Information Security

Information Security Standards				
Reference:	ISS-0009		Status:	Issued
Title:	Corporate PKI Certificate Policy and Practice Statement			
Version:	1-02	Date:	1 December 2014	© British Airways

BRITISH AIRWAYS

Corporate Public Key Infrastructure (PKI) Policy and Practice Statement (CP/CPS)

ISS-0009 v1-02

Date: 1st December 2014

British Airways

Information Security Standards				
Reference:	ISS-0009		Status:	Issued
Title:	Corporate PKI Certificate Policy and Practice Statement			
Version:	1-02	Date:	1 December 2014	© British Airways

CONTENTS

Information Security Standards				
Reference:	ISS-0009		Status:	Issued
Title:	Corporate PKI Certificate Policy and Practice Statement			
Version:	1-02	Date:	1 December 2014	© British Airways

1 INTRODUCTION

1.1 Overview

In public key cryptography any participating entity has a key pair. One of these keys is private and shall be kept secret, the other is public and can be made available for retrieval from a public key directory, much like telephone numbers in a public phone book.

Since anyone can create a public key with any given name, it is essential to verify that a certificate retrieved from a directory actually belongs to the entity named therein, otherwise digital signatures might be forged. A certificate issued by a Certificate Authority (CA) contains the entity's name, the name of the CA, the entity public key, and is digitally signed by the CA.

The main role of a CA is to provide digitally signed certificates that bind the entity's identity to its public key. Entities are identified before certificate generation through the use of a Registration Authority (RA).

This document provides a combination of certificate policies and practice statements that set out the ground rules for the governance and operation of the British Airways (BA) Corporate PKI (see Note 1 below). A Certificate Policy (CP) is a set of policies that define the operational principles of a Corporate PKI. A Certification Practice Statement (CPS) is a statement of the practices that a CA employs in issuing certificates to an entity as well as a description how the verification of data contained in a certificate is performed. This includes certificate application, use and revocation or suspension of certificates. A CA publishes a CPS to allow an estimation of the trustworthiness of the certificates issued from the CA.

This document is based on the Internet Request for Comment (RFC) 3647 and supports all the types of certificates issued by BA including but not limited to device certificates, individual certificates and code signing certificates.

This document (in combination with BA's organisation, processes, and procedures) is aligned to the standard "ETSI TS 102 042 – Policy requirements for certification authorities issuing public key certificates", Version 2.1.1 of the European Telecommunications Standards Institute (ETSI).

This document does not constitute a declaration of self-escrow, nor does it state legally binding warranties. Any legally binding statements between BA and the relevant entities are made outside this document.

BA CAs covered in this document provide or implement the following security management services:

- Certificate generation, re-key and distribution.

- Certificate revocation list (CRL) generation and distribution.
- Online certificate status protocol (OCSP).
- Directory management of certificate related items.
- Privilege and authorisation management.
- System management functions (e.g. security audit, configuration management, archiving).

Note 1: Policy and procedure documents are often separated once the Corporate PKI service is fully defined along with the environment and governance structure to support it.

1.2 Document Name and Identification

This document is titled and shall be referred to as: 'British Airways Corporate PKI Certificate Policy and Practice Statement', its reference is: ISS-0009 in BA's series of Information Security Standards (ISS) owned by BA's Information Security Department.

1.3 British Airways Corporate PKI Owner

The owner of the British Airways Corporate PKI shall be the Head of British Airways IT, who is: Paul Binks.

1.4 PKI Participants

1.4.1 CERTIFICATION AUTHORITIES

BA Corporate PKI is a three-level hierarchy with a trusted Root and two Subordinate CAs. Each Subordinate CA has a number of Issuing CAs (see Table 1.1 and figure below).

- **Root CA:** BA Corporate Root CA.
- **Subordinate CAs:**
  - Corporate Services Subordinate CA
  - Business Integration Subordinate CA.
- **Issuing CAs:**
  - Endpoint Services Issuing CA, Staff Applications Issuing CA and IT Operations & Infrastructure Issuing CA are located under the Corporate Services Subordinate CA.
  - Business Integration Issuing CA and eEnabled Aircraft (A/C) Issuing CA are located under the Business Integration Subordinate CA.
  - BEGSS Issuing CA which is an off-line CA.

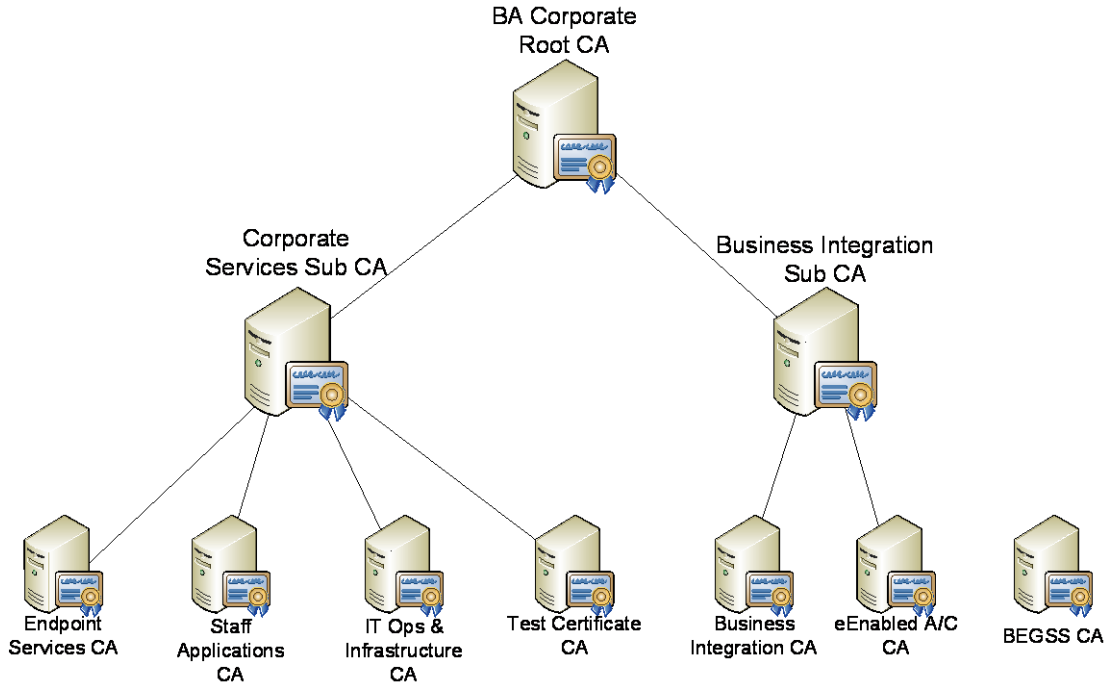

Table 1.1	
Issuing CA	**Description**
Endpoint Services CA	Issues internal BA certificates for all BA endpoint devices including but not limited to BA staff laptops, staff mobile devices and airport baggage scanners.
Staff Applications CA	Issues internal BA certificates to all corporate applications including but not limited to service management, payroll, HR and other back-office applications.
IT Operations & Infrastructure CA	Issues internal BA certificates to IT and network systems including but not limited to servers and network switches.
Test Certificate CA	Issues certificates to test systems and applications. Not to be used for any live systems.
Business Integration CA	Issues BA certificates to IT systems that integrate / communicate with external systems.
eEnabled A/C CA	Issues certificates to Boeing and Airbus systems and applications as required for eEnablement. Uses include signing and secure communications.
BEGSS CA	Issues certificates for the Boeing Electronic Flight Bag system. This CA is off-line.

1.4.2 REGISTRATION AUTHORITIES

BA Corporate PKI operates a single Registration Authority (RA) and this is the only entity that authorises the issuance of all certificates by any BA Issuing CAs.

