WellsSecure® PKI Certification Practice Statement

Issued by Wells Fargo Bank, N.A.

Version 13.3

Approved by the Wells Fargo PKI Management: August 2015

Effective: August 2015

Document Version	Document Date	Revision Details
Version 12	July 2009	Removed detailed physical and logical security information, copied implementation level details from WS CP, consistency with WS CP, removed all references to RPS, corrections to EV SSL text, CA names and CA hierarchy
Version 12.1	N/A	Version number 12.1 of this WS CPS was skipped to achieve consistency between the WS CP and WS CPS. Version 12.1 of this WS CPS was not created.
Version 12.2	September 2010	- Phased migration of 1024 bit keys and SHA-1, - Changes in requirements for RA Agreements, - Termination of Federal Bridge Cross Certification, - Minor changes
Version 12.3	June 2011	- Addition of SHA-2 CAs - Addition of Baltimore 2048-bit root - With removal of the Cross-Certificate to Federal Bridge, update various statements that represented Federal Bridge requirements. - IAPAC replaced with Wells Fargo PKI Management
Version 12.4	August 2012	- Updates to Trust Hierarchy - Removal of EV SSL and High Assurance Certificates - Renaming of SHA-2 CAs - Compliance to CA/B BRs and Mozilla's required statement - Remove references to High Assurance and EV SSL certificate support
Version 13.0	April 2013	- This CPS will now be called WellsSecure CPS, or WS CPS. - Compliance with the CA/Browser forum's Baseline Requirements detailed in section 3.2.6 was as of 8/8/2013
Version 13.1	January 2014	- Added sections 5.7.1.1–5.7.1.14 copied from the CP - Changed the term WFCMS in § 4.1.2.2 and § 4.1.2.3 to "RA Application" and removed the definition of WFCMS in section 10. - Updated the definition of RA Application in section 10. - Removed all occurrences of and references to Wells Fargo CA01, Wells Fargo Public Primary

		CA, EV SSL, and GTE CyberTrust Global Root - Minor textual or formatting revisions.
13.2	July 2014	- Updated Title page and footer. - Updated Table of Contents to show all sections. - Corrected header numbering errors. - Corrected section pointers that changed due to numbering changes (such as See section X.X). - Fixed formatting errors. - Modified sections: 1.2.4.2, 1.2.4.4, 1.3.1, 1.3.1.1, 1.3.1.2, 1.3.1.2.3, 1.3.5.2, 1.3.1.1.3, 1.3.1.1.4, 1.3.4, 1.3.5, 1.3.6, 1.3.7, Trusted Registrars, 1.5.1, 1.5.1.1, 1.5.1.2, 1.5.2, 1.5.3, 1.5.4, 2.1.1 f, 2.2, 2.3.2, 2.4, 3.1.5.1, 3.1.5.2, 3.2.2, 3.2.2.4, 3.2.4, 3.2.5, 3.2.6, 3.2.6, 3.2.6.1.a, 3.2.6.1.b, 3.2.6.1.c, 3.2.7, 3.2.8, 3.2.9, 3.2.10, 3.2.11, 3.3.2, 4.3.2, 4.3.3, 4.9.3.c.i, 4.9.3.c.ii, 4.9.3.c.iii, 4.9.3.c.iv, 4.9.5, 4.9.7.2, 4.9.12, 4.9.12.1, 4.9.13, 4.9.13.a, 4.9.13.b, 4.9.16, 5.1.1, 5.1.2.2, 5.1.2.4, 5.1.2.5, 5.1.8, 5.2.1, 5.2.4, 5.3.3, 5.5.1, 5.5.4, 5.5.5, 5.5.7, 5.6, 5.7.1.3, 5.7.3, 6.1.2, 6.1.2.1, 6.1.2.2, 6.1.2.3, 6.1.2.4, 6.1.2.5, 6.1.2.6, 6.1.5, 6.1.7, 6.2.10, 6.4.3, 7.1.3, 9.6.3, 9.9.2.1, Suspended Definition, Suspend, Suspension Definition, Wells Fargo PKI Management Definition.
13.3	June 2015	- Updated version number - Updated Table of Contents - Updated copyright date - Added section 4.2.4 outlining Wells Fargo's stance on CAA records as per the CA/B Baseline Requirements. - Replaced section 9 with updated content from the Wells Fargo legal department. - Removed references to the Verizon Global Root replacing it with the Baltimore CyberTrust Root - Changed TOG/IST references to CR/EIS

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Overview

The WellsSecure® Public Key Infrastructure ("WellsSecure PKI") established under the authority of the Wells Fargo PKI Management and managed by the Wells Fargo Organization Unit known as Corporate Risk / Enterprise Information Security (CR/EIS), has been created to enable reliable and secure authentication of identities, and to facilitate the confidentiality and integrity of certain electronic transactions.

This WellsSecure Certification Practice Statement (the "WS CPS") describes how the WellsSecure PKI will be initialized and operated to produce Certificates conforming to the requirements of the WellsSecure Certificate Policy (the "WellsSecure CP"), which is a separate "PKI Document" (herein after defined). This WS CPS is issued by Wells Fargo as one of several "PKI Documents" that taken together define and govern the WellsSecure PKI. These documents provide the framework under which all Certificates in the WellsSecure PKI will be created, issued, managed and/or used by "Program Members" (hereinafter defined).

This WS CPS is consistent with the Internet Engineering Task Force (IETF) Request for Comment (RFC) [RFC3647], Certificate Policy and Certification Practices Framework.

For each section title of this WS CPS, there is an identical section title in the WellsSecure CP. This WS CPS may not repeat the content of the WellsSecure CP but will simply refer to the WellsSecure CP. Where a section says "No stipulation," that means no requirements are imposed in this WS CPS for that section, and it further means that the same language ("No stipulation") appears in the WellsSecure CP.

1.1.1 Relationship Between A Certificate Policy And A Certification Practice Statement

The WellsSecure CP states what assurance can be placed in a Certificate issued by the WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2 or any WellsSecure Sub-CA. This WS CPS states how The WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2 and/or WellsSecure Sub-CAs establish that assurance.

In the event of any conflicts between the WellsSecure CPS and any other applicable PKI Document, this WellsSecure CPS will take precedence, with the following exception:

Because the WellsSecure PKI must conform to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org, in the event of any inconsistency between this WS CPS and such Requirements, such Requirements will take precedence over this WS CPS.

1.2 Document Name And Identification

This WS CPS is referred to as the "WellsSecure Certification Practice Statement", "WellsSecure CPS" or "WS CPS". It corresponds with Version 13 of the "WellsSecure Certificate Policy" or "WellsSecure CP" or "WS CP". The "Certificate Policies" field for each Certificate references the OID for the Certificate Policy under which it was issued.

1.2.1 Certificates Issued on or Before August 1, 2006

All Certificates issued by the WellsSecure PKI will identify the WellsSecure CP OID in the "Certificate Policies" field of such Certificate. Each Certificate will also identify a Certificate Policy OID corresponding to the Assurance Level of that Certificate.

1.2.1.1 Certificate Types

(a) The WellsSecure PKI supports multiple Certificate types. The types of Certificates supported by the WS CPS and the OIDs for each associated Certificate Policy are as follows:

(i) Wells Fargo Organization Certificate Policy – 2.16.840.1.114171.903.x.1.11

(ii) Wells Fargo Personal Certificate Policy – 2.16.840.1.114171.901.x.1.11

(iii) Wells Fargo System Certificate Policy – 2.16.840.1.114171.902.x.1.11

(iv) Wells Fargo Application Certificate Policy – 2.16.840.1.114171.904.x.1.11

(v) Wells Fargo PKI Component Certificate Policy – 2.16.840.1.114171.905.x.1.11

(b) For x in the OIDs in Subsections (a) (i) through (a) (v) above:

(i) "0" will signify a standard software key,

(ii) "1" will signify a Token generated key, and

(iii) "2" will signify a software key with higher protections (such as those offered by a Private Key camouflage scheme).

The "Certificate Policies" field of each Certificate must reference the OID for the Certificate Policy under which it was issued.

1.2.2 Certificates Issued Subsequent To August 1, 2006

All Certificates issued by the WellsSecure PKI will identify the WellsSecure CP OID in the "Certificate Policies" field of such Certificate. Each Certificate will also identify the Certificate Policy OID corresponding to the Assurance Level of that Certificate.

1.2.2.1 Certificate Assurance Levels

The WellsSecure PKI issues multiple types of Certificates at multiple Assurance Levels. The Assurance Levels supported by the WS CPS and the OIDs for each associated Certificate Policy are as follows:

(a) Low

Low Assurance = 2.16.840.1.114171.500.1 or 2.16.840.1.114171.500.2

Company Low Assurance = 2.16.840.1.114171.500.6

TEST Low Assurance = 2.16.840.1.114171.501.1 or 2.16.840.1.114171.501.2

TEST Company Low Assurance = 2.16.840.1.114171.501.6

(b) Basic

Company Basic Assurance = 2.16.840.1.114171.500.13

Basic Assurance = 2.16.840.1.114171.500.10

TEST Company Basic Assurance = 2.16.840.1.114171.501.13

TEST Basic Assurance = 2.16.840.1.114171.501.10

(c) Medium

Medium Commercial Assurance = 2.16.840.1.114171.500.3

Medium Commercial Assurance (Hardware) = 2.16.840.1.114171.500.4

Company Medium Assurance = 2.16.840.1.114171.500.7

Medium U.S. Assurance = 2.16.840.1.114171.500.11

Medium U.S. Assurance (Hardware) = 2.16.840.1.114171.500.12

TEST Medium Commercial Assurance = 2.16.840.1.114171.501.3

TEST Medium Commercial Assurance (Hardware) = 2.16.840.1.114171.501.4

TEST Company Medium Assurance = 2.16.840.1.114171.501.7

TEST Medium U.S. Assurance = 2.16.840.1.114171.501.11

TEST Medium U.S. Assurance (Hardware) = 2.16.840.1.114171.501.12

(d) Infrastructure

Infrastructure Policy = 2.16.840.1.114171.500.0.1

TEST Infrastructure Policy = 2.16.840.1.114171.501.0.1

For example, therefore, a Certificate that is issued on a smart card will have the policy OIDs:

2.16.840.1.114171.500.0.0 and also 2.16.840.1.114171.500.4

1.2.3 Certificate Policy Identifications Previously Used

Certificates issued before this version of the WS CPS came into effect may have been issued with different Certificate Policy OIDs. Previously acceptable Certificate Policy OIDs were published in earlier versions of the WellsSecure CPS, available upon request to the WellsSecure PKI Contact (see Section 1.5.2).

1.2.4 Other PKI Documents

1.2.4.1 Sub-CA Agreements

The WellsSecure Public Root CA and the WellsSecure Public Root CA 01 G2 may issue Issuer Certificates to one or more Organizations or WF Affiliate Organization Units for the purpose of establishing such Organizations as WellsSecure Sub-CAs. In such an event, the Organization or WF Affiliate Organization Unit seeking to become a WellsSecure Sub-CA must enter into a Sub-CA Agreement with WFBNA. The Sub-CA Agreement must bind such Organization or WF Affiliate Organization Unit to the terms and conditions of the WS CP, this WS CPS and other applicable PKI Documents. The Sub-CA Agreement must also specify such other terms and conditions applicable to the Organization or WF Affiliate Organization Unit's role as a WellsSecure Sub-CA.

1.2.4.2 RA Agreements

The WellsSecure PKI may delegate its obligations to one or more qualified Organizations or WF Affiliate Organization Units to perform RA Functions which shall mean: (i) administering the Registration Process; (ii) processing requests for Reissuance, Suspension, Reinstatement, and Revocation of Certificates; and (iii) conducting the corresponding identification and authentication ("I & A"), where required, of Applicants, Subjects, or Subscribing Customers. The process for the RA Agreement and the main contents of the RA Agreement are outlined below.

In the event the WellsSecure PKI seeks to delegate these RA functions, the intended Organization, or WF Affiliate Organization Unit (unless the WF Affiliate Organization Unit is a unit under WFBNA, in which case no RA Agreement is required) must enter into an RA Agreement with WFBNA. The RA Agreement must bind the Organization or such WF Affiliate Organization Unit to the terms and conditions of the WS CP, this WS CPS and including without limitation other applicable PKI Documents.

Each RA Agreement will incorporate the RA Policies and Procedures Manual, which shall include one or more specific Authentication Policies that must comply with WF Affiliate Organization or WF Affiliate Organization Unit "Know Your Customer Guidelines" and the appropriate authentication policies. These authentication policies include, but may not be limited to the WellsSecure Authentication Policy.

The RA Agreement must also specify such other terms and conditions applicable to the Organization or such WF Affiliate Organization Unit's role as an RA, including without limitation, requiring that the Subscriber that is issued a Certificate in connection with a request from an RA authorized by the WellsSecure PKI enter into the applicable Customer Agreement with the RA.

The Wells Fargo PKI Management has authorized CR/EIS to operate and manage the RA on behalf of the WellsSecure PKI. Nothing in this WS CPS or any other PKI Document will prevent the WellsSecure PKI from also: (i) delegating RA functions to a different Organization or WF Affiliate Organization Unit; or

(ii) authorizing one or more Organizations or WF Affiliate Organization Units to act as RAs under the WellsSecure PKI's control.

1.2.4.3 Customer Agreements and Terms of Use

(a) Customer Agreements

The rights and obligations of Subscribing Customers are set forth in the applicable Customer Agreement (and all PKI Documents incorporated therein by reference), the WS CP and this WS CPS. For Certificates issued at a Low level of assurance, a Customer Agreement may not be required.

For Certificates issued from the WellsSecure PKI to a Subscribing Customer at a Basic, Medium, or High level of assurance, the Subscribing Customer must enter into an applicable Customer Agreement. Notwithstanding the foregoing, if the Subscribing Customer is WFBNA, no Customer Agreement will be required. The Customer Agreement will bind such Subscribing Customer to the terms and conditions of the WS CP and this WS CPS, as well as specify such other terms and conditions applicable to the Subscribing Customer's role within the WellsSecure PKI.

(b) Terms of Use

For Certificates issued at all levels of assurance, the following Individuals shall affirmatively agree to the applicable terms of use relating to such Certificates based on the level of assurance:

(i) Individuals who are the Subject;

(ii) Individuals who are acting as the Individual Sponsor who is responsible for a Group; or

(iii) Individuals who are acting as the Individual Sponsor, if the Subject is a System or Device.

1.2.4.4 Cross-Certification Agreements

WFBNA may, from time to time, enter into Cross-Certification Agreements with other CAs. Notification of any cross-certification event shall be made to any and all other CA's to which the WellsSecure PKI is currently cross-certified.

Currently, WFBNA's WellsSecure PKI is cross certified as follows:

1) Baltimore CyberTrust Root CA has issued a Cross-Certificate to WellsSecure Public Root CA and WellsSecure Public Root CA 01 G2. See Section 1.3.1.1.3 for details.

1.2.4.5 Accrediting Parties

WFBNA may, from time to time, seek accreditation and enter into Agreements with external accrediting parties.

1.3 PKI Participants

1.3.1 Certification Authorities

This WS CPS supports the following Root CAs

1. SHA-1 Root CA: WellsSecure Public Root CA
2. SHA- 2 Root CA: WellsSecure Public Root CA 01 G2

This WS CPS supports the following Sub-CAs to issue Certificates. The Wells Fargo PKI Management has authorized CR/EIS to operate and manage these Sub-CAs on behalf of the WellsSecure PKI.

1. SHA-1 Sub-CA: WellsSecure CA
2. SHA-2 Sub-CA: WellsSecure CA 01 G2

1.3.1.1 SHA-1 CAs

1.3.1.1.1 WellsSecure Public Root CA

The WellsSecure Public Root CA is one of the highest level CAs for the WellsSecure PKI. It is intended to be for public consumption. The WellsSecure Public Root CA provides a self-signed Root Certificate and is generally accepted in the PKI and identity verification industries as a Trusted Root. It is operated by an internal WF Affiliate Organization Unit approved by the Wells Fargo PKI Management including the approval through a WFBNA PKI Governance Signoff to perform CA Services.

1.3.1.1.2 WellsSecure CA

The WellsSecure CA is part of the WellsSecure PKI. It has been issued a Certificate signed by the WellsSecure Public Root CA. The WellsSecure CA is considered a Subordinate CA within the WellsSecure PKI. The WellsSecure CA is operated by CR/EIS, and currently issues Certificates to Subscribers that identify:

(a) Individuals whose use of the Certificate shall be in connection with business or professional purposes and not consumer purposes,

(b) Organizations or Organization Units,

(c) Systems, or

(d) Devices.

The WellsSecure CA is an issuing CA only. There will be no CAs that are subordinate to the WellsSecure CA.

1.3.1.1.3 Baltimore Cybertrust Root CA

The Baltimore CyberTrust Global Root is a third-party Root Certificate Authority, with the following field identifiers: *subject name CN*=Baltimore CyberTrust Root, OU = CyberTrust, O =Baltimore, C = IE. The Root CA associated with this Root Certificate is not owned, operated or maintained by any WF Affiliate Organization or WF Affiliate Organization Unit and is not part of the WellsSecure PKI. The CyberTrust Root CA is owned, operated and maintained by Verizon Communications. The Baltimore CyberTrust Global Root has issued a Cross-Certificate to WellsSecure Public Root CA and WellsSecure Public Root CA 01 G2. The operations and procedures associated with the Baltimore CyberTrust Root, for issuing the Cross-Certificate to the WellsSecure Public Root CA do not fall within this WS CPS. The CP and CPS for the Baltimore CyberTrust Root CA may be found at the following URL:
http://cybertrust.omniroot.com/repository.cfm

1.3.1.2 SHA-2 CAs

The following CAs use the SHA-2 hashing algorithm.

1.3.1.2.1 WellsSecure Public Root CA 01 G2

The WellsSecure Public Root CA 01 G2 is also one of the highest level CAs for the WellsSecure PKI. It is intended to be for public consumption. The WellsSecure Public Root CA 01 G2 provides a self-signed Root Certificate and is generally accepted in the PKI and identity verification industries as a Trusted Root. This CA is operated by the WF Affiliate Organization Unit known as CR/EIS, on behalf of WFBNA, and only issues Certificates to CAs that are subordinate to itself. The Certificate for this Root CA is signed with the SHA-2 algorithm, and it issues Certificates using the SHA-2 algorithm.

1.3.1.2.2 WellsSecure CA 01 G2

The WellsSecure CA 01 G2 is part of the WellsSecure PKI. It has been issued a Certificate with the following field identifiers: *subject name CN=WellsSecure Certification Authority 01 G2, OU= WellsSecure Certification Authorities, O = Wells Fargo Bank, N.A., C=US*, signed by the WellsSecure Public Root CA 01 G2. The WellsSecure CA 01 G2 is considered a Subordinate CA within the WellsSecure PKI. The

WellsSecure CA 01 G2 is operated by CR/EIS, on behalf of WFBNA, and currently issues Certificates to Subscribers that identify:

(a) Individuals whose use of the Certificate shall be in connection with business or professional purposes and not consumer purposes,

(b) Organizations or Organization Units,

(c) Systems, or

(d) Devices.

The WellsSecure CA 01 G2 is an issuing CA only. This CA Certificate is signed with the SHA-2 algorithm, and it issues Certificates using the SHA-2 algorithm. There will be no CAs that are subordinate to the WellsSecure CA 01 G2.

1.3.1.3 Additional Subordinate CAs

Nothing in this WS CPS or any other applicable PKI Document will prevent the WellsSecure Public Root CA, or WellsSecure Public Root CA 01 G2 from issuing Issuer Certificates to an Organization or WF Affiliate Organization Unit for the purpose of establishing that Organization or WF Affiliate Organization Unit as a WellsSecure Sub-CA.

To be appointed a WellsSecure Sub-CA, an Organization or WF Affiliate Organization Unit must: (i) be authorized through a WFBNA PKI Governance Signoff; (ii) execute a Sub-CA Agreement with WFBNA; and (iii) agree to be bound by the terms and conditions of the WS CP, this WS CPS, other applicable PKI Documents, and any other requirements as the Wells Fargo PKI Management or the WellsSecure PKI may periodically establish.

1.3.2 Registration Authorities

The primary purpose of an RA is to perform RA Functions as described in Section 1.2.4.2 in accordance with this WS CPS and other applicable WellsSecure PKI Documents.

The Wells Fargo PKI Management has authorized CR/EIS to act as an RA and perform RA Functions on behalf of the WellsSecure PKI. Nothing in the WellsSecure CP or any other PKI Document will prevent the WellsSecure PKI from also: (i) delegating RA Functions to a different Organization or WF Affiliate Organization Unit; or (ii) authorizing one or more Organizations or WF Affiliate Organization Units to act as RAs under the WellsSecure PKI's control.

