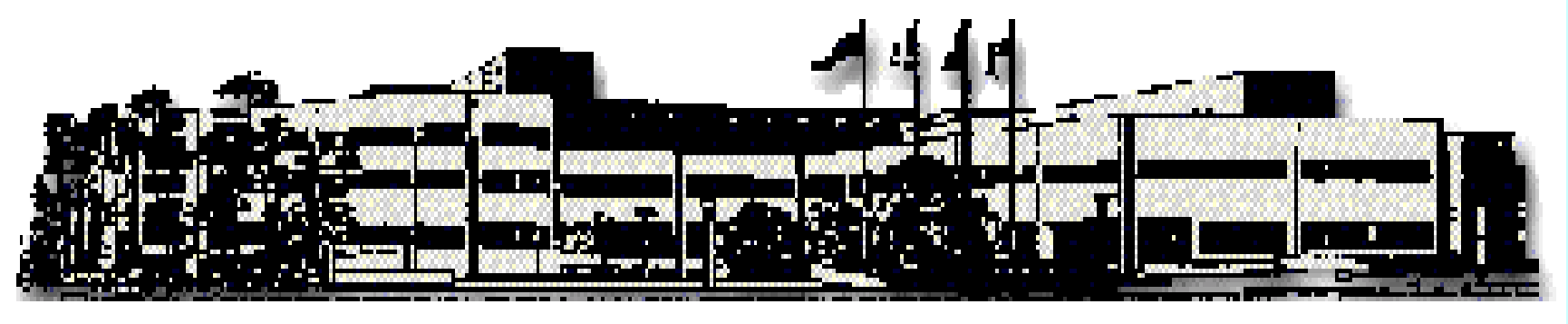
~ ATN Seminar – ATN Security ~

Chiang Mai, Thailand

December 2001



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

ATN Security Concepts and Overview

Tom McParland, BCI

(US FAA)

Security

- In a general sense, Security is about managing risks
- Risk management involves the application of controls which contribute to mitigation of risks
- A taxonomy of controls
  - Management controls
  - Technical controls
  - Operational controls

Security

- Management controls
  - focus on management of system and associated risks
  - Security reviews, security risk assessments
- Technical controls
  - address specific types of threats
  - may be sub-typed as: preventative technical controls, recovery technical controls, and support technical controls
- Operational controls
  - focus on operational procedures, personnel security measures, and physical security measures

ATN Security

- ATN Preventative Technical Controls
  - Authentication
  - Integrity
  - Key Establishment
  - Access Control
- ATN Support Technical Control
  - ATN Public Key Infrastructure

- The above controls have been specified in Edition 3 of Doc 9705; Confidentiality is not yet specified but is on work plan

SECURITY SERVICES AND MECHANISM

SECURITY SERVICES

CONFIDENTIALITY

AUTHENTICATION, INTEGRITY

KEY ESTABLISHMENT

AUTHENTICATION, INTEGRITY

SECURITY MECHANISMS

Cryptographic Schemes

Encryption Scheme

Digital Signature Scheme

Key Agreement Scheme

Message Authentication Code Scheme

Cryptographic Building Blocks

Asymmetric Encipherment (under public key)

Asymmetric Encipherment (under private key)

Asymmetric Encipherment (under private key)

