International Civil Aviation Organization

**ATN Seminar and Third ATN Transition Task Force Meeting**

Singapore, 26-30 March 2001

---

**Agenda Item 5: New ATN Features**

# AERONAUTICAL DATA LINK SECURITY

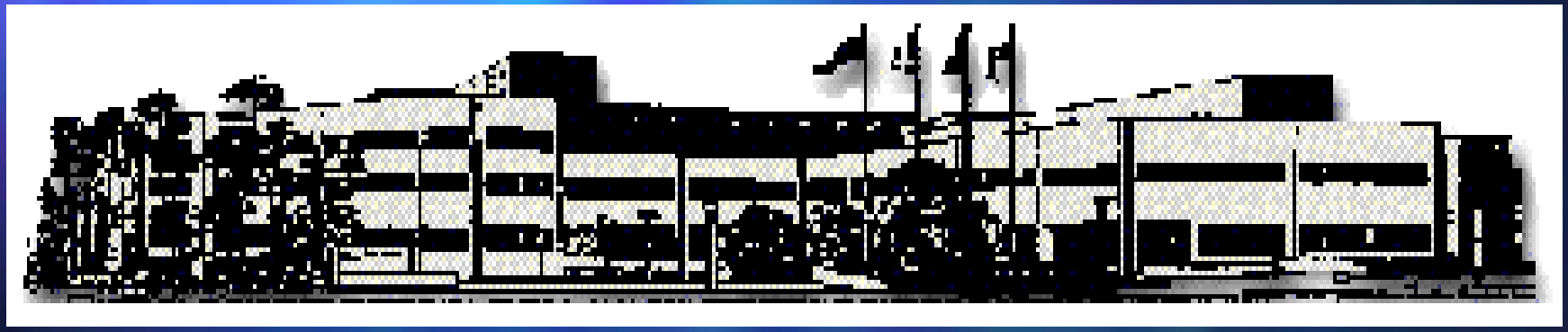
(Presented by Tom McParland, USA)

# Federal Aviation Administration (FAA)

## ~ ATN Seminar – Security~

## Singapore

*March 2001*



*Federal Aviation Administration (FAA) William J. Hughes Technical Center (WJHTC)*

## FAA/ACT-350

## ATN Technical Lead



# Aeronautical Data Link Security

*Tom McParland*

*(US FAA)*

# Presentation Overview

- **Current Status for Data Link Security**
  - ICAO ATN Standardization
- **Requirements for ATN Security**
- **Security Mechanisms**
  - Basic Mechanisms (Building Blocks)
    - Symmetric Encipherment
    - Asymmetric Encipherment
    - Hash Functions

# Presentation Overview

- Extended Mechanisms (Cryptographic Schemes)
  - Digital Signatures
    - Public Key Certificates
  - Key Agreement
    - Diffie-Hellman
  - Keyed Message Authentication Codes

# Presentation Overview

- **Security in ATN Systems**
  - ATN End Systems
  - ATN Intermediate Systems
  - AMHS Systems
- **Some Policy Issues**

# ICAO Standardization of ATN Security

- Technical Specification (Updates to ICAO Doc 9705) of ATN Security accepted at ATN Panel Working Group of the Whole Meeting, Berlin, Germany, August, 2000
- Minor Changes under CCB control to be submitted by end of March for publication by ICAO
- Associated Draft Guidance Material presented at ATNP Working Group Meeting, Hawaii, February-March, 2001
- Final due to ICAO in June 2001
- Security Sub-Group tasked to extend ATN security to support Confidentiality and to define options for Certificate Delivery Service

# Requirements for ATN Security

- ATN END SYSTEMS
  - ATN end systems shall authenticate the identity of peer end systems.
  - ATN end systems shall authenticate the source of application messages.
  - ATN end systems shall ensure the integrity of application messages.

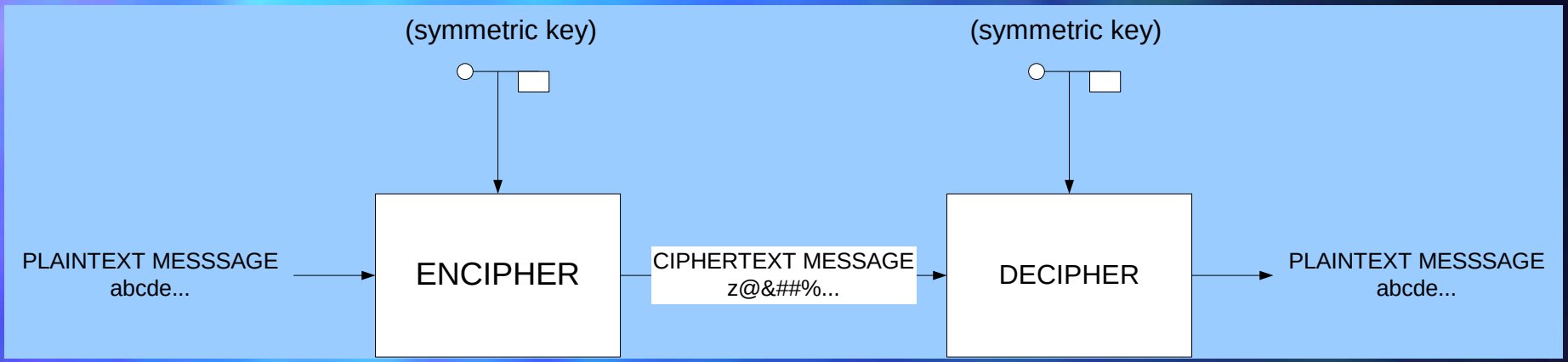
# Requirements for ATN Security

- ATN INTERMEDIATE SYSTEMS
  - ATN ground and air-ground boundary intermediate systems shall authenticate the identity of peer boundary intermediate systems.
  - ATN ground and air-ground boundary intermediate systems shall authenticate the source of routing information.
  - ATN ground and air-ground boundary intermediate systems shall ensure the integrity of routing information.