To be appointed as an RA, an Organization must: (i) be authorized through a WFBNA PKI Governance Signoff; and (ii) execute an RA Agreement with WFBNA.

To be appointed as an RA, a WF Affiliate Organization Unit must execute an RA Agreement unless the RA is a business unit under WFBNA in which case no RA Agreement is required.

All organizations and WF Affiliate Organization Units appointed as RAs must agree to be bound by the terms and conditions of this WS CPS, other applicable WellsSecure PKI Documents, and any other requirements as the Wells Fargo PKI Management or the WellsSecure PKI may periodically establish.

The WellsSecure PKI Documents applicable to an RA are: (i) the WS CP; (ii) this WS CPS; and (iii) the RA Policies and Procedures Manual and applicable Authentication Policies incorporated therein; and (iv) for Organizations and WF Affiliate Organization Units that are not units under WFBNA, the RA Agreement.

Trusted Registrars

A Trusted Registrar (TR) is an Individual authorized by a Subscribing Customer to perform I & A of potential Subjects to be named in Certificates issued to such Subscribing Customer.

A Wells Fargo Employee may become a TR; provided, however, that the employee must have been issued a Certificate with an Assurance Level that is at least as high as that of the highest Assurance Level Certificate that the employee approves as a TR.

In the event the Subscribing Customer has obtained its Certificates from an RA that has been authorized by the WellsSecure PKI to perform RA Functions, Trusted Registrars will only be permitted if the RA has specifically granted permission to such Subscribing Customer to use Trusted Registrars.

1.3.3 Subscribers

Parties who enter into a Customer Agreement with WFBNA, or an approved RA for the issuance of Certificates from the WellsSecure PKI at the Basic, Medium, Company Basic, and Company Medium levels of assurance are hereafter referred to as "Subscribing Customers".

(a) Organizations

In all events, any Organization seeking to become a Subscribing Customer must execute an applicable Customer Agreement (Certificate Subscriber Agreement for Digital Certificates) authorizing the WellsSecure Sub-CA to issue Certificates to it. Once an Organization has become a Subscribing Customer, the Organization can authorize one or more Applicants who can request Certificates from the WellsSecure Sub-CA. For each Certificate it requests, the Applicant must successfully complete the applicable Registration Process.

(b) Individuals

(i) Generally: For Basic, Medium (All Assurance Levels)

In all events, any Individual seeking to become a Subscribing Customer must execute an applicable Customer Agreement authorizing the WellsSecure Sub-CA to issue Certificates to him or her. Once an Individual has become a Subscribing Customer, the Individual is the only person who is authorized to request Certificates from the WellsSecure Sub-CA. The Individual Subscribing Customer cannot designate any other Individual to request Certificates on the Individual Subscribing Customer's behalf. For each Certificate he or she requests, the Individual must successfully complete the applicable Registration Process.

(ii) For Low Assurance Level Certificates

For Certificates issued with the Low Assurance level the Subscribing Customer may be an Individual based on his or her, or his or her Organization's, existing business relationship with a WF Organization, WF Affiliate Organization Unit, or the RA that is requesting the Certificate. The WF Organization, WF Affiliate Organization Unit or RA that has the relationship with the Individual or Organization that that Individual represents takes responsibility for the issuance and usage of the Certificate by that Individual. The Customer Agreement(s) (if any) executed or Terms of Use acknowledged and agreed to by such Individual Subscribing Customer before issuance are dependent upon the requirements of the WF Organization, WF Affiliate Organization Unit or RA, so long as the minimum language requirements as agreed between WFBNA and the RA are included in such Customer Agreement or Terms of Use.

(c) Applicable PKI Documents

The PKI Documents applicable to a Subscribing Customer are: (i) this WS CPS, (ii) the WS CP, (iii) the Customer Agreement (including any documents referenced therein) signed by such Subscribing Customer, and (ii) the Terms of Use.

1.3.4 Relying Parties

A Relying Party relies on a Subscribing Customer's Encryption Certificate or Signing Certificate for the purposes of: (a) authenticating identity; (b) verifying a Digital Signature on an electronic record; or (c) encrypting communications. Relying Parties are solely responsible for determining the suitability of relying on a Certificate in any given transaction. This evaluation must be done by each Relying Party in the context of a specific transaction and is not controlled in any manner by Wells Fargo or the WellsSecure PKI.

1.3.5 Other Participants

1.3.5.1 Trusted Registrars

A Trusted Registrar (TR) is an Individual authorized by a Subscribing Customer to perform I & A of potential Subjects to be named in Certificates issued to such Subscribing Customer.

A Wells Fargo Employee may become a TR; provided, however that the employee must have been issued a Certificate with an Assurance Level that is at least as high as that of the highest Assurance Level Certificate that the employee approves as a TR.

In the event the Subscribing Customer has obtained its Certificates from an RA that has been authorized by the WellsSecure PKI to perform RA Functions, Trusted Registrars will only be permitted if the RA has specifically granted permission to such Subscribing Customer to use Trusted Registrars.

1.3.5.2 Applicants And Subjects

1.3.5.2.1 Applicants

An Applicant is: (a) the individual who has the authority and ability on behalf of the subject named within the Certificate to request issuance of that Certificate. In the case of Certificates that have individuals as the Subject, the Applicant must be the named individual, or (b) For Certificates issued with a Low Assurance Level the Applicant may also be an Employee of a WF Affiliate Organization or WF Affiliate Organization Unit that has an existing business relationship with the Subscribing Customer, to undertake the Registration Process for Certificate Issuance for such Subscribing Customer.

1.3.5.2.2 Subjects

An Applicant can request, on behalf of a Subscriber, that a Certificate be issued to different types of Subjects, including Individuals, Organizations, Devices, or Systems.

(a) Individual Subjects

Individuals named as Subjects are Individuals who use the Certificate in connection with his or her business or professional purposes and not for consumer purposes.

(b) Organization Subjects

Organizations named as Subjects are either the Subscribing Customer itself or a related Organization or Organization Unit of the Subscribing Customer (e.g., a subsidiary or affiliate).

(c) Device and System Subjects

Devices and Systems named as Subjects must be under the direct control of the Subscribing Customer.

1.4 Certificate Usage

The CAs within the WellsSecure PKI issue Certificates at the Assurance Levels described in Section 1.2.2.1 and Section 1.4.1 below. These Certificates are issued pursuant to different practices and procedures and are suitable for different purposes based on the Assurance Levels. Each Certificate issued contains the assigned Policy OID in the Certificate Policies extension of the Certificate for that Assurance Level as specified in Section 1.2.2. The appropriate Certificate uses based on the Assurance Levels are found within Section 1.4.1.

WellsSecure PKI does not issue Certificate that can be used for MITM (Man in the Middle Attack), “data traffic management” of domain names, or IPs (IP addresses) that the Certificate holder does not legitimately own or control.

1.4.1 Appropriate Certificate Uses

Certificates issued by a WellsSecure Sub-CA to Subscribing Customers are approved only for the purposes set forth in the sub-sections below.

1.4.1.1 Low Assurance Level

This level provides the lowest degree of assurance. One of the primary functions of this level is to provide data integrity to the information being signed. This level is relevant to environments in which the risk of

malicious activity is considered to be low. It may be used for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used where Certificates having higher levels of assurance are unavailable, or where the Relying Party has determined that it is sufficient. It cannot be used for transactions requiring non-repudiation. Low Assurance Level Certificates are issued to Individual end users and not to Organizations, Systems or Devices.

1.4.1.2 Basic Assurance Level

This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious. Basic Assurance Level Certificates are issued to Individual end users and not to Organizations, Systems or Devices.

1.4.1.3 Medium Commercial Assurance Level

This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Medium Assurance Level Certificates are issued to Individual end users and not to Organizations, Systems or Devices.

1.4.1.4 Medium Commercial Hardware Assurance Level

This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Certificates with this Assurance Level can only be issued for use in level 2 of [FIPS140] certified, or higher, cryptographic containers. Medium Hardware Assurance Level Certificates are issued to Individual end users and not to Organizations, Systems or Devices. I & A for this Assurance Level will include face-to-face identity proofing.

1.4.1.5 Medium U.S. Assurance Level

This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Medium U.S. Assurance Level Certificates are issued to Individual end users and not to Organizations, Systems or Devices. I & A for this Assurance Level will include face to face identity proofing.

1.4.1.6 Medium U.S. Hardware Assurance Level

This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Certificates with this Assurance Level can only be issued for use in level 2 of [FIPS140] certified, or higher, cryptographic containers. Medium U.S. Hardware Assurance Level Certificates are issued to Individual end users and not to Organizations, Systems or Devices. I & A for this Assurance Level will include face to face identity proofing.

1.4.1.7 Test Assurance Levels

This level of assurance is used for testing with the WellsSecure PKI. In no case is a test Certificate to be relied upon for any use other than testing Certificate use. All Certificates that are issued with this Assurance Level will include the word “Test” in the Subject Name of the Certificate, or include some other clear indication of testing usage limitation.

1.4.1.8 PKI Component

PKI Component Certificates shall be issued only to components of the Public Key Infrastructure and may be used only by the PKI Component that is named in the "Common Name (cn)" section of the "Subject" field of such Certificate. PKI Component Certificates are issued as a part of the PKI setup process and

are not subject to any authentication policy as it relates to validating the identity of a Subscriber. PKI Component Certificates that are issued from the WellsSecure Public Root CA or WellsSecure Public Root CA 01 G2 will only be used within the WellsSecure PKI.

1.4.1.9 Company Low Assurance Level

This level provides the lowest degree of assurance relevant to environments in which the risk of malicious activity is considered to be low. This may include access to private information where the likelihood of malicious access is low. It is assumed at this security level that users are not likely to be malicious. Company Low Certificates are issued to Organizations, Systems or Devices and not to Individual end users. In the event a Company Low Certificate is issued to a System or Device, the Individual Sponsor's responsibilities further described in Sections 3.2.4 and 6.1.2 may be performed by a systems administrator for the Subscribing Customer.

1.4.1.10 Company Basic Assurance Level

This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious. Company Basic Certificates are issued to Organizations, Systems or Devices and not to Individual end users. In the event a Company Basic Certificate is issued to a System or Device, the Individual Sponsor's responsibilities further described in Sections 3.2.4 and 6.1.2 may be performed by a systems administrator for the Subscribing Customer. In the event a Company Basic Certificate is issued to an Organization, the Applicant is responsible for the Certificate.

1.4.1.11 Company Medium Assurance Level

This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Company Medium Certificates are issued to Systems, Devices, or the Organization and not to Individual end users. In the event a Company Medium Certificate is issued to a Device, the Individual Sponsor's responsibilities further described in Sections 3.2.4 and 6.1.2 may be performed by a systems administrator for the Device. Company Medium Assurance Level Certificates that are issued to an Organization as the Subject must be stored in an approved cryptographic hardware module. In the event a Company Medium Certificate is issued to an Organization, the Applicant is responsible for the Certificate. In all cases, the Applicant for a Company Medium Assurance Level Certificate must have their identity verified pursuant to the policy that is set forth for the Subject of a Medium Commercial Assurance Level Certificate.

1.4.2 Prohibited Certificate Uses

Certificates shall not be used for (a) any illegal purposes or any transaction prohibited by applicable law, including but not limited to any use in OFAC negative countries; (b) any transaction prohibited by regulatory requirements, (c) any use not in accordance with the applicable Customer Agreement, the Terms of Use, or applicable PKI Documents; or (d) where the Subscribing Customer acts as an agent for an undisclosed principal or otherwise is not acting as the principal in such transaction.

Subscriber shall not use the CA Service or the Validation Service, or Certificates in fraudulent manner, including in any of the following: manipulating the client clock to reflect anything other than the correct, current, regional time, and/or damaging, investigating, re-engineering, or otherwise interfering with the token, clock, Certificate, smart card chip, or other element of the WellsSecure PKI. Subscribers shall also not allow any of their Certificate holders to use the CA Service, the Validation Service, or Certificates in a fraudulent manner including those listed above.

1.5 Policy Administration

1.5.1 Organization Administering The Document

Wells Fargo Corporate Authentication Services PKI
2600 S. Price Road
MAC S3929-022
Chandler, AZ. 85286-2806

1.5.2 Contact Person

Wells Fargo Corporate Authentication Services PKI
2600 S. Price Road
MAC S3929-022
Chandler, AZ. 85286-2806

1.5.3 Persons Determining CPS Suitability For The Policy

The Wells Fargo PKI Management is responsible for asserting that the WellsSecure CP conforms to this WS CPS.

1.5.4 CPS Approval Procedures

The Wells Fargo PKI Management is responsible for approving any changes to this WS CPS.

1.6 Definitions And Acronyms

See Section 10.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

2.1.1 Obligations

Repository obligations in accordance with the WS CP, this WS CPS and applicable PKI documents are:

(a) Processing all CRLs received from the WellsSecure Issuing CA;

(b) Operating and maintaining the Directory, including incorporating all CRLs;

(c) Operating and maintaining the WellsSecure Online Certificate Status Protocol ("OCSP") Responder;

(d) Taking reasonable steps to provide the Directory with accurate and complete information on Certificate status;

(e) Containing all CA Certificates issued by or to any CA within the WellsSecure PKI and CRLs issued by any CA within the WellsSecure PKI; and

(f) Making CA Certificates and CRLs publicly available for retrieval from the Repository.

The Wells Fargo PKI Management has authorized CR/EIS to operate and manage the Repository on the WellsSecure PKI's behalf.

The PKI Documents applicable to the Repository are:

(i) this WS CPS;

(ii) the WellsSecure CP;

(iii) the Repository Agreement, if applicable; and

(iv) other agreements, manuals, or procedures as may be provided by the WellsSecure PKI.

The Directory provided by WellsSecure is a fully compliant X.500 online and searchable database of Certificate status information. The Directory contains the then current CRL for each WellsSecure Issuing CA, which is made available at the sole discretion of the WellsSecure PKI.

2.1.2 Purpose

The primary purpose of the Repository is to provide Certificate status information. The Certificate status information is also provided through an OCSP Responder [see Section 4.9.9].

2.2 Publication Of Certification Information

The WellsSecure PKI will make this WS CPS and selected PKI Documents available to authorized Participants. The WellsSecure Issuing CA will provide Certificate status information and Compromised User information to the Repository as set forth in this WS CPS. This WS CPS can be found on the Internet in .pdf format at: https://www.wellsfargo.com/repository

2.3 Time Or Frequency Of Publication

2.3.1 Certificate Status Information

Information relating to Compromised Certificates and Certificate Suspension, Reinstatement or Revocation (including the reason for such status) will be published in accordance with Section 4.9 of this WS CPS.

2.3.2 Changes To PKI Documents

The PKI Manager has the authority to modify this WS CPS with approval from the CR/EIS Executive Manager. Any suggestions for modifications should be communicated to the Contact Persons of this WS CPS [see Section 1.5.2].

In the event the PKI Manager proposes and obtains approval for significant changes to this WS CPS, as set forth in Section 9.12, the PKI Manager will make an electronic copy of the modified WS CPS publicly available to all Participants; see Section 1.5.2 for contact information. The new version of this WS CPS will become effective immediately for all Participants with which WFBNA does not have a contractual relationship relating to the WellsSecure PKI.

In the event WFBNA has a contractual relationship with a Participant that is a Relying Party, written notice of prospective WS CPS changes shall be communicated via U.S. Mail or email. The modified WS CPS will become effective twenty (20) days after the notice of the changes has been delivered to such Participants. After the twenty-day notice period, the new WS CPS will supersede all previous versions and will be binding on all such Participants from that point forward.

On or before the applicable effective date of the modified WS CPS, Subscribing Customers may revoke their Certificate(s) without obligating the Subscribing Customer to the terms of the new version of this WS CPS. A Subscribing Customer's decision not to Revoke its Certificate(s) within the twenty day notice period for the new version of this WS CPS constitutes acceptance of the terms of the new WS CPS.

The WellsSecure PKI has made publicly available through the Internet, a Repository containing Certificate status information, CA Certificates, CRLs and any other public and non-personal information Wells Fargo deems necessary to support:

a) the interoperation of the WellsSecure PKI with those PKIs for which a WellsSecure PKI's CA has been issued a Cross-Certificate; and
b) Relying Parties.

2.4 Access Controls On Repositories

The WellsSecure PKI has made publicly available through the Internet, a Repository containing Certificate status information, CA Certificates, CRLs and any other public and non-personal information Wells Fargo deems necessary to support:

a) the interoperation of the WellsSecure PKI with those PKIs for which a WellsSecure PKI's CA has been issued a Cross-Certificate; and
b) Relying Parties.

Table 2.1: CRL and OCSP: SHA-1 CAs

CA Common Name	CRL Distribution Point	OCSP URL
Baltimore CyberTrust Root CA	http://cdp1.public-trust.com/CRL/Omniroot2025.crl	
CN = Wells Fargo Certificate Authority 01	http://crl.pki.wellsfargo.com/ext.crl	http://ocsp-ext.pki.wellsfargo.com
CN=Wells Fargo Public Primary Certificate Authority	http://crl.pki.wellsfargo.com/ev.crl	http://validator.wellsfargo.com
CN = WellsSecure Certificate Authority	http://crl.pki.wellsfargo.com/wsca00.crl	http://validator.wellsfargo.com

Table 2.2: CRL and OCSP: SHA-2 CAs

CA Common Name	CRL Distribution Point	OCSP URL
CN = Baltimore CyberTrust Root CA	http://cdp1.public-trust.com/CRL/Omniroot2025.crl	
CN = WellsSecure Public Root Certification Authority 01 G2	http://crl.pki.wellsfargo.com/wsprca01G2.crl	http://validator.wellsfargo.com/
CN = WellsSecure Certification Authority 01 G2	http://crl.pki.wellsfargo.com/wsca01G2.crl	http://validator.wellsfargo.com/

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types Of Names

The WellsSecure PKI's CAs and all Wells Fargo Subscribing Customers and Subjects are assigned X.500 Distinguished Names (DNs) for inclusion in the "Issuer Distinguished Name" and "Subject" fields of Certificates.

The WellsSecure PKI's CAs requires the following fields to construct the DN:

(i) For Individuals: the First Name and Last Name of the Individual

(ii) For Individuals, Systems, Organizations and Devices, the:

(a) Company;

(b) Department; and

(c) Country; and

(iii) For Systems, and Devices: Make, Model or hostname tied to an IP Address and/or Serial Number or other uniquely identifying information, as appropriate.

3.1.2 Need For Names To Be Meaningful

The DNs assigned to the WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2, WellsSecure Sub-CAs, and all Organizations and Individuals to be identified in the "Issuer Distinguished Name" and "Subject" fields of a Certificate have a reasonable association with the WellsSecure PKI's CAs, Organization, and Individual to be identified.

3.1.3 Anonymity Or Pseudonymity Of Subscribers

No stipulation.

3.1.4 Rules For Interpreting Various Name Forms

Names shall be interpreted according to the Certificate Profiles for the applicable type of Certificate. The Certificate Profile information is outlined in Section 7.1. Details are available on a need-to-know basis; see Section 1.5.2 for contact information.

3.1.5 Uniqueness Of Names

Each DN used within WellsSecure PKI is unique within the Issuing CA, as provided in the Authentication Policies, except as otherwise provided in Sections 3.1.5.1, 3.1.5.2 and 3.1.5.3.

3.1.5.1 DN For A Signing And Encryption Certificate Key Pair

The same DN can be used for a Signing and Encryption Certificate Key Pair as defined in the WS CP and this WS CPS.

3.1.5.2 DN For Certificates Issued For Different Key Storage Systems

The same DN can be used for different types of Key Storage Systems.

3.1.5.3 A Low Assurance Domain Validated Certificate

A Low Assurance Domain validated Certificate issued for **.sub-domain.domain.com* is acceptable where supporting documentation is present. The same DN can be used for a Certificate issued to **.sub-domain.domain.com* form where the end-user has provided the RA with the following:

(i) a written requirement citing a technical limitation or undue hardship has been documented stating the need for a Domain Validated (a/k/a wildcard) Certificate, and

(ii) a written acceptance of the risk of a Domain Validated or wildcard Certificate issuance that takes explicit responsibility for securing the deployment of that Certificate to multiple sites.

3.1.6 Recognition, Authentication, And Role Of Trademarks

The WellsSecure Issuing CA will not knowingly allow any Subscribing Customer or Subject to use any name that a court of competent jurisdiction has determined it has no right to use. Once Certificates are issued, the WellsSecure Issuing CA will have no obligation, other than imposed by law, to re-issue the Certificate in the name of the proper party, or to otherwise make that name available to the correct Subscribing Customer or Subject. Although the WellsSecure PKI may take steps to honor private trademark rights, the WellsSecure Issuing CA makes no guarantee that it will at any point honor such rights.

