Apple Inc.
Certification Authority
Certification Practice Statement
.Mac

Version 1.3
Effective Date: July 10, 2008

Table of Contents

1. Introduction

This Certification Practice Statement ("CPS") describes the practices employed by the .Mac Subordinate Certification Authority (".Mac 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 .Mac 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 .Mac Sub-CA.

This CPS is intended to inform participants in Apple's Public Key Infrastructure ("PKI"), including entities that have been issued a Certificate by the Apple .Mac Subordinate Certification Authority ("Sub-CA") and entities that may choose to place reliance on those Certificates. These participants, called Subscribers and Relying Parties, respectively, should consider the practices of .Mac Sub-CA and practices of the Apple Root CA, as disclosed in the Apple CP, when choosing whether or not to participate in the Apple PKI. If the Subscriber and Relying Party choose to participate in the Apple PKI, they agree to be bound by the terms of the CP, this CPS, and applicable Subscriber and Relying Party agreements.

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® is a trademark of Apple Inc., registered 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, the term "Subscriber" refers to a registered MobileMe end-user (a customer of the Apple MobileMe service) who has been issued a Certificate signed by the .Mac Sub-CA. A "Relying Party" refers to an individual or organization that places reliance on a Certificate issued by the .Mac Sub-CA. 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 .Mac Sub-CA.

2.1. Identification

The practices set forth in this CPS apply exclusively to the .Mac Sub-CA. This CPS is structured similarly to the CP, disclosing details of the practices employed by the .Mac Sub-CA that address the more general requirements defined in the CP. This document assumes that 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 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, 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 .Mac Sub-CA, and their related management teams that generate, issue, distribute, revoke and manage cryptographic keys and Certificates, (2) Apple Registration Authorities ("Apple RA"), and (3) the Apple CA Policy Authority ("Apple PA," or "PA"). End Entities consist of (1) Subscribers of Certificates and (2) Relying Parties who agree to be bound by the conditions set forth in the CP and this CPS.

The .Mac 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 certificates issued by the .Mac Sub-CA:

- iChat Encryption Certificates
- Sharing Certificates
- OCSP Designated Responder Certificates

Certificates used exclusively for internal functions, such as event log signing Certificates, are not included within the scope of this CPS.

2.2.1. iChat Encryption Certificate

The .Mac Sub-CA signs, issues and administers Certificates for which the corresponding private key may be used to digitally sign and encrypt a Subscriber's iChat session such that the certified public key can be used by a Relying Party to:

- Verify that the iChat request is coming from the iChat screen name that appears in the iChat window; and
- Encrypt the iChat session

2.2.2. Sharing Certificate

The .Mac Sub-CA issues and administers certificates that are used to authenticate a client machine configured to use a particular Subscriber's account to another machine which offers services to clients associated with that Subscriber's account.

2.2.3. OCSP Designated Responder Certificate

The .Mac Sub-CA creates cryptographic key pairs and creates, issues, manages, and revokes OCSP Designated Responder Certificates employed exclusively to sign definitive OCSP responses.

2.3. Contact details

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

2.4. Apportionment of liability

For iChat Encryption and Sharing Certificates, a subscriber and relying party agreement is incorporated in the End User License Agreement for all users of the Apple operating systems, within which the CA functionality is enabled. For all other Relying Parties, the relying party terms and conditions can be obtained from a link embedded in the Certificate. Use of the Certificate during an iChat session is deemed acceptance of such agreement on the part of the Relying Party.

2.4.1. Warranties to Subscribers and Relying Parties

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

.Mac Sub-CA relying party agreements do not include a warranty to Relying Parties.

2.4.2. CA disclaimers of warranties

Except as otherwise permitted within this CPS and to the extent permitted by applicable law, relying party agreements shall disclaim all 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, relying party agreements 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 iChat Encryption and Sharing Certificates, subscriber agreements shall require Subscribers to warrant that:

- They will take no action to interfere with the normal operation of an encrypted iChat session.
- They are solely responsible for preventing any unauthorized person from having access to the Subscriber's private key stored on any computer from which the Subscriber has participated in an encrypted iChat session and/or Sharing session.

