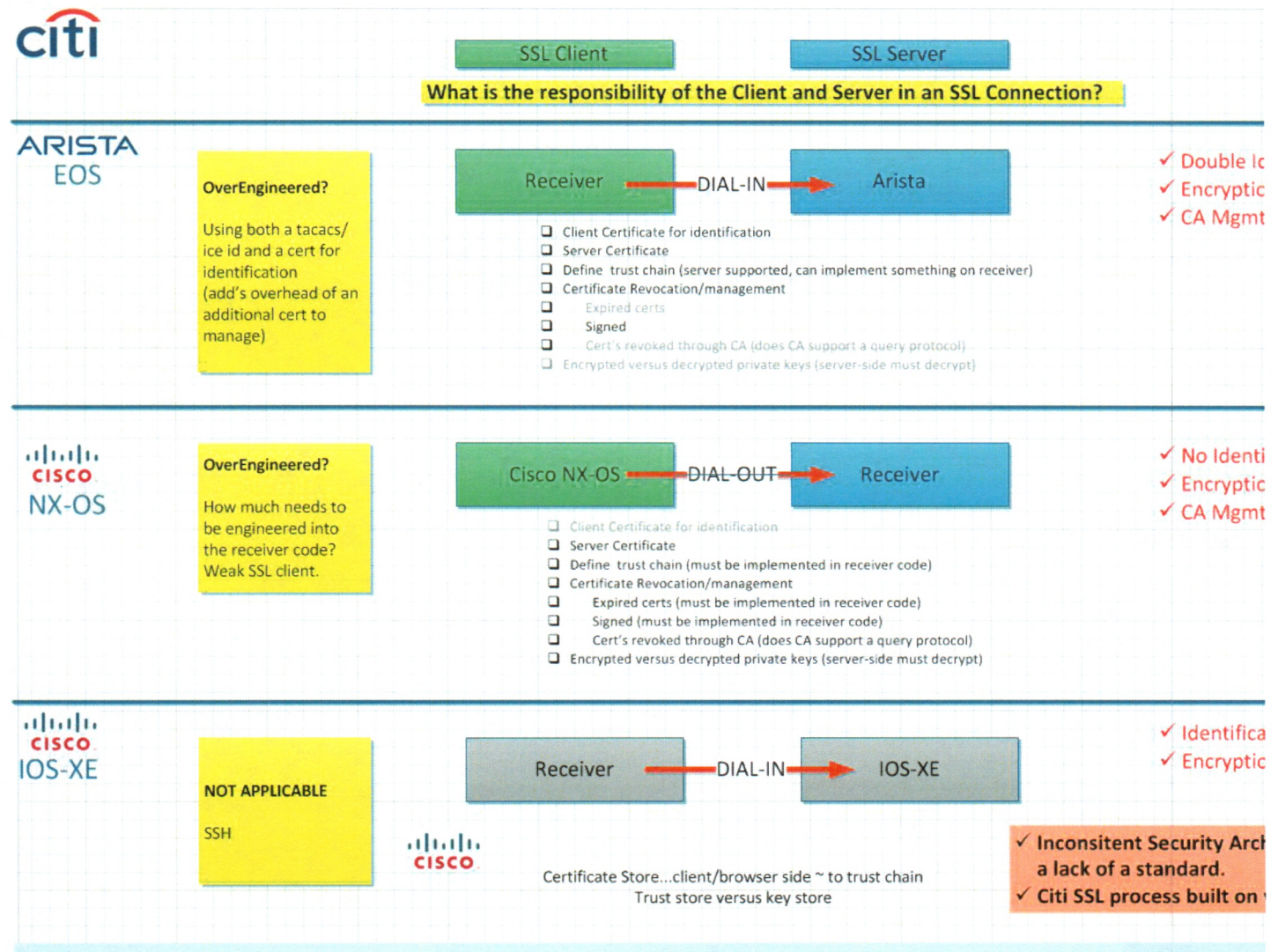
**Contents**

- 1 Overview
- 2 SSL Level of Support
- 3 ARISTA EOS AND CISCO NX-OS
- 4 Responsibility of Client and Server in SSL Connection

## Overview

There is no consistent telemetry implementation across vendors; indeed, even Cisco isn't consistent with its telemetry solution across its different network operating systems. Implementing SSL in telemetry is also not consistent, since the relationship between SSL client and SSL server can vary between the network device and the software receiver. In other words, for some vendors, the SSL client is the software receiver and the SSL server are the network devices. The following diagram summarizes SSL across the following NOS:

- ARISTA EOS
- CISCO NXOS
- CISCO IOS-XE

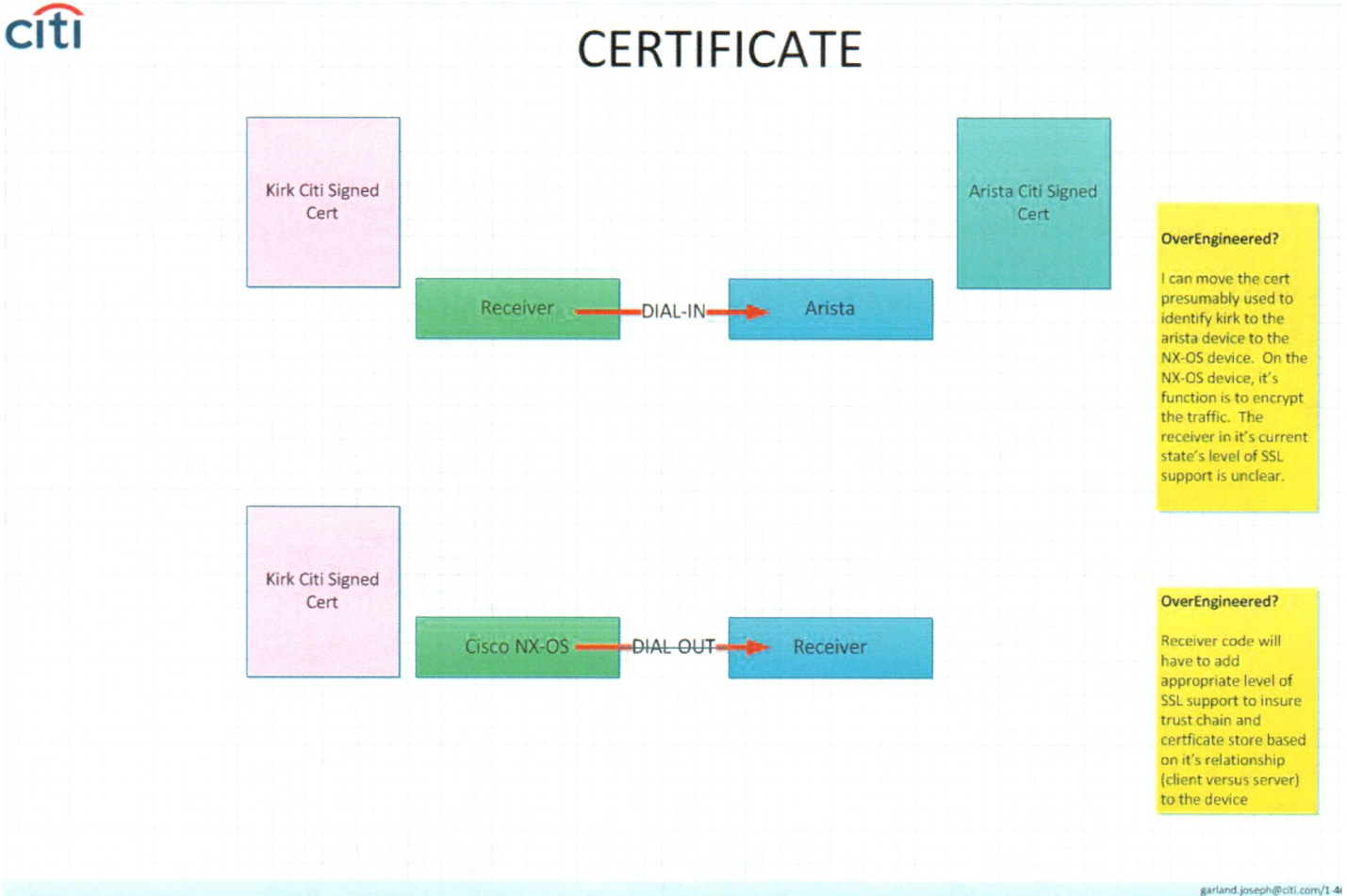


## SSL Level of Support

The following tasks represent various aspects of the SSL protocol and are important to understand the levels of SSL support provided by each vendor.

- Client Certificate for Identification
- Server Certificate
- Define Trust Chain
- Certificate Revocation/Management (CA)
  - Expired Certificates
  - Certificates revoked that CA (does CA support a query protocol for automation?)
- Encrypted Private Keys

### ARISTA EOS AND CISCO NX-OS



### Responsibility of Client and Server in SSL Connection

\* Keystore is used to store your credential (server or client) while truststore is used to store others credential (Certificates from CA)

\* Keystore is needed when you are setting up server side on SSL, it is used to store server's identity certificate, which server will present to a client on the connection while trust store

\* You can have both keystore and truststore on client and server side if the client also needs to authenticate itself on the server. In this case, client will store its private key and iden

\* In Java -jvax.net.ssl.keyStore property is used to specify keystore while -jvax.net.ssl.trustStore is used to specify trustStore

\* In Java, one file can represent both keystore vs truststore but it's better to separate private and public credential both for security and maintenance reason.

\* truststore vs keystore in Java6 When you install JDK or JRE on your machine, Java comes with its own truststore (collection of certificate from well known CA like Verisign, goDaddy, th

\* JAVA\_HOME/JRE/Security/cacerts where JAVA\_HOME is your JDK Installation directory.

\* keytool command (binary comes with JDK installation inside JAVA\_HOME/bin) can be used to create and view both keyStore and trustStore.

\* If you are still not clear with what is truststore and keystore In Java or difference between keystore and truststore than just remember one line keystore is used to store server's own ce

References: <http://www.java67.com/2012/12/difference-between-truststore-vs.html>

Retrieved from "http://ewiki.nam.nsroot.net/w/index.php?title=SSL\_and\_Telemetry&oldid=76178"

- This page was last modified on 4 December 2018, at 13:00.
- This page has been accessed 30 times.