Under no circumstances is the WellsSecure Issuing CA obligated to seek evidence of trademark ownership or court orders. Where the WellsSecure Issuing CA has issued a name that infringes on the proprietary rights of a third party, the Subscribing Customer is responsible for indemnifying the Wells Fargo Trusted Identity Entities in accordance with Section 9.9.2.2 herein.

3.2 Initial Identity Validation

A Subscriber seeking to obtain Certificates from a WellsSecure Issuing CA is required to have their identity validated before a Certificate is used.

For I & A of SSL Certificate requests and S/MIME Certificate requests, see Section 3.2.6 and Section 3.2.7 respectively.

3.2.1 Method To Prove Possession Of Private Key

In all cases where the Individual, Organization or Device identified in the "Common Name (CN)" section of the "Subject" field of the Certificate generates his, her or its own Private Key, the Subject of the Certificate (if issued to an Individual), Individual Sponsor (if issued to a System or Device) or Applicant (if issued to an Organization), will be required to prove possession of the Private Key corresponding to the Public Key in a Certificate request. Acceptable methods of proof of possession of a Private Key that is associated with a Public Key include, but are not limited to, requiring the Subscribing Customer to send the RA a digitally signed request or challenge as part of the Registration Process. In the case where a Private Key is generated by the CA or RA either (a) directly on the Individual, Organization or Device's Token; or (b) in a key generator that benignly transfers the Private Key to the Individual, Organization or Device's Token, then proof of possession is not required.

3.2.2 Authentication Of Organization Identity

I & A of the identity of Subscribers that are Organizations that are either Subscribers or approved Sub-CAs will be conducted in accordance with applicable Authentication Policies. Although I & A will generally be performed by the either the RA or by Wells Fargo or WF Affiliate Organization or WF Affiliate Organization Unit authorized Employees, in certain circumstances, the I & A may be performed by Trusted Registrars.

Previously performed I & A of an Organization will satisfy the I & A requirements under the WS CP, and this WS CPS if such I & A was substantially the same as the authentication policy applicable to the Assurance Level of the Certificate being requested by the Organization and: (a) the previously performed I & A of an Organization was in connection with the Organization's existing business relationship with another WF Affiliate Organization or WF Affiliate Organization Unit, or (b) the Organization is an existing Subscribing Customer.

The table below outlines the minimum requirements for authentication of Organization identity for each Assurance Level, more stringent practices may be used.

Table 3.1: Minimum Authentication Requirements for Organization Identity

Assurance Level	Applicable Authentication Policies	I&A performed by
Low, Company Low, Infrastructure, Test	None	n/a
Basic, Medium Commercial, Medium Commercial (Hardware), Medium U.S., Medium U.S. (Hardware)	WellsSecure Authentication Policy (part of RA Policies and Procedures)	RA, Wells Fargo, WF Affiliate Organization or WF Affiliate Organization Unit Authorized Employees
Company Basic, Company Medium	WellsSecure Authentication Policy (part of RA Policies and Procedures)	RA, Wells Fargo, WF Affiliate Organization or WF Affiliate Organization Unit authorized Employees

3.2.2.1 Authentication Of Organizations For CA Certificates

Requests for WellsSecure PKI's CA Certificates in the name of an organization should include the organization name, address, and documentation of the existence of the organization.

The WellsSecure RA verifies the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

3.2.3 Authentication Of Individual Identity

I & A of the identity of Subscribers, Subjects, or Sponsors that are Individuals is conducted in accordance with applicable Authentication Policies. Although I & A is generally performed by the RA or by Wells Fargo or WF Affiliate Organization or WF Affiliate Organization Unit authorized Employees, in certain circumstances, the I & A may be performed by Trusted Registrars or an entity certified by a State or Federal government as being authorized to confirm Individual identities. Information that is not verified is not to be included in Certificates.

The table below outlines the minimum requirements for authentication of Individual identity for each Assurance Level, more stringent practices may be used.

Table 3.2: Minimum Authentication Requirements for Individual Identity

Assurance Level	Applicable Authentication Policies	I&A performed by
Basic, Medium Commercial, Medium Commercial (Hardware), Medium U.S., Medium U.S. (Hardware)	WellsSecure Authentication Policy (part of RA Policies and Procedures)	Trusted Registrars, RA, Wells Fargo, WF Affiliate Organization or WF Affiliate Organization Unit authorized Employees, an entity certified by a State or Federal Government as being authorized to confirm Individual identities
Low, Test	None	n/a

3.2.4 Non-Verified Subscriber Information

For Certificates that are issued at the Basic, Company Basic, Medium Commercial, Medium Commercial (Hardware), Medium U.S., Medium U.S. (Hardware), or Company Medium Levels, information that is not verified is not included within the Certificate.

3.2.5 Validation Of Authority
No stipulation.

3.2.6 Criteria For Interoperation
No stipulation.

3.2.7 Authentication Of Individuals For Organization Certificates
(a) For cases where there are several Individuals within a single Subscribing Customer acting in one capacity (hereinafter referred to as a "Group"), a Certificate (hereinafter referred to as an "Organization Certificate") may be issued that corresponds to a Private Key that is shared by multiple Individuals who are members of such Group.

(b) In addition to the authentication of an Individual Sponsor for the Organization Certificate, the following procedures are performed for all Individuals included in the Group:

(i) The Individual Sponsor is responsible for ensuring control of the Private Key, including maintaining a list of Individuals who have access to use of the Private Key,

(ii) The subjectName DN must not imply that the Subject is a single Individual, e.g. by inclusion of a human name form;

(iii) The list of those holding the shared Private Key must be provided to, and retained by the RA or its designated representative;

(iv) The procedures for issuing Tokens for use with Organization Certificates must comply with all other stipulations of the WS CP and this WS CPS (e.g., Private Key generation, Private Key protection, and Subscribing Customer obligations); and

(v) Organizational Certificates must be issued with OIDs at the following Assurance Levels: Company Low, Company Basic, or Company Medium, as set forth in [Section 1.2.2] for situations that involve Shared Keys.

3.2.8 Identity Authentication And Verification Processes For SSL Certificates
WS PKI supports the following verification processes while handling Certificate requests for SSL Certificates by Applicants who are also Domain Name Registrants. WS PKI complies with the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org, including verification of controlling the Domain Name. Terms in this Section that are not otherwise defined in this WS CPS shall have the meanings set forth in the Baseline Requirements.

SSL Certificate requests for high risk Domain Names undergo additional vetting besides that specified in such Baseline Requirements.

3.2.8.1 Domain Name Authorization
Prior to issuing an SSL Certificate, WS PKI obtains authorization from all Domain Name Registrants included in the Certificate request. WS PKI verifies the Domain Name authorization as follows.

a) A minimum of two (2) WHOIS searches are performed for each registerable Domain Name in the Certificate request.
b) The administrative contact for the Domain Name Registrant identified by the WHOIS search is contacted and the results archived in email form.
c) Domain Names are checked against internal criteria to determine if additional verification is warranted prior to issuance of an SSL Certificate.
d) Domain Names and IP Addresses are checked against a WS PKI internally-maintained Denied List of Certificate Requests. This list includes the Certificate requests or the Certificates that have been previously denied or revoked for suspected reasons of phishing, or fraudulent usage.

3.2.8.2 IP Address Authorization

Each IP Address included in an SSL Certificate request is verified to be owned or under the control of the Domain Name Registrant.

a) Publicly routable IP Addresses are verified by performing a reverse lookup of the IP Address or checking the Internet assigned number authority for the corresponding geographic region to verify that the IP Address is owned or controlled by the Domain Name Registrant.

3.2.8.3 Subject Verification

For each SSL Certificate request, WS PKI performs the following processes for Subject verification.

a) Organization
    a. Any identity or address information that is to appear in an SSL Certificate for an organization will be verified through a government agency, third party database, site visit, or attestation letter.
b) DBA/Trade name
    a. Any DBAs or Trade names that are to appear in an SSL Certificate will be verified through documentation provided by a government agency, a Reliable Data Source, an Attestation Letter, or a utility bill, bank statement, or other form of identification that the WS PKI deems reliable.
c) Country Code Verification
    a. Any time a country code is to appear in an SSL Certificate, the WS PKI will ensure that the appropriate country code is present by checking against any one of the following: 1) IP Address ranges for the country listed, 2) the address for the organization, 3) information provided by the Domain Name Registrar, 4) a government agency, 5) a third party database, 6) a site visit, or 7) an Attestation Letter.

3.2.9 Identity Authentication And Verification Processes For S/MIME Certificate

An S/MIME Certificate request may be initiated by a regular Wells Fargo Employee or by an external entity Organization that has a business relationship with Wells Fargo. The following vetting processes are undertaken in addition to the identification and authentication requirements set forth in remainder of this WS CPS.

For Wells Fargo Employees, S/MIME Certificates are issued through internal vetting processes. The S/MIME Certificates issued to Wells Fargo Employees must use the Domain Names owned by Wells Fargo.

For non-Wells Fargo Organizations, an S/MIME Certificate may be issued to an external Employee of such Organization that has an existing relationship with Wells Fargo. The relationship to an external Organization must be managed by a Wells Fargo authorized representative. The Wells Fargo representative initiates the request for S/MIME Certificate on behalf of the associated external Organization, after obtaining approval from Wells Fargo management though the authorized representative. Next, the WS PKI provides an authorization code for this request to the Wells Fargo representative. The Wells Fargo representative provides this authorization code to the Employee of the external Organization over phone or some other out-of-band medium. The Employee of the external Organization uses this authorization code to access and open a link, which is separately emailed by WS PKI to such Employee. The Employee of the external Organization uses the link to accept or reject the terms and conditions for the S/MIME Certificate. Upon receiving acceptance of the terms and conditions, WS PKI emails the S/MIME Certificate to such Employee. The employee of the external Organization uses the above mentioned authorization code to open and install the S/MIME Certificate.

3.2.10 Multi-Factor Authentication

WS PKI requires multi-factor authentication for accounts that can directly cause Certificate issuance.

3.3 Identification And Authentication For Re-Key Requests

Certificates issued by the WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2 and WellsSecure Sub-CAs are not re-keyed or rolled over. A Subscribing Customer's Key Pair Expires contemporaneously with the Expiration of their associated Certificate's Operational Period. Subscribing Customers may have their Certificates Reissued pursuant to the provisions of Section 5.6.

The WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2, WellsSecure Sub-CA, RA, and OCSP Responder Certificates are not re-keyed or rolled-over. The WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2, WellsSecure Sub-CA, RA, or OCSP Responder may have Certificates Reissued pursuant to the provisions of Section 5.6.

3.3.1 Identification And Authentication For Routine Re-Key

Subscribing Customers may establish their identity through the use of a current and valid Signature Key, or through the Registration Process. All Subscribers must re-establish their identity through the Registration Process on a regular basis depending on the Assurance Level of the Certificate. Wells Fargo reserves the right to require re-establishment of identity through the Registration Process at any time.

Table 3.4: I & A Requirements for Certificate Renewal

Assurance Level	Routine issuance upon renewal requirements
Low	Identity may be established through the use of a current, valid Signature Key.
Basic (all policies)	Identity may be established through the use of a current, valid Signature Key, except that the identity is to be re-established through the Registration Process at least once every 15 years from the time of the initial Registration Process.
Medium (all policies)	Identity may be established through the use of a current, valid Signature Key, except that the identity is to be re-established through the Registration Process at least once every 9 years from the time of the initial Registration Process.

3.3.2 Identification And Authentication For Re-Key After Revocation

Following Certificate Revocation, Subscribing Customers must reapply for a new Certificate following the same process and procedures for obtaining a new Certificate. See Section 4.1.

3.4 Identification And Authentication For Revocation Request

See Section 4.9.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

All CA Services will comply with the requirements of:

(a) The WS CP;
(b) This WS CPS;
(c) Any other applicable PKI Documents; and
(d) Any agreements in force between the WellsSecure Issuing CA and any other Participant.

4.1 Certificate Application

To obtain a Certificate, a Subscribing Customer is required to complete all elements of the Registration Process detailed in Section 4.1.2 below.

4.1.1 Who Can Submit A Certificate Application

Applicants submit a Certificate Application.

4.1.2 Enrollment Process And Responsibilities

(a) Authentication Policies

All I & A procedures are set forth in one or more applicable Authentication Policies.

(b) Registration Process

The Registration Process for Basic and Medium Assurance Levels is as follows:

(i) A Subscribing Customer authorizes an Applicant to provide application information to an RA on the Subscribing Customer's behalf;

(ii) The Applicant submits application information to the RA in accordance with the applicable procedures;

(iii) I & A is performed to authenticate the identity and authority of the Applicant to apply on behalf of the Subscribing Customer and/or Subject;

(iv) The Subscribing Customer must execute an applicable Customer Agreement; and

(v) I & A is performed to authenticate the identity of the Subscribing Customer and the Subject to be named in the Certificate. In certain circumstances, I & A of potential Subjects may be performed by one or more Trusted Registrars.

If the foregoing I & A procedures are successful, and the Certificate request is approved, the RA or the TR authenticates to the WellsSecure Issuing CA and requests the generation of a Key Pair and a Certificate for the Subscribing Customer in question that will identify the Subscribing Customer and Subject in the applicable portions of the Certificate's “Subject” field, pursuant to key generation in accordance with the appropriate section(s) of the WS CP and this WS CPS.

For all other Assurance Levels, consult the applicable authentication policy (see Section 3.2.2).

For all enrollment processes, all communications among the components of the WellsSecure PKI, including, but not limited to the communication between the RA and the CA, supporting the Registration Process and issuance process shall be authenticated and protected from modification.

4.1.2.1 Applicant Obligations

Applicant obligations are set forth in the WS CP, this WS CPS, and other applicable PKI Documents. These include, but are not limited to the Certificate Subscriber Agreement for Digital Certificates, and may also include service request forms, and Certificate request forms.

(a) Basic and Medium Assurance Levels

For Basic and Medium (inclusive) Assurance Levels, an Applicant is responsible for:

(i) Obtaining the requisite authority from the Subscribing Customer to represent such Subscribing Customer in the Registration Process;

(ii) Undertaking the Registration Process on behalf of its authorizing Subscribing Customer;

(iii) Participating in the Registration Process, including providing complete and accurate information regarding:

(A) his or her own identity and authority to represent the Subscribing Customer;

(B) his or her relationship to the authorizing Subscribing Customer;

(C) the identity of the Subscribing Customer; and

(D) the identity of the Individual or Organization to be named as the Subject.

(b) All other Assurance Levels

For other Assurance Levels, the Applicant Obligations can be found within the applicable Customer Agreements. See Section 4.1.2.2 for EV Assurance level.

(c) Applicant as the Subject

An Applicant may undertake the Registration Process to obtain a Certificate naming the Applicant as the Subject.

4.1.2.2 Trusted Registrar Obligations

Trusted Registrar obligations are set forth in the WS CP, this WS CPS and other applicable PKI Documents for Trusted Registrar's appointed by the Subscribing Customer. Trusted Registrar obligations are also set forth in the RA Policies and Procedures Manual for Trusted Registrars that have been authorized by the RA.

(a) Responsibilities

A Trusted Registrar is responsible for:

(i) Obtaining the requisite authority from the Subscribing Customer to undertake I & A of potential Subjects on the Subscribing Customer's behalf. The Trusted Registrar is authorized to request that Certificates be issued only on behalf of the Subscribing Customer by whom the Trusted Registrar is employed;

(ii) Performing I & A of potential Subjects to be named in Certificates to be issued to the Subscribing Customer that has authorized the Trusted Registrar;

(iii) Performing I & A in accordance with standards and procedures set forth by the WellsSecure Issuing CA or the appropriate RA;

(iv) Taking all steps to ensure that any I & A information regarding potential Subjects is complete and accurate;

(v) Delivering all I & A information to the appropriate RA using a safe, secure and reliable method (e.g. digitally signed PDF, or USPS, or authenticating to the RA System using a Certificate); and

(vi) Any Trusted Registrar who has direct access to an RA Application must authenticate himself or herself to the RA Application with an assurance level that is no less than any Certificate that the Trusted Registrar issues.

(b) Liability

(i) The Subscribing Customer is solely responsible for the failure of a Trusted Registrar to fulfill any obligations of this Section 4.1.2.3.

4.1.2.3 RA Obligations

RA obligations are set forth in the WS CP, this WS CPS and other applicable PKI Documents. The RA is responsible for:

(a) Obtaining the requisite authority from the Subscriber to undertake I & A of potential Subjects on the Subscriber's behalf;

(b) Performing I & A of potential Subjects to be named in Certificates to be issued to the Subscriber; and

(c) Taking all steps to ensure that any I & A information regarding potential Subjects is complete and accurate; and

(d) All RAs that have direct access to an RA Application must authenticate themselves to the RA Application using their WellsSecure Digital IDs at the Basic Assurance Level or the Medium Assurance Level only.

4.1.2.4 Subject Obligations

Subject obligations are set forth in the WS CP, this WS CPS and other applicable PKI Documents. These include, but are not limited to, providing accurate information in all aspects of the Registration Process and the issuance of the Certificate.

4.2 Certificate Application Processing

See Section 4.1.2.

4.2.1 Performing Identification And Authentication Functions

See Section 4.1.2.

4.2.2 Approval Or Rejection Of Certificate Applications

See Section 4.1.2.

4.2.3 Time To Process Certificate Applications

No stipulation.

4.2.4 DNS Certification Authority Authorization (CAA)

The WellsSecure PKI does not review CAA records.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Once the Registration Process is completed, the Subject is approved for a Certificate, and the WellsSecure Issuing CA has received and verified a request from either the Subscribing Customer, or the RA on the Subscribing Customer's behalf, to issue a Certificate, the WellsSecure Issuing CA will take reasonable steps to:

(a) Ensure that the applicable I & A Procedures required by Section 4.1 have been completed;

(b) Verify the source of the request before issuing the Certificate;

(c) Generate a Certificate, containing appropriate Public Keys, OIDs and Activation Data, naming:

(i) the Subscribing Customer; and

(ii) the Organization, Individual, Device or System as the Subject in the "Common Name (cn)" section of the "Subject" field of that Certificate;

(d) Notify the RA of the Certificate's issuance using a reasonably secure and confidential method;

(e) Deliver the Certificate, and where a Token is used to store the Key Pair and Certificate, the Token to the RA or Subscribing Customer, as appropriate, using a reasonably secure and confidential method (e.g. USPS or commercial delivery service using tamper resistant packaging provided by that commercial delivery service for Tokens, or password protected PDF containing access or activation information);

(f) Ensure that if any RA delivers the Certificate, and where a Token is used to store the Key Pair and Certificate, the Token, to the Subscribing Customer using an appropriate delivery method (e.g. USPS or commercial delivery service using tamper resistant packaging provided by that commercial delivery service for Tokens, or digitally signed emails or password protected PDFs for software stored Certificates) and that the Activation Data has been separately and securely sent (e.g. via USPS, password protected PDF, or via phone, pursuant to appropriate authentication procedures; and

(g) For purposes of this WS CPS, Certificates will be deemed "delivered" when actually received by the Subscribing Customer or the Subject named in the "Common Name (cn)" section of the Certificate's Subject field.

4.3.2 Notification To Subscriber By The CA Of Issuance Of Certificate

See Section 4.3.1.

4.3.3 Shared Key Issuance

For cases where there are several affiliated Individuals acting in one capacity on behalf of a single Subscribing Customer, a Certificate may be issued that corresponds to a Private Key that is shared by these Individuals (hereinafter referred to as a "Shared Key"). In these cases:

(a) The subjectName DN must not imply that the subject is a single Individual, e.g. by inclusion of a human name form; and

(b) Organization Certificates must be issued with OIDs at the following Assurance Levels: Company Low, Company Basic, or Company Medium as set forth in Section 1.2.2 above for situations that involve Shared Keys.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Any use of a Certificate's Private Key by the Subject defined in that Certificate is deemed an acknowledgment of acceptance.

4.4.2 Publication Of The Certificate By The CA

No stipulation.

4.4.3 Notification Of Certificate Issuance By The CA To Other Entities

All cross-certified entities shall be notified upon issuance of new inter-organizational CA Cross-Certificates.

4.5 Key Pair And Certificate Usage

4.5.1 Subscriber Private Key And Certificate Usage

4.5.1.1 Subscribing Customers

For Low, Medium Hardware, Medium, and Basic Assurance, Subscribers shall protect their Private Keys from access by other parties. For all other Assurance Levels, there is no stipulation. High Assurance Level is not supported by WellsSecure PKI.

Restrictions in the intended scope of usage for a Private Key are specified through Certificate extensions, including the key usage and extended key usage extensions, in the associated Certificate.