- Encrypted iChat and Sharing sessions are being used exclusively for authorized and legal purposes, and in a manner consistent with this CPS.

2.4.5. Private key compromise

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

2.4.6. Relying Party liability

Relying parties acknowledge by using the Certificate that they have sufficient information to make an informed decision before relying on any type of Certificate, and that they are solely responsible for deciding whether or not to rely on a Certificate.

2.5. Financial responsibility

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

2.5.1. Indemnification by Subscribers and Relying Parties

Any subscriber and/or relying party agreement may at Apple's discretion, include an indemnification clause by Subscribers and/or Relying Parties.

2.5.2. Fiduciary relationships

If applicable, the fiduciary relationship between Apple and agents, fiduciaries, trustees, or other representatives of Subscribers or Relying Parties shall be set forth in subscriber and/or relying party agreements established by the .Mac Sub-CA.

2.6. Interpretation and enforcement

Interpretation and enforcement of any subscriber or relying party agreement for any user using an Apple operating system is governed by the terms and conditions in the operating system End User License Agreement ("EULA"). For other users the interpretation and enforcement are covered by terms and conditions obtained from a link embedded in the Certificate.

2.6.1. Governing law

Governing law of any subscriber or relying party agreement for any user using an Apple operation system is governed by the terms and conditions in the operating system End User License Agreement ("EULA"). For other users the Governing Law is covered by terms and conditions obtained from a link embedded in the Certificate.

2.6.2. Severability, survival, merger, notice

Severability, survival, merger and notice if applicable, of any subscriber or relying party agreement for any user using an Apple operating system is governed by the terms and conditions in the operating system End User License Agreement ("EULA"). For other users these are covered by terms and conditions obtained from a link embedded in the Certificate.

2.6.3. Dispute resolution procedures

Dispute resolution procedures if applicable of any subscriber or relying party agreement for any user using an Apple operating system is governed by the terms and conditions in the operating

system End User License Agreement ("EULA"). For other users the dispute resolution procedures are covered by terms and conditions obtained from a link embedded in the Certificate.

2.7. Fees

This section sets forth policies associated with any fees charged to Subscribers or Relying Parties for certification authority services for each class of Certificate.

2.7.1. Certificate issuance or renewal fees

Certificates issued by the .Mac Sub-CA are available based on the status of the associated account:

- iChat Encryption Certificates are available to MobileMe members as well as to MobileMe trial account members. No additional fees are charged for this service.
- Sharing Certificates are available to MobileMe members as well as to MobileMe trial account members. No additional fees are charged for this service.

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.

2.7.5. Refund policy

Not Applicable.

2.8. Publication and Repository

The .Mac Sub-CA operates a repository where public Certificates are published and accessible to Subscribers or Relying Parties.

Access to this repository will be allowed using the Online Certificate Status Protocol ("OCSP"). All OCSP responses are signed by the OCSP Designated Responder Certificate.

2.8.1. Publication of CA information

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

2.8.2. Frequency of publication

All public key Certificates issued by the .Mac Sub-CA will be published and made available in the .Mac Sub-CA repository within 24 hours of issuance.

2.8.3. Access controls

Subscribers and Relying Parties shall have access to the .Mac Sub-CA repository through supported interfaces. The status of any Certificate can be checked using the Online Certificate Status Protocol ("OCSP").

2.9. Compliance audit requirements

The .Mac 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 .Mac Sub-CA.

2.10.1. Permitted uses

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

iChat Encryption Certificate: This type of Certificate is used to encrypt a communication channel for an iChat session.

Sharing Certificate: This type of Certificate is used for the purpose of allowing a client computer to utilize Mac OS X's "Back to My Mac" feature.

