# Aeronautical Communication Panel

Working Group N – Networking
Subgroup N4 - Security

November 2004

New Orleans, LA, USA

# Application Level Security Considerations

Prepared By: Tom McParland, BCI/FAA ACB-250

Presented By: Tom McParland, BCI/FAA ACB-250

SUMMARY

The intent of this paper is to provide a framework for discussion by the Working Group on moving the ATN application security solution from the Upper Layer Communications Service to the Application Level.

# Table of Contents

# 1 Introduction

The current ATN application security solution is placed in the Upper Layer Communications Service (ULCS). This paper provides considerations for placement of the security solution at the application level. The remainder of this paper is organized as follows. Section 2 provides an overview of the ATN application solution. Section 3 provides a detailed view of the operation of the ATN security solution in the ULCS. Section 4 describes Context Management role in the ATN application security solutions. Section 5 provides a detailed view of placement of the security solution in the application. Two options are presented. One is for placement in the user-level; the other is for placement in the ASE. Section 6 identifies considerations for placement of security in the application generally and then for each option. Section 7 contains recommendations.

# 2 Overview of ATN Application Security Solution for CPDLC

CPDLC, like all ATSC applications, communicates via the ATN using a two-part operation, involving a support application called Context Management (CM). The basic operation is as follows:

1. An aircraft wishing to communicate via the ATN will "log-on" to the CM application. The log-on message contains the aircraft's flight identifier (ID) and its ATN network address. The network address is unique to the aircraft; however, the flight ID is assigned on a per-flight basis. The flight ID is the controller's reference for the aircraft. The network address is used by the automation systems to communicate with the aircraft. The concept is similar to a URL and IP address in the Internet.

2. For a controller to communicate with a pilot using data link, the supporting ground automation system queries the CM application with a Flight ID. If the aircraft has logged-on, the CM will return the corresponding ATN network address. Using this address, the CPDLC application in the supporting ground automation system establishes a communication session with the CPDLC application in the avionics. Once this session is established, CPDLC messages (e.g., clearances) may be exchanged between the aircraft and the ground.

Secure CPDLC Operation

The following is an overview of the ATN security solution using CPDLC as an example. SGN4 WP0307 presents a more detailed description and SGN4 WP0310 presents a more detailed description of the ATN PKI.

At Context Management logon (step 1), the aircraft sends a CM logon message that is signed using the ATN Digital Signature Scheme. Upon receipt of this message (step 2), the Ground CM retrieves the public key certificate for the aircraft and the ground CPDLC application. The Ground CM validates that the certificates are authentic (signed by the appropriate CA), and then using the retrieved aircraft public key verifies the signature on the logon message. These operations provide the Ground CM assurance of the identity of the airborne CM and assurance of the source and integrity of the logon message.

The Ground CM next (step 3) derives a CM Session Key using the ATN Key Agreement Scheme. The Ground CM then (step 4) sends its own Public Key Certificate and the Ground CPDLC application's public key in the CM Response message that is tagged using the ATN

MAC Scheme. Upon receipt of this message (step 5), the aircraft in turn derives the same CM Session Key using the ATN Key Agreement Scheme. The aircraft then (step 6) checks the CM Response message tag using the ATN MAC Scheme. This sequence of operations provides the aircraft CM assurance of the identity of the ground CM and assurance of the source and integrity of the logon response message. In addition, since the aircraft has authenticated the Ground CM, it is able to trust that the CPDLC public key is authentic. In other words, the aircraft trusts that the Ground CM has validated the CPDLC Public Key Certificate.

When the Ground CPDLC queries the CM application for the ATN network address of a particular flight (step 7), it also obtains the public key of the aircraft (along with other key derivation data). The Ground and Aircraft CPDLC applications are now able to derive a shared Session Key using the ATN Key Agreement Scheme (steps 8 and 9). Subsequent CPDLC messages are tagged and checked using the ATN MAC Scheme (step 10). Both the Aircraft and Ground CPDLC applications are thus assured of the identity of the peer system and they are assured of the source and integrity of each message.