In accordance with the WS CP, this WS CPS and other applicable PKI Documents, a Subscribing Customer is responsible for the obligations set forth in Subsections (a) through (j) below. Any Individuals authorized by a Subscribing Customer to act on its behalf may perform these Subscribing Customer's obligations, as set forth in this Section or elsewhere in the WS CP, this WS CPS, or other applicable PKI Documents. For example, a Subscribing Customer may authorize one or more Individuals, acting as Applicants, to undertake the Registration Process on its behalf. In all events, the Subscribing Customer bears full and sole responsibility for each such Individual's performance or failure of performance undertaken by any Individual acting on the Subscribing Customer's behalf regardless of capacity.

The Subscribing Customer's specific obligations regarding Private Key and Certificate usage are as follows:

(a) Authorizing Applicants to commence the Registration Process on its behalf;

(b) Appointing and authorizing, wherever expressly permitted by the RA, certain Individuals to act as Trusted Registrars;

(c) Ensuring that each Applicant provides complete and accurate information during the Registration Process regarding:

(i) the Applicant's relationship to the Subscribing Customer;

(ii) the Applicant's authority to represent both the Subscribing Customer and the Subject; and

(iii) the identity of the Applicant, Subscribing Customer, and Subject.

(d) Providing complete and accurate responses to all requests for information made by the RA during the Registration Process or thereafter;

(e) Ensuring, for any Certificate issued to the Subscribing Customer that for the duration of such Certificate's operational period:

(i) such Certificate is used in accordance with the provisions of the WS CP, this WS CPS and other applicable PKI Documents;

(ii) such Certificate is reviewed within seven (7) days after delivery for completeness and accuracy of information;

(iii) such Certificate is accepted or rejected within seven (7) days after delivery; and

(iv) all necessary precautions are taken to protect the confidentiality of all Private Keys and Activation Data.

(f) Immediately notifying the WellsSecure Issuing CA or the RA that administered the Registration Process for a Certificate of:

(i) any actual or suspected compromise of the Private Key or Activation Data for such Certificate;

(ii) any change in the relationship between the Subscribing Customer and the Subject named in such Certificate; and

(iii) any other change in information or circumstance that affects the accuracy or completeness of information contained in such Certificate.

(g) Immediately requesting the WellsSecure Issuing CA or the RA that administered the Registration Process for the Certificate to Revoke or Suspend such Certificate upon known or suspected loss, disclosure, or other compromise of the Private Key corresponding to the Public Key listed in the Certificate or of the Activation Data;

(h) Ensuring that it's Private Key or Certificate is not used in connection with any of the following transactions:

(i) those prohibited by applicable law or the applicable PKI Documents; or

(ii) those for which the Subscribing Customer is not acting either as principal or as agent for a principal that has been disclosed to the WellsSecure Issuing CA;

(i) Otherwise complying fully with all terms and conditions of participating in the WellsSecure PKI as set forth in the WS CP, this WS CPS or other applicable PKI Documents; and

(j) Documenting that all Individual Subjects acknowledge his or her obligations respecting protection of the Private Key and use of the Certificate before being issued the Certificate.

4.5.2 Relying Party Public Key And Certificate Usage

(a) Obligations

A Relying Party is expected to fulfill the following obligations:

(i) Ensure that its reliance on any Certificate is reasonable and prudent in light of all available information;

(ii) Act in good faith in light of all circumstances that were known or should have been known to it at the time of reliance;

(iii) Follow all other requirements of PKI Documents that are publicly available or otherwise provided to the Relying Party; and

(iv) Comply with all obligations in any agreement between the Relying Party and WFBNA related to the WellsSecure PKI.

(b) Assumption of Risk and Liability

A Relying Party assumes, without limitation, all risks and liability arising from any decision to rely on a Certificate if: (i) the Validation Service returns a response of Revoked or Unknown; or (ii) the Relying Party knows or has reason to know of any facts that would cause a person of ordinary business prudence to refrain from relying on the Certificate; or (iii) if the Relying Party fails to successfully receive a Validation Service response for any reason, including, but not limited to, not making the validation request.

4.5.3 Obligations Relating To Validation Service

The following is a general description of the Validation Service and its requirements.

(a) Validation Service Request

A Relying Party seeking to rely on or use a Subscribing Customer's Encryption or Signing Certificate must issue a Validation Service request to the WellsSecure PKI. A Validation Service request could be either an OCSP request to the appropriate WellsSecure OCSP Responder or a request to download the latest CRL available from the CA.

(b) OCSP Response

In the case of an OCSP request, the WellsSecure OCSP responder will Issue a status response of "Good," "Revoked" or "Unknown" as appropriate.

(c) Reliance

Where the result of any Validation Service request regarding Certificate status is either "Revoked" or "Unknown", any reliance upon such a Certificate is taken at the Relying Party's own risk and it assumes sole and full responsibility for any liabilities, losses, damages or claims that may arise out of or in connection with such reliance.

(d) CRL Request

In the case of a request to download the latest available CRL, the WellsSecure Repository will provide said CRL via a standard Internet communication protocol (typically http or LDAP). The most current CRL available for download may not necessarily reflect the most current status information for a given Subscribing Customer's Certificate; therefore a Relying Party is strongly encouraged to use OCSP instead of CRL validation wherever possible.

4.6 Certificate Renewal

The WellsSecure PKI does not support Certificate renewal. However, Certificates may be Reissued pursuant to the procedures set forth in Section 4.3. Certificate Reissuance includes issuance of a new Certificate consisting of a new Serial Number, new Validity Period, and may also include new information for other Certificate fields. See Section 5.6.1 for Certificate Reissuance.

4.6.1 Circumstance For Certificate Renewal

No stipulation.

4.6.2 Who May Request Renewal

No stipulation.

4.6.3 Processing Certificate Renewal Requests

No stipulation.

4.6.4 Notification Of New Certificate Issuance To Subscriber

No stipulation.

4.6.5 Conduct Constituting Acceptance Of A Renewal Certificate

No stipulation.

4.6.6 Publication Of The Renewal Certificate By The CA

No stipulation.

4.6.7 Notification Of Certificate Issuance By The CA To Other Entities

No stipulation.

4.7 Certificate Re-Key

The WellsSecure PKI does not support Certificate re-key. However, Certificates may be Reissued pursuant to the procedures set forth in Section 4.3. Reissuance requests shall only be accepted from the Subject of the Certificate or corresponding Subscribing Customer. Additionally, CAs and RAs may initiate reissuance of a Certificate without a corresponding request.

4.7.1 Circumstance For Certificate Re-Key

No stipulation.

4.7.2 Who May Request Certification Of A New Public Key

No stipulation.

4.7.3 Processing Certificate Re-Keying Requests
No stipulation.

4.7.4 Notification Of New Certificate Issuance To Subscriber
No stipulation.

4.7.5 Conduct Constituting Acceptance Of A Re-Keyed Certificate
No stipulation.

4.7.6 Publication Of The Re-Keyed Certificate By The CA
No stipulation.

4.7.7 Notification Of Certificate Issuance By The CA To Other Entities
No stipulation.

4.8 Certificate Modification
The WellsSecure PKI does not support Certificate modification. However, Certificates may be Reissued pursuant to the procedures set forth in Section 4.3.

4.8.1 Circumstance For Certificate Modification
No stipulation.

4.8.2 Who May Request Certificate Modification
No stipulation.

4.8.3 Processing Certificate Modification Requests
No stipulation.

4.8.4 Notification Of New Certificate Issuance To Subscriber
No stipulation.

4.8.5 Conduct Constituting Acceptance Of Modified Certificate
No stipulation.

4.8.6 Publication Of The Modified Certificate By The CA
No stipulation.

4.8.7 Notification Of Certificate Issuance By The CA To Other Entities
No stipulation.

4.9 Certificate Revocation And Suspension

4.9.1 Circumstances For Revocation

4.9.1.1 Request Made By A WellsSecure PKI Entity
The WellsSecure Issuing CA must Revoke a Certificate it has issued, and its RA must request Revocation of any Certificate it has requested the WellsSecure Issuing CA to issue, if, at any time either has knowledge or a reasonable basis for believing that any of the following events have occurred:

(a) The WellsSecure Issuing CA that issued the Certificate has ceased operations for any reason;

(b) Revocation of the WellsSecure Issuing CA's Certificate used to issue the Certificate in question;

(c) The Subscribing Customer’s Private Key for that Certificate has been compromised;

(d) Violation by the Subscribing Customer of any of its material obligations;

(e) Any material change in the information contained in the Certificate (e.g., Incapacity of the Organization to perform business activities due to bankruptcy, dissolution, acquisition, or otherwise, or termination of the Subject's employment or authorization to act on behalf of the Subscribing Customer);

(f) The Subscribing Customer's failure to pay fees as required;

(g) A determination, in the WellsSecure Issuing CA's or RA's sole discretion, that the Certificate was not issued in accordance with the terms and conditions of the WS CP, this WS CPS or other applicable PKI Documents;

(h) The Certificate in question has been Suspended for more than the allowable grace period as set forth in Section 4.9.16;

(i) Upon receipt of an authenticated Certificate Revocation request from an Individual or Organization authorized by the WS CP or this WS CPS to request Revocation; or

(j) A determination by the WellsSecure Issuing CA or RA that continued use of the Certificate is inappropriate or injurious to the proper functioning or intent of the WellsSecure PKI.

In all other circumstances, the WellsSecure Issuing CA may Revoke a Certificate it has issued at its sole discretion, provided such Revocation does not violate a Subscribing Customer's rights under the WS CP, this WS CPS or the applicable Customer Agreement.

4.9.1.2 Request Made By Subscribing Customer Or Subject

A Subscribing Customer or Subject must request Revocation of a Certificate when:

(a) Any material information in the Certificate changes or becomes obsolete;

(b) The Private Key associated with the Public Key listed in the Certificate, or the media holding such Private Key, is known to have been compromised; or

(c) The Activation Data for the Private Key associated with the Public Key listed in the Certificate is known, or is suspected, to have been compromised.

In all other circumstances, the Subscribing Customer may request, at its discretion, the Revocation of a Certificate that the Subscribing Customer originally requested or authorized the issuance of; Revocation of a Certificate may also be requested at the discretion of the Individual identified in the "Common Name (cn)" section of the Certificate's "Subject" field.

4.9.2 Who Can Request Revocation

Certificate Revocation can be initiated by:

(a) The Subscribing Customer that originally requested or authorized the issuance of the Certificate in question;

(b) The Individual identified in the "Subject" field of a Signing Certificate or Encryption Certificate;

(c) The RA that administered the Registration Process that resulted in the Certificate's issuance;

(d) The WellsSecure Issuing CA that issued the Certificate, or

(e) The TR associated with the issuance of the Certificate.

4.9.3 Procedure For Revocation Request

The requestor can submit the request to an RA in one of three ways.

1) The requestor can send a digitally signed e-mail with information identifying the Certificate and their reason for revocation.

2) The requestor can also contact the RA either in person or via the telephone if able to provide adequate proof of identification.

3) The requestor can log into a web site provided by the RA for the purposes of managing their own Certificates. After suitably authenticating themselves to the web site, the user can request revocation of Certificates s/he owns.

Additional stipulations:

(a) All Certificate Revocation requests must be made to either the WellsSecure Issuing CA or the RA that administered the Registration Process for the Certificate to be Revoked. All Certificate Revocation requests must identify the Certificate to be Revoked, include a reason for the request (e.g., suspected Private Key compromise), and must be authenticated (e.g., digitally or manually signed). The reason for Revocation will be stored in the Directory and in CRLs, and may accompany any Validation Service responses thereafter.

(b) A Subscribing Customer may, depending on availability and implementation, submit its Revocation request via the Internet, or by phone or e-mail, depending on the Subscriber and the associated level of authorization in the Subscriber's Certificate.

(c) In connection with a Revocation request, the WellsSecure Issuing CA or the RA that administered the Registration Process for the Certificate to be Revoked shall have the following obligations:

(i) For all Revocation requests, the WellsSecure Issuing CA or RA will be required to perform I & A of the requestor. After performing appropriate I & A, as specified in the applicable authentication policy, the WellsSecure Issuing CA or RA may in its sole discretion and subject to the provisions of Section 4.9.5, immediately Revoke or Suspend the Certificate in question. Suspension does not apply to SSL certificates;

(ii) For all requests, regardless of method, and prior to confirming the identity or authority of the requestor, the WellsSecure Issuing CA or RA receiving such a request may, in its sole discretion, immediately Suspend the Certificate pending further investigation. In such event, the WellsSecure Issuing CA or RA will bear no liability for Suspending or refusing to Suspend the Certificate in question. Suspension does not apply to SSL certificates;

(iii) The WellsSecure Issuing CA or RA will send an acknowledgment to the requestor that the Revocation request has been received. Following delivery of this acknowledgement, the WellsSecure Issuing CA or RA will take reasonable steps to process the request before the next CRL is published.

(iv) In circumstances where a request has been received but I & A cannot be immediately completed, the WellsSecure Issuing CA or RA should request Certificate Suspension as soon as practical, until such time as the identity and authority of the requestor is sufficiently established or the Suspension Grace Period Expires as set forth in Section 4.9.16, at which time the Certificate must be Revoked. Suspension does not apply to SSL certificates; and

(v) Revoked Certificates shall be included on all new publications of the Certificate status information until the Certificates expire.

(d) Acknowledgment of a Revocation request may be done by e-mail, phone or Fax to the Subscribing Customer of the Certificate in question. The details of how a Subscribing Customer and Subject are notified that their Certificate has been Revoked are contained within the applicable Customer Agreement.

4.9.4 Revocation Request Grace Period

No stipulation.

4.9.5 Time Within Which CA Must Process The Revocation Request

WellsSecure takes commercially reasonable steps to process revocation requests without delay.

4.9.6 Revocation Checking Requirement For Relying Parties
A Relying Party must use the Validation Service prior to relying on any Certificate. Reliance without using the Validation Service will be considered an unreasonable reliance on the Certificate in question.

4.9.7 CRL Issuance Frequency
See Section 2.4 for information to access CRLs or OCSPs. The specific frequency of CRL issuance for each CA is outlined below.

4.9.7.1 WellsSecure Public Root CA And WellsSecure Public Root CA 01 G2 CRLs
Information relating to the status of a Certificate issued by the WellsSecure Public Root CA or WellsSecure Public Root CA 01 G2, as being Suspended or Revoked, will be published to the Repository a minimum of once every three hundred and sixty five (365) days and within a commercially reasonable time whenever a PKI Component Certificate is revoked.

4.9.7.2 Subordinate CA CRLs
WellsSecure takes commercially reasonable steps to publish Information relating to the status of a Certificate issued by a WellsSecure Sub-CA, as being Suspended or Revoked, including the CRLs created by any CA, to the Repository without delay.

4.9.8 Maximum Latency For CRLs
CRLs shall be published no later than the time specified in the “nextUpdate” field of the previously issued CRL.

4.9.9 On-Line Revocation/Status Checking Availability
The WellsSecure OCSP Responder may be used by a Relying Party to verify the status of Subscribing Customer Certificates. The WellsSecure OCSP Responder will verify Certificate status information by checking the Directory. The WellsSecure OCSP Responder will generate a Certificate status response of Good, Revoked or Unknown depending on the information contained in the Directory or from other sources. The Relying Party acknowledges that cached status information may be used in providing a Certificate status response and accepts and solely assumes any risk associated with relying on such cached information. The Relying Party has the option of specifically requesting that the WellsSecure OCSP Responder use new information when verifying the status of a Certificate and acknowledges their using new information may result in a significant delay in the WellsSecure OCSP Responder responding to the Validation Services request.

4.9.10 On-Line Revocation Checking Requirements
See Section 4.9.6.

4.9.11 Other Forms Of Revocation Advertisements Available
No stipulation.

4.9.12 Special Requirements Regarding Key Compromise
If a Subscriber suspects that its Private Key has been compromised, that Subscriber must immediately initiate a Revocation or Suspension request as set forth in Section 4.9.3 of the WS CP and this WS CPS. In such request, the Subscriber must specify that the reason for the request is suspected or known key compromise. Suspension does not apply to SSL certificates.

4.9.12.1 Emergency Publication Of Root CA CRL
In the event of an issuing sub-CA Private Key is revoked for any reason, the WellsSecure Public Root CA or WellsSecure Public Root CA 01 G2 shall:

a) Take commercially reasonable steps to provide notice to any organizations with which the WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2, or any Sub CA, is cross-certified without delay.

b) Take commercially reasonable steps to generate and publish a new CRL without delay.

4.9.13 Circumstances For Suspension

In conformance with the CA/B Forum Baseline Requirements WellsSecure does not support suspension of SSL certificates.

Personal certificates may be Suspend for any of the reasons listed in Section 4.9.1 or the following:

(i) There is an unverified suspicion of Private Key compromise;

(ii) The Subscribing Customer fails to meet any of its obligations under the applicable Customer Agreement;

(iii) The Customer requests Suspension; or

(iv) The WellsSecure Issuing CA or the RA determines, in its sole discretion, that continued usage of the Certificate in question would jeopardize the effective functioning of the WellsSecure PKI.

4.9.14 Who Can Request Suspension

Certificate Suspension/Reinstatement can be requested by anyone listed in Section 4.9.2 of this WS CPS.

4.9.15 Procedure For Suspension Request

Any individuals cited in Section 4.9.2 that have the responsibility and authorization to request a Certificate revocation may also request a Certificate suspension. Process in Section 4.9.3 is followed to request Suspension of a Certificate. Upon receiving the suspension request, the RA then notifies the technical contact for that Certificate of the suspension, except in the case of a web site request, in which case the Certificates are suspended immediately.

In all cases, the processing time for Suspension requests will be the same as for Revocation requests as set forth in Section 4.9.5.

Reinstatement requests may only be made by phone, in-person, or in writing and must be authenticated according to applicable I & A procedures for the WellsSecure Issuing CA or the RA to whom such request is made. The details of how a Subscribing Customer and/or Subject are notified that their Certificate has been Suspended are contained within the applicable Customer Agreement.

4.9.16 Limits On Suspension Period

No Stipulation

4.10 Certificate Status Services

See Section 4.9.9.

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

No stipulation.

4.10.3 Optional Features

No stipulation.

4.11 End Of Subscription

No stipulation.

4.12 Key Escrow And Recovery

Only certain types of keys are escrowed within the WellsSecure PKI. See Section 6.1.1.2.

4.12.1 Key Escrow And Recovery Policy And Practices
No stipulation.

4.12.2 Session Key Encapsulation And Recovery Policy And Practices
No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

This Section describes the non-technical security controls of a physical, procedural, and personnel nature that are implemented by the WellsSecure PKI. These controls are intended to provide a secure environment for Key Pair generation, Applicant I & A, Certificate issuance, Certificate Suspension or Revocation, audit, and archival activities. Physical, Procedural and Personnel security controls are also governed by Wells Fargo security policies. These policies are set forth in Wells Fargo documents.

5.1 Physical Controls

The WellsSecure PKI has in place appropriate physical security controls to restrict access to all hardware and software (including the server, work stations, and any external cryptographic hardware modules or Tokens) used in connection with providing CA Services. Access to such hardware and software is limited to those personnel performing in a trusted role as described in Section 5.2.1. Access is controlled through the use of electronic access controls, mechanical combination lock sets, deadbolts, or other security mechanisms. Such access controls are manually or electronically monitored for unauthorized intrusion at all times. Only authorized personnel will be allowed access, either physical or logical, to the WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2, Sub-CAs, RA, Repository, and OCSP Responder.

(a) The physical security requirements are designed to:

- (i) Ensure no unauthorized access to the hardware is permitted;
- (ii) Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers;
- (iii) Ensure manual or electronic monitoring for unauthorized intrusion at all times;
- (iv) Ensure an access log is maintained and inspected periodically; and
- (v) Require two-person physical access control to both the cryptographic module and computer system.

5.1.1 Site Location And Construction

The WellsSecure PKI is operated in secure, geographically diverse data centers maintained by Wells Fargo.

5.1.2 Physical Access

Specific details of physical security are excluded for security reasons. Additional details are available on a strictly need-to-know basis; see Section 1.5.2 for contact information.

5.1.2.1 WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2 And Sub-CAs

The WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2 and Sub-CA Systems are located and operated from a Wells Fargo secure facility. These secure facilities are staffed 24 hours a day every day of the year. Detailed security procedures shall be described within the WellsSecure CP.

5.1.2.2 Offsite Records Storage

Records are stored in secure facilities managed through a centralized service provider within Wells Fargo.

5.1.2.3 Cryptographic Modules

Removable cryptographic modules, activation information used to access or enable cryptographic modules, and other sensitive CA equipment shall be placed in secure containers when not in use. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

5.1.2.4 Systems Hosting RA Application

The Systems that the RA uses to host any external applications and the workstations that allow administrator access to the WellsSecure RA Application are located in appropriate secured areas within Wells Fargo data centers, and are consistent with the physical security requirements that are set forth in

the WellsSecure CP and this WS CPS. Any RAs that are not under the direct control of the WellsSecure PKI are required to conform to the RA Agreement (for business units not within WFBNA) that is consistent with the WellsSecure CP and this WS CPS.

