Troubleshoot Certificate Issues for SSL VPN with CME

TAC **Document ID: 116638**

Contributed by Kurt Mai, Cisco TAC Engineer.
Oct 22, 2013

Contents

Introduction

This document describes the methodology to troubleshoot IP phone registration to Communications Manager Express (CME) via Secure Sockets Layer (SSL) VPN.

Prerequisites

Requirements

Cisco recommends that you have a basic understanding of security certificates, the packet capturing tool, and Communications Manager Express.

Components Used

The information in this document is based on these software and hardware versions:

- Communications Manager Express Release 8.6
- Cisco 7965 IP Phone Release 8.5.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Troubleshoot Certificate Issues

There are two methods to set up SSL VPN between an IP phone on the Internet and CME inside the corporate network.

- The CME is behind a Cisco Adaptive Security Appliance (ASA) which acts as the VPN Headend. In this scenario, CME and the ASA share the same certificate and the IP phone negotiates the security

setup with the ASA.
- The CME is connected to the Internet directly, and acts as the VPN Headend. It negotiates the security setup with the IP phone directly.

In both scenarios, establishing SSL VPN between an IP phone on the Internet and the CME consists of similar steps:

1. The CME generates or obtains a security certificate.
2. The CME "pushes" the hash of the certificate in Base64 format to the phone via the config file which the phone downloads from CME via TFTP.
3. The IP phone tries to log in with the VPN Headend and receives the certificate via Transport Layer Security (TLS) protocol.
4. The IP phone extracts the hash from the certificate and compares it with the hash which it downloaded from CME earlier. If the hash matches, then the phone trusts the VPN Headend and proceeds with further VPN negotiation.

Verify

In order to verify that the CME has pushed the hash to the IP phone, check the configuration file it generated for the secure phone. In order to simplify this step, you can configure the CME to generate a configuration file per phone and store it in flash:

```
R009-3945-1(config-telephony)#cnf-file perphone
R009-3945-1(config-telephony)#cnf-file location flash:
```

In order to ensure that new configuration is generated, it is recommended to recreate the configuration files:

```
R009-3945-1(config-telephony)#no create cnf-files
CNF files deleted
R009-3945-1(config-telephony)#create cnf-file
Creating CNF files
```

After the corresponding configuration file in the flash displays (for an ephone with vpn-group configured), you should see this near the end of the file content:

```
<vpnGroup>  <enableHostIDCheck>0</enableHostIDCheck>
  <addresses>
    <url1>https://10.201.160.201/SSLVPNphone</url1>
  </addresses>
  <credentials>
    <hashAlg>0</hashAlg>
    <certHash1>fZ2xQHMBcWj/fSoNs5IkPbA2Pt8=</certHash1>
  </credentials>
</vpnGroup>
```