1.4.3 APPLICANTS

Certificate Applicants ("Applicants") are consumers of the BA Corporate PKI service. Applicants can request certificates for their own use or on behalf of end entities such as a device or application. Only BA employees and authorised contractors can request certificates. Certificates shall not be issued to members of the general public or any non-BA organisation such as BA partners or third-parties.

Applicant's name or the name of the end entity is included as the subject of the certificate or as part of the name.

1.4.4 RELYING PARTIES

Relying Parties are the entities that rely on the binding of an Applicant's name to the public key identified in the certificate issued for the Applicant.

Authorised third parties may be Relying Parties of BA certificates (e.g. one issued by the Business Integration Issuing CA) if they are at the receiving end of the certificate exchange.

BA will comply with the security policy of third parties with regard to the use of keys and certificates. A third party can trust a BA issued certificate should they choose to do so.

1.4.5 OTHER PARTICIPANTS

No stipulation.

1.5 Certificate Usage

1.5.1 APPROPRIATE CERTIFICATE USES

Only X509 version 3 compliant certificates shall be issued. Custom profiles are permitted (e.g. Boeing eEnabled certificates).

BA certificates are used to for a number of purposes:

- Endpoint authentication.
- Encrypted network communication (e.g. TLS/SSL sessions).
- Other encryption services to provide confidentiality.
- Signing services to provide message integrity and non-repudiation.

Maximum key and certificate lifespan are as follows (see Note 2 below):

- SSL – up to 5 years, 24 months if data sensitive
- SSL on PCI servers – 12 months
- Network security (e.g. SSH) – 24 months
- Mobile and network devices for network access – 24 months
- Encrypting and / or signing data (including email) – 12 months
- Code signing – 12 months

Note 2: They can be less and it is up to individual services to make a risk based decision.

The list of allowed certificate use cases in BA per Issuing CA is as follows.

BA Endpoint Services CA
- Mobile Devices.
- Computers.

BA Staff Applications CA
- Any BA staff applications.

BA IT Operations & Infrastructure CA
- RADIUS servers
- Self Service Kiosks.
- Apache servers.
- Client & Server SSL.

BA Test Certificate CA
- All test system certificates.

BA Business Integration CA
- All certificates for IT systems that integrate / communicate with external systems.

BA eEnabled Aircraft (A/C) CA
- B787 e-enabled aircraft.
- A380 e-enabled aircraft.

BEGSS Root CA
- B787 Electronic Flight Bag.

1.5.2 PROHIBITED CERTIFICATE USES

BA certificates must not be used for any purpose other than the ones listed in1.5.1. Use of a BA certificate for purposes other than that for which it was issued is prohibited.

One key pair / one certificate per end point shall be used:
- The same private / public key on multiple end points is prohibited.
- Wildcard certificates are prohibited with the only exception being their use on non-production systems which is allowed.
- Subject Alternate Name (SAN) certificates are permitted.

1.6 Policy Administration

1.6.1 ORGANISATION ADMINISTERING THE DOCUMENT

The Information Security Team within the BA IT Operations Department shall be the organisation that administers this document.

1.6.2 CONTACT PERSON

The contact person shall be the Information Security Manager in the Information Security Team who has responsibility for Information Security Policy.

1.6.3 PERSON DETERMINING CP SUITABILITY FOR THE POLICY

The person who shall determine the CP suitability for the BA corporate policy shall be the Information Security Manager in the Information Security Team who has responsibility for Information Security Policy.

1.6.4 CP APPROVAL PROCEDURES

The CP shall be reviewed as part of the Information Security Team's annual review of BA's Information Security Policies and Controls. As a result of this annual review, the CP shall be updated if and as necessary, and subsequently approved for issue by the Information Security Manager in the Information Security Team who has responsibility for Information Security Policy.

The CP shall also be reviewed and revised outside the annual review cycle following significant changes to service requirements and any changes to the CA hierarchy.

1.7 Definitions and Acronyms

Table 1.2

Term	Definition
BA	British Airways
BASI	British Airways Standing Instructions
BEGSS	Boeing ePlane Ground Server System
CA	Certificate Authority
CMM	Capability Maturity Model
CN	Common Name
COBIT	Control Objectives for Information and Related Technology
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DMZ	Demilitarized Zone
DN	Distinguished Name
DR	Disaster Recovery
EFS	Encrypting File Service

Information Security Standards				
Reference:	ISS-0009		Status:	Issued
Title:	Corporate PKI Certificate Policy and Practice Statement			
Version:	1-02	Date:	1 December 2014	© British Airways

ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards
HR	Human Resources
HSM	Hardware Security Module
IAG	International Consolidated Airline Group
IAM	Information Assurance Manual
IAS	Internet Authentication Service
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
LDAP	Lightweight Directory Access Protocol
LSAPL	Loadable Software Aircraft Parts Library
MSP	Managed Service Provider
OCSP	Online Certificate Status Protocol
OID	Organisation Identity
ON	Organisation Name
OU	Organisation Unit
PCI	Payment Card Industry
PKI	Public Key Infrastructure
RA	Registration Authority
RAS	Remote Access Service
RFC	Request for Comment
RSA	Rivest-Shamir-Adleman
SAN	Subject Alternate Name
SLA	Service Level Agreement
SSH	Secure Shell
SSL	Secure Socket Layer
TCSEC	Trusted Computer System Evaluation Criteria
TLS	Transport Layer Security
UTC	Coordinated Universal Time

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

BA Corporate PKI's Root, Subordinate and Issuing CAs operate certificate repositories to support their PKI operations.

BA Corporate PKI shall adhere to the industry PKI standards to allow Relying Parties obtain certificates and CRLs, and validate certificate status through the use of OCSP from published locations or through CA repositories.

The Corporate PKI repository shall be available as required by the certificate information posting and retrieval stipulations of this document.

Upon system failure, service, or other factors that are not under the control of BA, BA makes best efforts to make the revocation status of the service available within the service levels described in this document.

Certificate revocation status is available for at least as long as the certificate's expiry date indicates.

Certificate information is included in but not limited to: Venafi, Mobile Device Management (MDM), Certificate Authorities and Active Directory.

2.2 Publication of Certification Information

All Issuing CAs under the Corporate Subordinate CA publish their CRL through:

- http://ba-pki.baplc.com/crl

The OCSP service under this Subordinate CA can be accessed through http://ba-pki.baplc.com/ocsp.

All Issuing CAs under the Business Integration Subordinate CA publish their CRL through:

- http://ba-pki.baplc.com/crl

The OCSP service under this Subordinate CA can be accessed through http://ba-pki.baplc.com/ocsp.

This document is published at:

- http://ba-cps.baplc.com

2.3 Time or Frequency of Publication

All Issuing CA CRLs under the Corporate Subordinate CA shall be updated and published as soon as possible when a certificate is revoked, but this must take no more than 24 hours.

All Issuing CA CRLs under the Business Integration Subordinate CA shall be updated and published as soon as possible when a certificate is revoked, but this must take no more than 2 hours.

A CRL from the corresponding CA must be updated and published immediately following a security compromise of a certificate.

2.4 Access Controls on Repositories

Only the application and user interfaces defined below shall be used to access the CA repository content.

Access to sensitive repository content, configuration and systems as defined below shall be restricted to authorised entities with respect to the standard BA access control policies and mechanisms.

The allowed application and user interfaces are as follows:

1. Venafi.
2. Mobile Device Management (MDM).
3. Certificate Authorities.
4. Active Directory.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 TYPES OF NAMES

All names specified in X509 certificates shall be expressed as non-null subject Distinguished Names (DNs) complying with the X500 standard.

Optionally, the *serialNumber* attribute may be included along with the Common Name (CN) – to form a terminal relative distinguished name set – to distinguish among successive instances of certificates associated with the same entity.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

Names used in the certificates shall identify the person, device, computer system or application to which they are assigned.