5.1.2.5 Wells Fargo Repository

The Systems that host the Wells Fargo Repository are located in appropriate secured areas and are consistent with the physical security requirements that are set forth in the WellsSecure CP and CPS.

5.1.3 Power And Air Conditioning

The WellsSecure PKI facility operates power and air conditioning mechanisms sufficient to support the operation of the Systems used to provide CA Services. Systems that provide power are maintained in a configuration that shall have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. Oracle's features, along with UPS servers ensure transactional integrity.

5.1.4 Water Exposures

The WellsSecure PKI has taken reasonable steps to ensure that its Systems are protected from water exposure.

5.1.5 Fire Prevention And Protection

The WellsSecure PKI has taken reasonable steps to ensure that its Systems are protected with an appropriate fire suppression System.

5.1.6 Media Storage

The WellsSecure PKI has taken reasonable steps to ensure that storage media used by it are protected from environmental threats such as temperature, humidity, and magnetism.

5.1.7 Waste Disposal

The WellsSecure PKI has taken reasonable steps to ensure that all media that stores or references Confidential Information or other sensitive confidential information, such as Key Pairs, Activation Data or its files, are sanitized or destroyed before released for disposal. Detailed waste disposal procedures shall be described within the WellsSecure CPS.

5.1.8 Off-Site Backup

Backups are stored in secure facilities managed through a centralized service provider within Wells Fargo.

5.2 Procedural Controls

5.2.1 Trusted Roles

(a) A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The Individual selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the WellsSecure PKI's CAs. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the Individual filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion. The requirements of the WS CP and this WS CPS are defined in terms of four roles.

5.2.1.1 Operator

An Operator is responsible for:
(a) installation, configuration, and maintenance of the CA;
(b) establishing and maintaining CA system accounts;
(c) configuring Certificate profiles or templates and audit parameters, and

(d) generating and backing up CA Keys.

Operators may only issue PKI Component Certificates.

5.2.1.2 Officer

An Officer is responsible for issuing Certificates, that is:
(a) registering new Applicants and requesting the issuance of Certificates;
(b) verifying the identity of Applicants and accuracy of information included in Certificates;
(c) approving and executing the issuance of Certificates, and
(d) requesting, approving and executing the Revocation of Certificates.

5.2.1.3 Auditor

An Auditor is responsible for:
(a) Reviewing, maintaining, and archiving audit logs; and
(b) Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with the WS CP and this WS CPS.

5.2.1.4 Administrator

An Administrator is responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.2 Number Of Persons Required Per Task

Only one Individual is required per task for CAs operating at the Low and Basic Levels of Assurance. Two or more Individuals are required for CAs operating at the Medium (all policies), or High Levels of Assurance for the following tasks:

(a) CA Key generation;

(b) CA Signing Key activation; and

(c) CA Private Key backup.

Where multiparty control for logical access is required, at least one of the Individuals shall be an Administrator. All Individuals must serve in a Trusted Role as defined in Section 5.2.1. Multiparty control for logical access shall not be achieved using Individuals that serve in the Auditor Trusted Role. Physical access to the CAs does not constitute a task as identified in this Section**.** Therefore, two-person physical access control may be attained as required in this Section and Section 5.1(b) (v).

5.2.3 Identification And Authentication For Each Role

At all Assurance Levels other than Low, an Individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.2.4 Roles Requiring Separation Of Duties

Role separation, when required as set forth below, may be enforced either by the CA equipment, or procedurally, or by both means. Requirements for the separation of roles, and limitations on use of procedural mechanisms to implement role separation, are described below for each level of assurance:

Table 5.1: Role Separation Rules

Assurance Level	Role Separation Rules
Low	No stipulation
Basic	Individuals shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role; however, no one Individual shall assume both the Officer and Administrator roles. This may be enforced procedurally. No Individual shall be assigned more than one identity.

Assurance Level	Role Separation Rules
Medium	Individuals shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may only assume one of the Officer, Administrator, Operator, and Auditor roles, The CA and RA Systems shall identify and authenticate their users and shall ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, nor assume both the Auditor and Officer roles. No Individual shall have more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, And Clearance Requirements

The WellsSecure PKI will enforce appropriate personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of its Personnel and of the satisfactory performance of their duties in a manner consistent with the WS CP and this WS CPS. All Individuals filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity.

5.3.2 Background Check Procedures

The Wells Fargo Human Resources department conducts background checks of WellsSecure PKI employees. Contract Agencies conduct background checks of managed resources.

5.3.3 Training Requirements

Individuals performing duties in the operation of a WellsSecure PKI's CA or RA will receive appropriate training in areas commensurate with the performing of their jobs.

5.3.4 Retraining Frequency And Requirements

Retraining will occur when a Wells Fargo or RA Personnel's duties change because that Employee will be performing a new role, when a new System or procedural upgrade is implemented, or for other reasons, at the discretion of Wells Fargo PKI Management, according to the training plan.

5.3.5 Job Rotation Frequency And Sequence

No stipulation.

5.3.6 Sanctions For Unauthorized Actions

The WellsSecure PKI will impose sanctions, including suspension and termination if appropriate, for its Personnel acting in trusted roles if they perform unauthorized actions, abuse their authority, or for other appropriate reasons, at Wells Fargo PKI Management's discretion.

5.3.7 Independent Contractor Requirements

The WellsSecure PKI may employ independent third party contractors to perform services associated with the operation and management of the WellsSecure PKI entities. Such contractors are bound to security and confidentiality requirements at least as restrictive as those applicable to WellsSecure PKI Employees.

5.3.8 Documentation Supplied To Personnel

The WellsSecure PKI will make the following documentation available as appropriate to its Personnel:

(a) This WS CPS;

(b) The WS CP;

(c) Hardware and software documentation related to the operation of the WellsSecure Issuing CA;

(d) Published Wells Fargo documentation that affects operation of the WellsSecure Issuing CA and its RA;

(e) Documentation identifying all personnel who received training and the level of training completed; and

(f) Appropriate other documents as necessary.

5.4 Audit Logging Procedures

5.4.1 Types Of Events Recorded

All WellsSecure PKI's CAs and RAs will record System and CA application events, and will create Certificate management logs. Auditable events, which can be digitally signed, will be digitally signed from the data collected in accordance with audit procedures. All security auditing capabilities of the WellsSecure Issuing CA operating System and CA applications required by the WS CP and this WS CPS shall be enabled. The following events will be recorded and the records regarding such events shall be made available during compliance audits:

(a) Auditable Events

(i) Security Audit

(A) Any changes to the Audit parameters, e.g., audit frequency, type of event audited.

(B) Any attempt to delete or modify the Audit logs.

(ii) Identification and Authentication

(A) Change in the value of maximum authentication attempts.

(B) Maximum number of unsuccessful authentication attempts during user login.

(C) An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts.

(D) An Administrator changes the type of authenticator, e.g., from password to biometrics.

(E) The number of unsuccessful authentication attempts exceeds the maximum authentication attempts during user login

(iii) Private Key load and storage

(A) The loading of Component Private Keys.

(B) All access to Certificate subject Private Keys retained within the CA for key recovery purposes.

(iv) Trusted Public Key entry, deletion and storage

All changes to the trusted Public Keys, including additions and deletions.

(v) Private Key export

The export of Private Keys (keys used for a single session or message are excluded).

(vi) Certificate Status change approval

The approval or rejection of a Certificate status change request.

(vii) Account administration

(A) Roles and users are added or deleted.

(B) The access control privileges of a user account or a role are modified.

(C) Successful and unsuccessful attempts to assume a role

(viii) Certificate profile management

All changes to the Certificate profile.

(ix) Revocation profile management

All changes to the Revocation profile.

(x) Certificate Revocation List profile management

All changes to the Certificate Revocation list profile.

(xi) Miscellaneous

(A) Installing hardware cryptographic modules.

(B) Removing hardware cryptographic modules.

(C) Destruction of cryptographic modules.

(D) Receipt of Hardware / Software.

(E) Attempts to set passwords.

(F) Attempts to modify passwords.

(G) Backing up CA database.

(H) Restoring CA database.

(I) File manipulation (e.g., creation, renaming, moving).

(J) Posting of any material to a Repository.

(K) Access to CA database.

(L) All Certificate compromise notification requests.

(M) Loading Tokens with Certificates.

(N) Zeroizing Tokens.

(O) Rekey of the CA.

(P) All security-relevant data that is entered in the System locally

(Q) All security-relevant messages that are received by the System remotely

(R) All successful and unsuccessful requests for security-relevant information

(S) The manual entry of secret keys used for authentication

(T) Shipment of Tokens

(U) Obtaining a third party time stamp

(V) Whenever the CA generates a Private Key

(W) All Certificate requests

(X) All Certificate revocation requests

(Y) Any security relevant changes to the configuration of the CA

(Z) Appointment of an Individual to a trusted role

(AA) Designation of personnel for multi-party control

(BB) Installation of the operating system

(CC) Installation of the CA

(DD) System start up

(EE) Logon attempts to CA applications

(FF) Configuration changes to the CA involving the following:

(i) Hardware

(ii) Software

(iii) Operating System

(iv) Patches

(v) Security profiles

(xii) Physical access / site security

(A) Personnel access to room housing CA.

(B) Access to the CA server.

(C) Known or suspected violations of physical security.

(xiii) Anomalies

(A) Software error conditions.

(B) Software check integrity failures.

(C) Receipt of improper messages.

(D) Misrouted messages.

(E) Network attacks (suspected or confirmed).

(F) Equipment failure.

(G) Electrical power outages.

(H) Uninterruptible Power Supply (UPS) failure.

(I) Obvious and significant network service or access failures.

(J) Violations of Certificate Policy.

(K) Violations of Certification Practice Statement.

(L) Resetting Operating System clock.

(b) Additional information requirements

The WellsSecure PKI will collect event information and create Certificate management logs using automated and manual practices and procedures that are internal to the WellsSecure PKI. All recorded events on the audit log, which can be digitally signed, shall be digitally signed and include the following information:

(i) The date and time of the event, identity of the Individual performing the event, type of event and success or failure of the event; and

(ii) The origin of the request for identification events (e.g., workstation identifier).

5.4.2 Frequency Of Processing Log

Audit logs shall be reviewed in accordance with the table below. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the log. Examples of irregularities include without limitation

discontinuities in the logs and loss of audit data. Actions taken as a result of these reviews shall be documented.

Table 5.2: Audit Log Review Frequency

Assurance Level	Review Audit Log
Low	Only required for cause
Basic	Only required for cause
Medium (all policies)	At least once every two (2) months. Statistically significant set of security audit data generated by the WellsSecure PKI's CA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity

5.4.3 Retention Period For Audit Log

Audit logs are kept for a period of at least seven (7) years, or longer if required by law. Audit logs shall be retained onsite until reviewed. This retention period includes the time for archived records (see Section 5.5.2).

5.4.4 Protection Of Audit Log

Audit logs will be: (a) protected from unauthorized access, modification, or deletion by appropriate operating system and security mechanisms, (b) protected from deletion or destruction prior to the end of the audit log retention period, and (c) moved to a safe, secure storage location separate from the WellsSecure PKI's CA equipment.

5.4.5 Audit Log Backup Procedures

Each WellsSecure Issuing CA performs incremental backups and full weekly backups on all electronic audit logs detailed in Section 5.4.1 above and stores such backups at a secure storage location separate from the WellsSecure Issuing CA equipment.

5.4.6 Audit Collection System (Internal Vs. External)

Audit processes shall be invoked at System startup, and cease only at System shutdown. Should it become apparent that an automated audit System has failed, and the integrity of the System or confidentiality of the information protected by the System is at risk, then the Certification Authority Administrator shall determine whether to Suspend the operation of the WellsSecure PKI (or the affected component(s) thereof) until the problem is remedied.

5.4.7 Notification To Event-Causing Subject

There is no notification requirement when an event is audited. However, the WellsSecure PKI must be notified when a process or action causes a critical security event or discrepancy. The WellsSecure PKI will investigate the event or discrepancy and will notify the affected Participants if, in its sole discretion, notification is warranted by the circumstances.

5.4.8 Vulnerability Assessments

Each WellsSecure Issuing CA will conduct annual vulnerability assessments for itself and all RAs, Repositories and OCSP Responders under its authority. The WellsSecure Issuing CA will provide a standard program for conducting vulnerability assessments, including routine assessments for evidence of malicious activity, and a standard format for reporting results.

5.5 Records Archival

5.5.1 Types Of Records Archived
Records archived include:

a) Audit records
b) Certificate application documents and information
c) Certificate lifecycle documents and information
d) Certificates, including Public Keys
e) Certificates, including Private keys (for key pairs generated by the WS PKI)
f) Additional documents relevant to the WS PKI.

5.5.2 Retention Period For Archive
Archived records must be retained for at least seven (7) years, or longer as required by law. Archived records will be made available for compliance audits. See Section 5.4.3 for Audit Log retention.

5.5.3 Protection Of Archive
The archive media is physically and environmentally protected and stored at a secured off-site location. No unauthorized user shall be permitted to write to, modify, or delete the archive. The contents of the archive shall not be released except in accordance with [Sections 9.3 and 9.4]. Records of individual transactions may be released upon request of any Subscribing Customers involved in the transaction or their legally recognized agents.

5.5.4 Archive Backup Procedures
Backup and recovery procedures are in place so that a complete set of backup copies will be available in the event of the loss or destruction of the primary archives. Incremental backups are performed daily and full backups are performed weekly.

5.5.5 Requirements For Time-Stamping Of Records
Automated records include a system generated time and date provided by a synchronized reliable time service.

5.5.6 Archive Collection System (Internal Or External)
The archive collection system is internal to the WellsSecure Issuing CA.

5.5.7 Procedures To Obtain And Verify Archive Information
Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

5.6 Key Pair Changeover
The WellsSecure PKI does not support automatic Key Pair changeover. However, Certificates may be Reissued pursuant to the procedures set forth in Sections 5.6.1, 5.6.2, and 5.6.3.

5.6.1 WellsSecure Sub-CA Certificate Reissuance
A WellsSecure Sub-CA's Certificate is not automatically Reissued at the end of its Operational Period. If the WellsSecure Sub-CA decides to have its Certificate Reissued, the WellsSecure Sub-CA may issue a request to the WellsSecure Public Root CA, or WellsSecure Public Root CA 01 G2 prior to the end of the Sub-CA Certificate's Operational Period. In such case, the WellsSecure Sub-CA will provide its request with at least three (3) months prior notice, take reasonable efforts to ensure that affected Participants are not inconvenienced by the Reissuance process. Indeed, Certificate Reissuance will be timed so that minimal interruption in CA Services should occur.

Notwithstanding the foregoing, the WellsSecure Sub-CA will not be required to apply for Reissuance of its Issuer Certificate or otherwise bear any liability or responsibility to any Participants for the Expiration of its

Issuer Certificate or for any lapse or termination in CA Services that may occur. Upon Expiration of all of the WellsSecure Sub-CA's Issuer Certificates, the WellsSecure Public Root CA and WellsSecure Public Root CA 01 G2 will comply with all provisions of [WS CP and this WS CPS Sections 5.7.1 and 5.8].

If the WellsSecure Sub-CA Key Pair is changed; from that time on, only the new Key Pair will be used for Certificate signing purposes. The older, but still valid, Public Key will be available to verify old signatures until all of the Certificates signed using the associated Private Key have also Expired. If the old Private Key is used to sign CRLs that cover Certificates signed with that Private Key, then the old Private Key will be retained and protected.

5.6.2 Program Member Certificate Reissuance (Non-Issuer Certificates Only)

(a) Reissuance of Subscribing Customers of Subjects' Certificates is not automatic. Each Key Pair of a Subscribing Customer or Subject Expires contemporaneously with the Expiration of their associated Certificate's Operational Period. Subscribing Customers and Subjects may apply to the RA for Reissuance of their Certificates and associated Key Pairs. Reissuance does not provide for the re-key or re-initialization of the current Certificate. Rather, Reissuance provides the Subscribing Customers and Subjects with a replacement Certificate and Key Pairs. However, Reissuance requests may be timed to ensure the Subscribing Customers and Subjects suffer no lapse in its ability to use the WellsSecure PKI.

(b) Reissuance pursuant to pending Expiration may only be granted if the following conditions are met:

(i) The Subscribing Customer or Subject submits a request for Reissuance before the Expiration of the current Certificate's Operational Period, to the RA that administered the Registration Process under which the Certificate was issued;

(ii) The current Certificate is designated as Good pursuant within the WellsSecure PKI;

(iii) The Subject for whom Reissuance is sought does not appear on any Government or Wells Fargo complied list of prohibited users; and

(iv) The Applicant has complied with all other obligations as imposed by the WS CP and this WS CPS and all applicable PKI Documents.

(v) If the I & A for a reissued Certificate is based on the I & A previously performed for an existing Certificate, the Operational Period of the reissued Certificate shall not expire any later than the periods identified in Section 3.3.1 above for re-validation requirements.

Where these conditions are met, the RA may, in its sole discretion, instruct the WellsSecure Issuing CA to issue a new Certificate and Key Pair to the Subscribing Customer or Subject pursuant to the procedures set forth in Sections 4.1, 4.2, 4.3, and 4.4 of the WS CP and this WS CPS without conducting further I & A on that Subscribing Customer or Subject.

(c) Reissuance not related to pending Expiration may only be granted if the following conditions are met:

(i) The Applicant submits a request for Revocation before the Expiration of the current Certificate's Operational Period, to the RA that administered the Registration Process under which the Certificate was issued, or the RA or CA do so on behalf of the Subscribing Customer;

(ii) The current Certificate is designated as Good pursuant to a review by the CA or RA of the WellsSecure Certificate status database at the time of the Revocation and Reissuance request;

(iii) Revocation occurs pursuant to the guidelines set forth in the WS CP and this WS CPS; and

(iv) The Applicant has complied with all other obligations as imposed by the WS CP, this WS CPS and all applicable PKI Documents.

Where these conditions are met the RA may, in its sole discretion, instruct the WellsSecure Issuing CA to issue a new Certificate and Key Pair to the Subscribing Customer or Subject pursuant to the procedures set forth in Sections 4.1, 4.2, 4.3, and 4.4 of the WS CP and this WS CPS without conducting further I & A on that Subscribing Customer or Subject.

(d) Once activated, the new Certificate and associated Key Pair will be listed in the Directory as Good. The old Certificate and associated Key Pair will immediately be Revoked and the Subscribing Customer or Subject will immediately cease using that Certificate and its associated Key Pair. The Directory should reflect that the old Certificate was Revoked pursuant to a Reissuance request and the Subject named in the "Common Name (cn)" section of the "Subject" field of the old Certificate should not be added to the Compromised Users list.

(e) The WellsSecure Issuing CA or RA has complete discretion to grant or deny a Subscribing Customer or Subject's Certificate Reissuance request. Neither the WellsSecure Issuing CA nor the RA will bear any liability to the Subscribing Customer or Subject for any denial of the Reissuance request. In the event the Reissuance request is denied, the Subscribing Customer or Subject may nevertheless request a new Certificate using the Registration Process.

Note that High Assurance Certificates are not offered by the WellsSecure PKI.

5.6.3 Root Key Reissuance

With respect to Root Key changeover, the Wells Secure Public Root CA and WellsSecure Public Root CA 01 G2 will use reasonable efforts to:

(a) Ensure that Root Key changeover causes minimal disruption to WellsSecure Sub-CAs in its chain of trust; and

(b) Provide WellsSecure Sub-CAs with a minimum of three (3) months' prior notice of planned Root Key changeover.

If The Wells Secure Public Root CA or WellsSecure Public Root CA 01 G2 Key Pair is changed; from that time on, only the new Key Pair will be used for Certificate signing purposes. The older, but still valid, Public Key will be available to verify old signatures until all of the Certificates signed using the associated Private Key have also Expired. If the old Private Key is used to sign CRLs that cover Certificates signed with that Private Key, then the old Private Key will be retained and protected.

5.7 Compromise And Disaster Recovery

5.7.1 Incident And Compromise Handling Procedures

The WellsSecure PKI has in place a disaster recovery/business resumption plan. This plan includes a complete and periodic test of readiness for such facility. Tests are performed no less frequently than annually. If the WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2, or a WellsSecure Issuing CA Certificate Expires or is Revoked (for any reason, including compromise or loss), the subject CA will:

(a) Immediately cease using its Certificate;

(b) Publish the serial number of the Revoked or Expired Certificate on the appropriate CRL; and provide such CRL to the Directory;

(c) Revoke all Certificates signed with the Private Key that corresponds to the Public Key listed in the Revoked Certificate;

(d) Take commercially reasonable steps to notify all affected Participants of the Revocation or Expiration (e.g. email sent from a Wells Fargo email address);

(e) Take commercially reasonable steps to cause all affected Participants to cease using, for any purpose, any Certificates that identify the subject CA and that are linked to the Revoked or Expired Certificate in question (e.g. notify, pursuant to all contractual notice provisions); and

(f) Notify all PKIs by which the WellsSecure PKI has been certified or cross-certified so that those PKIs may issue CRLs revoking any Certificates issued to the compromised CA.

