=

TESTING

Euro-PacketCable Certificate Requirements

--- Project Reference ---

Document Reference : Euro-PacketCable Certificate Requirements v9.0
Revision : 9.0
Author(s) : testing@excentis.com
Date : November 15, 2006
Distribution : www.excentis.com

1 Introduction

While Euro-PacketCable uses the security specifications from PacketCable [PKT-SP-SEC], some changes are needed in relation to the digital certificates that are used in a Euro-PacketCable environment. This document outlines these differences and specifies the structure and required information needed for Euro-PacketCable certificates. To keep Euro-PacketCable and PacketCable as much alike as possible, Euro-PacketCable uses all PacketCable security technology, including new revision of the security specifications [PKT-SP-SEC].

This document describes the elements of the Euro-PacketCable certificates that are different from the PacketCable certificates. For Euro-PacketCable the Euro-PacketCable certificates are the only valid certificates, any requirements that are stated in [PKT-SP-SEC] for PacketCable which refer to PacketCable Certificates are changed to the corresponding requirements for the Euro-PacketCable certificates.

Euro-PacketCable compliant embedded MTAs MUST have the Euro-DOCSIS root CVC CA's public key stored in the CM's non-volatile memory instead of the DOCSIS CVC CA's public key.

Euro-PacketCable compliant standalone MTAs must have the Euro-PacketCable CVC Root Certificate and the Euro-PacketCable CVC CA certificate stored in non-volatile memory. The CVC of manufacturers are verified by checking the certificate chain.

2 MTA device Certificate Hierarchy

2.1 Introduction

The MTA device Certificate Hierarchy is used to authenticate MTA devices to servers. Figure 1 shows the MTA device hierarchy.

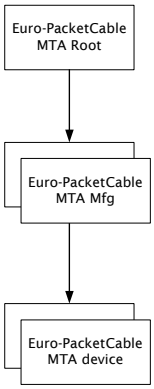

Figure 1: MTA device certificate hierarchy

The MTA root CA is used to authenticate MTA Mfg (Manufacturing) certificates, the MTA Mfg certificate is used to authenticate the MTA device certificates. The following sections specify the requirements for the different certificates.

2.2 Euro-PacketCable Root Device Certificate

The Euro-PacketCable Root Device Certificate has the following attributes:

countryName=BE

organizationName=tComLabs

organizationalUnitName=Euro-PacketCable

commonName= Euro-PacketCable Root Device Certificate Authority

The countryName, organizationName, organizationalUnitName and commonName attributes MUST be included and MUST have the values shown. Other attributes are not allowed and MUST NOT be included.

2.3 MTA manufacturer and device certificate

Please note that the <Company Name> in the organizationName MAY be different from the<Company Name> in the <commonName> for the manufactuer certificates.

The MTA manufacturer certificate has the following attributes:

countryName = <Country of Manufacturer>

organizationName = <Company Name>

[stateOrProvinceName = <state/province>]

[localityName = <City>]

organizationalUnitName = Euro-PacketCable

[organizationalUnitName = <Manufacturing Location>]

commonName = <Company Name> Euro-PacketCable CA

The MTA device certificate has the following attributes:

countryName = <Country of Manufacturer>

organizationName = <Company Name>

[stateOrProvinceName = <state/province>]

[localityName = <City>]

organizationalUnitName = Euro-PacketCable

[organizationalUnitName= <Product Name>]

[organizationalUnitName = <Manufacturing Location>]

commonName = <MAC Address>

3 Service Provider CA certificate hierarchy

3.1 Introduction

The Service Provider CA Certificate Hierarchy is used to authenticate servers to MTA devices. Figure 2 shows the Service Provider CA certificate hierarchy.

The Service Provider root CA is used to authenticate Telephony Service Provider certificates. The certificates for the KDC and DF can be authenticated directly by the Telephony Service Provider Certificate; alternatively they can be authenticated by a local system operator certificate which is authenticated by the Telephony Service Provider certificate.

