



**Apple Inc.**  
**Certification Authority**  
**Certification Practice Statement**  
**Apple Application Integration**

**Version 3.0**  
**Effective Date: December 22, 2011**



## Table of Contents

1.	Introduction.....	4
1.1.	Trademarks .....	4
1.2.	Table of acronyms .....	4
1.3.	Definitions .....	4
2.	General business practices.....	6
2.1.	Identification.....	6
2.2.	Community and applicability.....	6
2.3.	Contact details .....	6
2.4.	Apportionment of liability.....	7
2.4.1.	Warranties to Subscribers .....	7
2.4.2.	CA disclaimers of warranties .....	7
2.4.3.	CA limitations of liability.....	7
2.4.4.	Subscriber warranties.....	7
2.4.5.	Private key compromise .....	8
2.4.6.	Subscriber and Relying Party liability.....	8
2.5.	Financial responsibility .....	8
2.5.1.	Indemnification by Subscribers .....	8
2.5.2.	Fiduciary relationships.....	8
2.6.	Interpretation and enforcement.....	8
2.6.1.	Governing law.....	8
2.6.2.	Severability, survival, merger, notice.....	8
2.6.3.	Dispute resolution procedures .....	8
2.7.	Fees.....	8
2.7.1.	Certificate issuance or renewal fees.....	9
2.7.2.	Certificate access fees.....	9
2.7.3.	Revocation or status information access fees.....	9
2.7.4.	Fees for other services.....	9
2.7.5.	Refund policy.....	9
2.8.	Publication and Repository.....	9
2.8.1.	Publication of CA information.....	9
2.8.2.	Frequency of publication .....	9
2.8.3.	Access controls .....	9
2.9.	Compliance audit requirements.....	9
2.10.	Conditions for applicability.....	10
2.10.1.	Permitted uses .....	10
2.10.2.	Limitations on use.....	10
2.11.	Obligations .....	10
2.11.1.	General AAI Sub-CA obligations.....	10
2.11.2.	Notification of issuance by AAI Sub-CA to Subscriber.....	11
2.11.3.	Notification of issuance by AAI Sub-CA to others.....	11
2.11.4.	Notification of revocation by AAI Sub-CA to Subscriber.....	11
2.11.5.	Notification of revocation by AAI Sub-CA to others .....	11
2.11.6.	Registration Authority obligations .....	11
2.11.7.	Subscriber obligations to AAI Sub-CA .....	12
2.11.8.	Relying Party obligations to AAI Sub-CA .....	12
3.	Key life cycle management.....	13
3.1.	AAI Sub-CA key generation .....	13
3.2.	AAI Sub-CA private key protection.....	13
3.2.1.	AAI Sub-CA private key storage.....	13
3.2.2.	AAI Sub-CA private key control .....	13
3.2.3.	AAI Sub-CA key escrow .....	13
3.2.4.	AAI Sub-CA key backup .....	13
3.2.5.	AAI Sub-CA key archival.....	13



3.3.	AAI Sub-CA-provided Subscriber key management .....	13
3.4.	AAI Sub-CA public key distribution .....	13
3.5.	AAI Sub-CA key changeover.....	13
4.	Certificate life cycle management .....	15
4.1.	Certificate Suspension .....	15
4.2.	Certificate registration .....	15
4.3.	External RA requirements.....	16
4.4.	Certificate renewal.....	16
4.5.	Certificate rekey.....	17
4.6.	Certificate issuance.....	17
4.7.	Certificate acceptance.....	17
4.8.	Certificate distribution .....	17
4.9.	Certificate revocation .....	18
4.10.	Certificate suspension.....	18
4.11.	Certificate status.....	18
4.11.1.	CRL usage.....	19
4.11.2.	OCSP usage .....	19
4.11.3.	OCSP Designated Responder Certificates .....	19
4.12.	Certificate profile.....	19
4.12.1.	Apple ID Certificates.....	19
4.12.2.	Server Push Production Certificates.....	20
4.12.3.	Server Push Development Certificates .....	20
4.12.4.	Profile Signing Certificates .....	20
4.13.	OCSP Designated Responder Certificate.....	21
4.14.	CRL Profile .....	21
4.15.	Integrated circuit cards.....	21
5.	Environmental controls .....	22
5.1.	CPS administration .....	22
5.2.	CA termination .....	22
5.3.	Confidentiality .....	22
5.4.	Intellectual property rights .....	23
5.5.	Physical security.....	23
5.6.	Business continuity management .....	23
5.7.	Event logging .....	23
5.7.1.	Archiving .....	23
5.7.2.	Event journal reviews.....	23
6.	Revision history.....	24



## 1. Introduction

This Certification Practice Statement (“CPS”) describes the practices employed by the Apple Application Integration Subordinate Certification Authority (“AAI Sub-CA,” or “the Sub-CA”) in issuing and managing digital certificates and related services. These practices, and the structure of this document, are designed to align to the requirements defined in the Apple Certificate Policy (“CP”). Where the CP defines policies that all applicable Apple Sub-CA’s are required to follow, this CPS provides more detailed information about the practices employed by the AAI Sub-CA relating to certificate lifecycle services, such as issuance, management, revocation, renewal, and rekeying, as well as details relating to other business, legal, and technical matters specific to the AAI Sub-CA, collectively referred to as the AAI Public Key Infrastructure (“AAI PKI”).