# Cryptographic Building Blocks

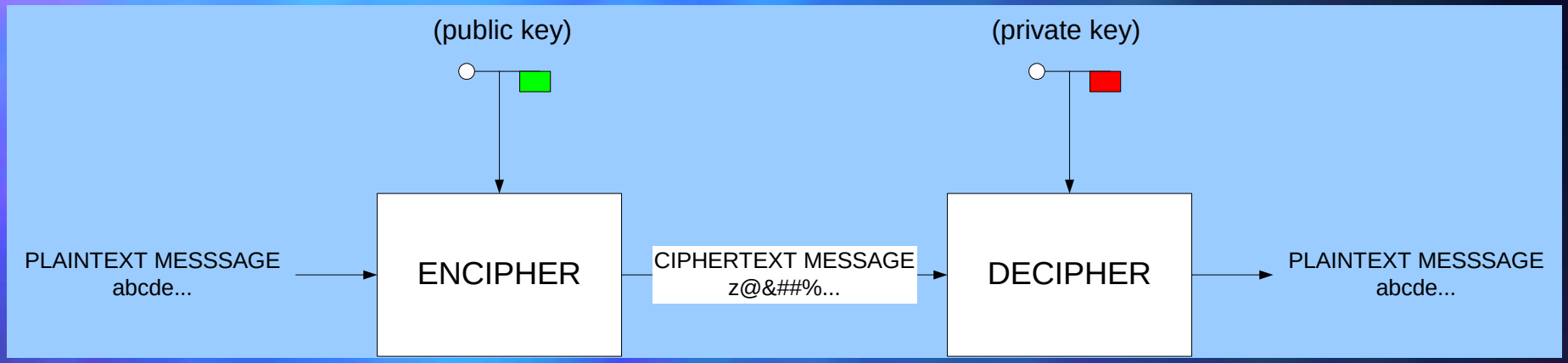

- Symmetric Encipherment
- Asymmetric Encipherment
  - Encipher under Public Key
  - Encipher under Private Key
- Hash Functions

# Symmetric Encipherment



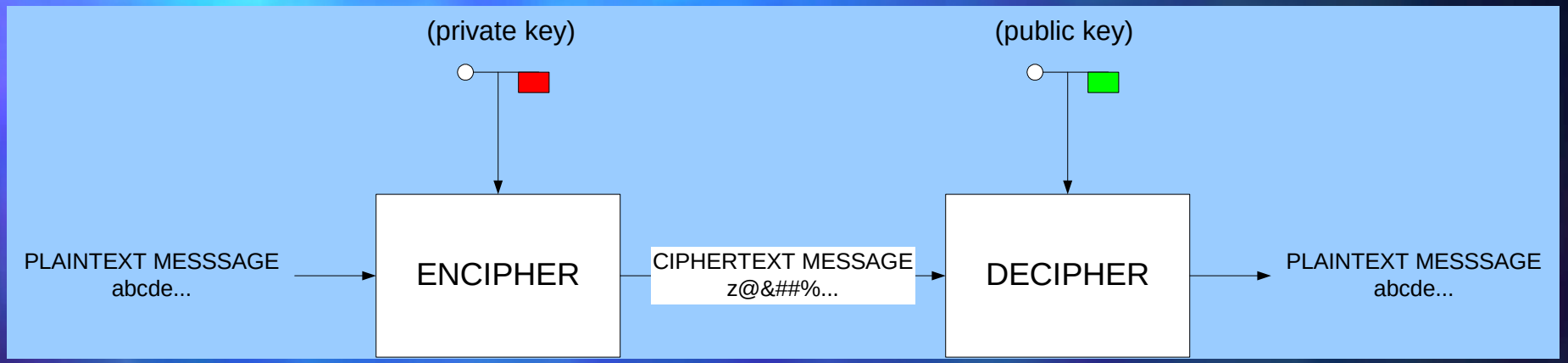

- Conceptually simple, same secret key used for enciphering and deciphering
- Efficient in terms of computational requirements and key size and works well for small group of authorized parties
- Used to build Encryption and Authentication Exchange Schemes

# Asymmetric Encipherment (encipher under public key)




- Only the private key need be kept secret.
- The public key can be freely distributed - *almost*
- Used to build Encryption Schemes

# Asymmetric Encipherment (encipher under private key)

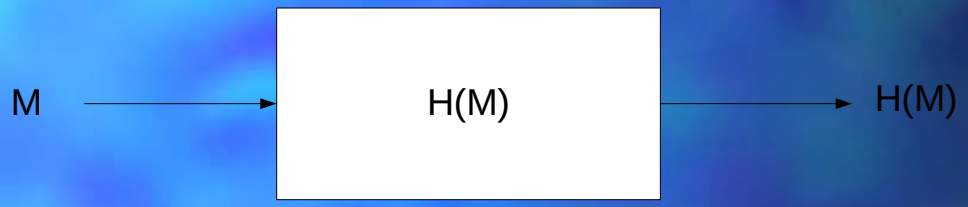



- Used to build Authentication Exchange Schemes

# Basis for Asymmetric Encipherment

- Integer factorization problem - 1977
  - RSA Encryption and Digital Signatures widely used
  - 1024 bit keys
- Discrete logarithm problem - 1976
  - Diffie-Hellman Key Agreement, Digital Signature Algorithm (DSA)
  - 1024 bit keys
- Elliptic curve discrete logarithm problem - 1985
  - ECDSA and EC Diffie-Hellman
  - 160 bit keys

# Hash Functions




- A cryptographic hash function is a mapping from an arbitrary long input M to a short (fixed-length) output value H(M)
- Like error correction code but with “collision resistance” and “pre-image resistance” which permit detection of deliberate modification
- Used to build Integrity Schemes

# Summary
# Cryptographic Building Blocks

| Symmetric Encipherment | Asymmetric Encipherment (under public key) | Asymmetric Encipherment (under private key) | Hash Functions |
|---|---|---|---|
| - Authentication Exchange<br>-Encryption | -Encryption | - Authentication Exchange | -Integrity |

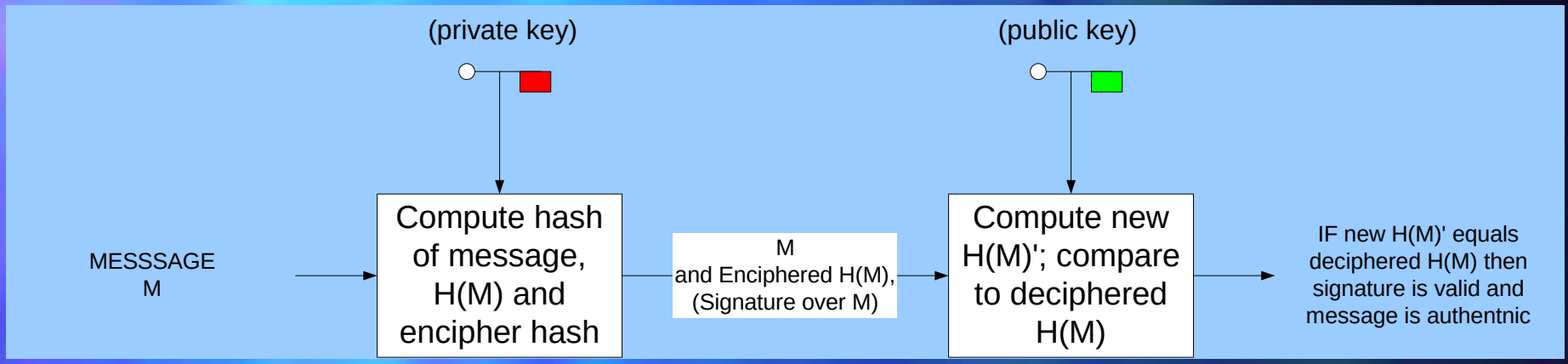
# Cryptographic Schemes

- Authentication Exchange Techniques
- Digital Signatures
  - Public Key Certificates
- Key Agreement
- Message Authentication Codes

# Public Key Authentication

- Using public key techniques, authentication can be accomplished by having the claimant demonstrate possession of her private key.