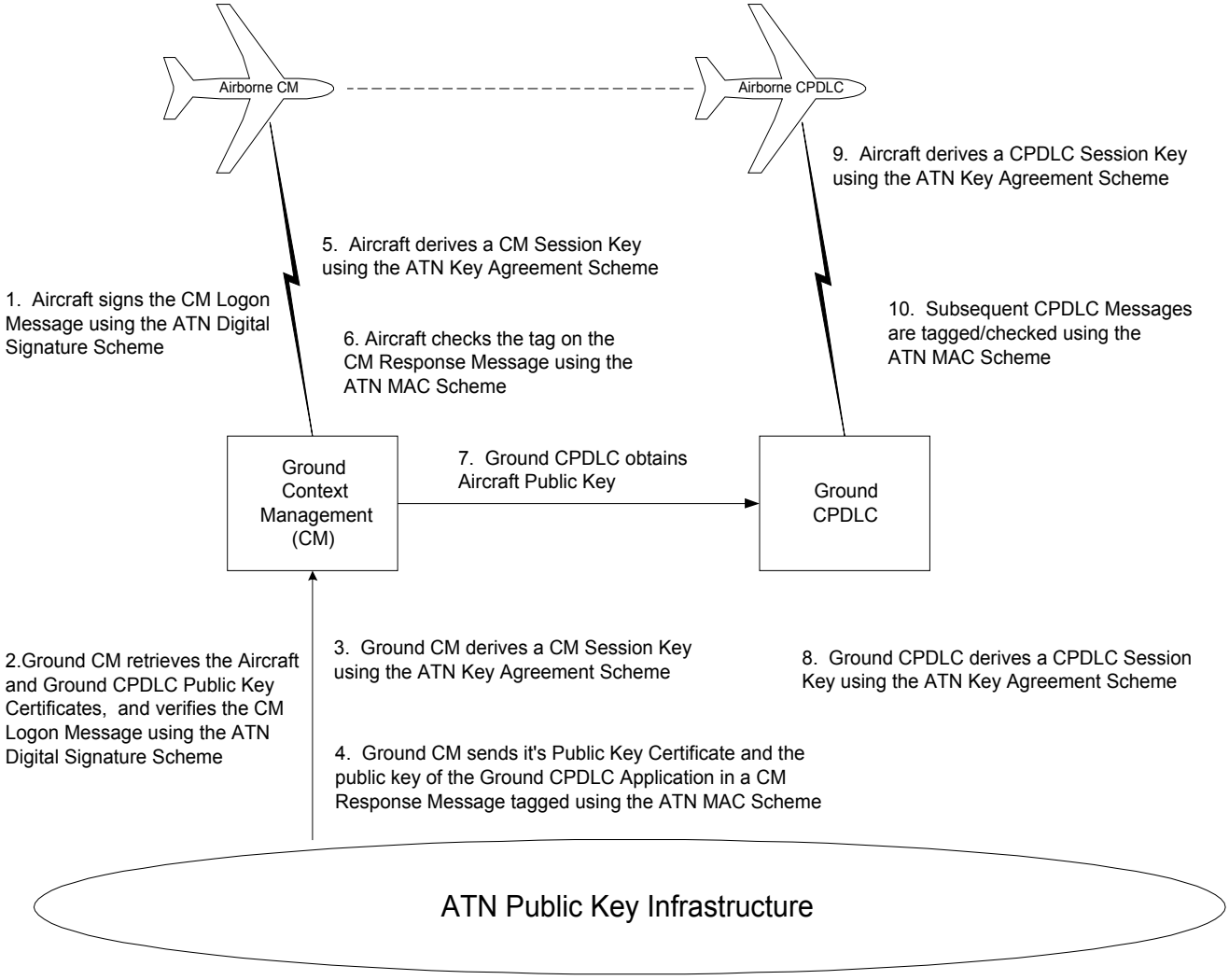


**Figure 1. – Overview of CPDLC Security Operation**

# 3 ATN Security in the ULCS

Figure 2 depicts the placement of security in the ULCS as defined in Edition 3 of Doc 9705. The general approach was to place security in the ULCS through the addition of a Security ASO, which in turn invokes SSO functions on behalf of an application based on the Dialogue Security Type signaled when the Dialogue Service is invoked. Edition 3 provides for a "Secured Dialogue Supporting Key Management" which is used in initial dialogue establishment between CM applications (Logon and Contact). This type provides for exchange of key agreement data and authentication. Edition 3 also provides for a "Secured Dialogue" which is provides authentication for applications.