Apple Inc. (“Apple”) established the Apple Root Certification Authority (“Apple Root CA”) and the Apple PKI in support of the generation, issuance, distribution, revocation, administration, and management of public/private cryptographic keys that are contained in CA-signed X.509 Certificates. The Apple PKI is intended to support internal and external Apple cryptographic requirements, where authentication of an organization or individual presenting a digitally signed or encrypted object to a Relying Party is of benefit to participants in the Apple PKI.

### 1.1. Trademarks

Apple, Mac OS X, and iOS are trademarks of Apple Inc., in the United States and other countries.

### 1.2. Table of acronyms

Please refer to the CP for a table of acronyms used within this document.

### 1.3. Definitions

For the purposes of this CPS:

- Apple OS refers to Mac OS X and/or iOS.
- “Subscriber” refers to one of the following:
  - a Mac OS X or iOS end user who has been issued a Certificate signed by the AAI Sub-CA for purposes of using Mac OS X or iOS product features that require an Apple ID Certificate
  - an end user who has been issued a Certificate for a licensed version of Mac OS X signed by the AAI Sub-CA for purposes of using the Apple Push Notification Service (“APNs”) available within the server administration console of Mac OS X Server
  - a third-party server end user who has been issued a Certificate signed by the AAI Sub-CA for the purpose of using the Apple Push Notification Services (“APNs”) through an authorized third-party vendor’s MDM server product.
- “Relying Party” refers to an individual or organization that places reliance on a Certificate issued by the AAI Sub-CA.
- Apple Push Notification Service (“APNs”) refers to the Apple mobile service that allows for propagation of information to iOS devices through the use of notifications pushed from the provider to the target iOS device.
- “Apple Push Certificates Portal” refers to an Apple Internet site where Push Notification Certificates can be managed (e.g. downloaded, revoked, etc.) by Subscribers. The management options available to Subscribers may vary by certificate type.



- “Keychain” refers to Apple’s password management system in Mac OS X and iOS. A Keychain can contain various types of data, including passwords, private keys, and digital certificates.

Please refer to the CP for all other definitions used within this document.



## 2. General business practices

This section establishes and sets forth the general business practices of the AAI Sub-CA.

### 2.1. Identification

The practices set forth in this CPS apply exclusively to the AAI Sub-CA. This CPS is structured similarly to the CP, disclosing details of the practices employed by the AAI Sub-CA that address the more general requirements defined in the CP. This document assumes the reader is familiar with the general concepts of digital signatures, certificates, and public key infrastructure. If the reader is new to public key infrastructure concepts, the reader may choose to consult the introduction and overview sections of the WebTrust Program for Certification Authorities, a guide published by the American Institute of Certified Public Accountants (AICPA) and freely available for download from their web site, [www.aicpa.org](http://www.aicpa.org). The guide contains an overview of PKI, including an orientation on key concepts such as digital signatures, asymmetric key pairs, Certification Authorities, registration authorities, policy and practice statements, and business issues and considerations.

For the purposes of this CPS, the term Apple PKI refers collectively to Apple PKI Service Providers and End Entities. Apple PKI Service Providers consist of (1) Apple Certification Authorities ("CAs"), including the Apple Root CA and the AAI Sub-CA, and their related management teams that generate, issue, distribute, revoke and manage cryptographic keys and Certificates, (2) Apple Registration Authorities ("Apple RAs"), and (3) the Apple CA Policy Authority ("Apple PA," or "PA"). End Entities are Subscribers of Certificates.

The AAI Sub-CA issues and administers Certificates in accordance with policies in the Apple CP document.

### 2.2. Community and applicability

This CPS is applicable to the following end-entity certificates issued by the AAI Sub-CA:

- Apple ID Certificates ("Apple ID Certificates")
- Server Push Service Production Certificates ("Server Push Production Certificates")
- Server Push Service Development Certificates ("Server Push Development Certificates")
- Configuration Profile Signing Certificates ("Profile Signing Certificates")

Certificates used exclusively for functions internal to Apple products and/or Apple processes are not included within the scope of this CPS.

### 2.3. Contact details

The CA's Certificate Policies are administered by the Apple CA Policy Authority. The contact information for this CPS is:

Apple CA Policy Authority  
C/O General Counsel  
Apple Inc.  
1 Infinite Loop  
Cupertino, CA 95014

(408) 996-1010  
[policy\\_authority@apple.com](mailto:policy_authority@apple.com)



## 2.4. Apportionment of liability

### Apple ID Certificate:

- For Apple ID Certificates, a Subscriber Agreement may be incorporated in the applicable End User License Agreement (“EULA”).

### Server Push Production Certificate and Server Push Development Certificate:

- For the Certificates issued to Mac OS X end users, a Subscriber agreement is incorporated in the applicable End User License Agreement (“EULA”) of Mac OS X Server.
- For the Certificates issued to end users of third-party servers that are authorized by Apple to use the Apple Push Notification Service (“APNs”), a Subscriber agreement is incorporated in the Program License Agreement (“PLA”) in the Apple Push Certificates Portal.

For Apple ID and Server Push Certificates there is not an applicable Relying Party agreement for the AAI Sub-CA Certificates as the Relying Parties are internal to Apple. Through normal use, the Apple OS may determine the status of the Certificate through a CRL or OCSP request, however Apple is considered to be the Relying Party in these instances.