# ymmetric Authentication by Digital Signatu




- Claimant (ALICE) demonstrates possession of private key.
- Relying party (BOB) verifies by decrypting using ALICE's public key
- In principle works, but in practice is subject to masquerade

# Authentication Exchange Masquerade

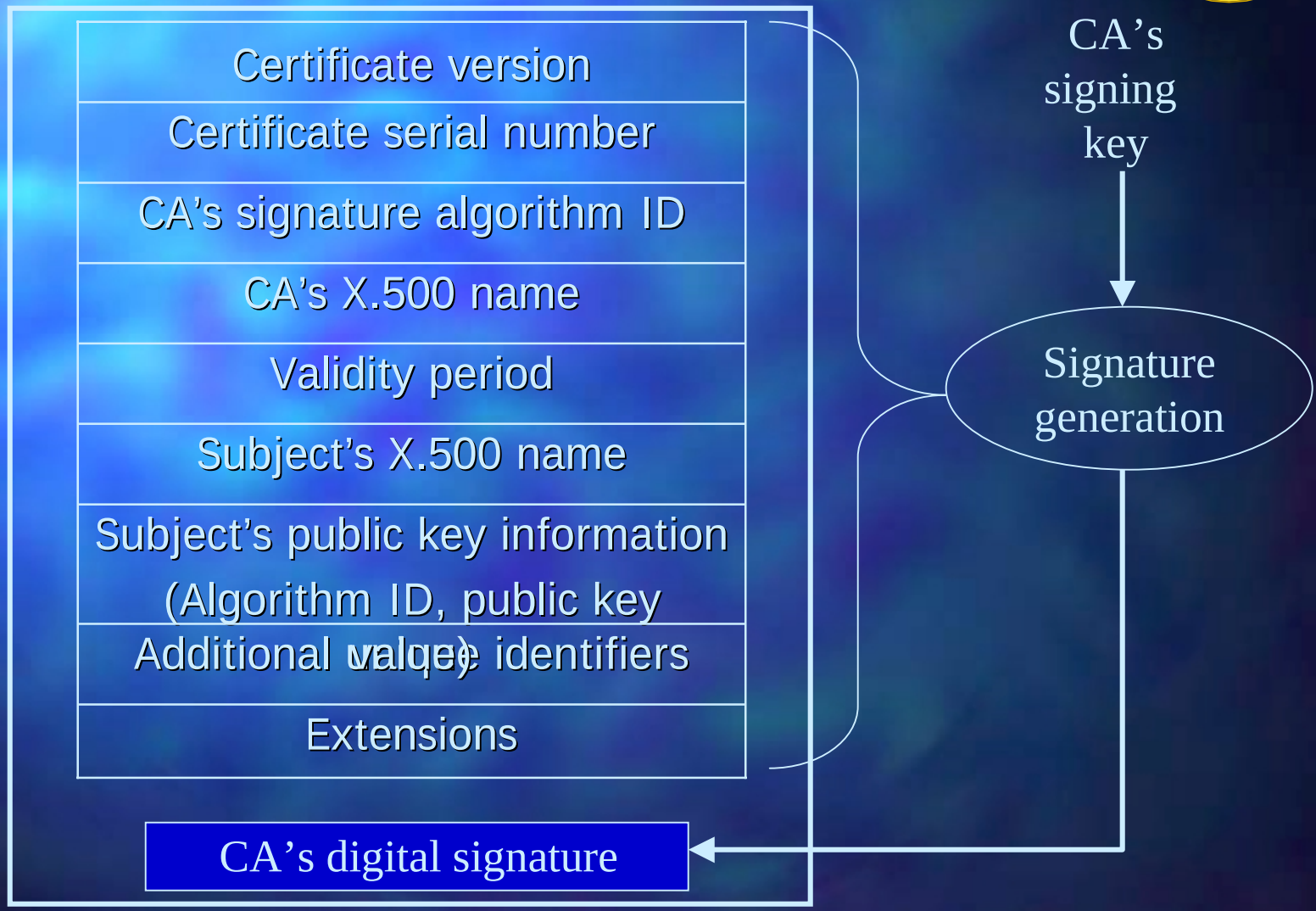
- Problem: in a public-key scheme, Bob needs a genuine copy of Alice's public key.
- Otherwise an attacker can substitute a fake key as Alice's public key and use this to masquerade as Alice.

# Solution: get Alice's key in a Public Key Certificate

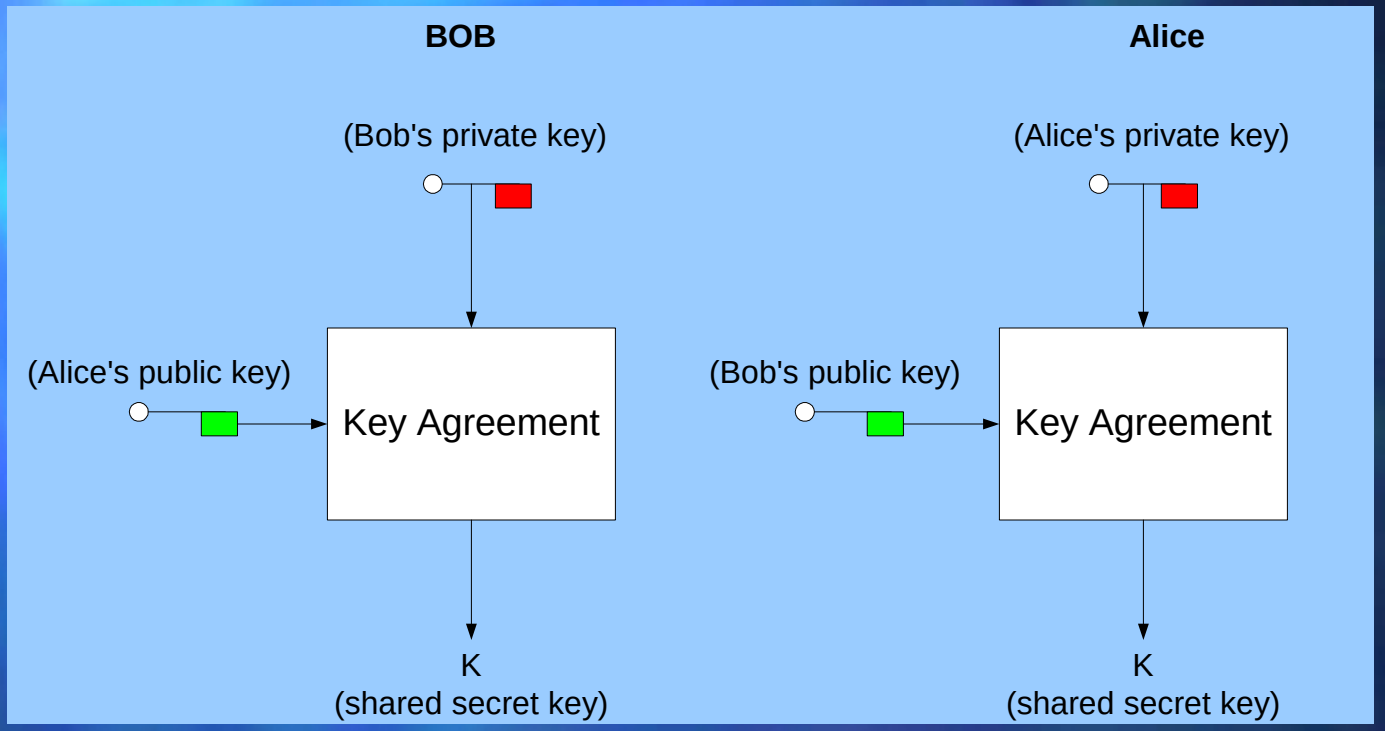
A trusted third party termed a Certificate Authority (CA) binds Alice and her public key.

