AeroMACS Public Key Infrastructure (PKI) Users Overview

1 Introduction

1.1 Introduction

The Aeronautical Mobile Airport Communication System (AeroMACS) Certification Authorities (CAs) provide hosting of the AeroMACS Public Key Infrastructure (PKI) hierarchy and supply device and server certificates for use in AeroMACS Networks.

This document describes the use of these certificates by AeroMACS Compliant devices and the process for obtaining those certificates.

1.2 X.509 Certificates

X.509 certificates and their associated keys are used in a PKI system to identify and authenticate the identity of devices and Authentication, Authorization and Accounting servers (servers). A PKI relies on public key cryptography to digitally sign certificates by using other certificates. These form a hierarchy of certificates, each signed by a higher certificate, back to a root certificate that signs itself.

The format and use of X.509 certificates are described in IETF RFC 5280.

The cryptographic algorithms, such as ECC and other related specifications are in the PKCs#1 through PKCs#13 specifications, available from International Telecommunication Union (ITU).

AeroMACS technology consists of two classes of PKI hierarchies, the device hierarchy that identifies devices and the server hierarchy that identifies servers.

AeroMACS uses a Managed PKI, hosted at the CAs and managed by Eonti Inc. (Eonti). At the root of the AeroMACS hierarchy is the root signing certificate. This root signs Subordinate CA (Sub-CA) certificates and those in turn sign either device certificates or server certificates, and are obtained through a certificate account, managed by Eonti. See ***Figure 1Figure 1*** for an example of the AeroMACS PKI hierarchy.

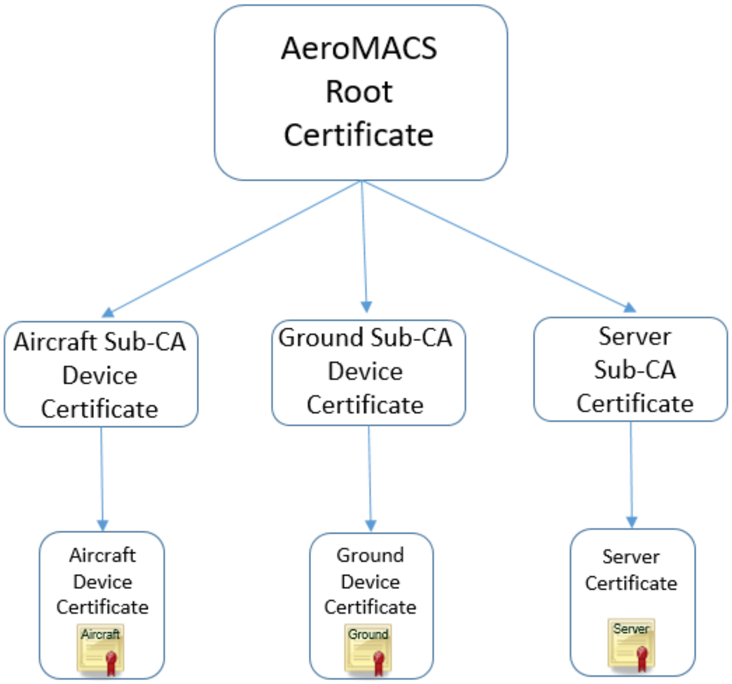
AeroMACS Root Certificate
Aircraft Sub-CA Device Certificate
Ground Sub-CA Device Certificate
Server Sub-CA Certificate
Aircraft Device Certificate
Aircraft
Ground Device Certificate
Ground
Server Certificate
Server

Figure 1 AeroMACS PKI Hierarchy

2 Provisioning Certificates in Devices and Servers

2.1 *The Certificates to be Provisioned in Devices and Servers*

Each device must be provisioned with its certificate chain and the private key associated with its own device certificate.

Similarly, the server must be provisioned with its own certificate chain and the private key associated with its own server certificate.

When a device communicates with a server, they exchange with each other, their Sub-CA certificate and end-entity certificate.

The following public root certificates exist for the AeroMACS Public Key Infrastructure (PKI) [only available to WiMAX Forum members in good standing and in the future may include additional Sub-CAs].

AeroMACS Root CA	Root CA001 created by DigiCert, Inc.
Ground Device Sub CA001	Ground Device Sub CA001 created by DigiCert, Inc.
Aircraft Device Sub CA001	Aircraft Device Sub CA001 created by DigiCert, Inc.
Server Sub CA001	Server Sub CA001 created by DigiCert, Inc.

NOTE: The Root CA certificate MUST be installed in all devices and all servers.