### Profile Signing Certificates:

- A relying party agreement is incorporated into the Mac OS X and iOS End User License Agreement (“EULA”). There is not an applicable Subscriber agreement as the Subscriber is internal to Apple.

#### 2.4.1. Warranties to Subscribers

The AAI Sub-CA does not warrant the use of any Certificate to any Subscriber.

#### 2.4.2. CA disclaimers of warranties

To the extent permitted by applicable law, Subscriber agreements, if applicable, disclaim warranties from Apple, including any warranty of merchantability or fitness for a particular purpose.

#### 2.4.3. CA limitations of liability

To the extent permitted by applicable law, Subscriber agreements, if applicable, shall limit liability on the part of Apple and shall exclude liability for indirect, special, incidental, and consequential damages.

#### 2.4.4. Subscriber warranties

For Apple ID Certificates, Server Push Production Certificates, Server Push Development Certificates, and Profile Signing Certificates, Subscriber agreements, if any, shall require Subscribers to warrant that:

- They will take no action to interfere with the normal operation of an Apple ID Certificate, a Server Push Production Certificate, a Server Push Development Certificate, or products that rely on such certificates.
- They are solely responsible for preventing any unauthorized person from having access to the Subscriber’s private key stored on any device from which the Subscriber has participated in the services where the CA functionality is enabled.



- The Apple ID Certificates, Server Push Production Certificates, Server Push Development Certificates, and Profile Signing Certificates are being used exclusively for authorized and legal purposes.

#### **2.4.5. Private key compromise**

Apple reserves the right to revoke any Certificates, without notice, if it believes the Subscriber's private key has been compromised, or upon request from the Subscriber.

#### **2.4.6. Subscriber and Relying Party liability**

Subscribers will hold Apple harmless from any and all liabilities, losses, actions, damages, or claims (including all reasonable expenses, costs, and attorneys fees) arising out of or relating to their use of any digital Certificate. Relying Party terms in the applicable End User License Agreement apply to the extent users are relying parties.

### **2.5. Financial responsibility**

This section sets forth policies as requirements on the AAI Sub-CA related to indemnification by Relying Parties and disclosure of fiduciary relationships in relying party agreements.

#### **2.5.1. Indemnification by Subscribers**

Any Subscriber agreement may, at Apple's discretion, include an indemnification clause by Subscribers.

#### **2.5.2. Fiduciary relationships**

There is no fiduciary relationship between Apple and Subscribers.

### **2.6. Interpretation and enforcement**

Interpretation and enforcement of any subscriber agreement is governed by the terms and conditions in the applicable End User License Agreement.

#### **2.6.1. Governing law**

Governing law of any subscriber agreement is governed by the terms and conditions in the applicable End User License Agreement ("EULA") or Program License Agreement ("PLA").

#### **2.6.2. Severability, survival, merger, notice**

Severability, survival, merger and notice if applicable, are governed by the terms and conditions in the applicable End User License Agreement ("EULA") or Program License Agreement ("PLA").

#### **2.6.3. Dispute resolution procedures**

Dispute resolution procedures of any subscriber agreement are governed by the terms and conditions in the applicable End User License Agreement ("EULA") or Program License Agreement ("PLA").

### **2.7. Fees**

This section sets forth policies associated with any fees charged to Subscribers for Certification Authority services for each type of Certificate.



### 2.7.1. Certificate issuance or renewal fees

No fees are charged for this service. Certificates are valid during the validity period as set forth in the Certificates unless otherwise revoked.

### 2.7.2. Certificate access fees

No fees are charged for this service.

### 2.7.3. Revocation or status information access fees

No fees are charged for this service.

### 2.7.4. Fees for other services

No other fees are charged for CA services.

### 2.7.5. Refund policy

Not Applicable.

## 2.8. Publication and Repository

### 2.8.1. Publication of CA information

The latest version of this CPS for the AAI Sub-CA can be found at <http://www.apple.com/certificateauthority/>.

### 2.8.2. Frequency of publication

Certificate status may be made available through a Certificate Revocation List ("CRL") which is published by Apple on a periodic basis. For some Certificates, the status may also be checked using the Online Certificate Status Protocol ("OCSP"). Refer to the CRL Distribution Point ("CDP") or the Authority Information Access ("AIA") extensions in the Certificates for the status information method used.

### 2.8.3. Access controls

Server Push Production and Development Subscribers shall have access to their Certificates through the Apple Push Certificates Portal and/or the Keychain local certificate store in Mac OS X.

For some Certificates, the CRL will be provided in the manner described by the CRL Distribution Points extension present in the end-entity Certificates issued by the AAI Sub-CA. For some Certificates, the status of a Certificate may be checked using the Online Certificate Status Protocol ("OCSP"). Refer to the CRL Distribution Point ("CDP") or the Authority Information Access ("AIA") extensions in the Certificates for the status information method used.

Apple may require Subscribers to agree to a Subscriber Agreement to access their own Certificates. There is no public repository of Certificates. Certificate status information is publicly available through OCSP and/or CRL, as described above. Apple has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

## 2.9. Compliance audit requirements

The AAI Sub-CA adopts wholly all policies under this section in the CP.



## 2.10. Conditions for applicability

This section sets forth practices related to the use of the AAI Sub-CA.