- Alice goes to the CA with her public key.
- CA issues a certificate to Alice containing her identity, her public key, and the CA's signature on her identity and public key.
- Bob obtains the CA's public key.
- Bob verifies the CA's signature on Alice's certificate and retrieves her public key. In this way Bob knows that he has an authentic copy of Alice's public key
- *Consider analog of driver's license or passport*

# X.509 Public Key Certificates

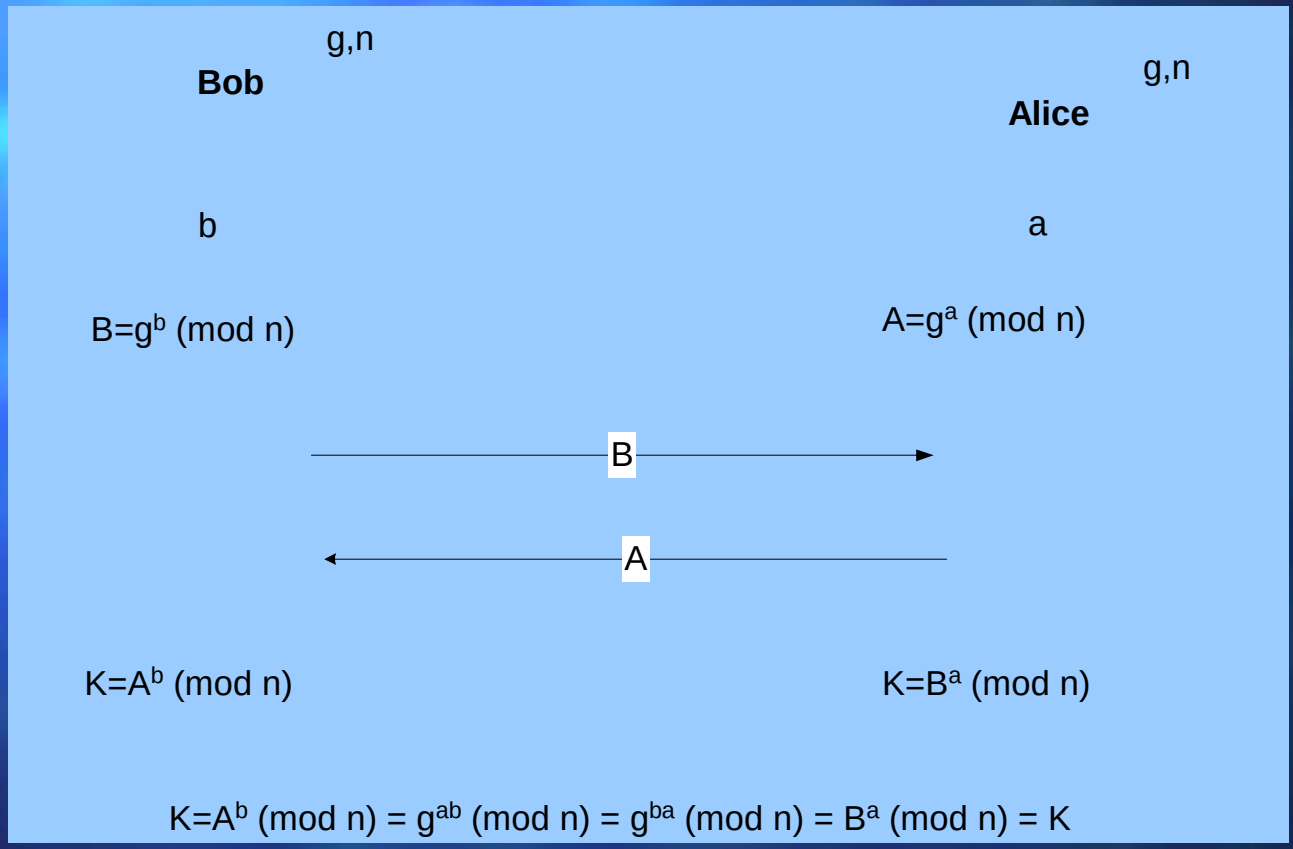


# Derivation of a Shared Secret Key by Key Agreement




- Key Agreement permits two entities (BOB and ALICE) to arrive at a shared secret key using each other's public key.
- They can ten use more efficient symmetric cryptographic schemes.

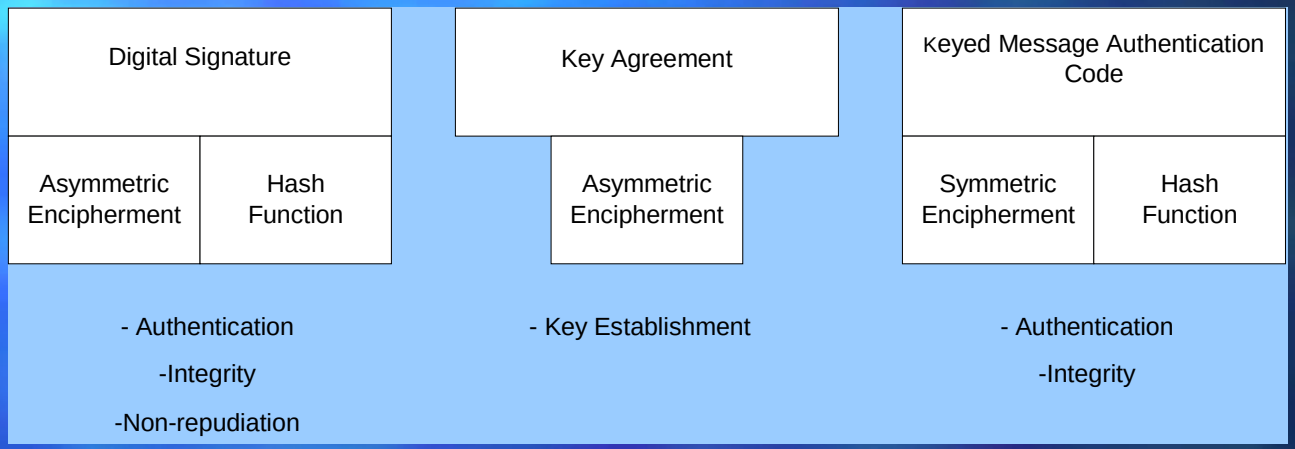
# Diffie-Hellman Key Agreement



# Symmetric Authentication using Keyed Message Authentication Code (HMAC)


- Alice and Bob agree in and advance to a secret key (k), or arrive at shared secret key (k) using Key Agreement
- Alice sends message with HMAC tag computed using a shared ( k)
- Bob verifies received HMAC tag and knows it is from Alice because only Alice is in possession of or could have generated (k) used in the HMAC