Names shall never be misleading.

The RA shall verify and validate the name requested for the certificate during the registration process. It is the responsibility of the Applicant to choose a meaningful and a valid name to receive the approval from the RA.

3.1.3 ANONYMITY OR PSEUDONYMITY OF APPLICANTS

The BA Corporate PKI does not use anonymous or pseudonymous certificates.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

Any X509 certificate issued to identify a person will have *OrganisationName* and *OrganisationalUnit* fields completed to identify Applicant in relation to BA organisation.

3.1.5 UNIQUENESS OF NAMES

Any DN in a X509 certificate issued by BA shall uniquely identify a single entity among all of BA's entities. If necessary, BA may append additional numbers or letters to an actual name in order to ensure the name's uniqueness according to name conventions in 3.1.1and 3.1.2.

The same Applicant may have different certificates all bearing the same subject DN, but no two separate Applicants may share a common DN (and be issued by the same CA). In any case, there shall not be two X509 certificates having the same DN and serial number.

Checks to validate uniqueness of names shall be performed automatically by the CA or RA systems or in some cases manually by the RA administrator. Further checks may be built in requesting systems to disallow entry of non-unique names.

3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

No stipulation.

3.1.7 NAME CLAIM DISPUTE RESOLUTION PROCEDURE

No stipulation.

3.2 Initial Identity Validation

In order to obtain a certificate, any Applicant shall apply for a certificate, and identify themselves and authenticate to the RA.

Certificates may be attributed to a device, system or application, or they may be attributed to a member of BA, such as an employee.

All certificates issued from an Issuing CA under the Corporate Subordinate CA shall be internal BA certificates (i.e. to be issued to BA entities only). No non-BA entity including BA partners and third-parties shall receive certificates from this CA.

All certificates issued from an Issuing CA under the Business Integration Subordinate CA shall be internal BA certificates (i.e. to be issued to BA entities only). No non-BA entity including BA partners and third parties shall receive certificates from this CA.

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

A Certificate Signing Request (CSR) provides assurance to the RA that the request has been sent by the owner of the appropriate key pair (i.e. the Applicant) when the RA successfully verifies the CSR.

In cases the Applicant or the underlying entity does not explicitly use a CSR, the CA gains implicit assurance of the key pair by generating or initiating the generation of the key pair.

3.2.2 AUTHENTICATION OF ORGANISATION IDENTITY

No stipulation.

It should be noted that future versions of this document may include considerations for International Airlines Group (IAG).

3.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY

A directory of individuals and access credentials shall be used to identify employees and support issuance, re-key and revocation activities.

3.2.4 NON-VERIFIED APPLICANT INFORMATION

In cases the Applicant or the underlying entity does not explicitly use a CSR, the CA gains implicit assurance of the key pair by generating or initiating the generation of the key pair.

3.2.5 VALIDATION OF AUTHORITY

The RA shall verify the authority of the Participant to request certificates for the presented key pair using appropriate authentication and key verification mechanisms (see 3.2) as part of the initial identity validation.

3.2.6 CRITERIA FOR INTEROPERATION

The BA Corporate PKI hierarchy currently does not support interoperability at CA trust relationship level with other CAs.

3.3 Identification and Authentication for Re-key Requests

Re-key means replacing an existing certificate by issuing a new certificate with a new key pair. Typically the certificate name stays the same. It is different from renewal, which is used to issue a new certificate with an extended validity period for the same key pair (see RFC 2828).

Certificate re-key is the only allowed mechanism in BA Corporate PKI for certificate replacement. It may also be used in cases where the existing key pair can no longer be used.

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

Applicants shall identify themselves through the use of their current key pair whose certificate has not yet expired or by using the initial identity validation process in 3.2.

For services that use auto-enrolment, certificate re-keying may be automated by the Corporate PKI software and thus no explicit authentication is required.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

After a certificate has been revoked, the Applicant shall generate a new key pair or initiate its creation and re-apply for a new certificate in accordance with the procedure described in 3.2.

3.4 Identification and Authentication for Revocation Requests

All revocation requests shall be authenticated.

Applicants or Relying Parties shall submit their revocation requests to the Corporate PKI administrator, who handles all requests following an authentication and approval process.

Corporate PKI administrator can also revoke certificates with no additional approval required without an individual request from an Applicant or a Relying Party in the case of a suspected compromise of keys or abuse of certificate usage conditions.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Request

The BA Corporate PKI implements an online interface where Applicants can request certificates for individual use or on behalf of the systems they are provisioning. An Applicant requesting a certificate will complete and submit an online application form.

Completed certificate requests are then submitted to the RA for processing resulting in either an approval or rejection of the application.

Devices, applications and IT systems acting on behalf of the Applicant can also submit a certificate issuance or renewal request using the 'auto-enrolment' option.

4.1.1 WHO CAN SUBMIT A CERTIFICATE REQUEST

Any Applicant, BA staff or contractor can submit a certificate request for individual use or on behalf of the systems they are provisioning.

Devices, applications and IT systems acting on behalf of the Applicant can also submit a certificate request using the 'auto-enrolment' option.

4.1.2 ENROLMENT RESPONSIBILITY

The Applicant shall provide accurate information in their certificate request and is responsible for entering accurate and valid information.

The RA is responsible for the validation and approval of the certificate request.

4.2 Certificate Request Processing

The RA performs a review of the request for accuracy of all the data, obtains all approvals required and triggers the identification and authentication process described in3.2.

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

Identity verification of Applicants must meet the requirements in 3.2 and 3.3.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE REQUESTS

The certificate request can result in two responses: The RA would either approve the certificate request or reject the certificate request and inform the Applicant about the reasons for rejection.

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

Manually requested certificates are processed by the PKI team's Enrolment Officers. A digital certificate request email template is available for applicants to complete and send to email group SECPKIAdmin.

The PKI Team have a 2 day SLA to acknowledge an email request and a 10 day SLA to process emailed certificate requests.

The only exception is in the B787 use case, the EFB Static Identity certificate request requires 4 weeks notice (20 days). The longer notice period is to allow the PKI Enrolment Officers enough time to organise the datacentre visit to bring the BEGSS Root CA online in order to issue the certificate.

The processing of auto enrolled certificates is done directly between the client and the Certificate Authority, these enrolments are not processed by the PKI Enrolment Officers.

4.3 Certificate Issuance

4.3.1 RA AND CA ACTIONS DURING CERTIFICATE ISSUANCE

The RA will verify that the Applicant is in possession of the correct key pair when receiving a certificate request and that the request contains accurate data.

The CA will issue certificates with the appropriate certificate format, validity periods and extension fields. Certificates are checked to verify that all required fields and extensions are appropriately populated.

Following successful verification and validation, the certificate is published on the repository at the end of the issuance process.

4.3.2 NOTIFICATION TO APPLICANT BY THE CA OF ISSUANCE OF CERTIFICATE

The CA shall issue the requested certificate to an Applicant or directly to an end entity, or inform the Applicant about any problems or inconsistencies.

Where an Applicant applies for a certificate, the certificate shall be delivered over the web, in a message containing the certificate or by other means to be decided during the delivery of the Corporate PKI service.

4.4 Certificate Acceptance

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

The act of downloading or installing a certificate from a message confirms that the Applicant has received the certificate. A disclaimer text will be displayed to explain to the Applicant the use policy of the BA certificate. The certificate shall then be

used with respect to the appropriate use policy in 1.5.1 and shall be made available for verification on the certificate repository.

By accepting a certificate the Applicant confirms that the following – provided as part of the request and identification process – are true and not misleading:

- Applicant and organisational information (e.g. OU) included in the certificate.
- All representations made by the Applicant including certificate use and purpose.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

After certificate issuance, the CA shall, where appropriate, publish the certificate on an X.500 or LDAP directory as specified in 2.2.