### 2.10.1. Permitted uses

The AAI Sub-CA will create keys, manage keys, issue Certificates, manage key life cycles, manage certificate life cycles, operate a private repository, and perform other functions to support distribution for the following types of Certificates:

- **Apple ID Certificates:** This type of Certificate may be used by an Apple OS to identify and authenticate a user's account and enable the use of Apple OS features. This authentication allows the use of collaborative features such as sharing or synchronizing files.
- **Server Push Production Certificates:** This type of Certificate may be used by a Mac OS X end user or a third party server end-user, to create and maintain SSL connectivity to the Apple Push Notification Service production environment. The certificates enable remote notifications of a designated Mac OS X feature (e.g. mail, calendar, contact, mobile device management) to be sent via the APN service Production server to an iOS device and/or a Mac OS X system.
- **Server Push Development Certificates:** This type of Certificate may be used by a Mac OS X end user, or a third party server end-user, to create and maintain SSL connectivity to the Apple Push Notification Service development environment. The certificates enable remote notifications of a designated Mac OS X feature (e.g. mail, calendar, contact, mobile device management) to be sent via the Apple Push Notification Service development server to an Apple iOS device and/or a Mac OS X system.
- **Profile Signing Certificates:** This type of Certificate may be used by Apple to sign configuration profiles for Mac OS X and iOS.

Certificates used exclusively for functions internal to Apple products and/or Apple processes are not included within the scope of this CPS.

### 2.10.2. Limitations on use

The AAI Sub-CA will not allow its Certificates to be used to create a Certification Authority or to allow its private key to sign a Certificate issued by another Certification Authority.

Except for internal-use Certificates, the AAI Sub-CA Certificates shall not be used for any purpose that is not identified in this CPS §2.10.1 as a permitted use.

## 2.11. Obligations

This section sets forth policies related to the obligations of the AAI Sub-CA.

### 2.11.1. General AAI Sub-CA obligations

The AAI Sub-CA shall:

- Conform its operations to the Apple CP and to this CPS as the same may be amended from time to time.
- Issue and publish Certificates in accordance with the Apple CP and this CPS.
- Revoke Certificates issued by the AAI Sub-CA, upon receipt of a valid request to revoke the Certificate from a person authorized to request such a revocation. The validity of the



request and the authorization of the person making the request will be determined by the AAI Sub-CA.

- Publish Certificate Revocation Lists (CRLs) on a regular basis in accordance with the Apple CP. As applicable, the CA shall notify the subscriber that the certificate has been revoked.

### 2.11.2. Notification of issuance by AAI Sub-CA to Subscriber

The AAI Sub-CA will notify Subscribers of the issuance of certificates according to the following:

- **Apple ID Certificates:** For Mac OS X, notification to Subscribers is deemed to have taken place when the Certificate is added to the Subscriber's Keychain. For iOS, notification to Subscribers is deemed to have taken place when the iOS product feature(s) utilizing certificates is used.
- **Server Push Certificates for Mac OS X:** For Server Push Certificates issued to end users of Mac OS X, including Production and Development certificate types, notification to Subscribers is deemed to have taken place when the Certificate is added to the Subscriber's Keychain. A Subscriber may verify the issuance, status, and contents of a Certificate using Mac OS X's Keychain Access application.
- **Server Push Certificates for Third-Party Servers:** For Certificates issued to end users of third party servers, notification is deemed to have taken place when newly issued Certificates are made available via the Apple Push Certificates Portal. A Subscriber may verify the issuance, status, and contents of a Certificate via the Apple Push Certificates Portal.
- **Profile Signing Certificates:** Profile Signing Certificates are issued internally to business groups within Apple. Therefore, no external notifications are sent.

### 2.11.3. Notification of issuance by AAI Sub-CA to others

The AAI Sub-CA does not provide notification of issuance to parties other than the Subscriber.

### 2.11.4. Notification of revocation by AAI Sub-CA to Subscriber

The AAI Sub-CA provides notification of certificate revocation to the Subscriber by email. Certificate status information is publicly available through OCSP and/or CRL.

### 2.11.5. Notification of revocation by AAI Sub-CA to others

The AAI Sub-CA does not provide notification of certificate revocation by email, except to the Subscriber. Certificate status information is publicly available through OCSP and/or CRL.

### 2.11.6. Registration Authority obligations

A Registration Authority ("RA") external to Apple is not used. The AAI Sub-CA performs limited RA services to provide reasonable assurance of the following:

- **Apple ID Certificates:** Certificates are issued only to Apple OS end users who present a valid Apple ID account name and password.
- **Server Push Certificates for Mac OS X:** Both Production and Development Certificates are issued only to Mac OS X end users who present a valid Apple ID account name and



password. Additionally, the CSR must have been created by a legitimate copy of Mac OS X.

- **Server Push Certificates for Third-Party Servers:** Both Production and Development Certificates are issued only to end users of third-party servers that are authorized by Apple to use the Apple Push Notification Service ("APNs"). Certificate applicants must present a valid Apple ID account name and password and provide a CSR that is digitally signed by a valid and designated Apple issued certificate issued to the third-party server vendor.
- **Profile Signing Certificates:** Profile Signing certificates are issued to Apple business groups that have demonstrated a need to sign configuration profiles for Mac OS X or iOS.