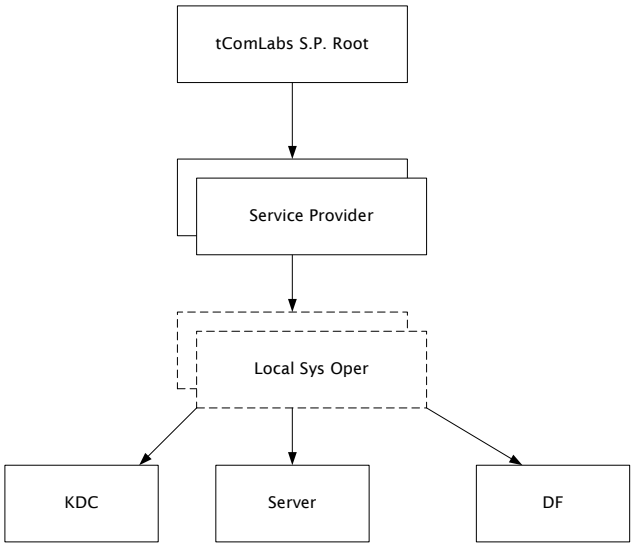

Figure 2: Service Provider Certificate Hierarchy

3.2 Euro-PacketCable Service Provider Root Certificate

The Euro-PacketCable Service Provider Root Certificate has the following attributes:

countryName=BE

organizationName=tComLabs

commonName=tComLabs Service Provider Root CA

3.3 Service Provider CA Certificate

The Service Provider CA Certificate has the following attributes:

countryName = <Country>

organizationName = <Company>

commonName = <Company> tComLabs Service Provider CA

3.4 Local System CA Certificate

The Local System CA certificate has the following attributes:

countryName = <Country>

organizationName = <Company>

organizationalUnitName = <Local System Name>

commonName = <Company> tComLabs Local System CA

3.5 Key Distribution Center Certificate

The Key Distribution Center Certificate has the following attributes:

countryName = <Country>

organizationName = <Company>

[organizationalUnitName = <Local System Name>]

organizationalUnitName = tComLabs Key Distribution Center

commonName = <DNS Name>

3.6 Delivery Function Certificate

The Delivery Function Certificate has the following attributes:

countryName = <Country>

organizationName = <Company>

[organizationalUnitName = <Local System Name>]

organizationalUnitName = Euro-PacketCable Electronic Surveillance

commonName = <IP address>

3.7 Euro-PacketCable Server Certificate

The Euro-PacketCable Server Certificate has the following attributes:

countryName = <Country>

organizationName = <Company>

organizationalUnitName = Euro-PacketCable

[organizationalUnitName = <Local System Name>]

organizationalUnitName = <Sub-system Name>

commonName = <Server Identifier[:<Element ID>]>

Please refer to [PKT-SP-SEC] for additional specifications on the commonName.

4 Euro-PacketCable Code Verification Certificate Hierarchy

4.1 Introduction

Figure 3 describes the CVC (Code Verification Certificate) hierarchy.

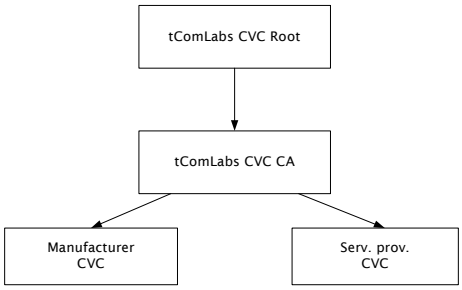

Figure 3: Code Verification Certificate Hierarchy

The Code Verification Certificate Hierarchy is generic in nature and can also be used for other projects. For embedded MTAs the Euro-DOCSIS Code Verification Certicate Hierarchy, specified in [Euro-DOCSIS Baseline Privacy Plus requirements]), is used instead of the Euro-PacketCable CVC Root.

4.2 Euro-PacketCable Code Verification Certificate Root Certificate

The Euro-PacketCable Code Verification Root Certificate has the following attributes:

countryName = BE

organizationName = tComLabs

commonName = tComLabs CVC Root CA

4.3 Euro-PacketCable Code Verification CA Certificate

The Euro-PacketCable Code Verification CA Certificate has the following attributes:

countryName = BE

organizationName = tComLabs

commonName = tComLabs CVC CA

4.4 Manufacturer Code Verification Certificate

The Manufacturer Code Verification Certificate has the following attributes:

countryName = <Country>

organizationName = <Company Name>

[stateOrProvinceName = <state/province>]

[localityName = <City>]

commonName = <Company Name> Mfg CVC

The Manufacturer Code Verification Certificate is signed by the Euro-PacketCable Code Verification CA Certificate.

4.5 Service Provider Code Verification Certificate

The Service Provider Code Verification Certificate has the following attributes:

countryName = <Country>

organizationName = <Company Name>

[stateOrProvinceName = <state/province>]

[localityName = <City>]

commonName = <Company Name> Service Provider CVC

The Service Provider Code Verification Certificate is signed by the Euro-PacketCable Code Verification CA Certificate.

5 References

[PKT-SP-SEC] PacketCable Security Specification, www.PacketCable.com

[Euro-DOCSIS Baseline Privacy Plus requirements] Euro-DOCSIS Baseline Privacy Plus requirements, www.Excentis.com