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Certificates are published as specified in 4.4.2. There is no additional mechanism to notify other entities.

4.5 Key Pair and Certificate Usage

4.5.1 PRIVATE KEY AND CERTIFICATE USAGE

Applicants shall protect their private keys from unauthorised access.

Applicants shall use private keys for appropriate purposes only as specified in 1.5.1. BA staff terms and conditions (for example British Airways Standing Instruction Number 8 – BASI 8) also mandate the proper use of BA IT systems and this shall include the use of private keys associated with digital certificates.

Private keys shall only be used after the Applicant has accepted the corresponding certificate. The Applicant shall discontinue using the private key following the expiration or revocation of the corresponding certificate.

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

Certificates shall specify restrictions on their purpose and use using certificate extensions.

Relying Parties must verify the full certificate chain prior to using a certificate.

Relying Parties shall check and abide by the certificate type, key usage and any other extensions as defined within a certificate to ensure they are used only for the purpose for which they were issued.

All CAs shall specify the current status of all unexpired certificates. Relying Parties shall check revocation status and start and end dates of any certificate.

<Insert standard accepted usage fields for each Issuing CA>

B787 e-Enabled Aircraft Certificate Templates:

- EGS Airplane Identity
- EGS Maintenance Laptop Identity
- EGS Application Identity
- EGS LSAPL Suite Object Signing
- EGS Trusted Agent

BEGSS Certificate Templates:

- RAS and IAS
- SSL Service
- EFB Static Identity
- EFB Root CA

A380 e-Enabled Aircraft Certificate Template:

- BACorpPKI Airbus SSL

Radius Servers Certificate Template:

- BACorpPKICiscoACS

Mobile Devices Certificate Templates:

- BACorpPKIWebServerExportable
- BACorpPKIMobiledevice

Self Service Kiosk Certificate Template:

- BACorpPKIWebServerExportable

4.6 Certificate Renewal

4.6.1 CIRCUMSTANCE FOR CERTIFICATE RENEWAL

Certificate renewal must not be used under normal circumstances. All certificates shall be re-keyed following expiry. Renewal may be granted in exceptional cases and documented by an approved security exception for a limited duration.

Standing exceptions (i.e. exceptions without a time limit) shall not be allowed for renewal requests.

Renewal is not allowed regardless of the exception approval if any of the following is true:

- If the certificate key pair has been compromised.
- If the certificate has expired.
- If other certificate fields have changed.
- If the subject name on the certificate or certificate attributes have changed.

4.6.2 WHO MAY REQUEST CERTIFICATION RENEWAL

Renewal requests shall be made by the Applicant by submitting a security exception request. The RA or the CA shall not automatically renew certificates.

User requested certificates will not be automatically renewed.
Auto-enrolment requested certificates will be automatically renewed.

The PKI Centre of Excellence shall deal with all security exception requests relating to certificate renewals.

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

If the security exception for renewal is approved, the RA shall approve certificate renewal following:

- Initial registration process as described in 3.2.
- Identification and authentication for re-key as described in 3.3.

4.6.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO APPLICANT

As described in 4.3.2.

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

As described in 4.4.1.

4.6.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

As described in 4.4.2.

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

As described in 4.4.3.

4.7 Certificate Re-key

Re-keying a certificate is the only allowed method for BA Corporate PKI to request replacement certificates (e.g. following certificate expiry).

Re-keying is similar to certificate issuance in that a new key pair is created along with a new certificate request while retaining the remaining contents of the old certificate that describe the Applicant.

4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY

All types of certificates can be re-keyed.

CA certificate re-key can be carried out where the current key pair can no longer be used or in the following circumstances:

- Key is compromised or suspected compromise.
- Certificate has to be revoked.
- Certificate has expired.

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

Re-key requests shall be made by the Applicant.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

The certificate re-keying process is identical to the new certificate issuance process. Certificate re-key identity verification is achieved using one of the following processes:

- Initial registration process as described in 3.2.
- Identity proofing for re-key as described in 3.3.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO APPLICANT

As described in 4.3.2.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

As described in 4.4.1.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

As described in 4.4.2.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

As described in 4.4.3.

4.8 Certificate Modification

Certificate modification must not be used in normal circumstances. Any certificate changes shall result in a new certificate request. Modification may be granted in exceptional cases and documented by an approved security exception for a limited duration.

Standing exceptions (i.e. exceptions without a time limit), shall not be allowed for modification requests.

An RA shall verify the updated information in the certificate. The validation process shall be identical to the identity proofing in 3.2.

The old certificate shall not be further re-keyed, renewed, or updated. Additionally, the old certificate shall be revoked if the Applicant no longer holds one or more of the affiliations explicitly stated in the old certificate.

4.8.1 CIRCUMSTANCE FOR CERTIFICATE MODIFICATION

Certificate modification is only allowed for exceptional cases accompanied with an approved security exception supported by a business case.

4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION

Modification requests shall be made by the Applicant by submitting a security exception request. The RA or the CA shall not automatically modify certificates.

The PKI Centre of Excellence shall deal with all security exception requests relating to certificate modifications.

4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS

Processing of CA certificate modification is identical to the process used for the initial application with the addition of the security exception process and an additional step to verify that the new certificate information has not been used in the old certificate.

4.8.4 CONDUCT CONSTITUTING ACCEPTANCE OF A MODIFIED CERTIFICATE

As described in 4.4.1.

4.8.5 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

As described in 4.4.2.

4.8.6 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

As described in 4.4.3.

4.9 Certificate Revocation and Suspension

A BA certificate can only be revoked, certificate suspension is not allowed.

Any BA certificate whose key pair has been compromised shall be revoked immediately. If there is a suspicion of compromise the Applicant shall still request a revoke of the corresponding certificate as soon as possible.

BA certificates may also be revoked if the Applicant no longer needs the certificate (e.g. following decommissioning of a service).

Upon revocation, the certificate becomes invalid as soon as the CA processes the revocation request. The certificate's serial number and time of revocation are included in the CRL and subsequent status inquiries to the certificate repository will result in a response citing the certificate as invalid.

4.9.1 CIRCUMSTANCES FOR REVOCATION

- When there is suspected loss, disclosure or other compromise of the private key of a certificate used by an Applicant, device, system or application.
- For personal certificates when an Applicant leaves BA.
- When the underlying service, system, application, etc. is no longer required.

4.9.2 WHO CAN REQUEST REVOCATION

Applicants can request revocation but only authorised Corporate PKI administrators shall revoke BA certificates after all necessary approvals are obtained.

The PKI Centre of Excellence shall deal with all requests relating to certificate revocations.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

Authorised Corporate PKI administrators can revoke BA certificates by logging on to the interface provided by the Corporate PKI service. Following a successful request, the certificate is added to the CRL of the corresponding Issuing CA.

4.9.4 REVOCATION REQUEST GRACE PERIOD

There is no grace period for revocation.

4.9.5 TIME WITHIN WHICH CA SHALL PROCESS THE REVOCATION REQUEST

Manually requested certificate revocations are processed by the PKI team's Revocation Officers.

The PKI Team has a 2 day SLA to acknowledge an email request and a 10 day SLA to process emailed certificate revocation requests. The Revocation Officers prioritise the revocation requests and are responsible for processing high importance revocations as a matter of urgency.

4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES

Revocation information to Relying Parties will be provided by CRLs and OCSP. Relying Parties shall check revocation status as per 4.5.2.

If revocation status cannot be checked the certificate must not be trusted.

If OCSP responds with a status of "unknown" the certificate should not be trusted.

4.9.7 CRL ISSUANCE FREQUENCY

All Issuing CAs CRLs under the Corporate Subordinate CA shall be updated and published as soon as possible when a certificate is revoked, but this must take no more than 2 hours.