### 2.11.7. Subscriber obligations to AAI Sub-CA

Subscribers are obligated to:

- Provide information to the AAI-CA that is accurate and complete to the best of the Subscribers' knowledge and belief regarding information in their certificates and identification and authentication information and promptly notify the CA of any changes to this information.
- Safeguard their private key from compromise.
- Use their Apple ID Certificates, Server Push Production Certificates, Server Push Development Certificates, and Profile Signing Certificates exclusively for legal purposes.
- Promptly request that the AAI Sub-CA revoke a Certificate if the Subscriber has reason to believe there has been a compromise of the Certificate's associated private key according to the process described in the section entitled "Certificate Revocation".
- Take no action to transfer their Certificate to any third-party.

### 2.11.8. Relying Party obligations to AAI Sub-CA

Relying Parties are obligated to:

- Acknowledge that they are solely responsible for deciding whether or not to rely on the information in a Certificate, and agree that they have sufficient information to make an informed decision. Apple shall not be responsible for assessing the appropriateness of the use of a Certificate.
- Acknowledge that, to the extent permitted by applicable law, Apple hereby disclaims all warranties regarding the use of any Certificates, including any warranty of merchantability or fitness for a particular purpose. In addition, Apple hereby limits its liability, and excludes all liability for indirect, special, incidental, and consequential damages.
- Restrict reliance on Certificates issued by the CA to the purposes for which those Certificates were issued, in accordance with the CP and this CPS.

### 3. Key life cycle management

This section sets forth practices related to the key life cycle management controls of the AAI Sub-CA.

#### 3.1.AAI Sub-CA key generation

The AAI Sub-CA signing key generation occurs using a secure cryptographic device meeting the requirements as described in CP §3.2.

The AAI Sub-CA's signing key is used to sign certificates and Certificate Revocation Lists (CRLs).

The maximum lifetime of the AAI Sub-CA private key is fifteen (15) years.

#### 3.2.AAI Sub-CA private key protection

##### 3.2.1. AAI Sub-CA private key storage

Each AAI Sub-CA private key is stored in a Hardware Security Module (HSM) that is tamper resistant and certified at a minimum level of FIPS 140-1 Level 4.

##### 3.2.2. AAI Sub-CA private key control

There is a separation of physical and logical access to each AAI Sub-CA private key, and a minimum of two individuals is required for physical access to the HSM where the Sub-CA's private keys are stored. The private key is stored in encrypted key fragments with split knowledge and ownership and  $m$  of  $n$  fragments are required for private key recovery.

##### 3.2.3. AAI Sub-CA key escrow

The AAI Sub-CA private key shall not be placed in escrow.

##### 3.2.4. AAI Sub-CA key backup

AAI Sub-CA private keys are backed up for recovery purposes. Backups are stored in a secured environment, and  $m$  of  $n$  key fragments are required for logical recovery.

##### 3.2.5. AAI Sub-CA key archival

The AAI Sub-CA shall archive any necessary keys for a period of time sufficient to support the responsibilities of the AAI Sub-CA.

#### 3.3.AAI Sub-CA-provided Subscriber key management

The AAI Sub-CA does not provide Subscriber key management services.

#### 3.4.AAI Sub-CA public key distribution

The AAI Sub-CA public key will be contained in an X.509 Certificate signed by the Apple Root CA, and provided to Subscribers and Relying Parties as necessary to support the AAI PKI.

#### 3.5.AAI Sub-CA key changeover

When a new private key is required, a new AAI Sub-CA signing key pair will be generated and all subsequently issued certificates and CRLs are signed with the new private signing key. The



corresponding new AAI Sub-CA public key Certificate is provided to Subscribers and Relying Parties as necessary to support the AAI PKI.



## 4. Certificate life cycle management

This section sets forth practices related to the certificate life cycle management controls of the AAI Sub-CA.

### 4.1. Certificate Suspension

The AAI Sub-CA does not support suspension of certificates.

### 4.2. Certificate registration

#### Apple ID Certificates:

- The issuance of an Apple ID Certificate is contingent upon the requesting Subscriber presenting a valid Apple ID account name and password through an Apple OS when features are enabled that require the use of an Apple ID certificate.
- The applicable Apple OS authenticates to Apple using the Apple ID account name and password presented by the user. If the account is valid, a private/public key pair and corresponding Certificate Signing Request ("CSR"), is generated by the applicable Apple OS Security Framework.
- The CSR is submitted to Apple by the applicable Apple OS. Once the CSR is validated by Apple, a Certificate is issued by the AAI Sub-CA and added to the Subscriber's Keychain.
- The common name associated with an Apple ID Certificate is a unique identification string assigned by Apple.

