ATNP WG3-18 WP – 32

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL

WORKING GROUP 3 (APPLICATIONS AND UPPER LAYERS)
Tokyo, Japan
December 1 - 3, 1999

CM Version 2 Issues

Prepared by: G. Saccone

SUMMARY

This paper gives an overview of some of the issues that need to be resolved for Version 2 CM.

1. Introduction

The version 2 CM SARPs present a number of enhancements, including services and user requirements supporting directory and security capability. There are some issues that have arisen while including these new functionalities in CM. This paper discusses those issues, details how they are currently handled in the Tokyo Draft CM Version 2 SARPs, and invites the working group to comment.

2. Security Discussion and Issues

Secure and Unsecure CM Services

The security approach for CM as first presented in Gran Canaria (WP 17-36) has changed somewhat. Security is now optional for Version 2, whereas it was thought to be mandatory at Gran Canaria. Optional security means that the ability to provide secure services must be supported, but it is recognized that security might not always be required in every region. This decision changed the conditions under which the server services (e.g. CM-server-facility-query and CM-server-facility-update) may be used. WP 17-36 stated that these new services could only be used when security was in use; currently the new services may be used in both secure and unsecure modes.

Removal of DEGRADED Mode

The decision to make security optional in CM version 2 also had an effect on a previous enhancement, the DEGRADED mode. The DEGRADED mode was added to allow a CM-air-user a means to perform a logon to a lower version ground system. With security enhancements, there is a requirement to be able to perform this function as well. However, a lower-version logon might need to be performed first, without going through the DEGRADED process. Additionally, the process by which the Security Requirements parameter is provided to the Dialogue Service (DS) would be complicated with the DEGRADED mode. Therefore, the concept of the CM-air-user providing an "Emulated Version" parameter was introduced. This allows a CM-air-user to provide a version number of the CM version it wishes the CM-air-ASE to emulate. In this way, if there is a known lower version CM ground system, the aircraft can perform a logon compatible with that version. Since this is similar functionality to the logic for the DEGRADED state and is more flexible, the DEGRADED requirements were removed.

Setting and Checking the DS Security Requirements Parameter

A security issue which needs to be discussed is whether the DS Security Requirements parameter should be provided by the user, the ASE, or a combination of both. This needs to be visited for each application, since there may be different requirements. For air-ground applications, the initial decision was made to have the user provide the Security Requirements parameter for the request primitive. The ASE just passes the Security Requirements parameter to the peer user in the form of the service indication. Based on whether or not the Security Requirements parameter is acceptable, the receiving user may choose to initiate a user abort. If the parameter was acceptable, the user invokes a service response (as per usual), and the ASE sets the Security Requirements parameter on the response to the same value as was received. Likewise, the receiving ASE checks the incoming Security Requirements parameter value to see if it is the same as was sent in the request. If not, a provider abort is issued. There is currently no need to confirm the Security Requirements parameter value to the initiating user, although this is done for the Tokyo Draft version CM SARPs for the CM-logon and CM-server-facility-update services.

This may present a problem for some of the CM services, in particular the CM-update, CM-server-facility-update, and CM-forward services. This is because there is currently no user-level response; as soon as the CM-air-ASE receives a D-START indication containing a CM-update (for example), it initiates a CM-update indication and then a D-START response. In order to keep the aforementioned user-level abort requirements, if the CM-air-user received the wrong Security Requirements value, it would abort. However, because the ASE has already responded, the dialogue may already be closed and therefore the ground would never receive the abort. This may not be operationally acceptable.

There are some solutions to this problem. One is to add user-level responses to any service which does not currently have them. This would in effect hold the ASE response until the user gives its OK, which would allow a proper user abort if there was a security problem. Another solution is to put some level of knowledge about security policy in the ASE, so the ASE knows enough whether or not to abort if the wrong Security Requirements parameter is used. If this is done, however, it would seem that the ASE would be able to handle most aspects of setting and checking the Security Requirements parameter. The current version 2 CM SARPs leave the situation as described in the previous paragraph, with the knowledge that sometimes even though all appears to be normal, the service was not performed as intended.

Key Domain Usage Information

There is a need to define the key domain usage boolean. The key domain usage boolean is provided with each key that is returned in a secure CM-logon response, and is meant to give an indication of the key's applicability to a domain. However, there needs to be an unambiguous definition as to what this means, and how an aircraft needs to react if it is provided. This issue was visited by WG3/SG2, and it was determined that better definition is needed, either by expanding upon the definition of the boolean, or changing the boolean to another more meaningful value.

3. New Services Issues

Lack of User-level Service Confirmations

The new CM services, CM-server-facility-query and CM-server-facility-update, follow the CM-logon and CM-update services closely in concept. One issue that has arisen from early implementations is the need for explicit results from services. While the CM-server-facility-query service has this capability, the CM-server-facility-update does not. This is following the same logic as for the current CM-update service. The working group is asked if this is sufficient, or if part of the version 2 enhancements should be confirmed services for the CM-update and CM-server-facility-update.

Subsetting Issues

Finally, there is the question of subsetting. Should these new services be allowed their own individual subsets (thereby greatly increasing the number of subsets) or should they follow the CM-logon and CM-update subsets (thereby possibly forcing implementations to implement functionality that will never be used)? It may also make sense to have support of the both of these services as a subset (i.e. if you support the CM-server-facility query you must also support the CM-server-facility-update, and vice versa). Currently, these subsets match the CM-logon and CM-update in order to minimize the number of subsets.

4. Conclusion

This paper points out a number of questions for discussion by the working group. To recap, they are:

1. Confirm optional use of security for version 2 CM,
2. Acknowledge the removal of the DEGRADED mode,
3. Confirm that the combination of user/ASE setting the Security Requirements parameter, as well as the fact that there may be cases where a wrong parameter is returned to the user, is OK or needs to be changed,
4. Clarify the key usage domain boolean variable,
5. Confirm whether or not the update and server facility update services need to be confirmed, and
6. Confirm whether or not the subsetting as currently defined is acceptable.

The working group is invited to comment on these issues.