(Keyed) Hash Function

OR

Symmetric Encipherment

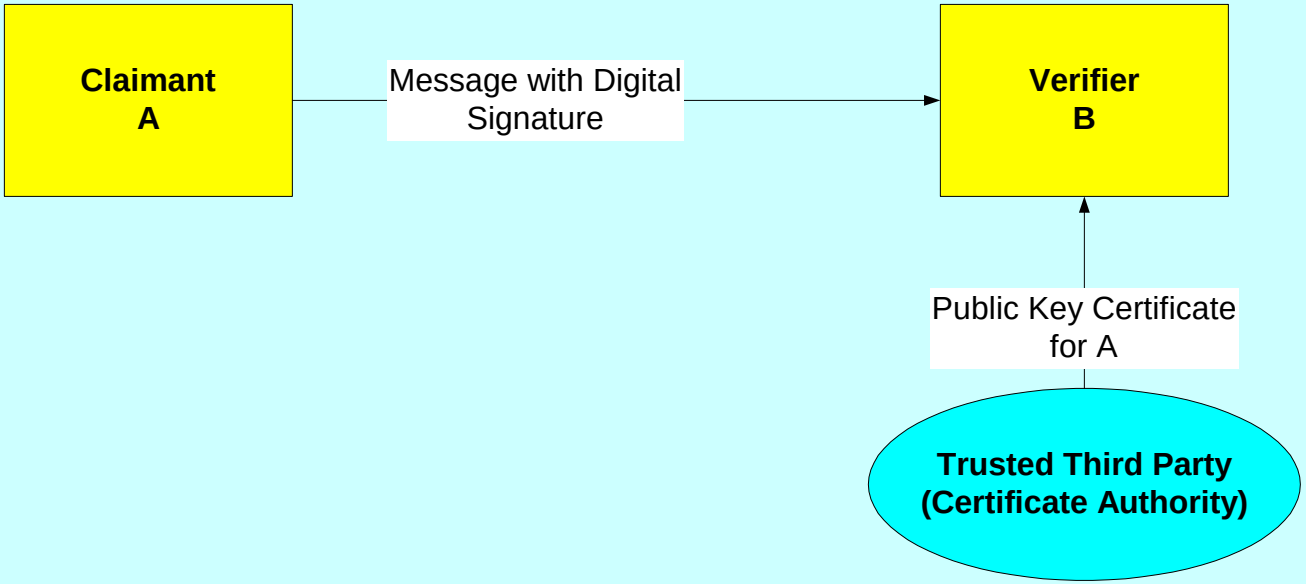
AND

Hash Function

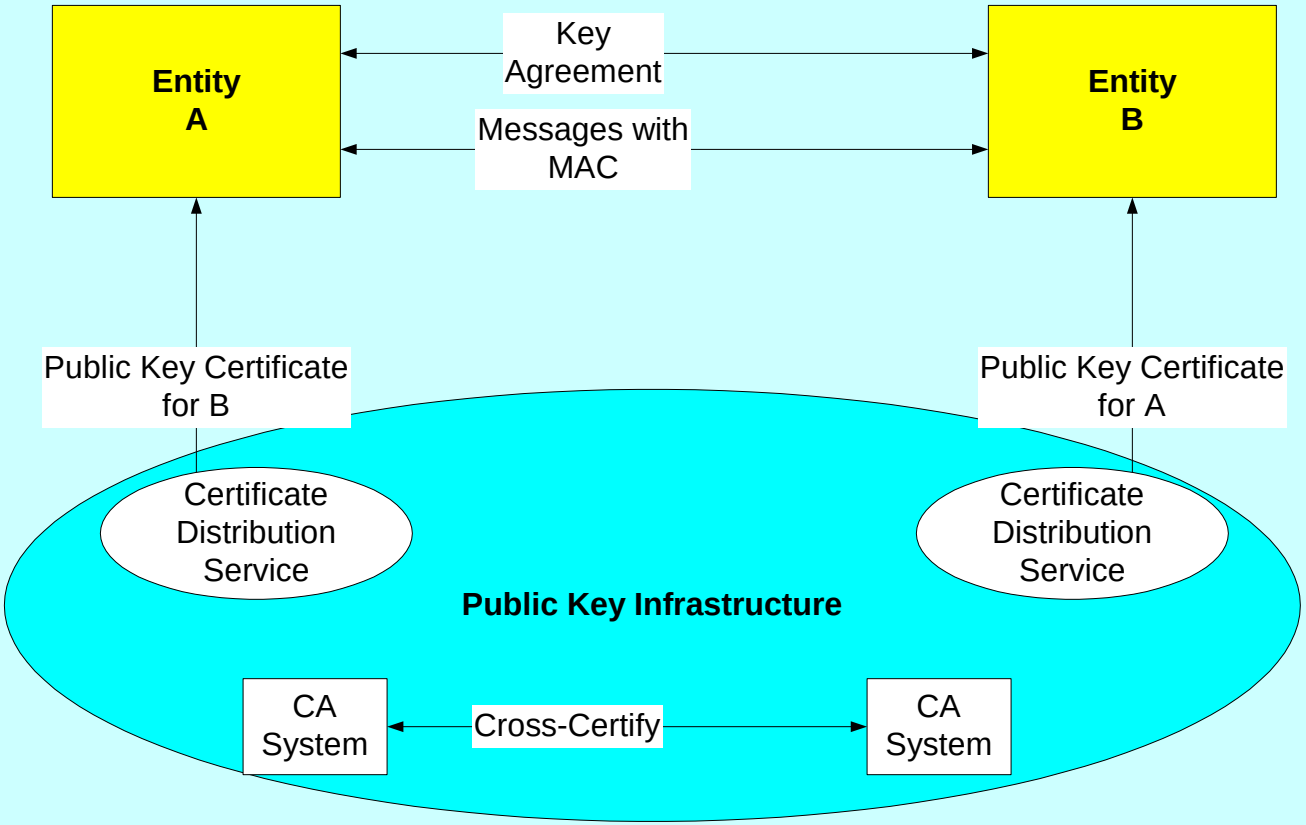
Authentication

- Authentication involves three entities
  - Claimant
  - Verifier
  - Trusted Third Party
- Examples
  - Traveler, Passport Control Agent, Passport Issuing Agency
  - Driver, Law Enforcement Officer, State Licensing Bureau