All Issuing CAs CRLs under the Business Integration Subordinate CA shall be updated and published as soon as possible when a certificate is revoked, but this must take no more than 2 hours.

A CRL from the corresponding CA must be updated and published immediately following a security compromise of a certificate.

For the B787 Maintenance Laptop Identity certificate use case a special long life CRL is used.

If a Maintenance Laptop Identity certificate is revoked due to a compromised laptop, the Aircraft Services CA CRL should be immediately loaded across the B787 fleet. This will ensure that a compromised Maintenance Laptop is unable to wirelessly connect to a B787.

There is a Create3YearAirplane CRL.bat script provided by Boeing for BA to create a long-lived CRL file for provisioning onto the aircraft.

4.9.8 MAXIMUM LATENCY FOR CRLS

The time needed to revoke the certificate after approving, validating and confirming the request shall not exceed 2 hours.

4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

BA Corporate PKI provides an on-line status checking service OCSP, for Relying Parties. Changes recorded on Corporate PKI are available to the Relying Parties to inquire and allow them make appropriate trust decisions.

The OCSP service can be accessed via: http://ba-pki.baplc.com/ocsp.

The service shall be updated within 10 minutes upon revocation or issuance of a certificate.

4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS

See 4.9.6.

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

No stipulation.

4.9.12 SPECIAL REQUIREMENTS REGARDING KEY COMPROMISE

If the Applicant suspects or has confirmed compromise of the private key an immediate revocation request shall be initiated.

4.9.13 CIRCUMSTANCES FOR SUSPENSION

Certificate suspension is not supported.

4.9.14 WHO CAN REQUEST SUSPENSION

No stipulation.

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

No stipulation.

4.9.16 LIMITS ON SUSPENSION PERIOD

No stipulation.

4.10 Certificate Status Services

4.10.1 OPERATIONAL CHARACTERISTICS

No stipulation.

4.10.2 SERVICE AVAILABILITY

The OCSP is a non-critical service and the business impact of this service becoming unavailable is very limited.

4.10.3 OPTIONAL FEATURES

No stipulation.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

Key escrow is not supported. Key backup is defined in 6.2.4.

5 FACILITY MANAGEMENT AND OPERATIONAL CONTROLS

5.1 Physical Controls

Physical controls shall be put in place to adequately mitigate risks to the BA Corporate PKI service including but not limited to the key generation environment, RA and CA infrastructure, databases for repositories and CRL and OCSP publishing points.

Data centre physical controls for the Corporate PKI Service must adhere to the physical security controls described for secure zones and infrastructure in: BA's Information Assurance Manual (IAM) Policies: 07-01 Secure Areas and 07-02 Equipment Security. As a minimum this shall include: locked racks and locked cabinets for CA, RA and HSM equipment which shall be placed in a secure, internal network zone sufficiently segregated from the rest of the network. These racks and cabinets shall be monitored by cameras and / or CCTV. Admin access to the secure zone shall be over a firewall that enforces 2-factor authentication.

5.2 Procedural Controls

Procedures based upon trusted roles and separation of duties shall be used to prevent or detect malicious operation of the CAs.

Corporate PKI roles and responsibilities with references to separation of duties are specified in the Corporate PKI - Operational Framework, which is held on the BA LAN share: im-eng-delivery (\\USERGROUP4).

5.3 Personnel Controls

5.3.1 QUALIFICATIONS, EXPERIENCE AND CLEARANCE REQUIREMENTS

BA staff with PKI operational responsibilities shall have the appropriate qualifications and experience to set up and operate the service. Required qualification and experience for Corporate PKI service staff are specified in the Corporate PKI - Operational Framework, which is held on the BA LAN share: im-eng-delivery (\\USERGROUP4).

Sensitive PKI operations such as key administration shall be performed by vetted staff with sufficient clearance. Personnel security and clearance and vetting requirements for BA staff are specified in the following documents:

1. IAM Policy 05-01 Personnel Security Prior to Employment.
2. IAM Policy 05-02 Personnel Security During Employment.
3. IAM Policy 05-03 Personnel Security on Termination or Change of Employment.
4. EG201: Recruitment and selection.

5. BA's Intranet: >Home >Helpcentre >People services >Criminal Record Check.

5.3.2 BACKGROUND CHECK PROCEDURES

Sensitive PKI operations such as key administration shall be performed by staff with sufficient background checks. Background check procedures for BA are specified on BA's Intranet: >Home >Helpcentre >People services >Criminal Record Check.

5.3.3 TRAINING REQUIREMENTS

PKI administrators shall receive appropriate training regarding their responsibilities managing CAs and undertaking certificate and key management processes. At a minimum, PKI administration training shall include:

- Operational training for certificate and key lifecycle management.
  - Venafi – Enterprise Key and Certificate Management tool
  - Microsoft CA Services
  - SITA
- Vendor training for operating PKI software and hardware.
  - SafeSign
  - SafeNet

Key custodians and supervisors shall receive operational training to be able to undertake their responsibilities in key lifecycle management.

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

BA staff with PKI operational responsibilities shall be retrained with the frequency specified in the Corporate PKI - Operational Framework, which is held on the BA LAN share: im-eng-delivery (\\USERGROUP4).

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

BA staff with any PKI operational responsibilities may be rotated as and when the business need dictates. Personnel security requirements for BA staff who move jobs are specified in the following documents:

1. IAM Policy 05-02 Personnel Security During Employment.
2. IAM Policy 05-03 Personnel Security on Termination or Change of Employment.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

Unauthorised access to and use of PKI services and private keys associated with BA certificates shall invoke disciplinary action against the offending party with respect to the BA HR policies for misuse of BA IT systems. Relevant BA Standing Instructions are:

1. BASI 8 - Data and Document Management.
2. BASI 16 - Information technology (IT).

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

Independent contractors that undertake PKI operational activities shall undergo the same level of vetting and background checks as permanent staff as specified in 5.3.1 and 5.3.2.

Contractors must not undertake critical PKI roles such as key custodian and key supervisor.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

BA staff performing PKI administration roles shall be provided with comprehensive BA and vendor documentation detailing the procedures.

BA staff using the certificates (both Applicants and Relying Parties) shall be provided user documentation that described the correct use policy and procedures.

5.4 Audit Logging Procedures

5.4.1 TYPES OF EVENTS RECORDED

Events recorded by IT Security:

- Subscriber Contacts handover of High Level Community (HLC) SITA smartcards.
- HLC smartcard PIN resets.
- HSM partition passphrase communication.
- Access to the PKI safes.
- Removal of PKI safe inventory.
- Tamperproof bag usage.
- Entry/Attempted Entry to Secure Racks in data centres.
- Unauthorised activity on issuing Certificate Authority servers.

Events logged in ArcSight:

- Eagle-i SNMP traps.
- Certificate Authority logs.

5.4.2 FREQUENCY OF PROCESSING LOG

Logs from Corporate PKI service components shall be processed at the same frequency as other critical BA systems.

5.4.3 RETENTION PERIOD FOR AUDIT LOG

The audit logs for all PKI events shall be retained for one year.

5.4.4 PROTECTION OF AUDIT LOG

Audit logs shall be accessed by authorised personnel only and protected from modification or deletion.

5.4.5 AUDIT LOG BACKUP PROCEDURES

The audit logs for all PKI events shall be held in ArcSight.

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

The audit logs for all PKI events shall be held in ArcSight.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

Individuals (e.g. BA staff) that misuse BA Corporate PKI services shall be notified with respect to the HR policies that specific misuse of BA IT systems. Any required disciplinary action shall be undertaken as specified in 5.3.6.

5.4.8 VULNERABILITY ASSESSMENTS

Penetration tests to the PKI environment shall be performed every year by an external reviewer. The scope of this test shall include both internal and external attacks and application layer testing.