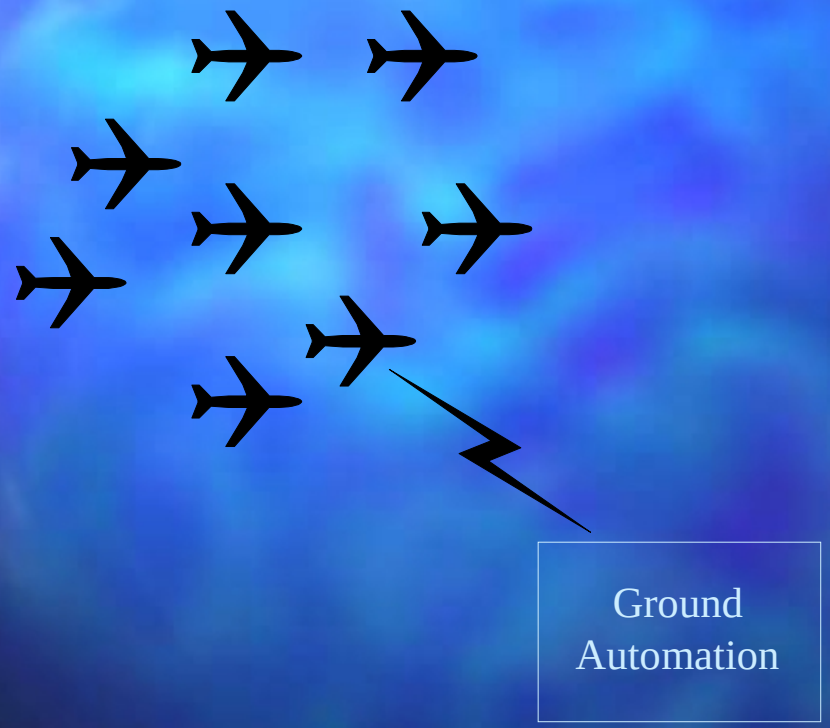
# Summary
# Cryptographic Schemes



# ATN Cryptographic Schemes

- The ATN Digital Signature Scheme uses the Elliptic Curve Digital Signal Algorithm with the Secure Hash Algorithm 1 (SHA-1) for the hash function.
- The ATN Key Agreement Scheme uses the Elliptic Curve variant of the Diffie-Hellman Key Agreement method
- The ATN Keyed Message Authentication Code Scheme uses the HMAC technique with SHA-1 for the hash function.

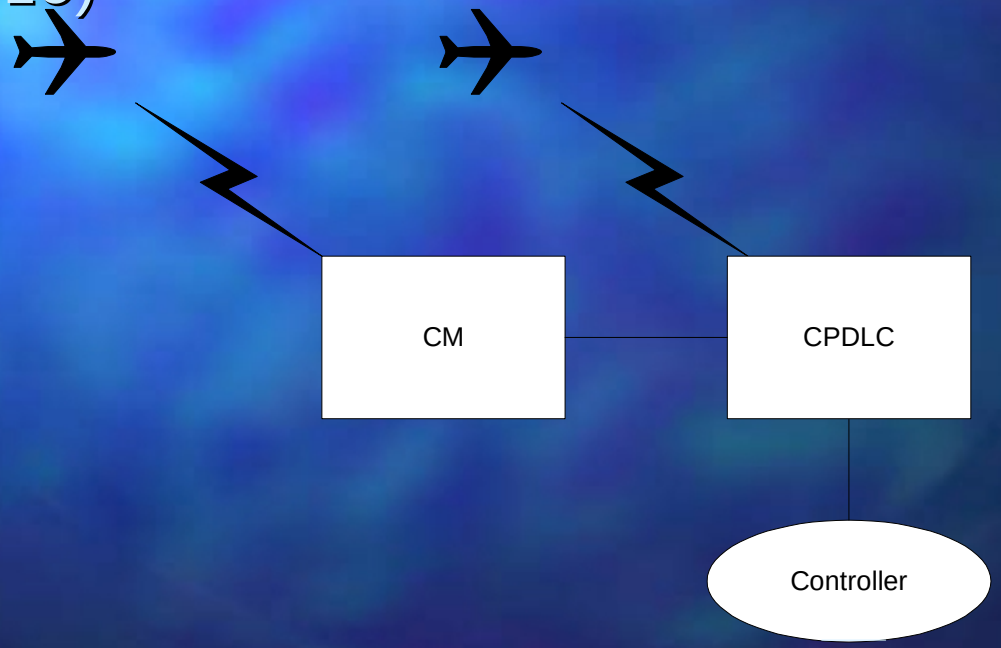
# Data Link Security Problem



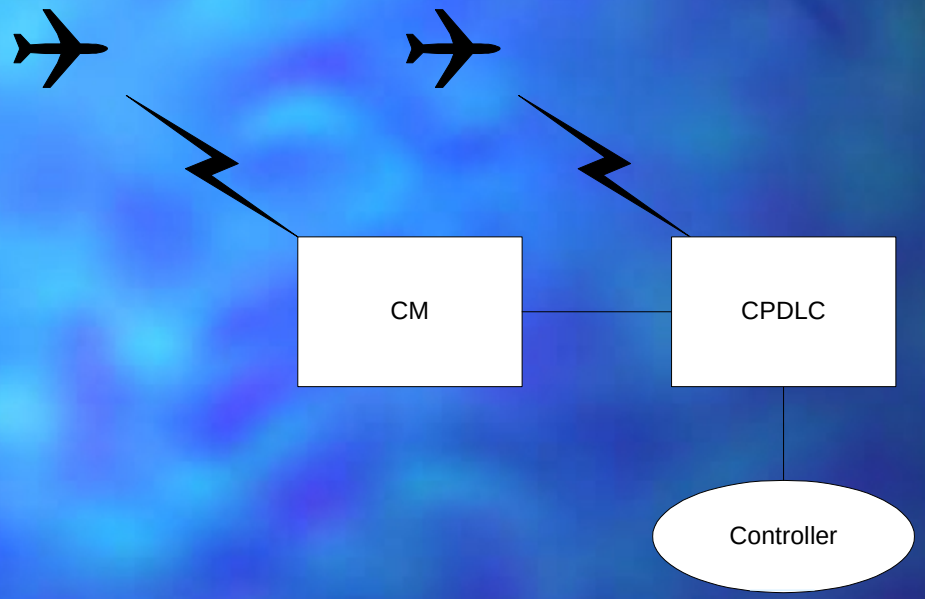

- Thousands of aircraft need to communicate securely with ground automation systems over air-ground sub-networks that are bandwidth limited.