OCSP Designated Responder Certificate: This type of Certificate is used for the purpose of signing OCSP responses.

2.10.2. Limitations on use

The .Mac 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.

The .Mac 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 .Mac Sub-CA, Subscribers and Relying Parties.

2.11.1. General .Mac Sub-CA obligations

The .Mac 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 a timely manner in accordance with the Apple CP and this CPS.
- Revoke Certificates the .Mac Sub-CA issued, 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 an Apple internal process.

2.11.2. Notification of issuance by .Mac Sub-CA to Subscriber

For iChat Encryption Certificates, notification of issuance of a new Certificate is deemed to have taken place when the Subscriber's iChat client displays "iChat encryption is enabled" in the Security tab corresponding to the selected .Mac and/or MobileMe accounts within the Accounts preference pane in iChat Preferences.

For Sharing Certificates, notification of issuance is deemed to have taken place when the Certificate is added to the user's Keychain.

A Subscriber may verify the issuance, status, and contents of a Certificate using Mac OS X's Keychain Access application.

2.11.3. Notification of issuance by .Mac Sub-CA to others

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

2.11.4. Notification of revocation by .Mac Sub-CA to Subscriber

Notification of revocation to the Subscriber is dependent upon whether the Subscriber, or other entity acting on the Subscriber's behalf, initiates the revocation process. If a Subscriber, or other entity acting on the Subscriber's behalf, requests revocation of the Subscriber's Certificate, the Subscriber will be notified by email after revocation is successful. The email is delivered to the Subscriber's MobileMe email account, if the account is active; otherwise, it will be sent to a secondary email address specified by the Subscriber in her account settings.

In other cases, such as those stated at CP §4.8 that are not initiated by a Subscriber or other external entity, revocation of a Subscriber's Certificate may employ transparent mechanisms involving minimal or no interaction with the Subscriber or other entities external to the .Mac Sub-CA. In all cases, a Subscriber may verify the status of a Certificate using Apple's Keychain Access application.

2.11.5. Notification of revocation by .Mac Sub-CA to others

Except through the online Certificate status checking services described in this CPS, the .Mac Sub-CA does not provide notification of revocation to parties other than the Subscriber and entities acting on the Subscriber's behalf.

2.11.6. Registration Authority obligations

A distinct registration authority is not used. The .Mac Sub-CA performs limited RA services to provide reasonable assurance that Certificates are only issued to MobileMe members, and that the Subject identifier in those Certificates matches the MobileMe member's user name.

2.11.7. Subscriber obligations to .Mac Sub-CA

For iChat Encryption and Sharing Certificates, Subscribers are obligated to:

- Safeguard their private key from compromise.
- Use their dependent features (iChat encryption and "Back to My Mac") exclusively for legal purposes and in accordance with the relevant CP and CPS.
- Promptly request that the CA revoke a Certificate if the Subscriber has reason to believe there has been a compromise of the private key corresponding to the public key listed in the Certificate. This is done via the MobileMe website (http://www.me.com). After authentication to the website, the Subscriber follows the link to the revocation page

and enters the details of the Certificate to be revoked. Only Certificates owned by the authenticated Subscriber can be revoked.

2.11.8. Relying Party obligations to .Mac Sub-CA

Relying parties shall be 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.
- Accept of all terms and conditions of the relying party agreement and to be bound by the limitations of liability and disclaimers of warranties. Users are deemed to have accepted by participating in an encrypted iChat session or using the "Back to My Mac" feature.
- Restrict reliance on Certificates issued by the CA to the purposes for which those Certificates were issued, in accordance with the CP, this CPS, and the relying party agreement available at http://www.apple.com/certificateauthority/rpa.html.

3. Key life cycle management

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

3.1. .Mac Sub-CA key generation

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

The .Mac Sub-CA private key will cease to be used, and replaced at the end of a designated period or when a compromise is known or suspected.