Audit logs shall be reviewed to identify attempted attacks against the PKI components.

5.5 Records Archival

5.5.1 TYPES OF RECORDS ARCHIVED

The following records shall be archived:

- Events and accompanying data described in 5.4.1.
- All issued CRLs.
- Internal and External Audit data.
- Certificate application information.
- Documentation supporting certification applications.

5.5.2 RETENTION PERIOD FOR ARCHIVE

The audit logs for all PKI events shall be retained for one year. All other PKI archives shall be retained for five years.

5.5.3 PROTECTION OF ARCHIVE

Audit logs for all PKI events shall be accessed by authorised personnel only and protected from modification or deletion in ArcSight. All other PKI archives shall be protected and held securely, making use of the PKI safes, as appropriate.

5.5.4 ARCHIVE BACKUP PROCEDURES

The audit logs for all PKI events shall be held in ArcSight. All other PKI archives shall be protected and held securely, making use of the PKI safes, as appropriate.

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

CAs shall time stamp all records using UTC taken from the system clock of the relevant machines which is set by the NTP protocol from central servers.

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

The audit logs for all PKI events shall be held in ArcSight. All other PKI archives shall be protected and held securely, making use of the PKI safes, as appropriate.

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

Audit logs for all PKI events shall be accessed by authorised personnel only and protected from modification or deletion in ArcSight. All other PKI archives shall be protected and held securely, making use of the PKI safes, as appropriate.

Authorisation for access to ArcSight may be applied for by means of BA's Corporate Directory. Authorisation for escorted access to all other PKI archives shall be via written request to the Corporate PKI team.

5.6 Key Changeover

The process for key changeover will follow the process for key pair generation and installation, specified in 6.1.

The root CA will have a self-signed certificate with a maximum 20 year life.

Subordinate CAs will have keys signed by the root CA, these will have a maximum 10 year life.

Issuing CAs will have their keys signed by the appropriate Subordinate CA and will have a maximum 5 year life.

Keys will be changed and new CA certificates issued before their expiry if a private key is suspected to have been compromised, or if the chosen key length becomes computationally feasible to break.

5.7 Compromise and Disaster Recovery

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

See IAM Policy 12-02 Management of Information Security Incidents and:

- ISP-0008 Security Data Breach Procedures.
- ISP-0003 Incident Response Procedures.

5.7.2 ENTITY PRIVATE KEY COMPROMISE PROCEDURES

In the event of a compromise, the certificate will be immediately revoked and the CRL and OCSP responder updated in line with 4.9.5.

An investigation will determine how the key was compromised following BA's procedures for security investigations:

- ISP-0008 Security Data Breach Procedures.
- ISP-0003 Incident Response Procedures.

5.7.3 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

BA shall maintain and operate a business continuity plan for the Corporate PKI service incorporating a disaster recovery plan.

In the event of a disaster, possibly requiring fall-back to a disaster recovery site, BA will endeavour to recover the issuing CAs at the earliest possible opportunity.

BA shall implement, document and periodically test the business continuity and disaster recovery capabilities of the PKI with respect to its corporate business continuity plans (held in BA's ARCHER system) and its corporate disaster recovery plans (held on the corporate LANs: OPSDOCS and COVERAGE).

5.8 CA or RA Termination

If an issuing CA is terminated, all Applicants and Relying Parties shall be notified in advance and all certificates shall be revoked no later than the time of termination.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 KEY PAIR GENERATION

The following considerations shall be observed in generating key pairs for Root and Subordinate CAs:

- Keys shall be generated on a FIPS 140-2 Level 2 certified hardware-based cryptographic module located in a dedicated, monitored and physically secured area.
- At least dual control shall be observed during key generation (e.g. by employing a key custodian and a key supervisor).
- Keys shall not leave the cryptographic modules other than for purposes described in 6.2.6.

The following considerations shall be observed in generating key pairs for Issuing CAs:

- Keys shall be generated on a FIPS 140-2 Level 2 certified secure system located in a secure network zone.
- At least dual control shall be observed during key generation (e.g. by employing a key custodian and a key supervisor).
- Keys shall not leave the cryptographic modules other than for purposes described in 6.2.6.

The following considerations shall be observed in generating key pairs for Applicants (e.g. users, services and applications):

- Keys for critical services shall be generated on a secure FIPS 140-2 Level 2 certified system located in a secure network zone.
- Keys for critical services shall not leave the cryptographic modules other than for purposes described in 6.2.6.

6.1.2 PRIVATE KEY DELIVERY TO APPLICANT

There are two alternatives for the generation and delivery of Applicant keys.

- In cases the key is generated by the Applicant on the target system, no key delivery is required. In this case the certificate request received from the Applicant contains all the information to issue certificates. The request shall be checked prior to certificate issuance to establish the link between the Applicant private key and the public key in the request using the procedure set out in 3.2.1.
- In cases the CA generates the key on behalf of the Applicant (e.g. during auto-enrolment), the private key shall be delivered to the Applicant over a secure channel.

Venafi generates the private key for the:

- A380 Wireless Airport Communication System (WACS).
- A380 On-board Asynchronous Messaging Service (OAMS).
- A380 Ground Asynchronous Messaging Service (GAMS).

These keys are stored on the \\lhrcbk-fsfb01\ encrypted LAN share and the passwords communicated to the Applicant following IT Security procedures.

The BEGSS CA generates the private key for the BEGSS Static Identity, this key is stored on the \\lhrcbk-fsfb01\ encrypted LAN share with the password communicated to the Applicant following IT Security procedures.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

In all cases other than auto-enrolment, the public key of the Applicant shall be delivered to the certificate issuer by the registered RA only.

During auto-enrolment the key pair is generated by the issuing CA so no delivery to the certificate issuer is required.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

CA certificates will be distributed to all Relying Parties using a secure mechanism prior to any certificate use.

CA certificates are published to the CDP http://ba-pki.baplc.com/CRL/

6.1.5 KEY SIZES

The standard private / public key pair length shall be 2048 bits. Under special circumstances 1024 may be allowed, but less than this will never be acceptable.

If 2048 bits becomes computationally feasible to break longer key lengths shall be adopted.

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

No stipulation.

6.1.7 KEY USAGE PURPOSES

The key usage field as per X509 version 3 shall be used to determine the allowed uses of the corresponding certificate.

BA shall only issue certificates to BA devices / applications / servers, etc. BA will not sign third party keys.

See Table 1.1 for service specific key usage purposes allowed for each Issuing CA.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

The Corporate PKI service shall employ hardware-based security modules (HSMs) to protect the keys for all Root, Subordinate and Issuing CAs. The HSMs shall feature at a minimum FIPS 140-2 Level 2 certification.

All cryptographic operations involving the CAs shall be performed on the HSM environment. The keys shall not leave the HSMs in clear form other than for administrative purposes (see 6.2.6). The keys shall be encrypted at all times if they are stored outside the HSM environment.

The Corporate PKI service shall support the use of HSMs to protect keys of critical services as deemed necessary by the Applicant.

6.2.2 PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL

Key management and access requirements shall comply with the procedures set out in 5.2.

6.2.3 PRIVATE KEY ESCROW

No stipulation.

6.2.4 PRIVATE KEY BACKUP

All CA keys and critical service keys shall be backed up, on secure storage, on a regular basis by authorised personnel from the Corporate PKI team. CA key backup procedures shall observe dual control procedures to extract and retrieve private keys as required.

6.2.5 PRIVATE KEY ARCHIVAL

All CA keys and critical service keys shall be archived following the expiry of the associated certificate.

Key archives shall be retained for five years as specified in 5.5.2.