# CM and CPDLC Operation

- Data Link (for air traffic) involves two applications:
  - Context Management (CM)
  - Controller Pilot Data Link Communications (CPDLC)

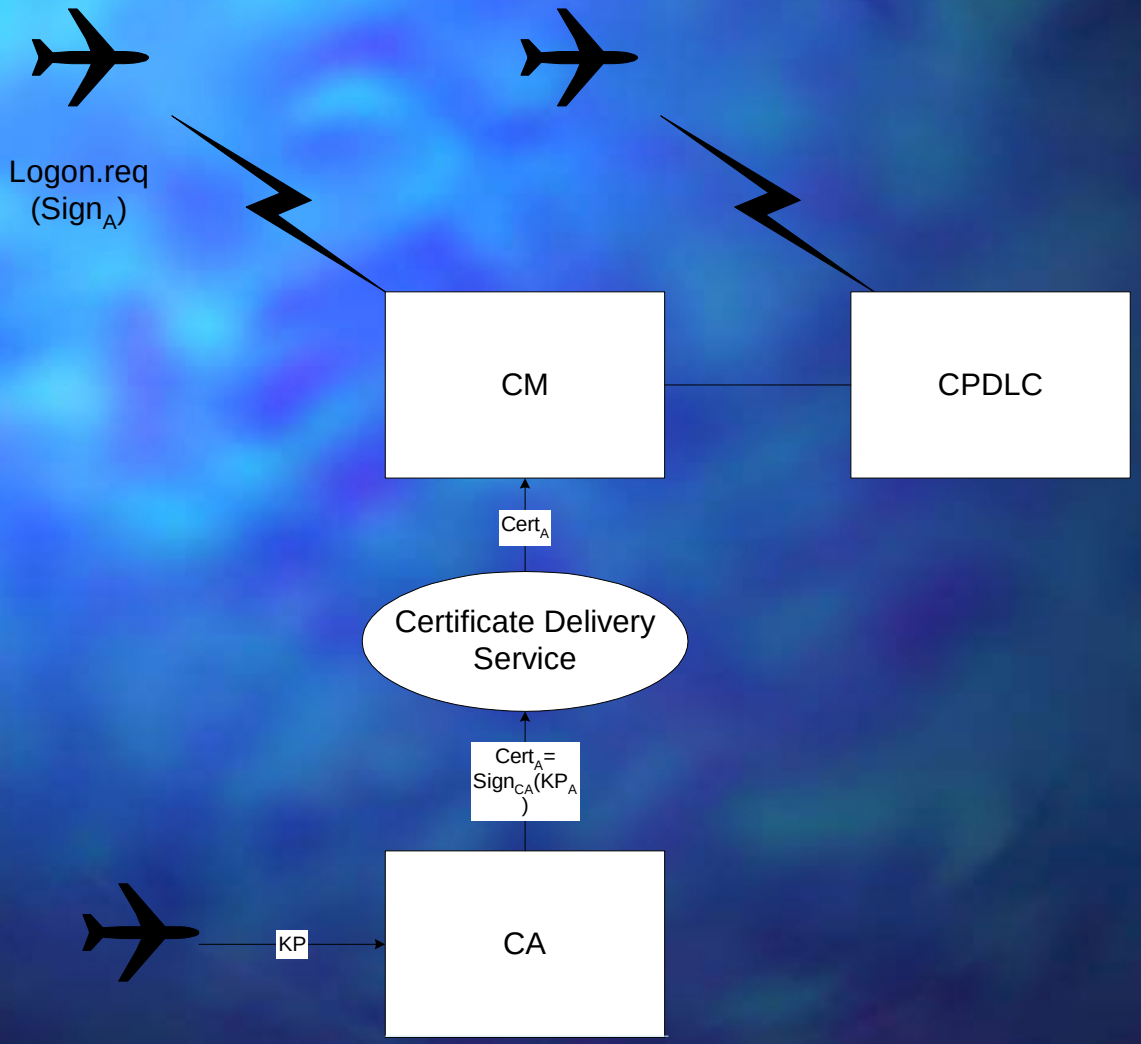


# Digital Signature for CM

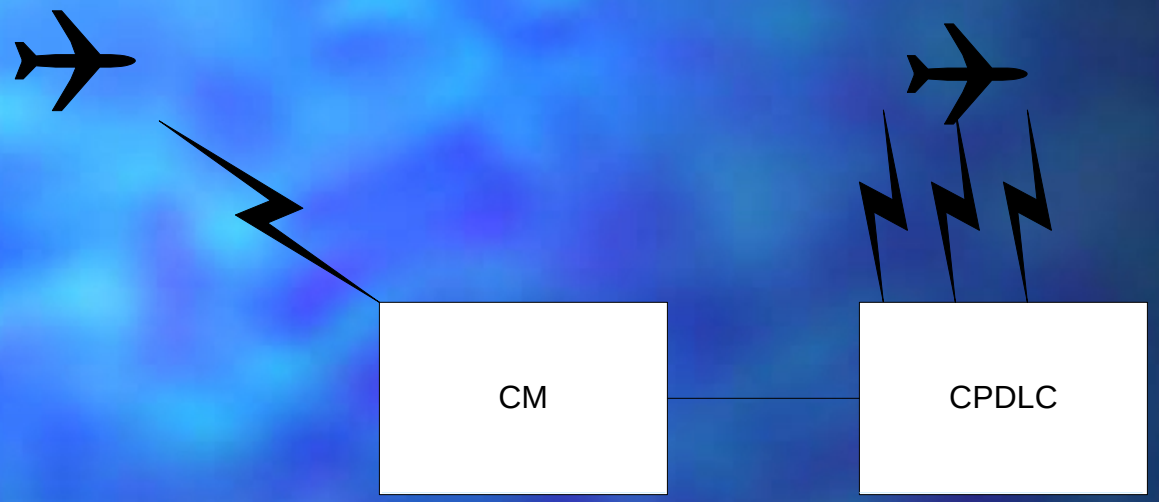



- Ground CM can authenticate the Logon message provided CM has the public key of the aircraft.
- There are two challenges:
  - Getting the key
  - Ensuring it is authentic