3.2. .Mac Sub-CA private key protection

3.2.1. .Mac Sub-CA private key storage

Each .Mac 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. .Mac Sub-CA private key control

There is a separation of physical and logical access to each .Mac Sub-CA private key, and a minimum of two individuals is required for physical access to the HSM where a private key is stored.

3.2.3. .Mac Sub-CA key escrow

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

3.2.4. .Mac Sub-CA key backup

.Mac Sub-CA private keys are backed up for recovery purposes. Backups are stored in a secured environment, and m of n secret shares are required for logical recovery.

3.2.5. .Mac Sub-CA key archival

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

3.3. .Mac Sub-CA public key distribution

The .Mac Sub-CA public key will be contained in an X.509 Certificate and made publicly available in the .Mac Sub-CA repository. As required to fulfill the function of validating iChat sessions or "Back to My Mac" connections, this public key and Certificate may be bundled in a software update or written to a relying user's local Apple key chain as needed.

3.4. .Mac Sub-CA key changeover

When a new private signing key needs to be put in place, a new .Mac Sub-CA signing key pair shall be generated. All subsequently issued Certificates shall be signed with the new private signing key. The corresponding new .Mac Sub-CA public key Certificate shall be openly provided to Subscribers, Relying Parties, or others, via an update to the operating system.

3.5. .Mac Sub-CA-provided Subscriber key management

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

4. Certificate life cycle management

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

4.1. External RA requirements

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

4.2. Certificate registration

When the iChat software identifies that a user's iChat screen name is one that supports the issuance of Apple iChat Encryption Certificates then a private/public key pair is generated on the client computer by request from the iChat application to the Mac OS X Security Framework.

In the case of the "Back to My Mac" feature, when the Mac OS X software is provided with a .Mac or MobileMe username and password combination, it contacts the MobileMe servers and verifies both their authenticity and that the matched account supports the issuance of Sharing Certificates. If both conditions are met, a private/public pair is generated on the client computer by Mac OS X's request to the Security Framework.

The public half of the key pair is then sent to the MobileMe servers as part of a Certificate Signing Request (CSR) to be authenticated via a digest authentication scheme. The public key, screen name, and other data necessary to provide a successful digest authentication are required in the CSR. Furthermore, the CSR is signed by the Subscriber's private key. This signature allows the MobileMe servers to validate that the private key held by the Subscriber corresponds to the public key submitted in the CSR. Once the CSR is received and authenticated, the .Mac server again verifies the account's ability to request a Certificate. The CSR is then passed along to the signing proxy server, so that the Certificate may be constructed and signed by the .Mac Sub-CA.

Once the Certificate has been constructed and signed, its status is made available via OCSP. Data returned to the client from the OCSP server is signed by a delegated leaf Certificate issued by the .Mac Sub-CA.

Account names must be unique within a domain (i.e. mac.com and me.com). However, it is possible that a name assigned to one member in the mac.com domain is assigned to a different member in the me.com domain. Uniqueness of the account name is enforced at account creation through the checking of the requested account name against a list of accounts that have been previously assigned to other users in the applicable domain.

There are no requirements for organizational or individual identity of the requester.

4.3. Certificate renewal

As both the iChat and "Back to My Mac" functions are serviced in the same manner, the more general term "client" will be used to describe how they both work for the purposes of this section 4.3.

When the client software detects that a user's applicable Certificate is about to expire, it checks with the MobileMe servers to ensure the account allows for the issuance of the applicable Certificate.

If the issuance conditions are met, the client will, via the Mac OS X Security Framework, issue a new CSR using the existing keys and submit the CSR to the MobileMe servers for Certificate construction and signing. This is the same process used at initial registration.

If the previous Certificate based on the Subscriber's key pair was marked as being revoked, renewal is not allowed by the client. A new key pair is generated and a new Certificate is issued as previously described.