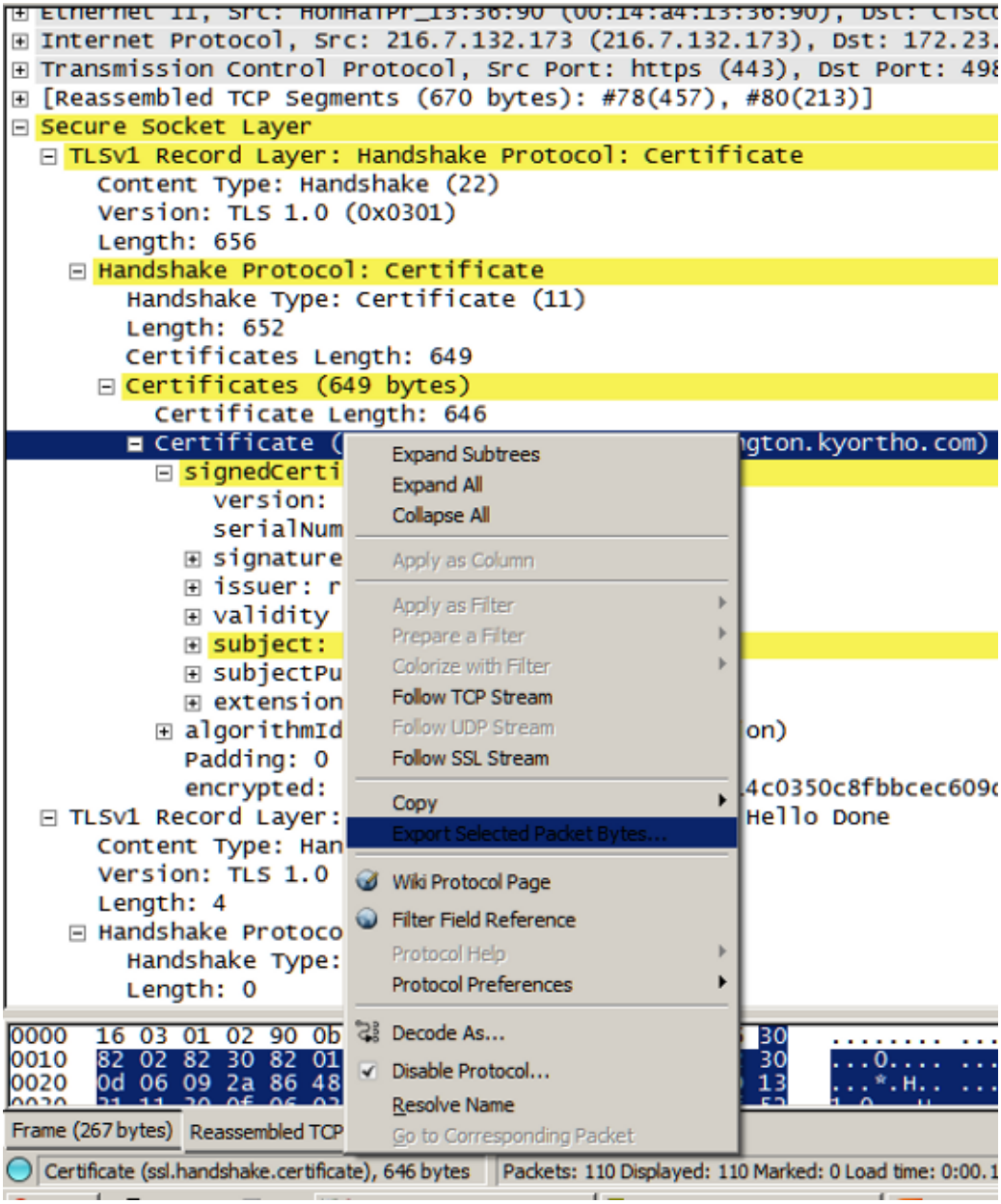
The ***certHash1*** value is the hash of the certificate. When the IP phone receives the certificate from VPN Headend during TLS setup, it expects the hash of the certificate to be same as the stored hash value. If the IP phone throws a "Bad Certificate" error, it could be that the hash values do not match.

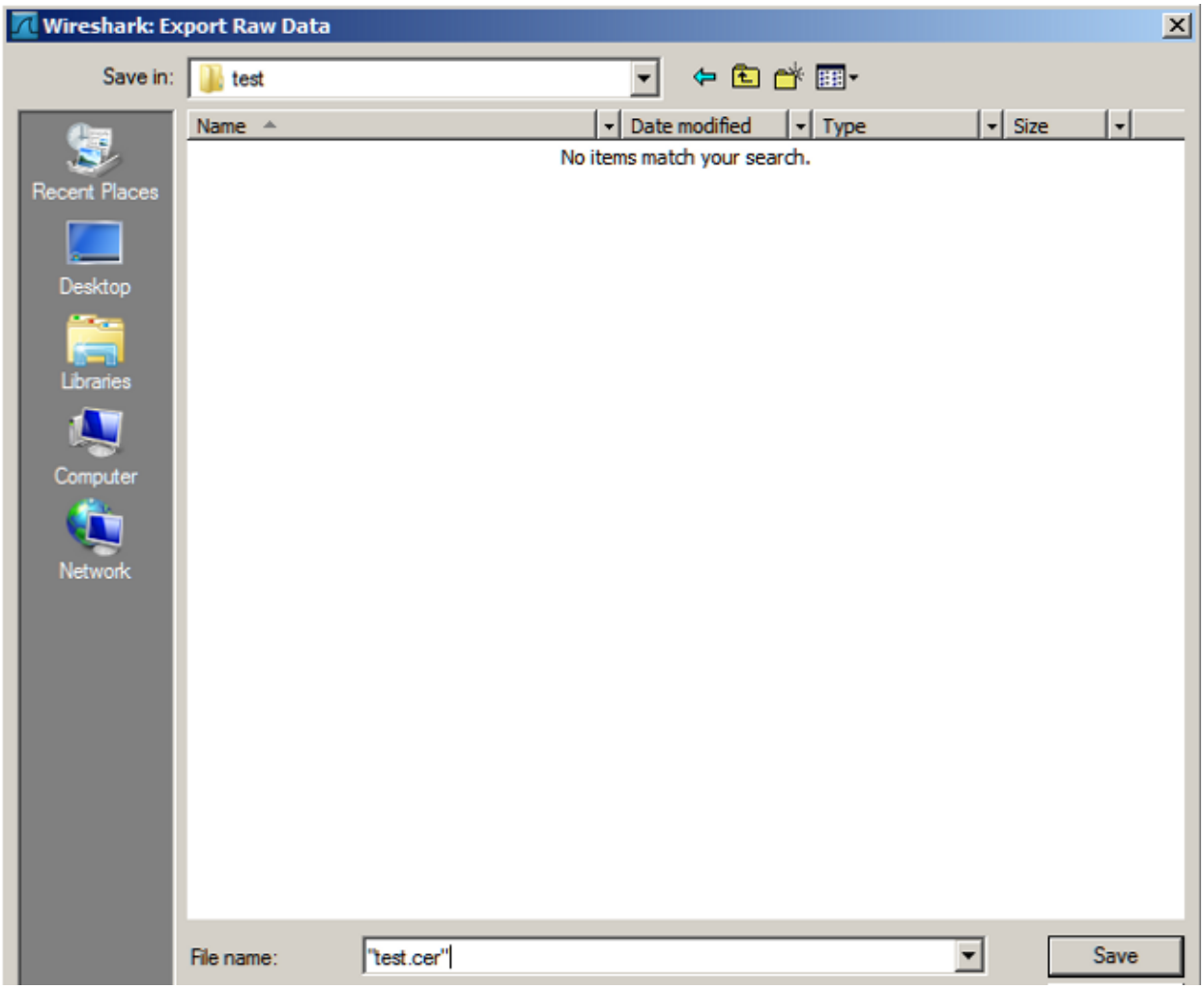
In order to verify, follow these steps to extract the hash value from the packet capture collected between the IP phone and the VPN Headend:

1. Locate the packet from the VPN Headend device to the IP phone that contains the certificate. It is typically in the TLS Server Hello packet.
2. Expand the packet content and locate the header:
   Secure Socket Layer > ***TLS V1 Record Layer*** > ***Handshake Protocol: Certificate*** > ***Certificates*** >

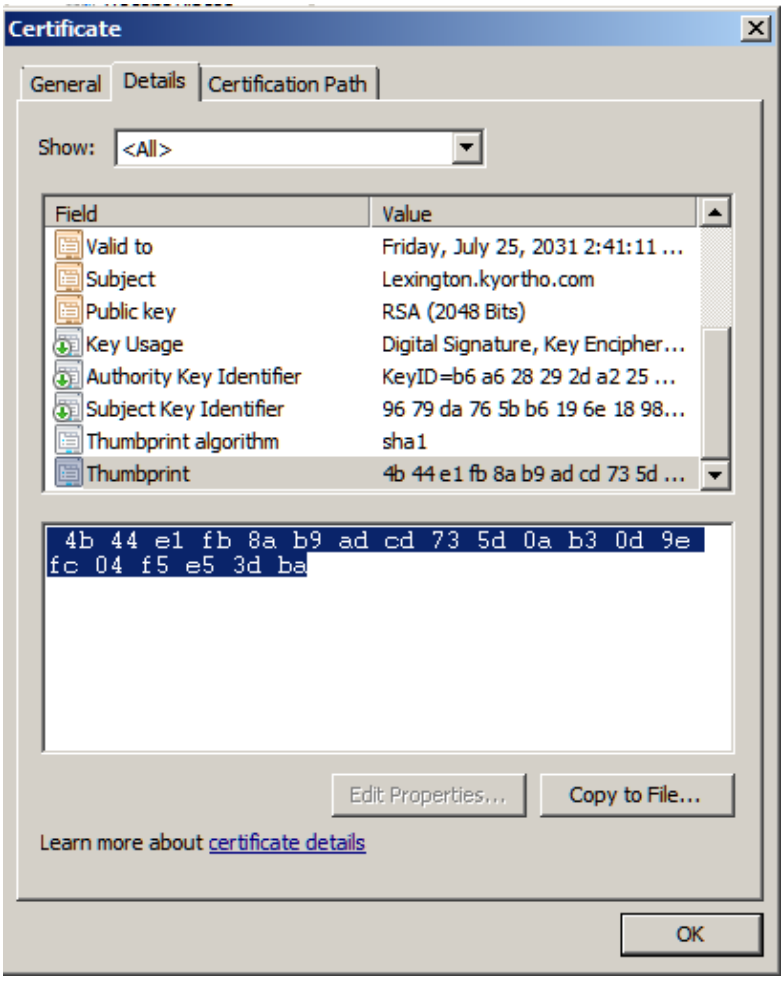
Certificate.

3. Right−click the Certificate header and export the values to a .CER file:





4. Open the .CER file, go to the Details tab, choose Thumbprint, and choose the values. The values are the hash in hex format:



5. Next, you convert the hash from hex to Base64 using any online Hex−to−Base64 conversion tool. The converted value can be compared to the hash value in the IP phone's configuration file if they do not match, then it means the hash received by the IP phone is from a different certificate than what is used by the VPN Headend for SSL.

Related Information

- ***Configuring SSL VPN Client for SCCP IP Phones***
- ***Technical Support & Documentation − Cisco Systems***

>

Updated: Oct 22, 2013 Document ID: 116638