5.7.1.1 Actions When A Root CA Or Issuing CA Certificate Expires Or Is Revoked

If a WellsSecure Root CA or WellsSecure Sub-CA Certificate Expires or is Revoked (for any reason, including compromise or loss), the CA that was issued such Certificate will:

(a) Immediately cease using its Certificate;

(b) Publish the serial number of the Revoked or Expired Certificate on an appropriate CRL and provide such CRL to the Directory;

(c) Revoke all Certificates signed with the Private Key that corresponds to the Public Key listed in the Revoked Certificate;

(d) Take commercially reasonable steps to notify all affected Participants of the Revocation or Expiration (e.g. email sent from a Wells Fargo email address);

(e) Take commercially reasonable steps to cause all affected Participants to cease using, for any purpose, any Certificates that identify the subject CA and that are linked to the Revoked or Expired Certificate in question (e.g. notify to the extent required by any contractual notice provisions); and

(f) Notify all PKIs by which the WellsSecure PKI has been certified or cross-certified so that those PKIs may issue CRLs revoking any Certificates issued to the compromised CA.

5.7.1.2 Priority

The CA Personnel must treat incident handling as a high priority effort, with prompt responses and actions. The site security officer, in consultation with the facility manager and other CA Personnel who traditionally respond to security or facility incidents, if appropriate and practical, should decide, based on the nature or suspected characteristics of the incident, on an action plan in response to the incident. This plan should include prioritizing the protection of the CA integrity and pursuit of the individual causing the incident or attack. CA Personnel should be informed accordingly so they know how to respond to the incident.

5.7.1.3 Preparation

A plan shall been developed to handle certain types of incidents and the Site Security Officer shall instruct personnel to maintain such plan in writing in a known place. Such plans may include the following:

a) Goals and objectives, such as determining how the incident occurred and the adverse effects of the incident, remediating the adverse effects of the incident, and correcting the causes of the incident in an effort to ensuring it does not occur again;

b) Forming an incident handling team as described in the following Section 5.7.1.4;
c) Identifying who to notify if an incident occurs;
d) Limiting damage resulting from the incident;
e) Eliminating the cause of the incident;
f) Follow-up actions;
g) Analyzing any legal implications for the CA for an incident and any causes of action against the individual causing the incident; and
h) Documenting the incident.

5.7.1.4 Incident Handling Team

The incident handling team shall include the facility manager, site security officer, one or more systems administrators, and other members of engineering and management teams as required. One or more corporate representatives may have to be consulted or included in the team. If necessary, external audit personnel may have to become involved, depending on the nature of the incident. Home telephone numbers or other means of reaching all individuals on the incident handling team should be known in advance to the facility manager and site security officer.

The facility manager will appoint one person, most likely the site security officer, to be the incident manager. The incident manager coordinates efforts from a technical standpoint relating to the incident plan. Another individual will be appointed the single point of contact (POC) for communicating to all external individuals and Organizations outside the CA and its related Organizations, such as management, customers, the public, media, or legal personnel.

5.7.1.5 Communication To The Media

The CA operational Personnel shall not communicate directly with news media. Any questions from the media directed at such Personnel shall be responded to with a "No Comment" and directed to the POC or a CA authorized designee such as a media representative or public relations manager. The POC, however, should be freely accessible to the media and should communicate openly to the extent possible. The POC will provide facts where known, but avoid speculation or excited talk. The POC will make announcements if and when directed by the CA's legal and communication groups per the processes set forth in Sections 5.7.1.11 through 5.7.1.14.

5.7.1.6 Incident Log

All incident handling events require a special log be kept of all events concerning the incident. A log will provide a recording of details, which assists in corrective action and damage control. It may also be used to provide evidence in the event of any prosecution efforts related to the incident. The log will also help in performing a final assessment of damage resulting from the incident and will provide the basis for later phases of the incident handling process: such as eradication, recovery and follow-up "lessons learned." The log will have important information as it becomes known along with the date and time, and which can be signed for evidence.

5.7.1.7 Containment

The purpose of containment is to limit the adverse effects of an incident. An essential part of containment is decision-making. A key decision is whether to shut down or disconnect the CA from the Internet. During containment the following predetermined procedures should be carried out by the incident handling team:

(a) Attempt to determine the scope of the incident: i.e. what information, systems or infrastructure has been affected and how severely;
(b) Define acceptable risks in dealing with an incident;
(c) Prescribe specific actions and strategies accordingly; and
(d) Procedure for notifying the appropriate authorities.

5.7.1.8 Review Audit Logs

Audit logs for the time around the incident should be examined to help determine what happened. Past logs should also be examined to help determine if abnormal events occurred that could help understand the type of problem and the extent to which penetration has occurred. Events that could be significant include:

a) System crashes, denial of service, or reduced performance;
b) New user accounts, files, or modifications to files;
c) Accounting discrepancies; and
d) Attempts to probe or write to the system.

Checksums, and the signatures of the audit log, should also be checked to verify if any changes to software or audit logs have occurred.

5.7.1.9 Eradication

Once the incident has been contained, steps should be taken to eradicate the cause. Steps include collecting all necessary information about the compromised system(s) and the cause of the incident, and saving bogus files or other abnormal data before eradicating it, as this information will otherwise be lost

when cleaning up the WS PKI. The site security officer shall decide how much data or system elements should be replaced and how to detect and eliminate any suspected corrupted system elements.

5.7.1.10 Recovery

The goal of recovery is to return the WS PKI to normal. In general, services are brought up in the order of demand to allow a minimum of user inconvenience is the best practice. The facility manager and a system administrator will provide guidance in returning the WS PKI to complete functionality. If a virus or other bogus software is a possibility, it is important to ensure that only "clean" programs and files are reinstalled, and to use old enough versions that it is presumably before any attacks began, otherwise the WS PKI can become re-infected.

5.7.1.11 Reputational And Legal Issues

If the incident is serious enough, as determined by the incident manager, a corporate communication and legal representative shall be appointed. Reputational and legal issues to be considered might include:

a) Whether to publicize the incident;
b) Whether notice to the affected Participants regarding the incident is required;
c) Liability considerations;
d) Where to distribute information (e.g., other sites that might be similarly attacked); and
e) Whether to prosecute an individual or individuals are known or suspected to have caused or contributed to the incident.

5.7.1.12 Follow-Up

Once it is believed that the WS PKI has been restored to a “safe” state, it is still possible that issues related to the cause of the incident exist. In the follow-up stage the WS PKI shall be monitored for unusual behavior or issues that may have been missed during the cleanup stage. The most important element of the follow-up stage is performing a postmortem analysis including determining how and when the incident occurred, how well the CA Personnel responded to the incident, and how useful emergency procedures were, and what could have been done differently.

5.7.1.13 Notification To Participants

Affected Participants should be made aware of the incident in accordance with this WS CPS. Such notice may include how the incident was handled and an assessment of any damage that may have been caused to Participant.

5.7.1.14 Aftermath Of An Incident

In the wake of an incident several actions should take place. They can be summarized as follows:

a) An inventory should be taken of the WS PKI’s assets;
b) The lessons learned as a result of the incident should be included in a revised security plan to prevent the incident from re-occurring;
c) An evaluation of how the incident team performed and the effectiveness of the incident plan;
d) A new risk analysis and policy/plan should be developed in light of the incident; and
e) An investigation and prosecution of the individuals who caused the incident should commence if it is deemed desirable.

5.7.2 Computing Resources, Software, And/Or Data Are Corrupted

The WellsSecure PKI maintains a backup site in a remote location that mirrors its primary facility, so that if any software or data is corrupted it can be restored from the backup site via a reasonably secure connection. In the event of a business resumption occurrence, WellsSecure PKI will reestablish operations as quickly as possible; provided that the reestablishment of Revocation capabilities shall take precedence over all other operations.

Tape backups of all relevant software and data are taken on a regular basis, and not less than weekly, at both sites so that if any software or data cannot be restored via a secure, SSL connection the restoration can be performed via backup tapes stored at the local site.

5.7.3 Entity Private Key Compromise Procedures

In the event that a WellsSecure Issuing CA's Private Key is compromised, The WellsSecure Public Root CA or WellsSecure Public Root CA 01 G2, as appropriate, will immediately Revoke the Issuer Certificate and follow the procedures set forth in Section 5.7.1 of WS CP and this WS CPS. If the WellsSecure PKI's CA continues to operate, it will:

(a) Generate a new WellsSecure Issuing CA Key Pair in accordance with procedures set forth by the applicable Root CA (either, WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2, or Baltimore CyberTrust Global Root CA, depending on the Certificate) and those in the WS CP and this WS CPS; and

(b) Request new WellsSecure Issuing CA Certificates be issued to WellsSecure from those Organizations with whom the WellsSecure Issuing CA was either a Sub-CA or those PKIs with whom WellsSecure Issuing CA was cross-certified also in accordance with the WS CP and this WS CPS.

The Wells Fargo fraud team shall also investigate and report what caused the compromise or loss, and what measures have been taken to preclude recurrence. For the compromise of the Private Key of Participants, the procedures in Section 4.9.12 must be followed.

5.7.4 Business Continuity Capabilities After A Disaster

Building security and contracted security personnel will monitor the WellsSecure PKI facility after a natural or other type of disaster to protect against loss, additional damage to, and theft of sensitive materials and information. The WellsSecure PKI shall, at the earliest feasible time, securely advise Wells Fargo Organizations and Wells Fargo Organization Units, and affected Participants in the event of a disaster where the WellsSecure PKI installation is physically damaged and all copies of the WellsSecure Issuing CA Signature Keys are destroyed.

5.8 CA Or RA Termination

5.8.1 WellsSecure Issuing CA Termination

When it is necessary to terminate operation of an Issuing CA in the WellsSecure PKI, the impact of the termination is to be minimized as much as possible in light of the prevailing circumstances. This includes:

(a) Providing practicable and reasonable prior notice to all affected Participants;

(b) Assisting with the orderly transfer of service, and operational records, to a successor Certificate Authority, if any;

(c) Preserving any records, including a full archival of all records, not transferred to a successor CA, prior to termination; and

(d) Revoking all Certificates issued by the WellsSecure Issuing CA no later than at the time of termination.

In cases where the termination of the WellsSecure Issuing CA is voluntary, and no successor CA is contemplated, no less than ninety (90) days' notice will be provided to all affected Participants. The WellsSecure PKI will also undertake applicable obligations set forth in Section 5.7.1 of the WS CP and this WS CPS.

5.8.2 RA Termination

Where it is necessary to terminate the operation of any RA, the WellsSecure PKI will take reasonable steps to notify all affected Participants of such termination and of the contact information for any successor RA for the purpose of directing any requests for RA services.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation And Installation

6.1.1 Key Pair Generation

6.1.1.1 WellsSecure PKI's CA And RA Key Pairs

Key Pairs for The WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2, WellsSecure OCSP Responders, and WellsSecure Sub-CAs are generated in Tokens or an HSM from which the Private Keys cannot be extracted.

CA Key Pair generation must create a verifiable audit trail that the security requirements for procedures were followed. For all levels of assurance, the documentation of the procedure must be detailed enough to show that appropriate role separation was used.

An independent third party shall validate the execution of the Key Pair generation procedures either by witnessing the Key Pair generation or by examining the signed and documented record of the Key Pair generation.

6.1.1.2 Subscribing Customer Key Pairs

(a) The WellsSecure PKI distributes Subscribing Customer Key Pairs in one of three methods:

(i) Low Assurance

Private Keys for a Subscribing Customer who requests Low Assurance Level credentials are generated and stored on the customer's machine, or generated in the CA and stored in the customer's machine. These Private Keys may be backed-up, escrowed or archived.

(ii) Basic Assurance

Private Keys for a Subscribing Customer who requests Keys Pairs be stored in Basic Assurance Level Key Modules are generated using a [FIPS140] approved method, in a FIPS 140 validated module, as set forth in Section 6.2.1 below, and stored in an encrypted form. Key Pairs may be generated by the WellsSecure Sub-CA, or by the Subject, Individual Sponsor or RAs. If Key Pairs are generated by the Subject, Individual Sponsor or RA, delivery of the Public Key from the Subject, Individual Sponsor or RA to the CA must be in accordance with Section 6.1.3 below, and stored in a FIPS 140 validated Module. If Key Pairs are generated by the WellsSecure Sub-CA, after the Private Key is generated it is loaded into a secure software cryptographic Device with higher protections such as found in a camouflage scheme. Once the Private Key is loaded into the software cryptographic Device, all other copies are destroyed.

(iii) Medium Assurance

Private Keys for a Subscribing Customer who requests Keys Pairs be stored in Medium Commercial or Medium US (non-hardware) Assurance Level Key Modules are generated using a [FIPS140] approved method in a FIPS 140 Validated module, as set forth in Section 6.1.3 below, and stored a FIPS 140 Level 1 validated module, or better. Once the Private Key is loaded into the FIPS validated module, all other copies are destroyed. Except for the Certificates issued by the Wells Fargo Enterprise CAs for Smart Cards, Key Pairs are generated by the WellsSecure Sub-CA, not by Subject, Individual Sponsor or RAs. Private Keys for a Subscribing Customer who requests Key Pairs be stored in Medium Commercial or Medium US Hardware Assurance level Key Modules are generated using a [FIPS140] approved method and stored in an encrypted form. After a Private Key is either generated on a Token or loaded onto a Token, all other copies are destroyed.

(a) The hardware cryptographic Devices used by Subscribing Customers must meet Level 2 of [FIPS140] according to the Assurance level of the Certificate that is requested.

(b) For Key Pairs that are issued under the Basic or Medium Assurance levels, Subject or Individual Sponsor Signature Keys shall not be escrowed, backed-up or archived.

(c) The WellsSecure Sub-CAs do not issue Subject or Individual Sponsor private dual use Key Pairs.

(d) The WellsSecure Sub-CAs do not allow Key Pair recovery for Key Pairs that are issued under the Basic or Medium Assurance levels.

6.1.2 Private Key Delivery To Subscriber

If Subjects that are Devices or Systems or the Individual Sponsors of such Devices or Systems generate their own Key Pairs, then there is no need to deliver Private Keys, and this Section does not apply. When CAs or RAs generate Private Keys on behalf of the Subject or Individual Sponsor, then the Private Key must be delivered securely to the Subject, and in the case of Certificates issued to Devices, the Individual Sponsor for such Device (whose responsibilities regarding authentication are further described in [WS CP and this WS CPS Section 3.2.4]). Private Keys may be delivered electronically or may be delivered on a hardware cryptographic module.

In all cases, the following requirements must be met: (a) the CA or RA that generates a signing Private Key for a Subject shall not retain any copy of the Private Signing Key after delivery of the Private Key to the Subject or Individual Sponsor, as applicable; and (b) the Private Signing Key must be protected from activation, compromise, or modification during the delivery process.

The Subject or Individual Sponsor, as applicable, shall acknowledge receipt of the Private Key(s).

For Basic and Medium Assurance Levels where acknowledgment is required, Subjects using the secure software cryptographic device acknowledgment of receipt is deemed to have occurred once the Subject has completed the creation of the required secret questions and answers as well as set up a PIN.

Delivery shall be accomplished in a way that ensures that the correct Tokens and Activation Data are provided to the correct Subject or Individual Sponsor in the following manner:

(a) For hardware modules, accountability for the location and state of the module must be maintained until the Subject or Individual Sponsor accepts possession of it.

(b) For electronic delivery of Private Keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the Private Key. Activation data shall be delivered using a separate secure channel.

The WellsSecure PKI's CA or RA must maintain a record of the Subject and Individual Sponsor's acknowledgement of receipt of the token.

6.1.3 Public Key Delivery To Certificate Issuer

Key Pair Generation will be configured by the WellsSecure Issuing CA so that the Public Key for a Certificate is delivered to the WellsSecure Issuing CA at the time it is generated using a reasonably secure connection. Where Key Pairs are generated by the Subject, Individual Sponsor or RA, the Public Key and the Subject's identity must be delivered securely to the WellsSecure Issuing CA for Certificate issuance. The delivery mechanism shall bind the Subject's verified identity to the Public Key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the Certificate.

6.1.4 CA Public Key Delivery To Relying Parties

The WellsSecure Issuing CA, WellsSecure Public Root CA, and the WellsSecure Public Root CA 01 G2, make their Public Keys available from the Repository. When the WellsSecure Issuing CA, WellsSecure Public Root CA, or WellsSecure Public Root CA 01 G2 updates its signature Key Pair, it shall distribute the new Public Key in a secure fashion. The new Public Key may be distributed in a self-signed Certificate, or in a new CA Certificate (e.g., Cross-Certificate) obtained from the issuer(s) of the current CA Certificate(s).

6.1.5 Key Sizes

For SSL certificates the WellsSecure PKI issues certificates using key sizes that are consistent with the CA/B Forum's Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates for key sizes. All other certificates are issued with a minimum key size of 2048 bit RSA.

6.1.6 Public Key Parameters Generation And Quality Checking

Public Key parameters shall be generated in accordance with [FIPS186]. Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with [FIPS186].

6.1.7 Key Usage Purposes (As Per X.509 V3 Key Usage Field)

6.1.7.1 Subscriber Key Usage Purposes

Keys are used for the purposes and in the manner described in the WS CP, this WS CPS and any other applicable PKI Documents. Certificates shall assert Key usages based on the intended application of the Key Pair. These Keys uses will include, but are not limited to:

(a) Signing

Certificates to be used for Digital Signatures (including authentication) shall set the *digitalSignature* and/or *nonRepudiation* bits.

(b) Encryption

Certificates to be used for key or data encryption shall set the *keyEncipherment* and/or *dataEncipherment* bits.

(c) Agreement

Certificates to be used for key agreement shall set the *keyAgreement* bit.

6.1.7.2 Sub-CA Key Usage Purposes

All Sub-CA Certificates issued by the WellsSecure Public Root CA and WellsSecure Public Root CA 01 G2 shall set two Key usage bits: (a) *cRLSign*, and/or (b) *keyCertSign*. Where the Subject signs OCSP responses, the Certificate may also set the *digitalSignature* and/or *nonRepudiation* bits.

6.2 Private Key Protection And Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards And Controls

All Private Keys that are generated in Token, SKSS or HSM, shall be generated by a [FIPS140] approved method in a FIPS validated module as set forth below in this Section 6.2.1. OIDs in the Certificate that distinguish the storage mechanism by which the Private Keys are stored are set forth in [Section 1.2.2]. The table below summarizes the minimum requirements for cryptographic modules; higher levels may be used, stronger modules may be used.

Table 6.2: Minimum Requirements for Cryptographic Modules

Assurance Level	CA	Subscriber	RA
Low	Level 3 hardware	None	None
Basic	Level 3 hardware	Level 1	Level 1
Medium	Level 3 hardware	Level 1	Level 2 hardware
Medium	Level 3	Level 2	Level 2 hardware

Hardware	hardware	hardware	

6.2.2 Private Key (N Out Of M) Multi-Person Control

WellsSecure PKI's Root CAs are operated in offline mode. The participation of multiple trusted individuals is required to perform sensitive CA Private Key operations such as HSM activation, Sub-CA Certificate signing, CRL signing, CA key backup, and CA key recovery.

The Issuing CA is operated in online mode. The participation of multiple trusted individuals is required to perform sensitive CA Private Key operations such as HSM activation, CA key backup, and CA key recovery.

6.2.3 Private Key Escrow

All WellsSecure Issuing CA's Private Keys are not escrowed. Subject Private Keys may be escrowed as detailed in Section 6.1.1.2.

6.2.4 Private Key Backup

All WellsSecure Issuing CAs and OCSPs will have their Private Keys backed up as described within the WS CP. Subject Private Keys may be backed up as detailed in Section 6.1.1.2 and this Section. Subjects or Individual Sponsors must retain control over their Private Keys per Section 4.4. Backed up Subject Private Key management keys shall not be stored in plain text form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the Subscriber's cryptographic module.

6.2.5 Private Key Archival

WellsSecure Issuing CAs' Private Keys are not archived. Subject Private Encryption Keys may be archived as detailed in [Section 6.1.1.2].

6.2.6 Private Key Transfer Into Or From A Cryptographic Module

All Keys shall be generated by and in a cryptographic module pursuant to the table set forth in [Section 6.2.1]. In the event that a Private Key is to be transported from one cryptographic module to another, the Private Key must be encrypted during transport; Private Keys must never exist in plaintext form outside the cryptographic module boundary. Private or Symmetric Keys used to encrypt other Private Keys for transport must be protected from disclosure. Any WellsSecure Issuing CA's Private Keys may be exported from the cryptographic module only to perform CA Private Key backup procedures.