# X.509 Certificates

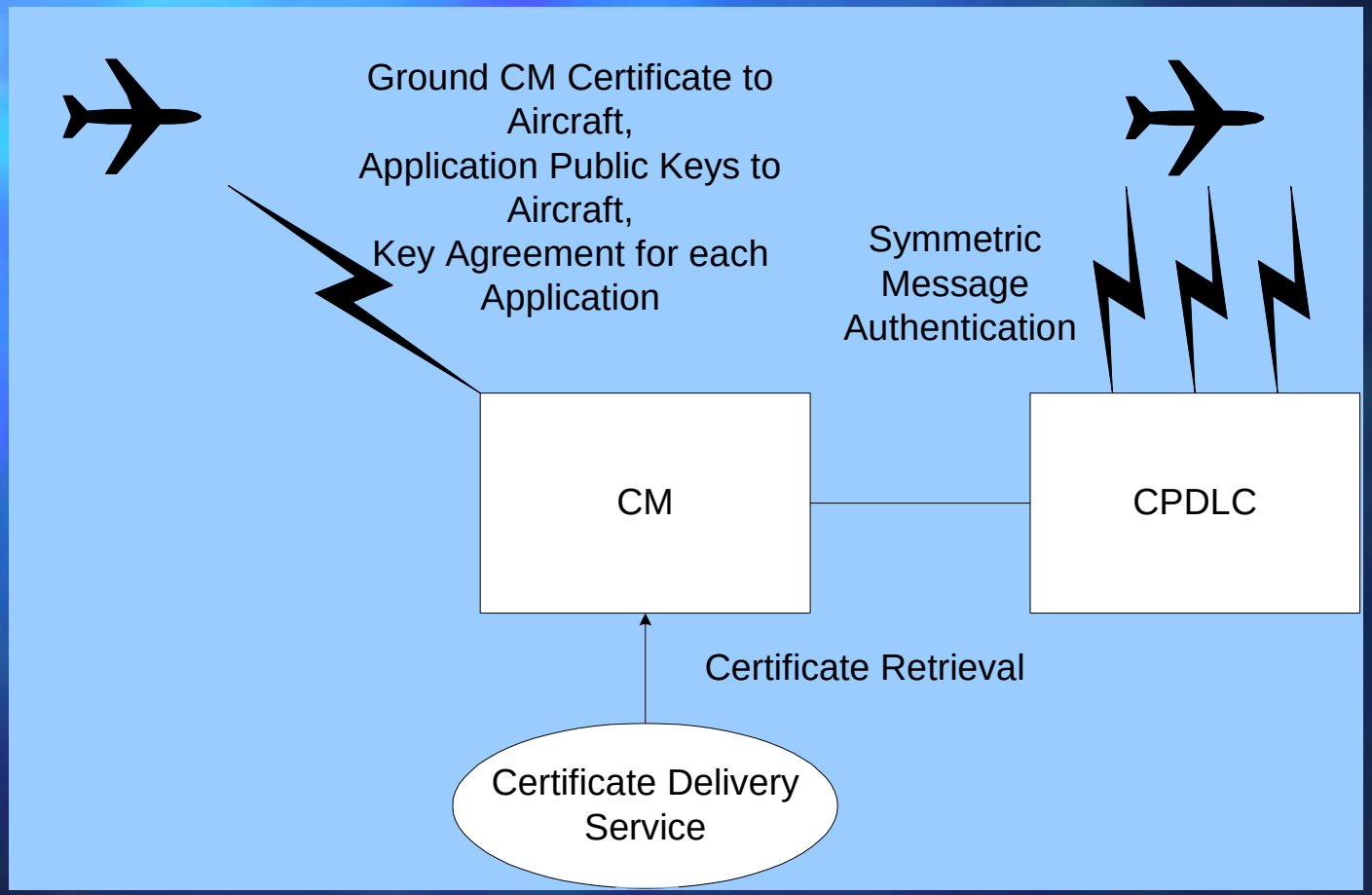


# Data Origin Authentication of CPDLC Messag

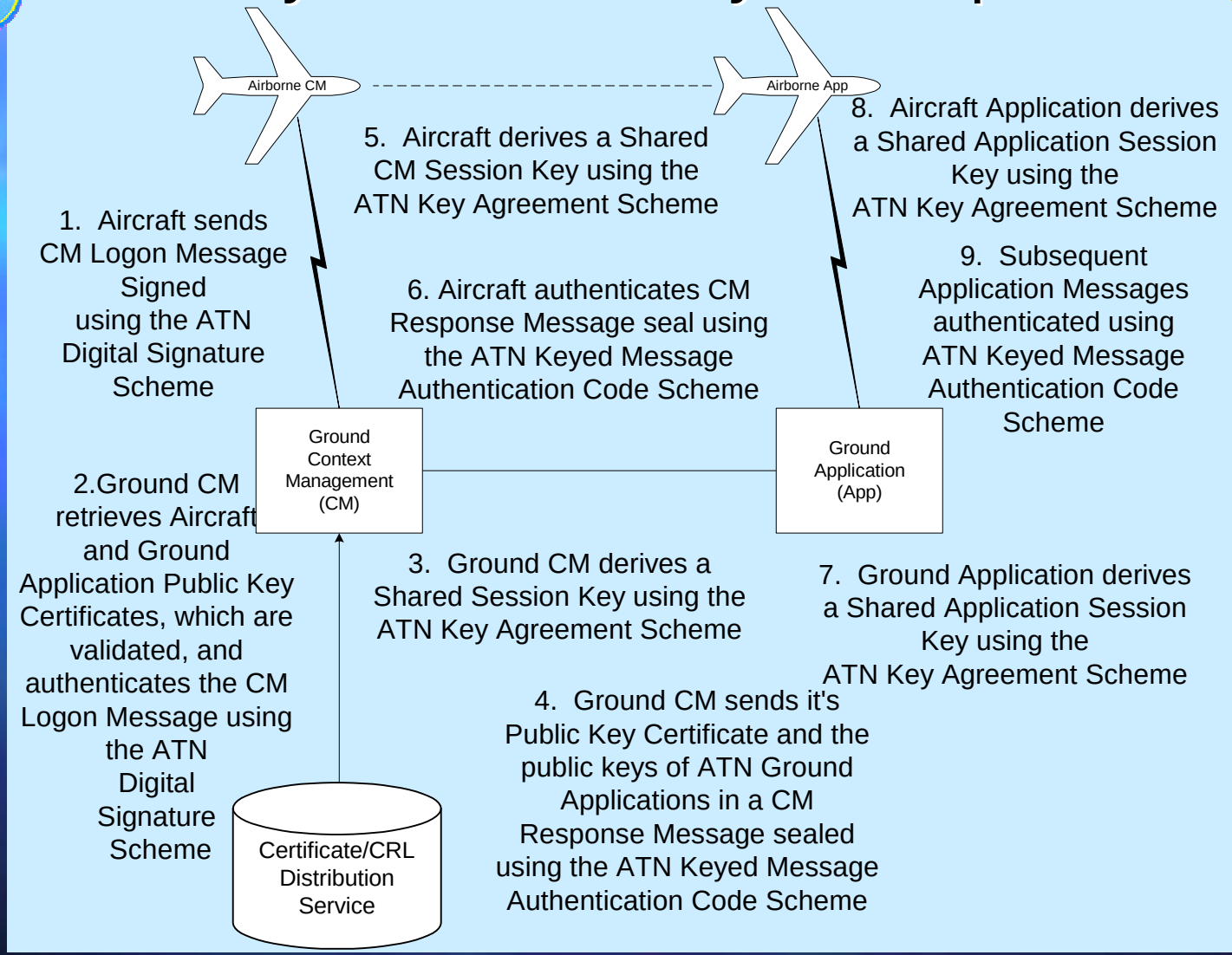



- There are numerous application messages exchanged
- Digitally signing each message incurs too much overhead.

