



# Key/Certificate Management Life Cycle

*An Overview Adapted from PP823 Part 2*



AEEC NIS Meeting  
12-16 November 2007 – San Diego, CA

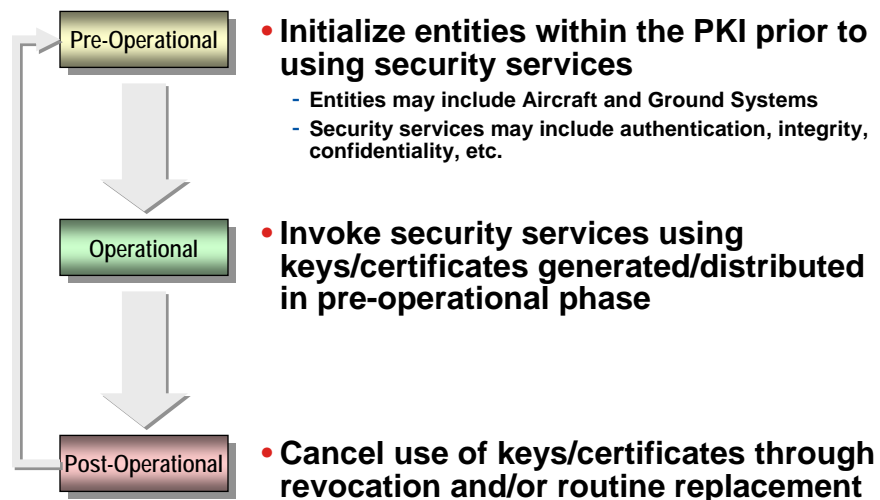


Michael Olive  
Honeywell

**Honeywell**

## Key/Certificate Life Cycle Overview

**Honeywell**



References: 1. NIST SP 800-57, *Recommendation for Key Management, Part 1: General Guideline*, March 2007  
2. *Understanding Public Key Infrastructure*, Carlisle Adams & Steve Lloyd, 1999, Macmillan

AEEC NIS – 12-16 November 2007

2

# Key/Certificate Life Cycle Processes

(from PP823p2)

Honeywell

Key Life Cycle Phase	Public Key Life Cycle Processes (Document Section)	Private Key life Cycle Processes (Document Section)
Pre-Operational Phase	3.2.1 Key Pair Generation	3.3.1 Key Generation
	3.2.2 Certificate Issuance	3.3.2 Key Backup 3.3.3 Key Distribution 3.3.4 Key Installation / Activation
Operational Phase	3.2.3 Certificate/CRL Retrieval	3.3.5 Key Storage 3.3.6 Key Use 3.3.7 Key Recovery
	3.2.4 Certificate/CRL Validation	
	3.2.5 Certificate Expiration-Renewal	
Post-Operational Phase	3.2.6 Certificate Expiration-Replacement	3.3.8 Key Replacement
	3.2.7 Certificate Revocation	3.3.9 Key Archive 3.3.10 Key Destruction

Source: Adapted from NIST SP800-57.

Note that these processes are similar for secret key systems.

AEEC NIS - 12-16 November 2007

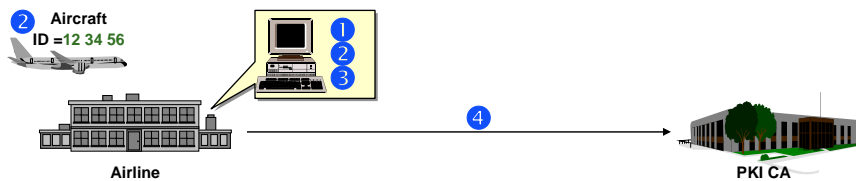
3

## Pre-Operational Phase [1/3]

Honeywell

### Key Pair Generation

1. **Generate Public/private key pair (P / p)**
  - Generated by the organization (e.g., airline) responsible for the entity (e.g., aircraft) for which the keys are intended
2. **Assign public key name**
  - Unique identity of the entity with which the public key is associated
3. **Assign public key usage**
  - E.g., Digital signature, key agreement, non-repudiation, etc.
4. **Deliver public key to a Certificate Authority (CA)**
  - In accordance with CA's Certificate Policy (CP) and business operating procedures
  - CA can be internal or out-sourced (i.e., make-vs.-buy)



AEEC NIS - 12-16 November 2007

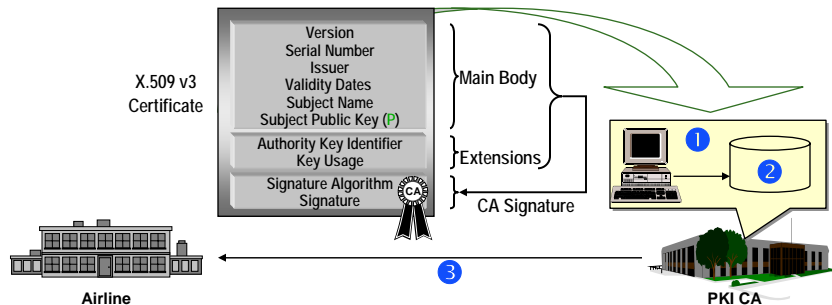
4

## Pre-Operational Phase [2/3]

Honeywell

### Certificate Issuance

1. Format and digitally sign public key certificate
  - In accordance with the certificate profile specified in the CP
2. Publish to a certificate repository
  - May be publicly accessible
  - At a minimum, accessible to all entities that rely on certificates issued by the CA
3. Advise requester that certificate issuance is complete