The same key pair is used for each renewal unless the key pair has been revoked. When a new key pair is required, the procedure for initial registration is followed.

4.4. Certificate rekey

Upon receipt of a valid CSR, Certificates will be rekeyed rather than renewed if the existing Certificate has expired or been revoked. Rekeying a Certificate follows the same process as a new Certificate request, as described in CPS § 4.2.

4.5. Certificate issuance

The .Mac Sub-CA shall issue Certificates to Subscribers automatically when a MobileMe member elects to encrypt an iChat session or enable the "Back to My Mac" feature, and that member does not have a valid Certificate. This process uses an Application Programming Interface (API) that allows access to the MobileMe certificate issuance service from the Subscriber's computer. Certificates are retrieved from the MobileMe servers by the Subscriber's computer after the Certificate is issued and made available in the repository.

iChat Encryption and Sharing Certificates are valid for a maximum of one (1) year.

Certificates are signed using the .Mac Sub-CA signing key.

4.6. Certificate acceptance

For iChat Encryption and Sharing Certificates, once the .Mac Sub-CA generates a Certificate, the Certificate will be pulled from the .Mac servers to the Subscriber's computer and installed automatically.

4.7. Certificate distribution

For iChat Encryption and Sharing Certificates, Certificates will be distributed to the Subscriber immediately as described in CPS §4.5.

For iChat Encryption Certificates, relying parties will receive the Certificate when both parties elect to encrypt the chat session.

4.8. Certificate revocation

Effective immediately for Certificates issued on or after July 10, 2008 and effective August 10, 2008 for Certificates issued before July 10, 2008, a Subscriber Certificate may be revoked for any of the following reasons:

- The Subscriber, or other entity with an expressed or implied responsibility for safeguarding the Subscriber's private key, has reason to believe the Subscriber's private key has been compromised.
- The .Mac Sub-CA has reason to believe the Subscriber's private key has been compromised.
- Any information or documents provided by the Subscriber are, or become false or inaccurate, and/or the Subscriber has materially breached an obligation, representation, or warranty under the applicable subscriber agreement.
- The Subscriber Agreement with the Subscriber has been terminated.
- The Subscriber requests revocation.
- Apple is required by law, regulation or other governmental or court order to take such action.

- Apple has reason to believe that such action is prudent or necessary.
- The applicable MobileMe membership expires or is cancelled.

A MobileMe member may revoke his or her Certificates using the Account Settings functionality made available at http://www.me.com after the user has authenticated himself to the MobileMe servers.

A Certificate is revoked once its status is marked as "revoked". When an iChat Encryption Certificate or Sharing Certificate is revoked, it will be revoked as of a specific date. Revoked Certificates will not be accepted by the iChat or OS software to allow users to utilize their respective features.

The certificate revocation process will commence upon receipt of a valid request to revoke the Certificate from the Subscriber via a web page. The Subscriber will be required to login to the web site using their MobileMe credentials. After authentication the Subscriber will indicate that they wish to revoke their Certificate by clicking on the revocation link. Once the Subscriber has clicked the link the Certificate will be deemed revoked.

Revoked Certificates will have their status changed from "good" to "revoked" in accordance with the specification for OCSP.

The status changes are recorded and will be kept indefinitely. Only valid Certificates are subject to revocation and Certificates marked as "revoked" can never be re-marked as "good".

All Subscribers and Relying Parties must use OCSP to determine the status of the Certificate as this will be the only mechanism for notification. OCSP requests that are not signed should not be accepted as true by the Subscriber.

4.9. Certificate suspension

Certificate suspension is not supported. Compromised keys result in completely new key sets and Certificates being issued.

4.10. Certificate status

4.10.1. OCSP usage

All Subscribers and Relying Parties will use OCSP to determine the status of a particular Certificate.

Revoked Certificates remain marked as "revoked" permanently.