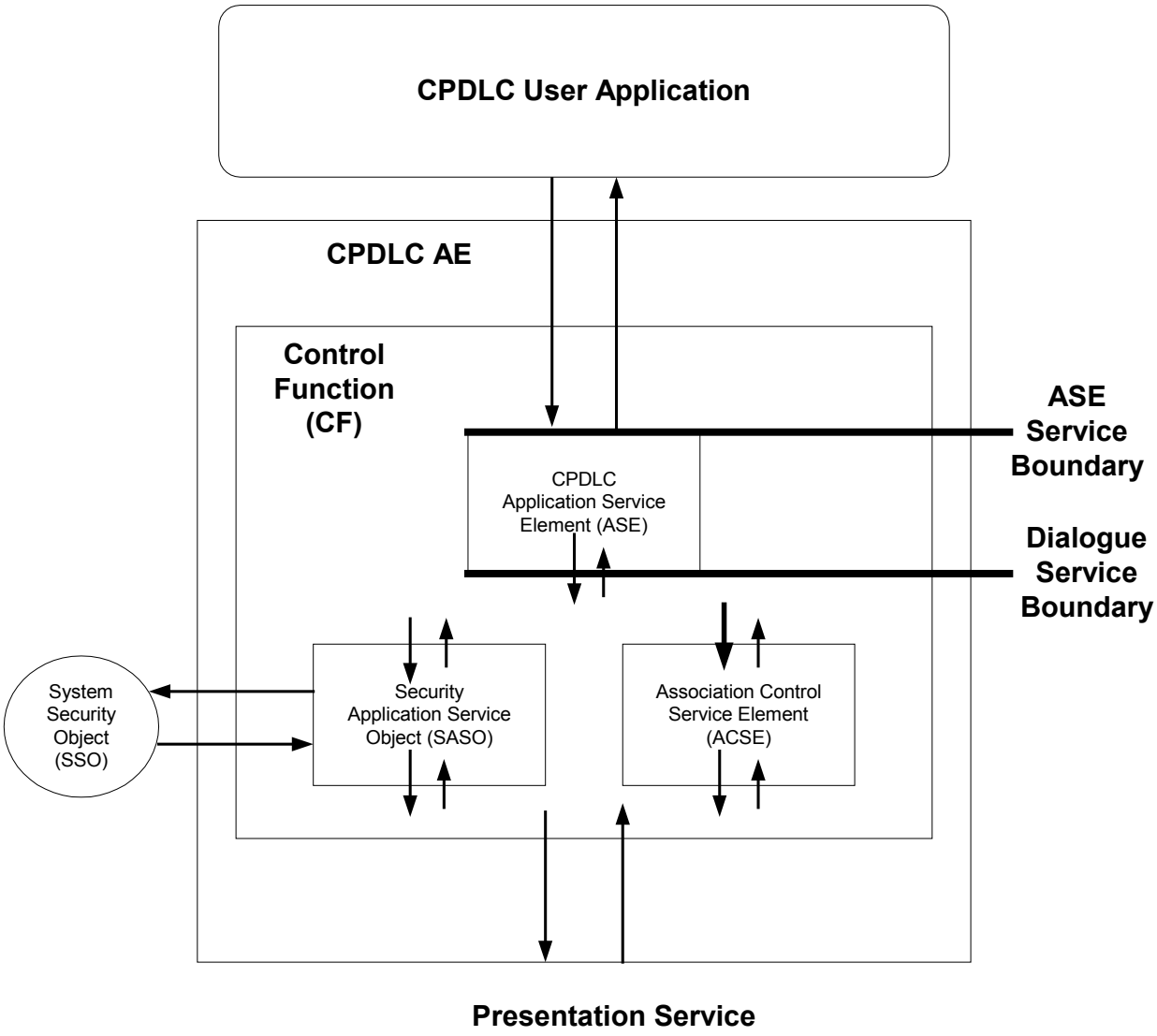


**Figure 2. – CPDLC Security using Edition 3 ULCS**

# 4 ATN Security in Context Management

As noted above Context Management uses "Secured Dialogue Supporting Key Management" if security is required. It should be noted however that ion doing so, Context Management must also perform certain application processing. Specifically Context Management (not the ULCS) must exchange key management data in application messages.

# 5 ATN Security at the Application Level

There are logically two options for implementing ATN Security at the application level as depicted in Figure 3. Under Option 1 the CPDLC User Application invokes the SSO while under Option 2 the SSO is invoked by the ASE.