6.2.7 Private Key Storage On Cryptographic Module

Private Keys for The WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2, WellsSecure Sub-CAs, RAs and WellsSecure OCSP Responders, are generated, stored in an encrypted form, and backed up on an industry-standard cryptographic module, per [Section 6.2.11].

6.2.8 Method Of Activating Private Key

6.2.8.1 WellsSecure Issuing CA Private Keys

Activating any WellsSecure Issuing CA Private Keys shall be described within the WellsSecure CPS. Entry of Activation Data shall be protected from disclosure (i.e., the data shall not be displayed while it is entered). Activation requires multiparty control as described in Section 5.2.2.

6.2.8.2 Subscribing Customer Private Keys

A Subscribing Customer's Private Key is activated after:

(a) The Subscribing Customer has been issued a Token or SKSS with the Key Pair; or the Key Pair was generated by said customer on their computer, depending on the level of service required by such customer;

(b) The applicable Customer Agreement has been executed (for Assurance Levels other than Low) and the Terms of Use have been acknowledged and agreed to by the Subject; and

(c) Entry of Activation Data shall be protected from disclosure (i.e., the data shall not be displayed in clear text while it is entered).

See also Section 6.4.

6.2.9 Method Of Deactivating Private Key

Private Keys for The WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2, WellsSecure Sub-CAs, WellsSecure OCSP Responders, and RA Systems are deactivated by removing Tokens from the corresponding Systems, and shutting down operational software or the Token reader. CA, RA and OCSP cryptographic modules shall be removed and stored in a secure container when not in use.

6.2.10 Method Of Destroying Private Key

Where required, private keys under the control of the WS PKI are destroyed in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key..

6.2.11 Cryptographic Module Rating

The cryptographic devices used by The WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2, WellsSecure Sub-CAs, and WellsSecure OCSP Responders meet level 3 of [FIPS140] using FIPS validated cryptographic modules.

6.3 Other Aspects Of Key Pair Management

6.3.1 Public Key Archival

See [Section 5.5.1].

6.3.2 Certificate Operational Periods And Key Pair Usage Periods

(a) Public and Private Key pairs are valid until Expiration. Public and Private Key Pairs associated with a Revoked or Suspended Certificate are not valid and cannot be used for any given purpose.

(b) Certificates shall be valid for the Operational Period specified within the Certificate itself. Certificates, other than CA Certificates and the Certificates set forth below, shall have an Operational Period of not more than five (5) years from the date of issuance. However, the PKI Manager may grant approval for an Operational Period of up to ten (10) years for such Certificates. CA Certificates shall have an Operational Period not more than twenty (20) years. CRL signing and OCSP responder Certificates shall have an Operational Period not more than ten (10) years. The Operational Periods for each Certificate issued at the request of an RA shall be in accordance with the terms of the applicable RA Agreement (for business units not within WFBNA) with WFBNA. Specific Operational Periods shall in every case be set to Expire no later than the expiration of the issuing CA's Certificate.

6.4 Activation Data

The Private Keys of all Participants are stored in encrypted form, and requires the entrance of Activation Data to unlock. Activation Data is provided to all Subscribing Customers separately from the Key Pair.

6.4.1 Activation Data Generation And Installation

A passphrase or PIN, in addition to the Token, is required to operate cryptographic modules that comply with level 3 of [FIPS140] (e.g., OCSP Responder).

A passphrase or PIN, in addition to the Token, is required to operate cryptographic modules that comply with level 2 of [FIPS140] to operate the Medium Hardware Assurance Token.

A passphrase or PIN, in addition to the SKSS, is required to operate the Basic level software Key Module.

Where passwords are used as Activation Data, the password data shall be generated in conformance with [FIPS112]. Where any WellsSecure Issuing CA uses passwords as Activation Data for the CA Signature Key, at a minimum the Activation Data shall be changed upon CA re-key.

Activation Data shall have an appropriate level of strength for the Key Pair or data to be protected, and shall be transmitted to the Certificate holder in a method and manner that is different from that used to transmit the cryptographic module.

The Activation Data protection mechanism on FIPS140 level 2 and 3 devices shall also include a facility to temporarily suspend access to the Subject Private Keys after five (5) failed login attempts.

6.4.2 Activation Data Protection

Cryptographic module passphrases used to activate any WellsSecure Issuing CA Private Keys are stored in a locked safe at a secured site. The Activation Data protection mechanism shall also include a facility to temporarily suspend access to or terminate the operation of the WellsSecure Issuing CA hardware and software, after five (5) failed login attempts. The protection mechanism for other Activation Data shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts.

6.4.3 Other Aspects Of Activation Data

Token and SKSS passphrases are stored in secured locations at multiple sites, and are secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module. Token and SKSS passphrases are valid until the appropriate users change them. In order to activate Tokens or SKSS Key Modules, the appropriate user must change the initial activation data to a personalized PIN or Password.

6.5 Computer Security Controls

All WellsSecure Issuing CA system information is protected from unauthorized access either through protections provided by its operating system, or through a combination of operating system, physical safeguards, and network safeguards.

6.5.1 Specific Computer Security Technical Requirements

For information on network security controls, refer to Section 6.7.

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards.

(a) Require authenticated logins;

(b) Provide Discretionary Access Control;

(c) Provide a security audit capability;

(d) Restrict access control to CA services and PKI roles;

(e) Enforce separation of duties for PKI roles;

(f) Require identification and authentication of PKI roles and associated identities;

(g) Prohibit object re-use or require separation for CA random access memory;

(h) Require use of cryptography for session communication and database security;

(i) Archive CA history and audit data;

(j) Require a trusted path for identification of PKI roles and associated identities; and

(k) Enforce domain integrity boundaries for security critical processes.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The WellsSecure PKI uses software and/or object or source code that has been designed and developed under a formal, documented development methodology.

Hardware and software procured to operate the WellsSecure PKI is purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).

Hardware and software developed specifically for the WellsSecure PKI shall be developed in a controlled environment, and the development process shall be defined and documented. Security requirements were achieved through a combination of software verification and validation. The foregoing requirement does not apply to commercial off-the-shelf hardware or software.

All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the WellsSecure PKI physical location.

The WellsSecure PKI hardware and software shall be dedicated to meeting the obligations of the WellsSecure PKI in accordance with this policy. There shall be no other applications, hardware devices, network connections, or component software installed, which are not part of the WellsSecure PKI operation.

Proper care shall be taken to prevent malicious software from being loaded onto CA and RA equipment. Only applications required to perform the operation of the CA shall be obtained from sources authorized by local policy. CA and RA hardware and software shall be scanned for malicious code on first use and periodically thereafter.

Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

System security management is controlled by the privileges assigned to its operating system accounts, and by the trusted roles described in [Section 5.2.1].

A formal configuration management methodology shall be used for installation and ongoing maintenance of the WellsSecure PKI System.

The WellsSecure PKI's CA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

The networks on which the WellsSecure Issuing CAs, RAs, OCSP Responders and the WellsSecure PKI Repository reside are protected from unauthorized users through a series of firewalls and other network and host-based monitoring and detection systems. Networking equipment shall turn off unused network ports and services. WellsSecure shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks.

6.8 Time-Stamping

No stipulation.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

Some of the key fields of Certificate Profiles are included in Section 7.1.2. Detailed profiles for each Certificate type are available upon request. See Section 1.5.2 for Contact Information.

7.1.1 Version Number(s)

The WellsSecure PKI supports and uses X.509 version 3 Certificates.

7.1.2 Certificate Extensions

Recommended Certificate extensions for each Certificate type specified in Section 1.4.1 are detailed in the applicable Certificate profile that is available upon request (see Section 1.5.2). All use of standard Certificate extensions shall comply with [RFC3280] for SHA-1 CAs and corresponding End-entities, and comply with [RFC5280] for SHA-2 CAs and corresponding End-entities. CA Certificates shall not include critical private extensions.

Subscriber Certificates may include critical private extensions so long as interoperability within the community of use is not impaired.

7.1.3 Algorithm Object Identifiers

Algorithm object identifier OIDs are allocated to algorithms supported and used by the WellsSecure PKI and are in compliance with x.509 standards.

Certificates issued by any Issuing CA that chains up to The WellsSecure Public Root CA, or WellsSecure Public Root CA 01 G2 shall identify the signature algorithm using one of the following OIDs:

Table 7.1: OIDs for Signature Algorithms

id-dsa-with-sha1	1.2.840.10040.4.3
sha-1WithRSAEncryption	1.2.840.113549.1.1.5
sha256WithRSAEncryption	1.2.840.113549.1.1.11
ecdsa-with-SHA1	1.2.840.10045.4.1
ecdsa-with-SHA224	1.2.840.10045.4.3.1
ecdsa-with-SHA256	1.2.840.10045.4.3.2
ecdsa-with-SHA384	1.2.840.10045.4.3.3
ecdsa-with-SHA512	1.2.840.10045.4.3.4

Certificates issued from an Issuing CA that chains up to The WellsSecure Public Root CA, or WellsSecure Public Root CA 01 G2 shall identify the cryptographic algorithm associated with the subject public key using one of the following OIDs:

Table 7.2: OIDs for Subject Public Key Algorithms

id-dsa	1.2.840.10040.4.1
RsaEncryption	1.2.840.113549.1.1.1
Dhpublicnumber	1.2.840.10046.2.1
id-ecPublicKey	1.2.840.10045.2.1

7.1.4 Name Forms
Names for the "Issuer" and "Subject" fields of each Certificate type specified in Section 1.4.1 are of the X.500 DN form. Distinguished names shall be composed of standard attribute types, such as those identified in [RFC3280] for SHA-1 CAs and corresponding End-entities, and in [RFC5280] for SHA-2 CAs and corresponding End-entities.

7.1.5 Name Constraints
No stipulation.

7.1.6 Certificate Policy Object Identifier
Each Certificate issued by a WellsSecure Issuing CA contains the OID in the Certificate policy extension. Each Certificate also contains an OID from Section 1.2.2 in the Certificate policy extension.

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
The profile for the CRL issued by a WellsSecure Issuing CA conforms to the standards as described in [RFC3280] for SHA-1 CAs and corresponding End-entities, and in [RFC5280] for SHA-2 CAs and corresponding End-entities. The CRL profile is x509 v2.

7.2.1 Version Number(s)
The WellsSecure PKI issues and uses X.509 version 2 CRLs.

7.2.2 CRL And CRL Entry Extensions
Recommended CRL and CRL entry extensions are detailed in the WellsSecure CP and applicable CRL profile that is available upon request (see Section 1.5.2). All use of standard CRL and CRL entry extensions shall comply with [RFC3280] for SHA-1 CAs and [RFC5280] for SHA-2 CAs.

7.3 OCSP Profile
The profile for the OCSP requests received and OCSP responses issued by the WellsSecure OCSP Responder conforms to the standards as described in [RFC2560].

7.3.1 Version Number(s)
The WellsSecure OCSP Responder expects OCSP version 1 requests and issues OCSP version 1 responses.

7.3.2 OCSP Extensions

All use of standard OCSP request and response extensions shall comply with [RFC2560].

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency Or Circumstances Of Assessment

The WellsSecure PKI, including external RAs and external TRs, will be audited at least once every year for compliance with the practices and procedures set forth in the WS CP and this WS CPS.

8.2 Identity And Qualifications Of Assessor

All compliance audits will be performed by Wells Fargo Audit or another third party that meets the qualifications as set forth by the General Auditor of Wells Fargo; which qualifications shall include without limitation: (a) demonstrated competence in the field of compliance audits, and (b) familiarity with requirements, which the WellsSecure PKI imposes on the issuance and management of its Certificates. The compliance Auditors who perform external compliance audits shall perform the same as a primary responsibility.

8.3 Assessor's Relationship To Assessed Organization Or Organization Unit

The compliance audit of the WellsSecure Issuing CAs and all RAs operating under their authority will be performed by Wells Fargo Auditors that are sufficiently organizationally separated from the WellsSecure line of business to provide an unbiased, independent evaluation or by a third party, as authorized by the Wells Fargo PKI Management and permitted by law. The compliance audit of external RAs and TRs may be performed by either a Wells Fargo Auditor or a third party that meets the qualifications set forth in Section 8.2.

8.4 Topics Covered By Assessment

The compliance audit will evaluate compliance of the WellsSecure Issuing CAs, RAs and TRs against the WS CP and other applicable PKI Documents.

8.5 Actions Taken As A Result Of Deficiency

Upon receipt of the results of a compliance audit report that details any deficiencies, the WellsSecure Issuing CA, RA or TR will use reasonable measures to promptly correct any such deficiencies. If the compliance audit report recommends remedial action, the WellsSecure Issuing CA, RA or TR will initiate corrective action within thirty (30) days of receipt of such audit report.

If the compliance auditor finds a discrepancy, the following actions shall be performed:

The compliance auditor shall document the discrepancy;
The compliance auditor shall promptly notify the responsible party; and
The WellsSecure PKI shall determine what further notifications or actions are necessary to meet the requirements of the WS CP, this WS CPS, and any relevant cross-certification agreements. The WellsSecure PKI shall proceed to make such notifications and take such actions within ten (10) days of receipt of notice of deficiency.

8.6 Communication Of Results

The results of all compliance audits will be communicated to the Wells Fargo PKI Management. Other Participants have no right to access the compliance audit results. If the audit is one that is engaged into in order to obtain industry certification or approval to provide a public assurance of compliance with the WS CPS, (such as a WebTrust Audit) Wells Fargo may, in its sole discretion, make the summary of such audit's results available on the same web page as the WS CPS is accessed.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Wells Fargo may charge Subscribers fees for the issuance, management and renewal of or access to Certificates, or for other services. Such fees, if any, and the policy relating to the refund of any such fees shall be set forth in the Subscriber Agreement.

9.1.1 Certificate issuance or renewal fees

See Section 9.1.

9.1.2 Certificate access fees

See Section 9.1.

9.1.3 Revocation or status information access fees

No fees will be charged for Revocation or status information access.

9.1.4 Fees for other services

See Section 9.1.

9.1.5 Refund policy

See Section 9.1.

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 following categories of information are considered to be “Confidential Information”. These categories of information are subject to the provisions of Section 0.

(a) Private Keys, whether held by Subscribing Customers (including Individuals representing Subscribing Customers), CAs, RAs, Repositories, or OCSP Responders, must be held in the strictest confidence. Each party is responsible for keeping its own Private Key confidential and, after Certificate issuance, no other party will have access to or be responsible for another's Private Key;

(b) All PKI Documents;

(c) Any information or data that is required to be kept confidential by applicable law or agreement;

(d) Information held in audit trails, including annual audit results, is confidential to the WellsSecure Issuing CA and will not be disclosed except as authorized in this WellsSecure CPS;

(e) The WellsSecure CA security plan, measures and safeguards, including its disaster recovery plans; and

(f) All personal and corporate information submitted as part of the Registration, I & A process, Certificate status checking, or Certificate Reissuance, Suspension, Reinstatement, or Revocation processes, that is not published as part of a Certificate, in the Directory or CRL, or in this WellsSecure CPS.

9.3.2 Information not within the scope of confidential information

Notwithstanding Section 0, the following categories of information are not considered Confidential Information:

(a) Information contained in Certificates, the Directory and CRLs, and Compromised User lists, (including the status of a Certificate and the reason code related to a Revocation or Suspension);

(b) PKI Documents that are made publicly available by the WellsSecure PKI; provided, however, that references in a publicly available PKI Document to another PKI Document that is not made publicly available shall not cause the latter to be outside the scope of Confidential Information as defined in this WellsSecure CPS;

(c) Revocation or Suspension information; and

(d) Any information that: (i) is lawfully obtained from a third party under no obligation of confidentiality; (ii) is independently developed without reference to any Confidential Information; or (iii) is or becomes available to the public without breach of obligation of confidentiality by a Participant.

9.3.3 Responsibility to protect confidential information

(a) Permitted Disclosures. The WellsSecure Issuing CAs and WellsSecure RAs will be entitled to disclose Confidential Information on a "need-to-know" basis to any of their Personnel, and WF Entities and their Personnel, that are assisting in the verification of information supplied in Certificate applications or that are assisting in the operation of the WellsSecure Issuing CAs or RAs. The WellsSecure Issuing CAs and RAs will also be entitled to disclose Confidential Information to the following third parties: (i) legal and financial advisors, assisting in connection with any legal, judicial, administrative, or other proceedings required by law or by this WellsSecure CPS, and (ii) legal counsel, accountants, banks and financing sources and their advisors in connection with mergers, acquisitions, or reorganizations, and (iii) contractors providing services to Wells Fargo, in such a case Wells Fargo will ensure that a suitable agreement is in place extending the terms of this policy to cover handling of the information by that contractor. Any such disclosures will be permissible provided that the WellsSecure Issuing CAs and RAs use reasonable efforts to ensure that all such third parties will protect the Confidential Information at the same level as such Confidential Information is protected in this WellsSecure CPS.

(b) Disclosures required by law. Confidential Information may be disclosed to law enforcement officials on receipt of judicial order, or order of some other competent decision-maker, or as otherwise required by law. Unless prohibited by law, and to the extent reasonably practical, all interested Subscribing Customers, Applicants or Subjects should be provided reasonable prior notice before such information is disclosed. Confidential Information may be disclosed during the course of any arbitration, litigation, or any other legal, judicial, or administrative proceeding. To the extent not prohibited by law, all interested Subscribing Customers, Applicants or Subjects should be given reasonable prior notice before such information is disclosed.

(c) Disclosures at the request of third parties. Confidential Information may be disclosed to third parties upon receipt of a valid request from the appropriate Subscribing Customer, Applicant, or Subject that originally provided the Confidential Information. Reasonable steps will be taken to ensure that the Organization or Individual making the request is the owner of the Confidential Information, but in no event will the Wells Fargo Trusted Identity Entities have liability of any kind for any errors in disclosure.

(d) Safeguards. The WellsSecure Issuing CAs and their RAs will take reasonable steps to protect the confidentiality of Confidential Information (as defined in Section 0) disclosed by Subscribing Customers,

Applicants and Subjects in accordance with all applicable privacy laws. Confidential Information may not be disclosed to a third-party without the prior consent of the disclosing party, except as otherwise provided herein or to the extent necessary to provide the CA Services and the Validation Services associated with the WellsSecure PKI.

Appropriate precautions will be applied to protect personal information from unauthorized disclosure, modification or loss. These will include:

(i) Procedural controls
(ii) Ensuring that staff are aware of their responsibilities for safeguarding personal information,
(iii) Physical security including locked filing cabinets and locked rooms,
(iv) Logical security such as passwords and access control lists,
(v) Ensuring that personal information is accessible only to the staff who will require it to fulfill their duties,
(vi) Contractual controls on staff and any third parties who may at any time have access to the systems and facilities where the information is held.

Where such a disclosure is made, the event will be logged recording the date of disclosure, the information provided, the entity to whom it was disclosed and justification for the disclosure. Any actual or potential breach of confidentiality will be treated as a security incident and notification appropriate entities as established in PKI Operations Manual will apply. Records of personal information acquired by Wells Fargo will be disposed of securely when no longer required. Paper copies will be disposed of by shredding or burning. Electronic media will be either securely erased or physically damaged to render them unreadable.

(e) Indemnification Obligations for proper disclosures. Subscribing Customers, Applicants, or Subjects that provide Confidential Information to the WellsSecure PKI or any authorized third-party RA or Repository agree to indemnify and hold harmless the Wells Fargo Trusted Identity Entities from and against any and all liabilities, losses, damages, costs, or expenses (including reasonable attorneys' fees, costs, and expenses) arising from or in connection with improper disclosures made to third-parties where the WellsSecure PKI disclosed such information with a reasonable belief that the disclosure request was proper.

(f) Subscribing Parties obligations upon termination. If at any time any Subscribing Customer's Certificate's Operational Period Expires without Certificate Reissuance, or the relationship between the Subscribing Customer and the CA is otherwise terminated, the Subscribing Customer will cease any use of all Confidential Information, which is proprietary to any WF Affiliate Organization or WF Affiliate Organization Unit. The Subscribing Customer will also promptly return all such Confidential Information in tangible form and all copies thereof in its possession or under its control, and will destroy all copies thereof on its computers, disks and other digital storage devices.

9.4 Privacy of personal information

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

See this WellsSecure CPS section 9.3.1.

9.4.3 Information not deemed private

See this WellsSecure CPS section 9.3.2.

9.4.4 Responsibility to protect private information

See this WellsSecure CPS section 9.3.3.