Once an OCSP request has been validated there will be a signed response back to the requestor indicating the status of the Certificate and showing the request was successful.

The OCSP request must contain the Certificate serial number to receive a valid request. For users of Apple systems this will be automatic.

Failed OCSP requests will generate a failure status back to the requestor.

A delegated leaf Certificate is used to sign all OCSP responses. This leaf is signed by the .Mac Sub-CA's private key.

4.10.2. OCSP Designated Responder Certificates

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

- Effective life of the Certificate is 16 days
- 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
- OCSP Designated Responder Certificates are never renewed or rekeyed.
- Suspension of the OCSP Designated Responder Certificates is not supported

4.11. Certificate profile

4.11.1. iChat Encryption Certificate

A Certificate issued by the .Mac 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)
- Certificate Name
- Certificate Policies extensions listing the CP
- Policy mapping extension set to NULL
- Policy constraint extension listing the CP
- Certificate qualifiers listing this CPS (URL)
- User notice qualifier

4.11.2. Sharing Certificate

A Certificate issued by the .Mac 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)
- Certificate Name
- Certificate Policies extensions listing the CP
- Policy mapping extension set to NULL
- Policy constraint extension listing the CP
- Certificate qualifiers listing this CPS (URL)
- User notice qualifier

4.11.3. OCSP Designated Responder Certificate

A Certificate issued by the .Mac Sub-CA for the purposes 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
- User notice qualifier
- Certificate Policies extension listing the CP

4.12. CRL profile

The .Mac Sub-CA shall not issue a CRL. Status of any Certificate can only be obtained using the Online Certificate Status Protocol ("OCSP"). All request responses will be signed.

4.13. Integrated circuit cards

Not applicable.

5. Environmental controls

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

5.1. CPS administration

Apple has designated a management group with final authority and responsibility for specifying and approving the .Mac 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 .Mac 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 .Mac 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 .Mac Sub-CA shall be approved by the executive sponsor. The Apple Executive Team must ratify such decision to terminate CA services prior to its effective date.

The .Mac Sub-CA will revoke all Certificates and issue a software patch to the iChat and Mac OS X software that will negate the certificate management hooks currently installed.

The .Mac Sub-CA keys will be destroyed using the key destruction method supported by the .Mac Sub-CA HSM.

The HSM devices supporting the .Mac Sub-CA will be physically destroyed.

Apple will make arrangements for the long-term storage of sensitive Subscriber records.

5.3. Confidentiality

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

- All private signing keys
- Security and annual audits and security parameters
- Personal or non-public information on .Mac Sub-CA Subscribers and Relying Parties
- Security mechanisms

Except as required to support the WebTrust audit performed by an independent external audit firm, confidential information should not released to 3rd 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 the public Certificates
- The .Mac Sub-CA public Certificate

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

5.4. Intellectual property rights

All public and private keys, Certificates, information provided in the OCSP, the CPS and 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 .Mac Sub-CA facilities. Details of the physical security policies and procedures are in appropriate security documents.

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

5.6. Business continuity management

The .Mac Sub-CA has business continuity plans to maintain or restore the .Mac 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 .Mac 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 .Mac 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 a validation of the event journals' integrity, and the identification and follow-up of exceptional, unauthorized, or suspicious activity.

6. Revision history

Issue Number	Issue Date	Details
1.0	10/31/05	Initial release.
1.1	05/18/06	Updated sections 1.1, 1.2, 1.3, 2.3, 2.7, 2.11, 4.3, 4.4, 4.6, 4.9, 4.10 and 5.1. Added sections 4.9.1 and 4.10.1
1.2	10/26/07	Made updates to reflect addition of new Shared Computers Certificate type and change in company name.
1.3	07/10/08	Made updates to reflect the new service name, MobileMe, and the addition of me.com domain Certificates. Also updated the name Shared Computers Certificates to Sharing Certificates for clarification, and added content to section 4.8, Certificate revocation.