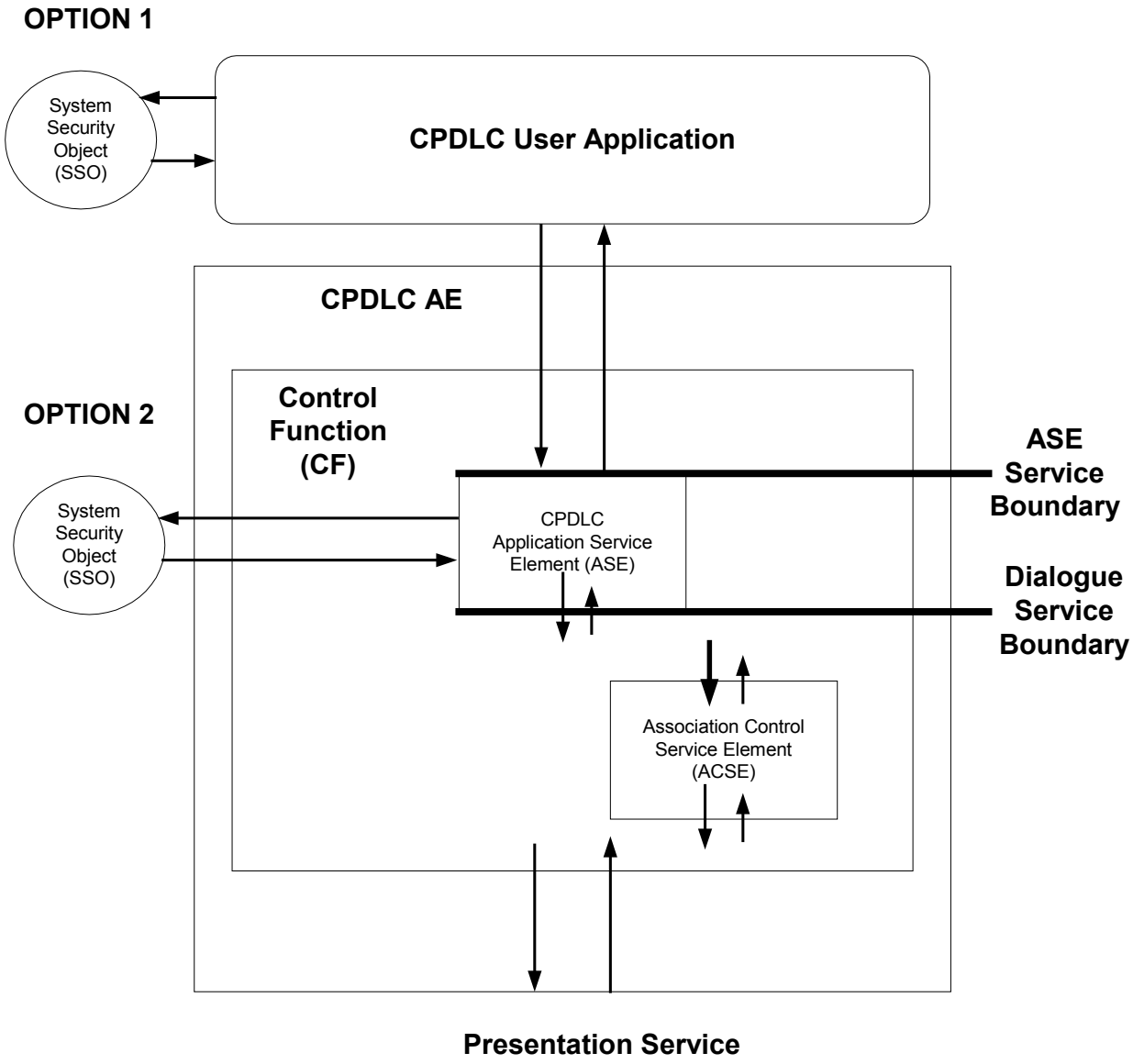


**Figure 3. – Options for CPDLC Application-Level Security (with Edition 2 ULCS)**

# 6 Considerations for Application-level Security

General Considerations

The first consideration is whether to adopt application-level security in general and when to do so. Ultimately this should be based on an integrated safety-security case. [see SGN4 WP0314] The motivation to adopt application-level security is to follow the PM_CPDLC approach while recognizing that Context Management already has application-level processing for the transport of keying information. Further motivation derives from on-going analysis of Edition 3 ULCS [see WGN03-WP13 and SGN4 WP0312] to better define security ASO service boundaries, a proposal to eliminate the SESE from the SASO [see SGN4 WP0311] and potentially not having to implement Edition 3 ULCS.

While potentially appropriate for CPDLC, it is not clear that application-level security is appropriate for other currently defined applications. For currently defined air-ground applications (ADS and FIS) the planned near and far-term use of these applications as well as their security-safety case should be considered. It has been recognized that AIDC has its own upper layer architecture, which although similar to the ULCS, does not have a currently defined security solution. [see SGN4 WP0108]

Another consideration is that "future" applications, which may be based on a modified or otherwise alternative upper layer architecture [see WGN03-WP02] or even be IP or web-based.

Considerations Common to Option 1 and Option 2