The retention period for a key can be extended if there is data on any BA systems that is encrypted or signed by the corresponding key.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

Private keys generated on an HSM shall be stored on the HSM at all times. Secure transfer of the keys to or from the HSM may be allowed in the following circumstances:

- Backup or restoration of private keys.
- Private key archiving.
- On-line or off-line key sharing between HSMs.

See SafeNet documentation: \\im-eng-delivery\B4Y PKI Project\SafeNet docs\

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

All CA and critical service private keys shall be stored on HSMs. Any keys shall be stored in encrypted format and/or on secure storage if outside the HSM environment (e.g. for administrative purposes specified in 6.2.6).

All other Applicant keys shall be stored on secure storage areas on the target system. For example, software-based encrypted key stores on Windows and Linux systems.

6.2.8 METHOD OF ACTIVATING PRIVATE KEY

See SafeNet documentation: \\im-eng-delivery\B4Y PKI Project\SafeNet docs\

6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

See SafeNet documentation: \\im-eng-delivery\B4Y PKI Project\SafeNet docs\

6.2.10 METHOD OF DESTROYING PRIVATE KEY

All CA and critical service private keys shall be archived for the duration specified in 6.2.5.

Following the retention period, and if deemed appropriate following that, all CA and critical service private keys shall be destroyed securely either by overwriting the storage media or physically destroying it.

6.2.11 CRYPTOGRAPHIC MODULE RATING

The Corporate PKI service shall use HSMs with at a minimum FIPS 140 Level 2 rating.

6.3 Other Aspects of Key Pair Management

6.3.1 PUBLIC KEY ARCHIVAL

No stipulation.

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

Key pair period or lifetime shall be aligned to the certificate operational periods.

6.4 Activation Data

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

No stipulation.

6.4.2 ACTIVATION DATA PROTECTION

No stipulation.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

No stipulation.

6.5 Computer Security Controls

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

The following are relevant documents:

1. CA server access controls, documented in:
   \\im-eng-delivery\B4Y PKI Project\Key Ceremony\KSC process docs\…
   - "PKI Servers UserIn Process.doc".
   - "Logical access summary v0.2_withPBAdditions".
2. IAM Policy 08-09 Monitoring.
3. IAM Policy 09-01 Business Requirement for Access Control
4. IAM Policy 09-02 User Access Management.
5. IAM Policy 09-03 User Responsibilities.
6. IAM Policy 09-04 Operating System and Database Access Control.
7. IAM Policy 09-05 Application and Information Access Control.
8. IAM Policy 10-02 Network Access Control.

6.5.2 COMPUTER SECURITY RATING

CA components shall make use of EAL4+ or FIPS 140-2 level 2 evaluated products where practical.

Table 6.1

HSMs	Details	Security Rating
SafeNet LUNA G5 USB (offline)	▪ Stores Root & Subordinate CAs keys (1 Root + 2 Subs)	Includes a FIPS 140-2 L2 & L3 cryptographic module
SafeNet LUNA SA5 (networked)	▪ Stores Issuing CAs #1, #2, #3, #4 & #5 keys (5 CAs)	FIPS 140-2 Level 2 validated

6.6 Life Cycle Technical Controls

6.6.1 SYSTEM DEVELOPMENT CONTROLS

The following are relevant documents:

1. IAM Policy 11-01 Security Requirements for Information Systems.

2. IAM Policy 11-02 Correct Processing in Applications.
3. IAM Policy 11-03 Cryptographic Controls.
4. IAM Policy 11-04 Security of System Files.
5. IAM Policy 11-05 Security in Development and Support Processes.
6. IAM Policy 11-06 Technical Vulnerability Management.
7. IAM Policy 11-07 Web Services.
8. IAM Policy 11-08 Mobile Applications.

6.6.2 SECURITY MANAGEMENT CONTROLS

The following are relevant documents:

1. The Luna G5 and SA5 HSM PIN Entry Device (PED) keys, documented in: \\im-eng-delivery\B4Y PKI Project\Key Ceremony Safenet SmartKey Layout.doc
2. IAM Policy 08-01 Operational Procedures and Responsibilities.
3. IAM Policy 08-02 Third Party Service Delivery Management.
4. IAM Policy 08-03 System Planning and Acceptance.
5. IAM Policy 08-04 Protection Against Malicious and Mobile Code.
6. IAM Policy 08-05 Back-up.
7. IAM Policy 08-06 Media Handling.
8. IAM Policy 08-07 Exchange of Information.
9. IAM Policy 08-08 Electronic Commerce Services.
10. IAM Policy 08-09 Monitoring.
11. IAM Policy 08-10 Cloud Computing.

6.6.3 LIFE CYCLE SECURITY CONTROLS

The following are relevant documents:

1. IAM Policy 01-01 Framework and Taxonomy.
2. IAM Policy 01-02 Leadership Team Commitment to Information Security.
3. IAM Policy 01-03 Information Security Organisation.
4. IAM Policy 01-04 External Parties.
5. IAM Policy 02-01 Establish Information Security Policy.
6. IAM Policy 03-01 Information Risk Management.

6.7 Network Security Controls

The following are relevant documents:

1. IAM Policy 10-01 Network Security Management.
2. IAM Policy 10-02 Network Access Control.
3. IAM Policy 10-03 Network Encryption.
4. IAM Policy 10-04 Public Key Infrastructure.

6.8 Time-stamping

CAs and the RA shall time stamp all records using UTC taken from the system clock of the relevant machine, the system clock will be set from the corporate NTP servers.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 VERSION NUMBER(S)

Only X509 version 3 compliant certificates will be issued. Custom profiles are allowed (e.g. Boeing e-Enabled certificates).

It should be noted that future versions of this document may include additional service-dependent certificate versions as required.

7.1.2 CERTIFICATE EXTENSIONS

At a minimum, BA shall use the standard X509 version 3 extensions in accordance with RFC 2459 and RFC 3280. The use of additional, service-dependent certificate extensions as defined below shall not modify the base extensions.

The certificate extensions for the A380 aircraft to ground wireless communications have followed the requirements detailed in the following Airbus document - A380 Certificate Management on OWAG-CS - Technical Report (Reference: L46RP0819087).

It should be noted that future versions of this document may include additional service-dependent certificate extensions as required.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

BA currently supports the hash function / digital signature algorithm combinations:

- md5withRSAEncryption
- sha1withRSAEncryption
- sha256WithRSAEncryption
- sha384WithRSAEncryption
- sha512WithRSAEncryption

The subfield algorithmIdentifier:algorithm contains the appropriate object identifier (specified in RFC 3280) for any of the above algorithms.

The standard private / public key pair length shall be 2048 bits. Under special circumstances 1024 may be allowed, but less than this will never be acceptable.

If 2048 bits becomes computationally feasible to break longer key lengths shall be adopted.

It should be noted that future versions of this document may include additional service-dependent algorithm objects as required.

7.1.4 NAME FORMS

Each of the X509 certificate subject and issuer fields shall be completed with a unique DN in accordance with the attribute type as specified in RFC 3280.

At a minimum, certificates issued by BA shall contain the following information in the issuer field:

- Version number(s) supported.
- Certificate extensions populated and their criticality.
- Cryptographic algorithm object identifiers.
- Name forms used for the CA, RA, and Applicant names.
- Name constraints used and the name forms used in the name constraints.

Corporate PKI has the following branch of the BA OID 1.3.6.1.4.1.20972.1.2
The link to the CPS is published in the Subordinate CA certificates 1.3.6.1.4.1.20972.1.2.1.1.

It should be noted that future versions of this document may include additional service-dependent name forms as required.

7.1.5 NAME CONSTRAINTS

It should be noted that future versions of this document may include service-dependent name constraints as required.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

No stipulation.

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

No stipulation.

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

No stipulation.

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION

No stipulation.

7.2 CRL Profile

At a minimum, CRLs issued by BA shall contain the following information:

- Version to which the CRL conforms.
- Signature.
- CA that issued the CRL (and the revoked certificate).