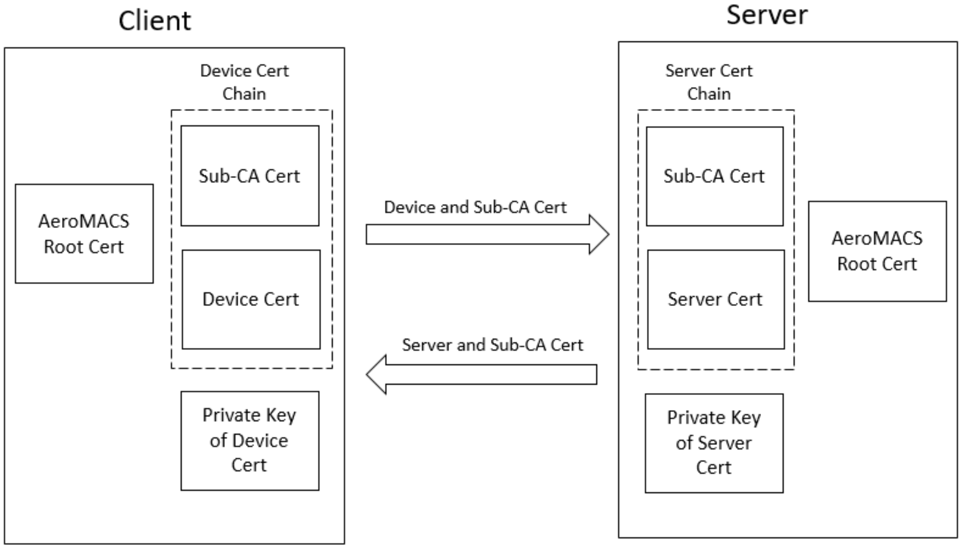

Figure 2 Certificates Provisions in Devices

2.2 *Certificates and Keys to Obtain from a Sub-CA*

When obtaining a device certificate from the Registration Authority (RA) to provision in an AeroMACS compliant device, the RA must supply:

- The root certificate in the device's certificate chain;
- The Sub-CA certificate signed by the root;
- The device certificate itself, signed by the Sub-CA certificate; and
- The device certificate private key (if applicable).

When obtaining a server certificate from the RA to provision in an AeroMACS PKI server, the RA must supply:

- The root certificate in the server's certificate chain;
- The Sub-CA certificate signed by the root;

- The server certificate itself, signed by the Sub-CA certificate; and
- The private key of the server certificate.

The certificate chain can also be obtained from the WiMAX Forum website.

The server and device Sub-CA certificate(s) may change (e.g., to limit the size of Certificate Revocation Lists (CRLs)). Therefore an updated version of the Sub-CA certificate will be included with each certificate delivery to ensure that consistent certificate chains are provisioned.

3 Obtaining Certificates

Only members of the WiMAX Forum in good standing are eligible to receive AeroMACS PKI Certificates. To learn about the process for obtaining certificates, please visit the ***AeroMACS PKI webpage***. Members of the WiMAX Forum can log in and follow the links. If you are not a member of the WiMAX Forum and wish to learn more about the benefits of membership or wish to become a member, please visit the ***WiMAX Forum Membership*** webpage.

3.1 Setting up an Authorized User

An "Authorized User" is a Device Manufacturer or a Network Operator that the WiMAX Forum, as authorization administrator, has authorized to receive Public Key Cryptography Standards (PKCs) from an AeroMACS CA. Authorized Users must be set up with a certificate account prior to requesting device or server certificates.

The process for setting up Authorized Users and ordering certificates is available on the WiMAX Forum website for users who are employees of active member companies of the WiMAX Forum.

The WiMAX Forum, as Management Authority (MA), has established the AeroMACS PKI, which is described in the AeroMACS PKI Certificate Policy (i.e., Governing Documents). The AeroMACS PKI provides a mechanism that permits Authorized Users to obtain PKCs through CAs and managed by Eonti. In support of maintaining a high level of security and integrity for the AeroMACS PKI and the networks established and operated using the PKCs, the WiMAX Forum requires that each Applicant wishing to receive PKCs accept the AeroMACS PKI Terms & Conditions before the Applicant is approved as an Authorized User. The WiMAX Forum is willing to approve the Applicant as an Authorized User, subject to the Applicant's faithful performance of all of its obligations described in the AeroMACS PKI Terms & Conditions.

3.2 Requesting Ground Device Certificates

Once an Applicant has been approved as an Authorized User, orders for ground device certificates (surface vehicle, video sensor, ground critical, or ground default) can be requested through a certificate account managed by the AeroMACS Registration Authority, Eonti. Eonti will direct Authorized Users through the certificate issuance process.

3.3 Requesting Aircraft Device Certificates

Once an Applicant has been approved as an Authorized User, orders for Aircraft device certificates can be requested through a certificate account managed by Eonti. Eonti will direct Authorized Users through the certificate issuance process.

3.4 Requesting a Server Certificate

Once an Applicant has been approved as an Authorized User, orders for server certificates can be requested through a certificate account managed by Eonti. Eonti will direct Authorized Users through the certificate issuance process.

3.5 Retrieving Root Certificate Lists

The WiMAX Forum publishes the approved AeroMACS root certificates on its website.