A number of items have been identified with direct invocation of the SSO by ATN Applications [SGN4 WP03013]. These items include determining an alternate entity identification method, defining alternate ASN.1 wrappers or modifying functions which are directly invoked, requiring the applications to encode abstract syntax, defining constraints on invocation of SSO functions, and extending PM-CPDLC to permit certificate exchange or use pre-stored certificates.

Considerations for Option 1

.In general, under this option either a Checksum or Cryptographic Integrity check would be computed based on CMA signaling of whether or not security is performed. With Option 1 the changes are isolated to the User Application. Whether this is an advantage depends on the implementation architecture. If there are many physical instances of the user application there must be may instances of the security software and associated keys. In addition depending on the architecture there are considerations related to assurance level of this software. Specifically the complete security solution may have to be certified at have to be at a high assurance level.

Considerations for Option 2

Under Option 2 it may be possible to have an architecture that continues to use PM-CPDLC (presumably at a high assurance level) and insert the security solution in the Application Entity, which by definition is that part of the overall application concerned with communications (and

potentially at a lower assurance level). See Figure 4. Given PM-CPDLC still generates a checksum there are two ways to "add in" the cryptographic integrity check, i.e. HMAC tag. One method is to simply overwrite the checksum with the HMAC tag. In this case the end-to-end integrity check moves to the AE. Alternatively, the HMAC tag may be XORed with the checksum. In this case the original checksum-based "integrity" check is maintained while at the same time application level authentication may be added to the AE.