AEEC NIS - 12-16 November 2007

5

## Pre-Operational Phase [3/3]

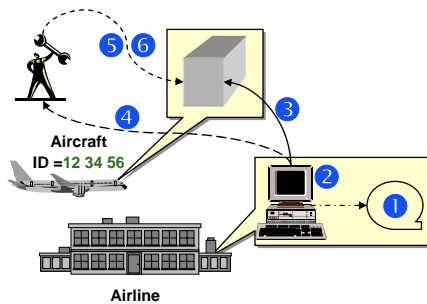
Honeywell

### Private Key Backup (optional)

1. Store back-up copy of private key to support key recovery

### Private Key Distribution

2. Protect the private key
  - E.g., Password-based encryption of private key
3. Deliver protected private key to the entity with which the key is associated
4. Deliver the activation data (e.g., PW) via separate channel



### Private Key Installation and Activation

5. Install protected private key
  - E.g., Data-loader
6. Activate private key
  - E.g., Enter password to recover private key

Note: Same process steps for a secret key.

AEEC NIS - 12-16 November 2007

6

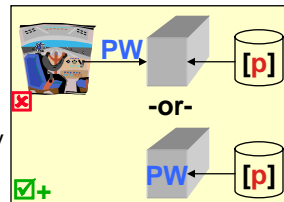
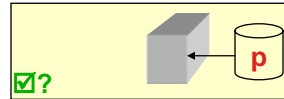
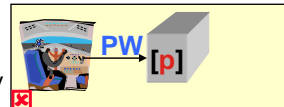
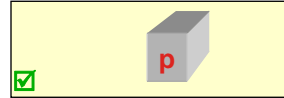
## Operational Phase [1/3]

Honeywell

### Private Key Storage

Note: Same options for a secret key.

- **Option 1A: Internal, Unprotected**
  - Private key is stored in unprotected form in the entity with which the key is associated
- **Option 1B: Internal, Protected**
  - Private key is stored in protected form in the entity with which the key is associated
  - Activation data must be entered to unlock key
- **Option 2A: External, Unprotected**
  - Private key is stored in unprotected form in external storage accessible by the entity with which the key is associated
  - Risk if other systems can access storage
- **Option 2B: External, Protected**
  - Private key is stored in protected form in external storage accessible by the entity with which the key is associated
  - Activation data must be entered to unlock key
  - OR-
  - Activation data may be stored in entity itself



AEEC NIS – 12-16 November 2007

7

## Operational Phase [2/3]

Honeywell

### Certificate Retrieval

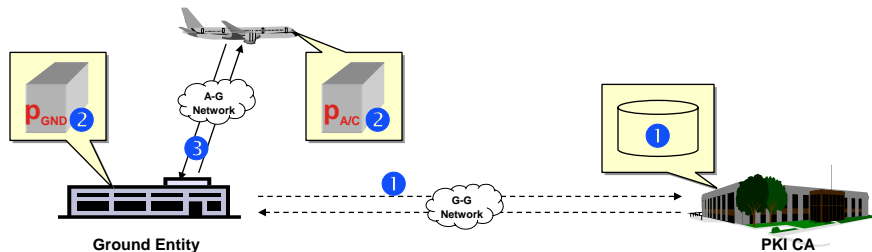
1. Retrieve certificate from certificate repository
  - Certificates may also be cached locally (optional)

### Certificate Validation

2. Validate certificate prior to use
  - E.g., signed by a trusted CA, correct identity, correct key usage, within specified validity period, not revoked, etc.

### Use Keys

3. Provide security services using public/private keys



AEEC NIS – 12-16 November 2007

8

## Operational Phase [3/3]

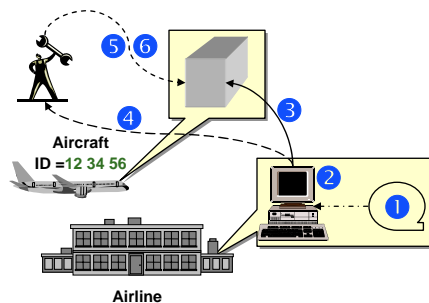
Honeywell

### Private Key Recovery

If Private Key was backed up

1. Retrieve private key from backup storage
2. - 4. Private Key Distribution
  - Same as initial distribution
5. - 6. Private Key Installation / Activation
  - Same as initial installation / activation

No impact on associated Public Key Certificate



AEEC NIS – 12-16 November 2007

9

-OR-

If Private Key was not backed up, then perform full key/certificate replacement (see next slide)

## Post-Operational Phase [1/3]

Honeywell

### Certificate Revocation

- Remove certificate from service in response to:
  - Known or suspected compromise of the private key
  - Loss of use of the private key
  - Change in organization affiliation (e.g., transfer of ownership)
  - End of service life
  - Etc.