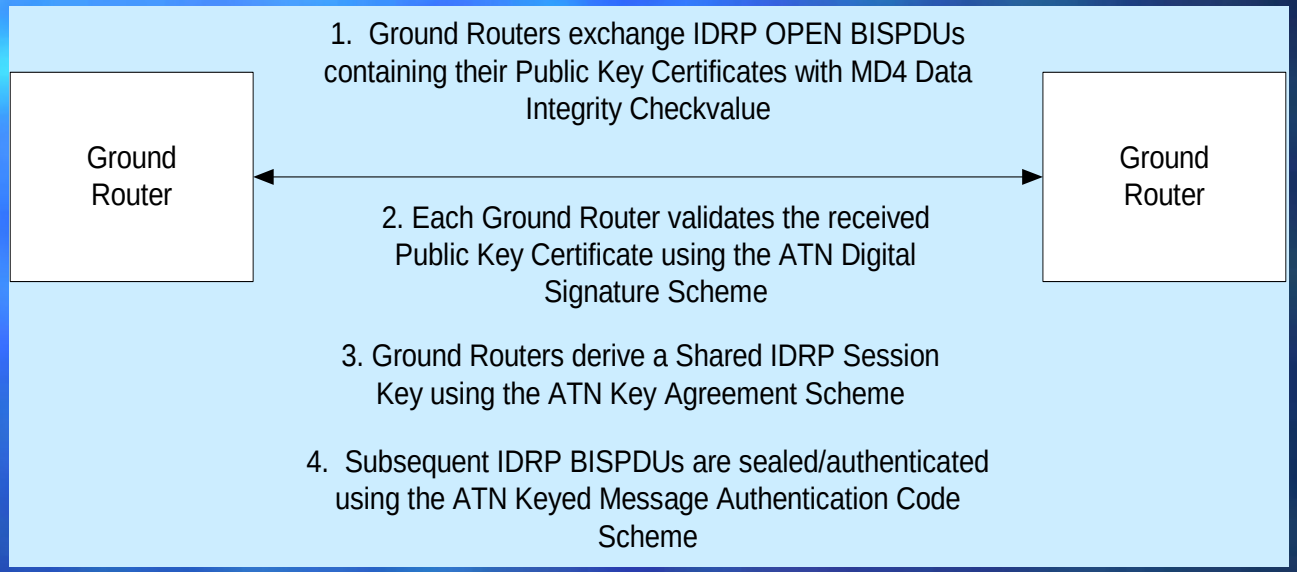
# Key Agreement - Keyed Message Authentication



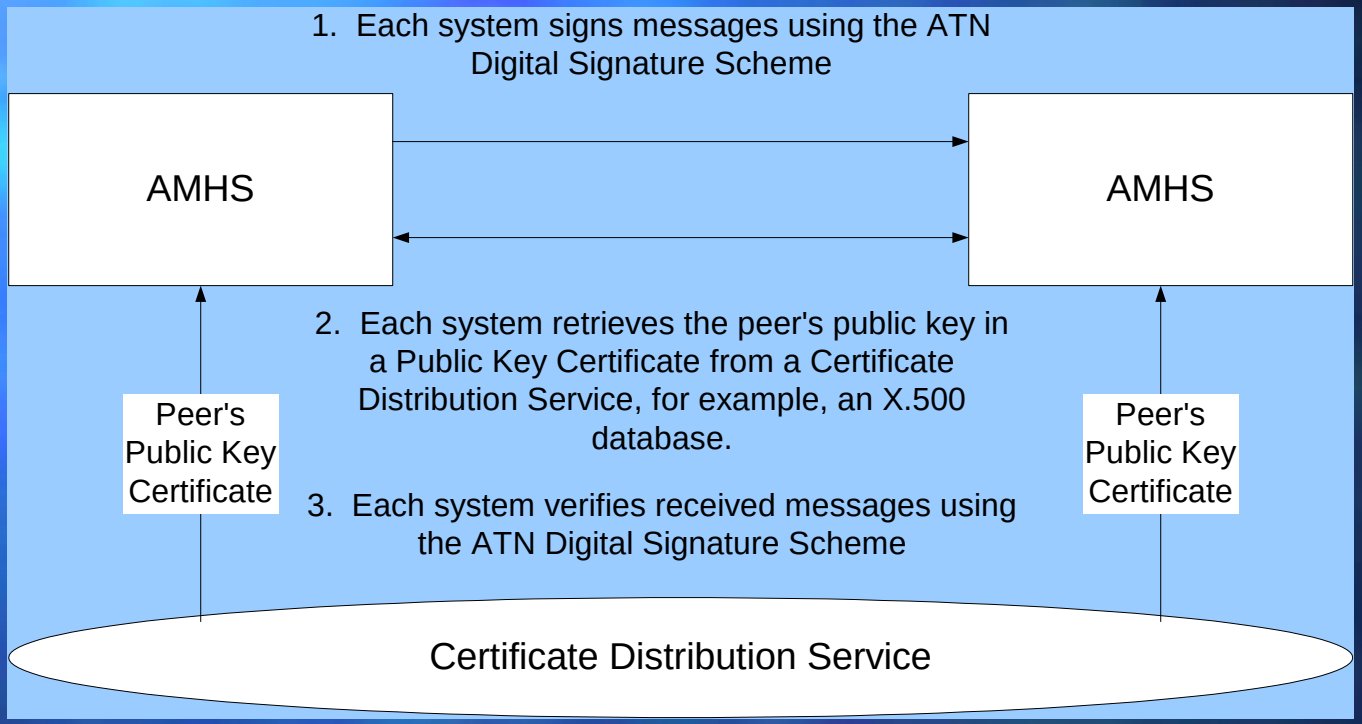
# Summary of ATN End System Operation



# Ground-Ground Intermediate System Operation



# ATN MESSAGE HANDLING SYSTEM Operation



# Some Policy Issues for ATN Security

- When to implement security - sunset date(s)
- Establishment of Bilateral Agreements
  - for Certificate Distribution Service
  - for CA Cross Certification