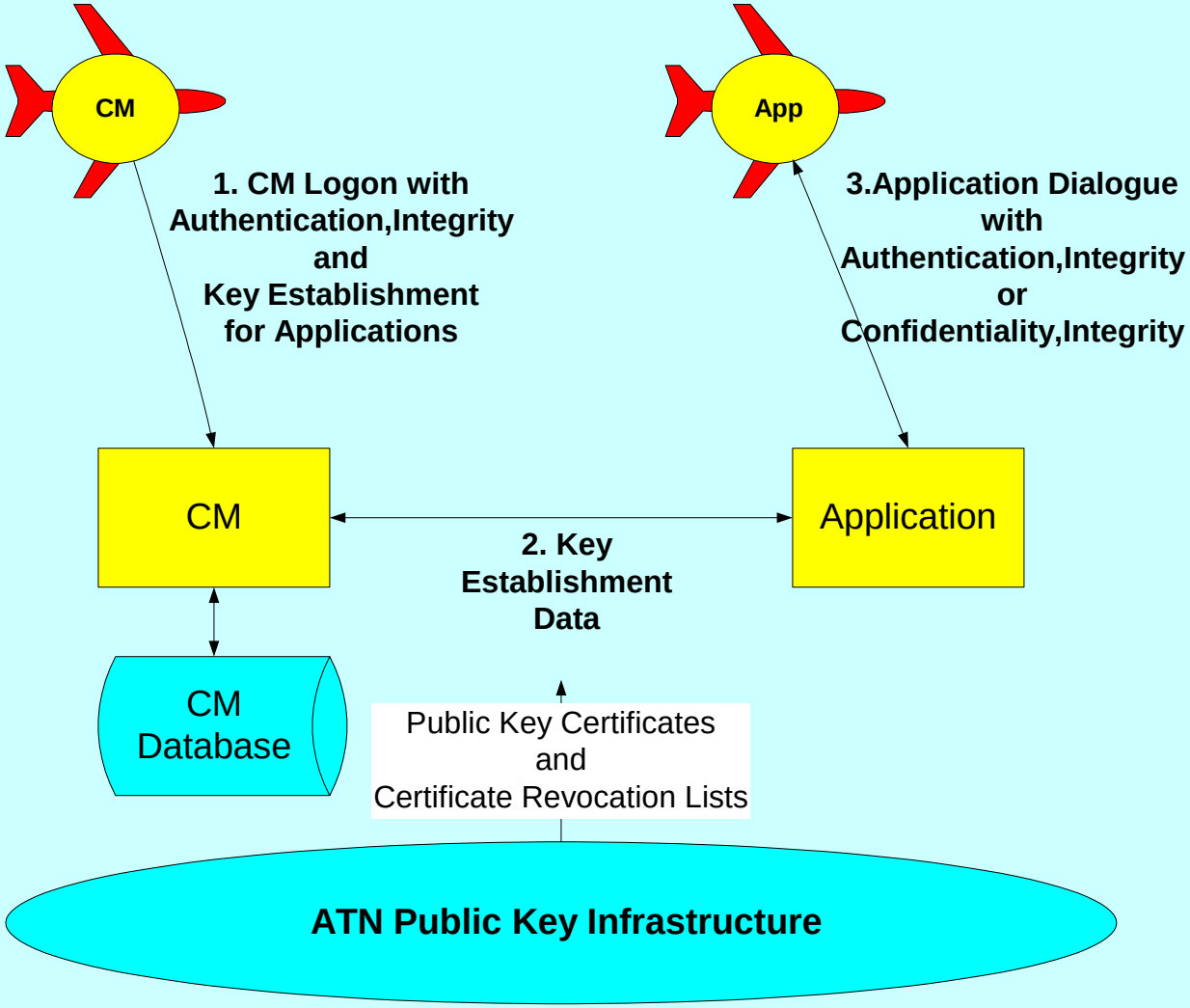
Authentication with Digital Signature



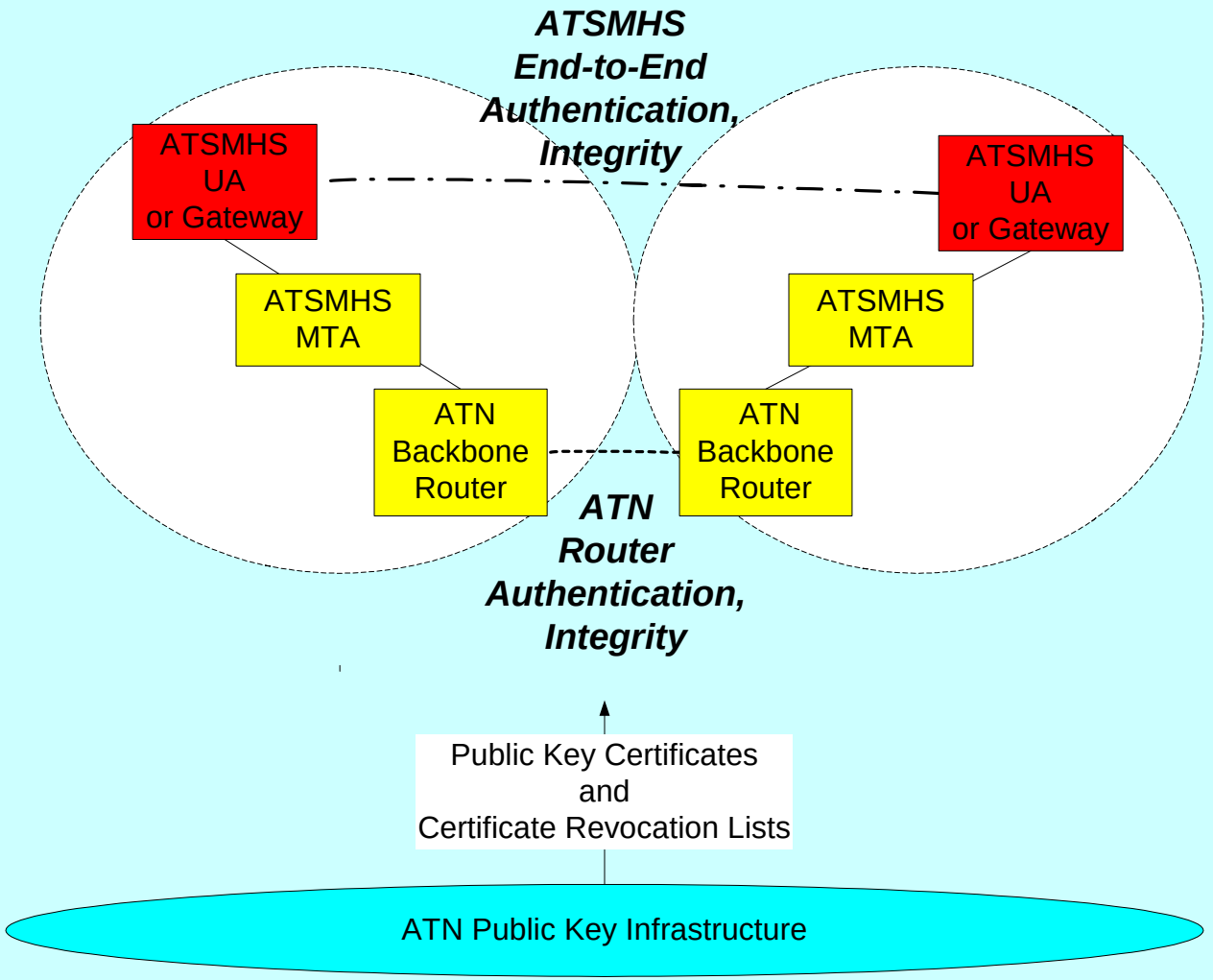
Authentication with Message Authentication Codes



Air-Ground Application Security



IDRP and Message Handling Security



ATN Security Summary

- What will it take to implement ATN Security:

1. Implement Edition 3 SARPs security changes
2. Establish a Public Key Infrastructure
   a. Certificate Authority (CA) System
   b. Certificate Distribution System
3. Develop Certificate Policy and Practices
4. Establish bilateral security agreements (e.g. for cross-certification)
5. Prepare staff for system operation
6. Begin secure service with operational controls