#### Server Push Certificates for Mac OS X:

- Server Push Certificates for Mac OS X are issued as a set, where separate certificates are used for different Mac OS X features (e.g. email, calendar, contacts, mobile device management). Certificate life cycle events (e.g. issuance, revocation, etc.) are applied to the full set, and the certificates are not managed separately.
- For both Production and Development certificate types, the issuance of a set of Server Push Certificates to Mac OS X end users requires the requesting Subscriber to present a valid Apple ID account name and password within the server administration console of Mac OS X. Additionally, the Apple ID account must be associated with a verified email address, and the Subscriber must have a legitimate copy of Mac OS X.
- Mac OS X authenticates to Apple using the Apple ID account name and password presented by the Mac OS X Server user in the server administration console. Mac OS X creates a set of Certificate Signing Requests ("CSRs") using corresponding private/public key pairs that are generated by the Mac OS X Security Framework. The CSRs are subjected to additional processing by Mac OS X to demonstrate they were generated by a legitimate copy of Mac OS X.
- Mac OS X submits the CSRs to Apple. The Apple ID account name and password are first validated by Apple, after which the CSRs are also validated to confirm that it was signed using the certificate in the Mac OS X bootstrap library that has been digitally signed by the Apple Root CA. Once the CSRs are validated, a set of Certificates is issued by the AAI Sub-CA and downloaded automatically to the Keychain local certificate store of Mac OS X. Each Certificate supports a specific Apple Push Notification Service feature, such as mail, contact, calendar, and mobile device management.



- The common name associated with Server Push Certificates for Mac OS X is a unique identification string assigned by Apple.

#### **Server Push Certificates for Third-Party Servers:**

- Certificates for Third-Party Servers are managed individually. The issuance of Server Push Certificates requires Subscribers to be end users of third-party servers that are authorized by Apple to use the Apple Push Notification Service ("APNs"). Subscribers also must present a valid Apple ID account name and password with a verified email address.
- The third-party server vendor holding a Server Push Notification Certificate that is designated for at least one of the push features (e.g. email, calendar, contacts, mobile device management), receives a certificate request from the Subscriber and generates a CSR on their behalf, countersigned using the third-party server vendor's private key. This demonstrates that the Subscriber is a user of the authorized third-party server. The Subscriber authenticates to the Apple Push Certificates Portal using his or her Apple ID account name and password, completes a registration form, and uploads the CSR digitally signed with the third-party server vendor's private key to Apple.
- Apple verifies that the CSR is signed using the private key of the third-party server vendor's Server Push Notification Certificate that is designated for at least one of the push features (e.g. email, calendar, contacts, mobile device management). Upon verification, the CSR is processed by Apple and the Certificate is issued by the AAI Sub-CA. The Subscriber is notified that the Certificate is available for download from the Apple Push Certificates Portal.
- The common name associated with a Server Push Certificate for Third-Party Servers is a unique identification string assigned by Apple.

#### **Profile Signing Certificates:**

- The issuance of Profile Signing Certificates, for use by Apple business groups, is controlled by an internal identification and authentication process.

### **4.3.External RA requirements**

An external Registration Authority is not utilized by the AAI Sub-CA.

### **4.4.Certificate renewal**

#### **Apple ID Certificates:**

- When an Apple OS detects that a Subscriber's applicable Certificate will expire within 30-days of the 12-month validity period, it automatically generates a new CSR with a new key pair and submits the CSR to Apple for Certificate generation. This is the same process as the initial issuance. The old Certificate and private key are deleted from the Subscriber's local Keychain upon successful renewal.

#### **Server Push Certificates for Mac OS X:**

- During the 30-day period before the Certificate expires, both for Production and Development certificate types, the Subscriber is notified that the Certificate will expire by email. Upon the end user's request in the server administration console of Mac OS X, a set of new CSRs will be issued and submitted to Apple for Certificate generation and signing using the same process as the initial issuance.

**Server Push Certificates for Third-Party Servers:**

- During the 30-day period before the Certificate expires, the Subscriber is notified by email that the Certificate is about to expire. He or she must return to the Apple Push Certificates Portal and submit new CSR(s). This is the same process used at initial Certificate issuance.

**Profile Signing Certificates:**

- Profile Signing Certificates are manually renewed as needed via an internal process.

## 4.5. Certificate rekey

The AAI Sub-CA does not rekey certificates. Compromised keys result in completely new key sets and certificates being issued.

## 4.6. Certificate issuance

Certificates are issued to the ISO 9594/X.509 standard. Certificates are signed using the AAI Sub-CA signing key. Refer to CP §2.11.2 for the requirements of an Apple CA to notify Subscribers about issuance of a Certificate. Refer to CP §4.11 for Certificate format, profile requirements, and required extension fields.

## 4.7. Certificate acceptance

For all Certificate types, the following conduct constitutes certificate acceptance:

- Downloading a Certificate, or using product features that utilize a certificate, constitutes the Subscriber's acceptance of the Certificate.
- Failure of the Subscriber to object to the certificate or its content constitutes Certificate acceptance.

## 4.8. Certificate distribution

**Apple ID Certificates:**

- Apple ID Certificates will be distributed to the Subscriber directly in the Subscriber's Keychain local certificate store in Mac OS X or iOS upon issuance. There is no public distribution of the Apple ID Certificates.

**Server Push Certificates for Mac OS X:**

- For Certificates issued to Mac OS X end users, Certificates will be distributed to the Subscriber directly to the Subscriber's Keychain local certificate store in Mac OS X upon issuance. There is no public distribution of the Certificates.

**Server Push Certificates for Third-Party Servers:**

- Server push certificates for third-party servers will be distributed to the Subscriber through the Apple Push Certificates Portal upon issuance. There is no public distribution of the Certificates.

**Profile Signing Certificates:**

- Profile Signing Certificates are made available for use by Apple business groups and included with applicable configuration profiles.



