

**AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL**

**WORKING GROUP 3 (APPLICATIONS AND UPPER LAYERS)**

**Tokyo, Japan**

**December 1 - 3, 1999**

**CM Directory Concept**

Prepared by: G. Saccone

**SUMMARY**

This paper gives an overview of how CM version 2 may interact with the Directory services as proposed by Subvolume 7.

## 1. Introduction

The version 2 CM SARPs present two new services that may be used in conjunction with a directory on the ground to provide enhanced CM service. These services return information for specific ground facilities. One of the ways that this information may be obtained is by use of the Directory specified in Subvolume 7. Additionally, in order to support secure data link services, key information will need to be obtained by CM. While there are other methods that may be used to obtain this information, the Directory as specified in Subvolume 7 has the capability to handle all of the requisite information. It should be noted that there will still need to be additional requirements in order to perform Directory services, and that implementing states will need to perform more in-depth operational analysis and develop operational concepts for the implementation of Subvolume 7 services.

## 2. CM Directory Concept

CM users are viewed to interact with the Directory (or "directory function", hereafter called "directory") for the following main purposes:

- To retrieve security information for the local facility's applications
- To retrieve information for other facilities' and aircrafts' applications
- To provide updates to the information contained in the directory
- To retrieve organizational and administrative information, including contact addresses, phone numbers, names of operational support personnel, etc.

For inclusion into the CM SARPs, the first three bullets are applicable. The last one, while definitely useful for the user of a directory service, will be more of a local implementation and needn't be done directly through the CM-ground-user. Note that presently, only obtaining the security information is a requirement in the CM SARPs; obtaining application information from the directory is a recommendation and updating directory information is mentioned in a note, as the actual conditions and data updated will be driven by local requirements.

The first two bullets from above are broken down into the CM services that need the information followed by what the request of the directory will contain and what the response from the directory will contain.

- Security Needs (logon, update, facility server queries and updates, not needed for contact or forward)

Request:

- Facility for which keys are needed
- Applications (AEQualifiers)

Response:

- Facility for which keys are applicable
- CM regional/key usage indication

- Keys for each application
  - Key usage indication for each application
  - AE Qualifier, Version for each application/key/usage group
- Ground application information retrieval (logon (in case of a CM server), contact, logon facility designation request, facility server queries, facility server update, but not update)

Request:

- Facility(ies) information is desired for
- Indication on whether or not CM address is required

Response:

- Facility for which information is applicable
  - AEQualifiers, version numbers and (as applicable) addresses for all applications
- Aircraft application information retrieval (non-secure only update)

Request

- Aircraft flight ID
- Aircraft 24 bit address
- Optionally flight plan information (tbd)

Response

- Aircraft flight ID
- Aircraft 24 bit address
- AEQualifiers, version numbers and (as applicable) addresses for all applications

## Security Needs

One of the main requirements for a directory function is to enable key and security information distribution. This information is necessary for secure ATN operation. Currently, the only information that needs to be retrieved by the CM-ground-user is the key agreement public keys and key usage indication for each ground application. If this information is unable to be retrieved through a function of the SSO (e.g. using the SSO-GetPublicKey function), then a directory query must be performed. This query would include: the 4-8 character facility designation, and optionally, identification of the applications that are needed.

In response, the directory will supply the requested security information including: the facility designation for which the information is relevant; the key agreement public keys, an indication of domain limits/usage for each key, the application identifier (AE Qualifier) for which it's relevant (assume we don't need the addresses again, but may

want to allow them optionally so, for example, a CM server could get all the keys and addresses at the same time).

#### Ground application request needs

Another one of the basic tenets for CM is to supply information for facilities that are requested by the aircraft. This is done through the CM-logon service in versions 1 and 2 by providing the facilityDesignation element of the CMLogonRequest and via the CM-facility-query service in version 2. Also, the CM-contact service may require this in order to get the CM address of the facility which it will then send to the aircraft in the CM-contact service.

The request message for this will indicate the facility (or facilities) for which information is desired. Also, there may need to be an indication of whether or not only a CM address is needed. This indication is meant to be whether or not just CM for that facility is needed in order to provide the necessary information for a contact or whether all addresses (including CM) for that facility are needed.

In response, the directory will provide the requested application information (AEQualifiers, version numbers and applications addresses, as applicable), as well as the indication of the facility for which it is applicable, for each facility requested. Key information is also provided.

#### Aircraft application request needs

It is also feasible for a CM-ground-user to need to request information for a particular aircraft from the directory. This may be done for use with the CM-update or CM-server-update services.

The request message for this will indicate the aircraft for which information is required. This will include at least the aircraft flight ID and 24 bit aircraft address, and may also need to include some flight plan information in order to ensure that the correct information is provided. Note that the directory will need a way to make aircraft register so that this information is current.

In response, the directory will provide the aircraft flight ID and 24 bit address as well as the AEQualifiers, version numbers and applications addresses (as applicable). Key information is also provided.

#### Ground/Aircraft Information Updates

This would be a request only, and would be subject to local rules and directory update rules. All of the information contained in the CM-logon request will be made available to the directory. In addition, ground application information (CM information, if a CM server configuration, or CM and other application information, if a CM end system

configuration) should be made available to the directory if the information changes or on other local rules (e.g. time period).

### **3. Conclusion**

This paper describes a number of ways in which CM can use a directory. Whether or not the Directory of Subvolume 7 is implemented, CM will still need to obtain key information as well as information applicable to other facilities. Version 2 CM contains the user requirements to allow this, and also contains new services to allow an aircraft and ground system greater capability in requesting information for ground facilities. The working group is invited to note the outlined uses of the directory by CM.