- The date and time when the CRL was issued.
- The date when this CRL becomes invalid.
- The serial numbers of the unexpired revoked certificates.
- The public key to use in verifying the authenticity of the CRL.

7.2.1 VERSION NUMBER(S)

BA shall issue X509 version 2 CRLs.

7.2.2 CRL AND CRL ENTRY EXTENSIONS

It should be noted that future versions of this document may include service-dependent CRL extensions as required.

7.3 OCSP Profile

7.3.1 VERSION NUMBER(S)

It should be noted that future versions of this document may include service-dependent OCSP profiles as required.

7.3.2 OCSP EXTENSIONS

It should be noted that future versions of this document may include additional service-dependent OCSP extensions as required.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The BA Corporate PKI service is subject to internal and external audits that will consider all of the requirements specified in this document.

8.1 Frequency or Circumstances of Assessment

The frequency and circumstances of all audits and assessments of the Corporate PKI service shall be determined by BA's Internal Control Department.

The BA Corporate PKI Service shall undergo an internal review every 2 years to examine ongoing compliance with this CPS and other relevant regulation.

The BA Corporate PKI Service shall undergo an external review every 4 years to examine ongoing compliance with this CPS and other relevant regulation.

8.2 Identity/Qualifications of Assessor

Internal audits and assessments of the Corporate PKI service shall be conducted by appropriately qualified staff from BA's Internal Control Department.

External audits and assessments of the Corporate PKI service shall be conducted by appropriately qualified organisations deemed suitable by BA's Internal Control Department.

8.3 Assessor's Relationship to Assessed Entity

Audits and assessments of the Corporate PKI service shall be performed by BA's Internal Control Department which is independent from the Information Security Team which owns and governs the Corporate PKI service through this policy document.

External audits and assessments of the Corporate PKI service shall be performed by external organisations sufficiently independent from the set up and operation of the BA Corporate PKI Service.

8.4 Topics Covered by Assessment

The topics to be covered by audits and assessments of the Corporate PKI service shall be determined by BA's Internal Control Department. At a minimum, the topics shall include the following:

- Management and administration of PKI keys.
- Set up and operation of the Corporate PKI service.
- Logical and physical security controls that apply to the Corporate PKI environment.
- Governance of the Corporate PKI service.

8.5 Actions Taken as a Result of Deficiency

The actions to be taken as a result of audits and assessments of the Corporate PKI service shall be determined by BA's Internal Control Department, who shall advise on the severity and timescales for remediation as necessary.

Senior BA management that owns and are accountable for the BA Corporate PKI service shall be responsible for the closure of any internal or external audit findings within the specified timescales.

8.6 Communication of Results

Communication of the results of audits and assessments of the Corporate PKI service shall be made by BA's Internal Control Department. Recipients shall include the following:

- The owner of the Corporate PKI service.
- The Head of Internal Control.
- BA Chief Executive Officer.
- Head of IT Operations.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

No fees will be charged for the issuance, use and management of the BA certificates issued from any of the Issuing CAs under Corporate or Business Integration Subordinate CAs.

9.2 Financial Responsibility

9.2.1 INSURANCE COVERAGE

No stipulation.

9.2.2 OTHER ASSETS

No stipulation.

9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

The BA PKI information will be handled as INTERNAL, CONFIDENTIAL or STRICTLY CONFIDENTIAL in accordance with the BA Standing Instruction (BASI) 8:

Table 9.1

BA PKI Information	Classification
Technical and physical specification of BA PKI	INTERNAL
Security Health Check results	CONFIDENTIAL
Audit Logs	INTERNAL
Private keys	STRICTLY CONFIDENTIAL
HSM and CA activation data	STRICTLY CONFIDENTIAL
PKI business continuity and disaster recovery plans	INTERNAL
PKI security incidents	STRICTLY CONFIDENTIAL

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

The following are not considered BA confidential information:

- BA internal certificates issued by any Issuing CA in the scope of this CPS.
- Public keys of BA internal certificates.
- CRLs and OCSP information published from any CAs in the scope of this CPS.
- Certificate policy documents and practice statements.

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

BA confidential information shall be protected in accordance with BASI 8 and EG801.

9.4 Privacy of Personal Information

9.4.1 PRIVACY PLAN

The PKI service shall implement a privacy policy in accordance the BA corporate policies stated in BASI 8 and BA Information Assurance Manual. The policy shall be compliant with the Data Protection Act 1998.

9.4.2 INFORMATION TREATED AS PRIVATE

The following information shall be treated as private in addition to 9.3.1:

- Sensitive PKI staff information such as vetting details.
- Any information on staff disciplinary actions.

9.4.3 INFORMATION NOT DEEMED PRIVATE

The following information is not deemed private:

- Public information about BA staff in certificates.
- Public information about BA staff in CRLs.
- Public information about BA staff in OCSP responses.

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

Personal information that may appear on certificates and PKI systems shall be protected in accordance with the existing BA corporate policies.

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

By subscribing to the BA PKI service the Applicant gives consent to use of private information specified in 9.4.2 and to publish information specified in 9.4.3.

Any use of private information listed in 9.4.2 shall adhere to existing BA corporate policies on use of personal information.

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

As per BA corporate policies on disclosure of personal information.

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

As per BA corporate policies on disclosure of personal information.

9.5 Intellectual Property Rights

No stipulation.

9.6 Representations and Warranties

9.6.1 CA REPRESENTATIONS AND WARRANTIES

No stipulation.

9.6.2 RA REPRESENTATIONS AND WARRANTIES

No stipulation.

9.6.3 APPLICANT REPRESENTATIONS AND WARRANTIES

No stipulation.

9.6.4 RELYING PARTY REPRESENTATIONS AND WARRANTIES

No stipulation.

9.6.5 REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS

No stipulation.

9.7 Disclaimers of Warranties

No stipulation.

9.8 Limitations of Liability

No stipulation.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 TERM

CA and RA term shall follow procedures set out in 5.8.

9.10.2 TERMINATION

CA and RA termination shall follow procedures set out in 5.8.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

No stipulation.

9.11 Individual Notices and Communications with Participants

No stipulation.

9.12 Amendments

9.12.1 PROCEDURE FOR AMENDMENT

Any amendments to this policy will be approved by BA following the procedures set out in 1.6.4 and will be reflected in an updated version.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

CP/CPS will be reviewed annually following the procedures set out in 1.6.4 and a new version will be published.

9.12.3 CIRCUMSTANCES UNDER WHICH OID SHALL BE CHANGED

No stipulation.

9.13 Dispute Resolution Provisions

No stipulation.

9.14 Governing Law

The BA PKI service shall be governed by English Law.

9.15 Compliance with Applicable Law

BA shall ensure compliance with the governing law (see 9.14) and any other regulations that are relevant to the operation of BA services that use digital certificates issued by the CAs covered by this CPS.

9.16 Miscellaneous Provisions

No stipulation.

9.16.1 ENTIRE AGREEMENT

No stipulation.

9.16.2 ASSIGNMENT

No stipulation.

9.16.3 SEVERABILITY

No stipulation.

9.16.4 ENFORCEMENT (ATTORNEYS' FEES AND WAIVER OF RIGHTS)

No stipulation.

9.16.5 FORCE MAJEURE

BA shall not be held responsible to any Relying Parties due to events considered as Force Majeure in accordance with the relevant corporate policies.

9.17 Other Provisions

No stipulation.

Document Version Change Control Record		
Version	Date	Reason for Version Change
1-00	5 September 2014	First formal version published.
1-01	29 September 2014	Update to correct errors in Section 6: text should read: FIPS 140-2 Level 2.
1-02	1 December 2014	Update to allow use of wildcard certificates for non-production systems only.