### Certificate Expiration-Replacement

- Routine replacement of keys/certificates
  - Public/private key pair is nearing crypto-period expiration
  - To achieve private key recovery when private key is not backed up
  - In response to certificate revocation action
- Utilizes same processes as Pre-Operational Phase, except relationship already established with CA
  - Key Pair Generation
  - Certificate Issuance
  - Private Key Backup, Distribution, Installation/Activation
- Should be timed with aircraft maintenance cycle (next slide)

AEEC NIS – 12-16 November 2007

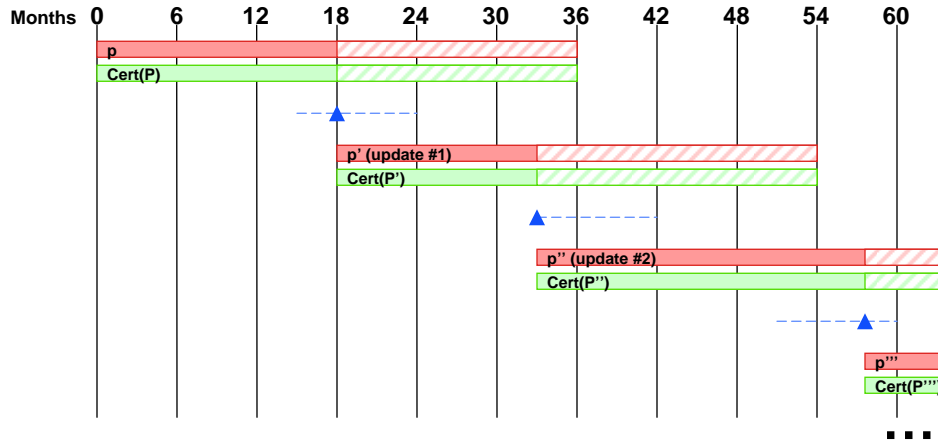
10

## Post-Operational Phase [2/3]

Honeywell

### • Example Key/Certificate Replacement Scenario:

- Assume private key (**p**) cryptoperiod is **36 months** (NIST recommendation)
- Assume public key certificates (**Cert(P)**) are valid for **36 months**
- Assume aircraft maintenance cycle is **18 months** (nominally)



AEEC NIS – 12-16 November 2007

11

## Post-Operational Phase [3/3]

Honeywell

### Private Key Archive (*optional*)

#### 1. Upon crypto-period expiration or key replacement, archive private key

- To support recovery of messages stored in secure form
- As necessary to comply with regulatory or business requirements

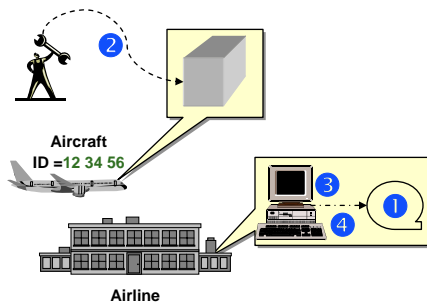
### Private Key Destruction

#### 2. Delete private key stored in end entity

- Automatic upon key replacement

#### 3. Delete backup copies of private key maintained to support key recovery

#### 4. Delete archived copies of private key when no longer needed to support archive recovery



Note: Same process steps for a secret key.

AEEC NIS – 12-16 November 2007

12

## Key Management Approach vs. Compromise Impact and Recovery

Honeywell

Assume: N = Number of aircraft

M = Number of ground systems with which aircraft communicate

KEY MANAGEMENT APPROACH	TOTAL No. OF KEYS REQUIRED	POTENTIAL IMPACT OF COMPROMISE		COMPROMISE RECOVERY ACTIONS
PKI-based	One per entity (N + M)	A/C	1 aircraft entity	Revoke existing certificate; replace key, issue new certificate
		GND	1 ground entity	Revoke existing certificate; replace key, issue new certificate
Secret Key – Pairwise-Unique	One per entity pair (N x M)	A/C	1 aircraft + 1..M ground	Replace 1..M keys in aircraft entity AND in each ground entity with which it shares a key
		GND	1 ground + 1..N aircraft	Replace 1..N keys in ground entity AND in each aircraft entity with which it shares a key
Secret Key – Aircraft-Unique	One per aircraft (N)	A/C	1 aircraft + 1..M ground	Replace key in aircraft entity AND in each ground entity with which it shares a key
		GND	up to N aircraft + M ground	Replace keys in all ground entities AND in each aircraft entity with which the ground entities share a key
Secret Key – Fleet-Unique	One per fleet (1)	A/C or GND	up to N aircraft + M ground	Replace fleet key in ALL aircraft and ALL ground systems that share the key

AEEC NIS – 12-16 November 2007

13

## Contact Info

Honeywell

Michael Olive  
 Sr. Principal Systems Engineer  
 Honeywell  
 Aerospace Advanced Technology  
[mike.olive@honeywell.com](mailto:mike.olive@honeywell.com)  
 +1 (410) 964-7342

AEEC NIS – 12-16 November 2007

14