## 4.9. Certificate revocation

### Apple ID Certificates:

- The certificate revocation process for Apple ID Certificates will commence upon receipt of a valid request to reset the password for the Apple ID account of the Subscriber via the <https://iforgot.apple.com>. The Subscriber is asked to follow the process, providing applicable credentials (e.g. answer to secret security question) to reset the password. All Apple ID Certificates associated with the Apple ID will be revoked upon reset of the password. Once a certificate has been revoked, its revocation status cannot be modified. After revocation, a new certificate can be requested according the initial issuance process.
- Certificates may be revoked by the AAI Sub-CA for any reason.

### Server Push Certificates for Mac OS X:

- The certificate revocation process will commence upon receipt of a valid request to revoke the set of Certificates from the Subscriber via the Apple Push Certificates Portal. The Subscriber will be required to authenticate using his or her Apple ID account name and password. After authentication, the Subscriber will indicate that they wish to revoke their set of Certificates by clicking on the revoke button. Once a certificate has been revoked, its revocation status cannot be modified. An email is sent to the Subscriber to notify that the certificate has been revoked.
- Certificates may be revoked by the AAI Sub-CA for any reason.

### Server Push Certificates for Third-Party Servers:

- The certificate revocation process will commence upon receipt of a valid request to revoke the Certificate from the Subscriber via the Apple Push Certificates Portal. The Subscriber will be required to log into the Apple Push Certificates Portal using his or her valid Apple ID account name and password. After authentication, the Subscriber will click on the revocation link for the Certificate they intend to revoke. An email is sent to Subscribers to notify that the certificate has been revoked.
- Certificates may be revoked by the AAI Sub-CA for any reason.

### Profile Signing Certificates:

- The Certificate revocation process will commence upon a request to revoke the certificate from an authorized Apple employee.
- Certificates may be revoked by the AAI Sub-CA for any reason.

## 4.10. Certificate suspension

Certificate suspension is not supported. Instead, Subscribers are required to revoke their current Certificates and request new ones.

## 4.11. Certificate status

The AAI Sub-CA utilizes two methods for certificate validation: Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP). Refer to the CRL Distribution Point ("CDP") or the Authority Information Access ("AIA") extensions in the Certificates for the status information method used for each Certificate type.



#### 4.11.1. CRL usage

Subscribers and/or Relying Parties may use a CRL, which is updated periodically at Apple's sole discretion, to determine the status of a particular Certificate. Revoked Certificates remain in the CRL until the Certificates have expired. More than one CRL may be valid at a particular time.

Certificates and CRLs issued by the AAI Sub-CA shall be retained for a period of not less than two (2) years.

#### 4.11.2. OCSP usage

Subscribers and/or Replying Parties may use OCSP to determine the status of a particular Certificate. Revoked Certificates remain marked as "revoked" for the certificate lifetime. Delegate Certificates signed by the AAI Sub-CA are used to sign all OCSP responses. More than one OCSP responder Certificate can be in operation at the same time.

OCSP status requests must contain at a minimum the certificate serial number to receive a valid response. Once an OCSP request has been validated, a signed response is sent to the requestor indicating the status of the Certificate and showing the request was successful. Failed OCSP requests will generate a failure status back to the requestor.

#### 4.11.3. OCSP Designated Responder Certificates

Details of the Certificate used to sign the OCSP responses are as follows:

- Effective life of the Certificate may vary at Apple's discretion.
- More than one valid OCSP Designated Responder Certificate may exist at one time.
- Each OCSP Designated Responder Certificate will have a unique public/private key pair.
- Suspension of the OCSP Designated Responder Certificates is not supported.

### 4.12. Certificate profile

#### 4.12.1. Apple ID Certificates

A Certificate issued by the AAI Sub-CA shall conform to the X.509 Certificate format and shall contain, at a minimum, the following data elements:

- Serial Number
- Subject Distinguished Name
- Issuer Distinguished Name
- Algorithm used (RSA)
- Modulus (Size in bits)
- Validity period
- Certificate Policies extensions listing the CP
- Certificate Policies extension, non-critical, Apple ID Sharing Certificate Policy (1.2.840.113635.100.5.7.1)
- Certificate qualifiers listing this CPS (URL)
- User notice qualifier



#### 4.12.2. Server Push Production Certificates

A Client SSL Certificate issued by the AAI Sub-CA for the purposes of creating and maintaining SSL connectivity and providing client authentication for the Apple Push Notification Service Production environment shall conform to the X.509 Certificate format and shall contain, at a minimum, the following data elements:

- Serial Number
- Subject Distinguished Name
- Issuer Distinguished Name
- Algorithm used (RSA)
- Modulus (Size in bits)
- Validity period
- Certificate Policies extensions listing the CP
- Certificate qualifiers listing this CPS (URL)
- User notice qualifier
- Apple Production Push Services Certificate Extension (1.2.840.113635.100.6.3.2)

#### 4.12.3. Server Push Development Certificates

A Client SSL Certificate issued by the AAI Sub-CA for the purposes of creating and maintaining SSL connectivity and providing client authentication for the Apple Push Notification Service Development environment shall conform to the X.509 Certificate format and shall contain, at a minimum, the following data elements:

- Serial Number
- Subject Distinguished Name
- Issuer Distinguished Name
- Algorithm used (RSA)
- Modulus (Size in bits)
- Validity period
- Certificate Policies extensions listing the CP
- Certificate qualifiers listing this CPS (URL)
- User notice qualifier
- Apple Development Push Services Certificate Extension (1.2.840.113635.100.6.3.1)

#### 4.12.4. Profile Signing Certificates

The Profile Signing Certificates issued by the AAI Sub-CA for the signing of Mac OS X and iOS configuration profiles shall conform to the X.509 Certificate format and shall contain, at a minimum, the following data elements:

- Serial Number



- Subject Distinguished Name
- Issuer Distinguished Name
- Algorithm used (RSA)
- Modulus (Size in bits)
- Validity period
- Certificate Policies extensions listing the CP
- Certificate qualifiers listing this CPS (URL)
- User notice qualifier
- Configuration Profile Signing Certificate Extension (1.2.840.113635.100.6.14.1)

#### 4.13. OCSP Designated Responder Certificate

A Certificate issued by the AAI Sub-CA for the purpose of signing OCSP responses shall conform to the X.509 Certificate format and shall contain, at a minimum, the following data elements

- Serial Number
- Subject Distinguished name
- Issuer Distinguished name
- Validity date range
- Modulus (Size in bits)
- Signature Algorithm

#### 4.14. CRL Profile

A CRL issued by the AAI Sub-CA shall conform to the X.509 version 2 CRL format. Each CRL shall contain the following fields:

- Signature Algorithm using SHA-1 with RSA Encryption
- Issuer matching the AAI Sub-CA Certificate's Distinguished Name
- "Last Update" field with the time of CRL issuance
- "Next Update" field defining the period of validity
- Authority Key Identifier extension
- List of Revoked Certificates

#### 4.15. Integrated circuit cards

Not applicable.



## 5. Environmental controls

This section sets forth practices related to the environmental controls of the AAI Sub-CA.

### 5.1.CPS administration

Apple has designated a Policy Authority (PA) group with final authority and responsibility for specifying and approving the AAI Sub-CA's CPS.

This authorized body has performed an assessment to evaluate business risks and determine the security requirements and operational procedures to be included in the CPS for the following:

- Key life cycle management controls
- Certificate life cycle management controls
- CA environmental controls

The AAI Sub-CA makes available its public CPS to all Subscribers and Relying Parties, including any revisions that occur from time to time.

Any changes to the AAI Sub-CA's CPS, along with the effective date of the changes, shall be reviewed by the PA, and posted in a timely manner.

### 5.2.CA termination

As set forth in this section, any decision to terminate the AAI Sub-CA shall be approved by a member of the Apple Executive Team prior to the effective date of termination.

At the time to termination, Apple will develop a termination plan addressing the following:

- Provision of notice to related parties affected by the termination,
- The revocation of certificates issued by the Sub-CA,
- The preservation of the Sub-CA's archives and records

### 5.3.Confidentiality

The AAI Sub-CA shall keep the following information confidential at all times:

- All private signing and client authentication keys
- Security and annual audits and security parameters
- Personal or non-public information about AAI Sub-CA Subscribers
- Security mechanisms

Except as required to support the WebTrust audit performed by an independent external audit firm, confidential information should not be released to third parties unless required by law or requested by a court with jurisdiction over the CA. The information will be kept confidential even after the termination of the CA.

The following information shall not be considered confidential:

- Information included in Certificates
- The AAI Sub-CA public Certificate



- Information contained in the CA's CPS and CP documents
- Any Certificate status or Certificate revocation reason code

## 5.4. Intellectual property rights

Certificates and CRLs issued by the AAI Sub-CA, information provided via OCSP, the CPS and the CP are the property of Apple.

## 5.5. Physical security

Physical protection is achieved through the creation of clearly defined security perimeters with appropriate physical barriers to entry around the business premises and AAI Sub-CA facilities. Details of the physical security policies and procedures are in appropriate internal security documents.

Equipment is located or protected to reduce the risks from environmental threats and hazards, including but not limited to power and air conditioning disruption or failure, water exposure, fire, telecommunications disruption or failure and opportunities for unauthorized access.

Media maintained securely within the AAI Sub-CA facilities and is subject to the same degree of protection as the CA hardware.

At end of life, cryptographic devices are physically destroyed or zeroized in accordance to manufacturers' guidance prior to disposal.

## 5.6. Business continuity management

The AAI Sub-CA has business continuity plans to maintain or restore the AAI Sub-CA's business operations in a timely manner following interruption or failure of critical business processes.

## 5.7. Event logging

### 5.7.1. Archiving

The AAI Sub-CA archives event journal data on a periodic basis.

A risk assessment has been performed to determine the appropriate length of time for retention of archived event journals.

The AAI Sub-CA maintains archived event journals at a secure off-site location for a predetermined period.

### 5.7.2. Event journal reviews

Current or archived event journals may only be retrieved by authorized individuals and only for valid business or security reasons.

Event journals are reviewed periodically.

The review of current and archived event journals includes the identification and follow-up of exceptional, unauthorized, or suspicious activity.



## 6. Revision history

Issue Number	Issue Date	Details
1.0	July 20, 2011	Initial release.
2.0	September 30, 2011	Added Server Push Certificates for Third-Party Servers.
3.0	December 22, 2011	Added additional usage of Apple ID certificates in iOS. Added Profile Signing Certificates.