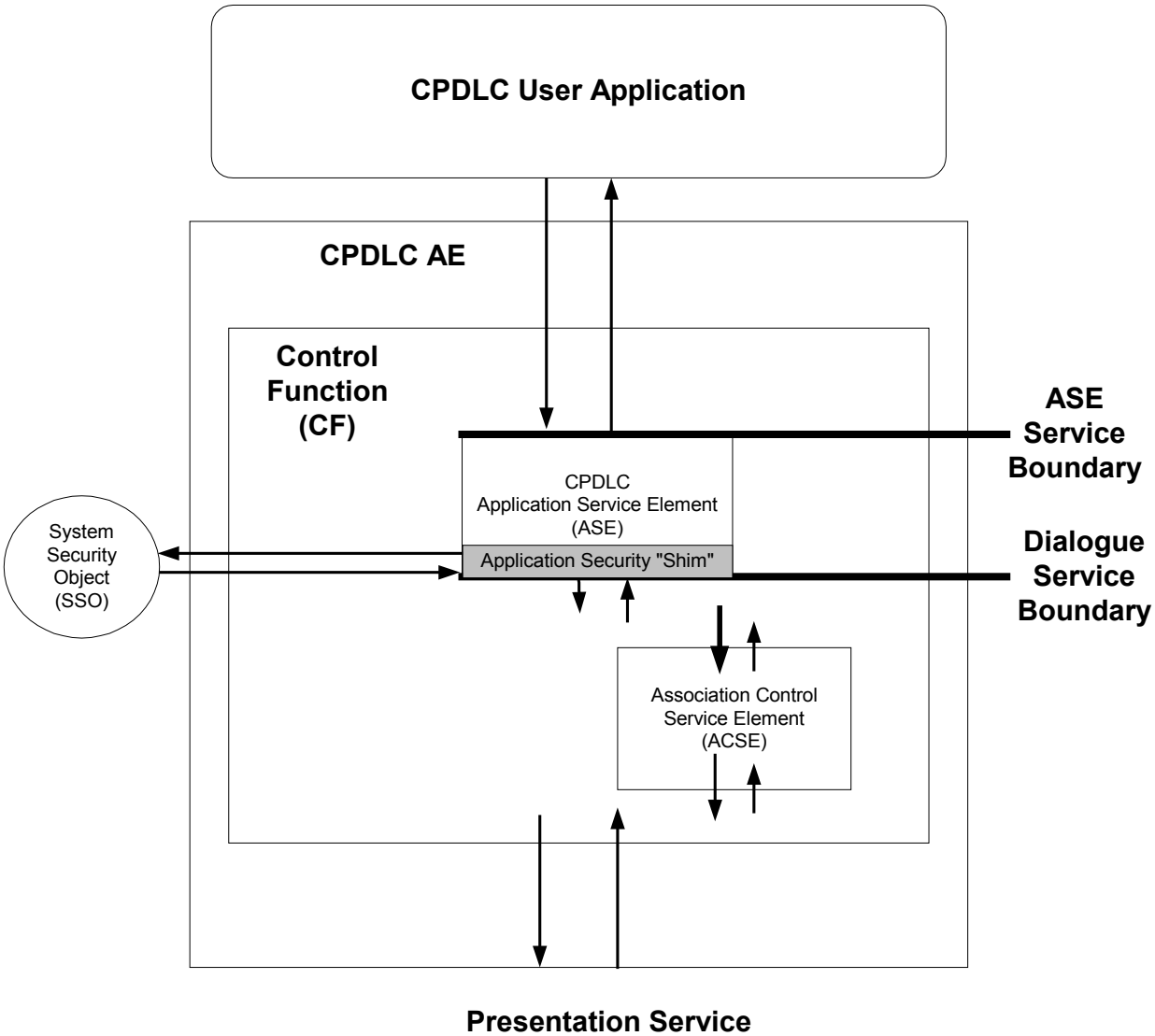


**Figure 4. – CPDLC Application-Level Security as a Shim**

# 7 Recommendation

The working group is invited to comment on the considerations for application level security and identify further considerations. After review of such considerations and the associated more detailed working papers it is recommended that the Working Group decide: whether to develop application level security, which option to develop, and whether or not to retain (or deprecate) the Edition 3 ULCS.