9.4.5 Notice and consent to use private information
See this WellsSecure CPS section 9.3.3.

9.4.6 Disclosure pursuant to judicial or administrative process
See this WellsSecure CPS section 9.3.3.

9.4.7 Other information disclosure circumstances
See this WellsSecure CPS section 9.3.3.

9.5 Intellectual property rights

9.5.1 Reservation of rights
Participants agree and acknowledge that the Wells Fargo Trusted Identity Entities own and shall retain all respective rights, title and interest in and to, and all intellectual property rights embodied in or associated with the WellsSecure PKI and the issuance, delivery and use of any Certificate, OIDs, Token(s), SKSS, Key Pairs, trademarks or other intellectual property and PKI Documents. Such right, title and interest shall extend without limitation to any content, software, graphics, design materials, technology, methods, architecture, publications, business plans and other tangible or intangible intellectual property-based assets of any kind in machine readable, printed or other form and all revisions, enhancements, improvements, technical know-how, patents, copyrights, moral rights and trade secrets associated with any Certificate, OIDs, Token(s), SKSS, Key Pairs, trademarks or other intellectual property, and/or PKI Documents. Except as expressly stated in this WellsSecure CPS or other applicable PKI Document, Participants will have no rights of any kind in or to any Certificate, OIDs, Token(s), SKSS, Key Pairs, trademarks or other intellectual property, or PKI Documents. There are no implied licenses under this WellsSecure CPS, and any rights not expressly granted under this WellsSecure CPS or the Customer Agreement are reserved by the Wells Fargo Trusted Identity Entities.

9.5.2 License
In applicable Sub-CA Agreement, RA Agreement (for business units not within WFBNA), Repository Agreement, or Customer Agreements, the WellsSecure Issuing CA may grant Participants a revocable, nontransferable, non-sublicensable license to use their Certificates and Private Keys in accordance with this WellsSecure CPS and other applicable PKI Documents. The license is granted for the use of Certificate and Private Key exclusively by such Participant and only for the limited purposes and term set forth in this WellsSecure CP/CPS, the applicable Sub-CA Agreement, RA Agreement (for business units not within WFBNA), Repository Agreement, or Customer Agreement, and other applicable PKI Documents. Any use not in compliance with the foregoing is explicitly prohibited.

In certain circumstances, Participants may be given the right to use certain WellsSecure or Wells Fargo trademarks or other intellectual property. Such use will be set forth in an applicable Sub-CA Agreement, RA Agreement (for business units not within WFBNA), Repository Agreement, or Customer Agreement.

Participants may not use Wells Fargo or WellsSecure trademarks or other intellectual property prior to execution of the Sub-CA Agreement, RA Agreement (for business units not within WFBNA), Repository Agreement, or Customer Agreement applicable to their role and all subsequent use will be subject to the terms of any applicable license contained in that Agreement.

9.5.3 Termination
On termination of the Subscribing Customer's participation in the WellsSecure PKI or the Sub-CA Agreement, RA Agreement (for business units not within WFBNA), Repository Agreement, or Customer Agreement, all uses of any Wells Fargo or WellsSecure trademarks or other intellectual property will immediately cease and any Wells Fargo or WellsSecure intellectual property in the possession of the Participant who was party to such Agreement at the time of termination will either be returned to Wells Fargo or WellsSecure or will be destroyed.

9.5.4 Modifications

The terms and conditions of this Section 0 may be supplemented or altered by applicable Sub-CA Agreement, RA Agreement (for business units not within WFBNA), Repository Agreement, or Customer Agreements between Wells Fargo, WellsSecure and Subscribing Customers.

9.6 Representations and warranties

9.6.1 CA representations and warranties

The applicable Customer Agreement, Relying Party Agreement, RA Agreement (for business units not within WFBNA), or Cross Certification Agreement sets forth any representations and warranties made by the WellsSecure Issuing CA.

9.6.2 RA representations and warranties

The RA Agreement (for business units not within WFBNA) sets forth any representations and warranties made by the WellsSecure RA or a third party RA authorized by the WellsSecure Issuing RA.

9.6.3 Subscriber representations and warranties

In addition to the representation and warranties contained in the applicable Customer Agreement and the Terms of Use, the Subscriber and Subject (or in the case of a Certificate issued to a System or Device, the Individual Sponsor), through its acceptance of the Certificate, represent and warrant that:

(a) Subject information contained in the Certificate is accurate and complete. If the Subscriber has not, within seven (7) days after delivery of the Token or SKSS containing the Key Pair and associated Certificate, or the Certificate itself, for those Certificates that are not stored in a Token or SKSS and include the appropriate OID indicated to the RA that there are errors or omissions in the Certificate, all information in the Certificate will be deemed by the WellsSecure Issuing CA to be correct whether or not the Private Key has been used. The RA will provide the Subscriber instructions on how to check the information contained in the Certificate;

(b) Subject will at all times retain control of the Private Key corresponding to the Public Key listed in the Certificate;

(c) all representations made by the Subscriber and the Subject during the Registration Process, including those made by Applicant on the Subscriber's behalf are complete and accurate;

(d) Subscriber and Subject are responsible for the use of the Certificate, which will be used only for authorized and legal purposes consistent with the WS CP and other applicable PKI Documents;

(e) Subscriber and Subject consent to allow the WellsSecure Issuing CA to deliver information related to its Certificate to the Repository;

(f) Subscriber and/or the Subject will immediately inform the RA that administered the Registration Process of any event that may invalidate or otherwise diminish the integrity of the Certificate, such as known or suspected loss, disclosure, or other compromise of its Private Key associated with its Certificate; and

(g) Subscriber and the Subject agree the WellsSecure Issuing CA or RA has the authority to Revoke or Suspend the Certificate as set forth in this WellsSecure CPS.

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

EXCEPT TO THE EXTENT PROVIDED IN SECTION 9.6.1, THE WELLS FARGO TRUSTED IDENTITY ENTITIES DISCLAIM ANY AND ALL OTHER WARRANTIES, BOTH EXPRESS AND IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF TITLE, QUALITY MERCHANTABILITY, ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF ACCURACY OF INFORMATION PROVIDED WITH RESPECT TO THE PARTICIPATION OF ALL NON-WELLS FARGO PARTICIPANTS IN THE WELLSSECURE PKI, INCLUDING USE OF KEY PAIRS, CERTIFICATES, THE CA SERVICE, THE VALIDATION SERVICE OR ANY OTHER GOODS OR SERVICES PROVIDED BY THE WELLSSECURE PKI. THE WELLS FARGO TRUSTED IDENTITY ENTITIES FURTHER DISCLAIMS ANY AND ALL WARRANTIES, BOTH EXPRESS AND IMPLIED, THAT PARTICIPATION IN THE WELLSSECURE PKI WILL AFFECT IN ANY MANNER THE LEGAL RECOGNITION OR ENFORCEABILITY OF A DIGITAL SIGNATURE.

9.8 Limitations of liability

9.8.1 Limitations on amount and type

Subject to Section 9.8.2, and except as expressly provided in an applicable Sub-CA Agreement, RA Agreement (for business units not within WFBNA), Repository Agreement, Customer Agreement or other agreement between a Participant and WFBNA , the liability of the Wells Fargo Trusted Identity Entities to a Non-Wells Fargo Participant in connection with the performance of CA Services, the Validation Services, or any other obligations under the WellsSecure PKI, including negligence and misconduct and whether in contract, tort or otherwise, shall be exclusively limited to direct damages only, and shall not exceed the following: (i) $1,000 per claim or transaction, or (ii) $10,000 in the aggregate with respect to each Non-Wells Fargo Participant or any single Certificate in a calendar year.

9.8.2 Exclusions of certain damages

(a) THE WELLS FARGO TRUSTED IDENTITY ENTITIES WILL HAVE NO LIABILITY, EXCEPT WHERE, AND TO THE EXTENT, SUCH LIABILITY IS FINALLY DETERMINED TO HAVE BEEN CAUSED BY THE INTENTIONAL OR FRAUDULENT CONDUCT OF THE WELLS FARGO TRUSTED IDENTITY ENTITIES TO NON-WELLS FARGO PARTICIPANTS WHATSOEVER FOR ANY AND ALL LIABILITY, LOSSES, CLAIMS, DEMANDS, DISPUTES, DAMAGES OR COSTS OF ANY KIND, INCLUDING, WITHOUT LIMITATION, REASONABLE ATTORNEYS' FEES AND COSTS OF LITIGATION, (COLLECTIVELY, "LOSSES AND LIABILITIES"):

(i) Due to an unauthorized use of a Certificate issued by a WellsSecure Issuing CA, the use of such a Certificate beyond authorized limits, or the use of such a Certificate returned with "Revoked" or "Unknown" response; provided that such unauthorized use is by any Individual or Organization or Organization Unit other than Wells Fargo;

(ii) Due to the accuracy or authenticity of information and/or identification credentials presented or submitted to the WellsSecure Issuing CA and/or WF Entities in connection with a request for a Certificate;

(iii) Caused by (A) improper, fraudulent, or negligent use, (B) any transaction prohibited by applicable law, including but not limited to any use in OFAC negative countries, or (C) any transaction for which the Individual or Organization or Organization Unit to which the Certificate has been issued by the WellsSecure Issuing CA is not acting either as principal or as agent for a principal that has been disclosed to the WellsSecure Issuing CA and/or WF Entities; provided that such improper or unauthorized uses are by an Individual or Organization or Organization Unit other than the WellsSecure Issuing CA and/or WF Entities;

(iv) Due to inadequate protection or safekeeping of a Certificate issued by The WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2, WellsSecure Sub-CA and/or WF Entities provided that such unauthorized use is by any Individual or Organization or Organization Unit other than the WellsSecure PKI's CAs and/or WF Entities; or any Individual or Organization or Organization Unit's failure to promptly request Suspension or Revocation of an Invalid Certificate;

(v) Related to the validity, veracity, or legality of the content of any message, transaction or other data accompanying the Certificate issued by the WellsSecure Issuing CA; and/or

(vi) Due to any Individual or Organization or Organization Unit other than the WellsSecure Issuing CA and/or WF Entities, causing an intrusion into, interference with, compromise, or destruction of the WellsSecure PKI or any WellsSecure Issuing CA, or any component or element thereof, or due to acts of God affecting the WellsSecure PKI or any WellsSecure Issuing CA, or any component or element thereof, unless any such events occur as a result of the WellsSecure Issuing CA and/or WF Entities having failed to take commercially reasonable protective measures, if available, against such intrusion, interference, compromise or destruction.

(b) IN NO EVENT SHALL THE WELLS FARGO TRUSTED IDENTITY ENTITIES BE LIABLE FOR EXEMPLARY, PUNITIVE, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, ANY LOSS OF PROFITS, LOSS OF GOODWILL, LOSS OF BUSINESS, LOSS OF ANTICIPATED SAVINGS, LOSS OF DATA, COST OF PROCUREMENT OF SUBSTITUTE SERVICES AND/OR CERTIFICATES, OR ANY OTHER INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, HOWSOEVER CAUSED, AND ON ANY THEORY OF LIABILITY, WHETHER FOR BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY), OR OTHERWISE. THESE LIMITATIONS WILL APPLY WHETHER OR NOT THE WELLS FARGO TRUSTED IDENTITY ENTITIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER OR NOT THE WELLS FARGO TRUSTED IDENTITY ENTITIES COULD HAVE FORESEEN SUCH DAMAGES AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. SUBJECT TO THE FOREGOING, THE WELLS FARGO TRUSTED IDENTITY ENTITIES LIABILITY FOR DIRECT DAMAGES OF ANY KIND OR NATURE IN CONNECTION WITH THIS AGREEMENT SHALL IN NO EVENT EXCEED THE LIMITS SET FORTH IN SECTION 9.8.1 OR APPLICABLE SUB-CA AGREEMENT, RA AGREEMENT (FOR BUSINESS UNITES NOT WITHINT WFBNA), REPOSITORY AGREEMENT, CUSTOMER AGREEMENTS OR OTHER AGREEMENT BETWEEN NON-WELLS FARGO PARTICIPANT AND WFBNA FOR ALL TRANSACTIONS ARISING OUT OF THE CERTIFICATE, CA SERVICE, OR VALIDATION SERVICE, AS APPLICABLE, WHICHEVER IS LESS. NON-WELLS FARGO PARTICIPANTS ALSO ACKNOWLEDGE AND AGREE THAT THEY HAVE REVIEWED AND FREELY CONSENTED TO THE LIMITATIONS OF LIABILITY IMPOSED IN THIS SECTION.

9.8.3 Liability for WellsSecure Issuing CA Authorized RAs and Repositories

All liability for RAs and Repositories operating under the authority of a WellsSecure Issuing CA is subsumed by the WellsSecure Issuing CA and is subject to the limitations specified in Section 0. Despite the foregoing, nothing in this Section will prevent the WellsSecure Issuing CA from pursuing its remedies against any Organization approved to undertake RA or Repository obligations on behalf of the WellsSecure Issuing CA, pursuant to the applicable RA Agreement (for business units not within WFBNA) or Repository Agreement.

9.9 Indemnities

Where the Wells Fargo Trusted Identity Entities (referred to in this Section as the “Indemnified Parties”) are, or will be, indemnified pursuant to the provisions of this WellsSecure CPS or other applicable PKI Documents, the Indemnified Parties will provide the non-Wells Fargo Participant with prompt written notice of the Losses and Liabilities to be indemnified, and will cooperate, if reasonably requested by the non-Wells Fargo Participant and at the non-Wells Fargo Participant's expense, in the investigation of such Losses and Liabilities and any action or suit giving rise to such Losses and Liabilities. If the indemnification tender is accepted, the non-Wells Fargo Participant will have full and sole control and authority to investigate, defend and/or settle any action or suit giving rise to such Losses and Liabilities, provided, however, that (a) the Indemnified Parties may participate in such defense with their own counsel and at their own expense and (b) the consent of the Indemnified Parties will be required for any settlement that does not provide a full and complete release from liability for the Indemnified Parties. If the indemnification tender is not accepted, the Indemnified Parties and non-Wells Fargo Participant will each participate in the defense of the claim with their own counsel, subject to a claim for indemnification

for any Losses and Liabilities suffered or incurred by the Indemnified Parties resulting from a settlement or final judgment against the non-Wells Fargo Participant, based on the proportion of liability borne by the Indemnified Party and non-Wells Fargo Participant subject to the settlement or judgment. In the event the settlement or judgment fails to apportion liability, the Indemnified Parties or Customer may invoke the appropriate dispute resolution procedures, as are set out in Section 9.13.

9.9.1 Indemnification by RAs And Repositories

All RAs and Repositories shall indemnify and hold harmless the Indemnified Parties as defined in this Section 0 from and against any and all liabilities, losses, damages, costs, or expenses (including reasonable attorneys' fees, costs, and expenses) arising out of or in connection with such RA or Repository's: (a) performance of RA functions as described in Section 1.3.2 or Repository function as described in Section 2,1 that affect any Individual or Organization that has not executed an appropriate RA Agreement with WFBNA (see Section 1.2.4.2) for the provision of such services; or (b) failure to comply with its obligations, or breach of its representations or warranties as set forth in this WellsSecure CPS and other applicable PKI Documents; and (c) failure to comply with its obligations under applicable law.

9.9.2 Indemnification by Subscribing Customers

9.9.2.1 Each Subscribing Customer shall indemnify and hold harmless Participants, the Indemnified Parties as defined in this Section 0, and their directors, officers, Employees, agents, subsidiaries, parents and affiliates, irrespective of their active or passive negligence, against any and all Losses and Liabilities resulting from or in any way connected with: (i) the Subscribing Customer's breach of any representations and warranties and any obligations of the Subscribing Customer set forth in this WellsSecure CPS and the PKI Documents; (ii) the actions or omissions of any Applicant authorized by the Wells Fargo Subscribing Customer to initiate the Registration Process; (iii) any misidentification of a Subject's authority or identity by any Trusted Registrar; (iv) the use of any name or materials infringing upon third-party intellectual property rights; (v) any use of the Subscribing Customer's Private Keys other than as expressly set forth in this WellsSecure CPS and other applicable PKI Documents; (vi) any unreasonable repudiation of a Certificate validated by any WellsSecure Issuing CA; and (vii) the use of its Certificates in any transaction with a party that does not possess a Certificate issued by The WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2 or Sub-CA. Any further indemnity obligations of the Subscribing Customer shall be more specifically set forth in the applicable Customer Agreement.

9.9.2.2 If a Subscribing Customer provided incorrect information in order to receive a name in its Certificates that infringes upon the proprietary rights of a third party, the Subscribing Customer hereby agrees to indemnify and hold harmless the Wells Fargo Trusted Identity Entities for any Losses or Liabilities arising out of the WellsSecure Issuing CA's use of such name.

9.9.3 Indemnification by the Relying Party

Each Relying Party shall indemnify and hold harmless Participants, the Indemnified Parties as defined in this Section 0, and their directors, officers, Employees, agents, subsidiaries, parents and affiliates, irrespective of their active or passive negligence, against any and all Losses and Liabilities resulting from or in any way connected with: (a) Relying Party's breach of any representations and warranties and any obligations of Relying Party set forth in the WS CP and the PKI Documents; (b) the use of any name or materials infringing upon third-party intellectual property rights; (c) any reliance on a Certificate that is not reasonable under the circumstances, including reliance on a Certificate when its status has not been verified; (d) any use of a third-party service provider to initiate or process any Validation Service request on behalf of the Relying Party; and (e) the use of its Certificates or the Validation Service in connection with any transaction involving a party that does not possess a Certificate issued by the WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2 or Sub-CA.

9.9.4 Indemnification by Subject

The Subject agrees to indemnify and hold harmless all affected Participants for any Losses and Liabilities arising from: (a) reliance on incorrect representations made by the Subject, Individual Sponsor or by Applicant; (b) any failure to disclose material facts which if known, would have affected the decision to

issue the Certificate or its continued validity; and (c) any other breach of the Subjects obligations under the WellsSecure PKI.

9.9.5 Indemnification by Applicant

The Applicant and either (a) the Subscribing Customer for which the Applicant is Personnel, or (b) the Subscriber, as applicable, shall indemnify and hold harmless all affected Participants for any and all Losses and Liabilities, for any breach of the Applicant's representations and warranties as set forth in Section 9.6.4 and for any failure of the Applicant to perform its obligations identified under Section 4.1.2.1.

9.10 Term and termination

9.10.1 Term

This WellsSecure CPS is effective upon publication and remains in full force and effect until an updated version is published.

9.10.2 Termination

Subject to section 9.10.3, this WellsSecure CPS may be terminated by Wells Fargo and such termination shall be effective thirty (30) days after publication of the same.

9.10.3 Effect of termination and survival

The terms of this WellsSecure CPS shall survive and continue apply so long as a Certificate issued by the WellsSecure Issuing CA remains active.

9.11 Individual notices and communications with participants

Unless otherwise specified in an agreement between the parties, all notices and requests in connection with this WellsSecure CPS communicated to Wells Fargo shall be deemed received as of the day they are actually received, when delivered either by messenger, nationally recognized delivery service, postage pre-paid, U.S. mail certified or registered, return receipt requested, and addressed to the Contact Persons set forth in Section 1.5.2, above. Notices and requests sent via first class U.S. mail will be deemed to be received by Wells Fargo within five (5) days after delivery.

PKI Participants shall use commercially reasonably and industry standard methods to communicate with each other based on the sensitivity or subject matter of the communication.

9.12 Amendments

All Participants understand and agree that this WellsSecure CPS may require periodic modifications and that Wells Fargo has the authority to modify this WellsSecure CPS. Any suggestions as to modifications should be communicated to the Contact Persons listed in Section 1.5.2 of this WellsSecure CPS.

9.12.1 Procedure for amendment

Changes to this WellsSecure CPS that, in the judgment of the Wells Fargo PKI Management, will have no or only a minimal effect on Participants, may be made without requiring the issuance of a new version of this WellsSecure CPS and without notification to Participants.

Changes that, in the judgment of the Wells Fargo PKI Management will have a significant impact on Participants will be made with only prior notice to Participants as set forth in Section 2.3.

9.12.2 Notification mechanism and period

Wells Fargo posts revisions of this WellsSecure CPS to the Wells Fargo website, but does not guarantee or set a notice and comment period and may make changes to this WellsSecure CPS without notice and without changing the version number. Wells Fargo may provide additional notice in the event that it makes any material changes to this WellsSecure CPS. Wells Fargo is solely responsible for determining what constitutes a material change of this WellsSecure CPS.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute resolution provisions

For all disputes between the Wells Fargo Trusted Identity Entities, on the one hand, and any Subscribing Customer, on the other, arising out of or in connection with their participation in the WellsSecure PKI, the dispute resolution procedures set forth in the subsections below ("Dispute Resolution Procedures") will be used. Disputes solely between Subscribing Customers that do not include claims against the Wells Fargo Trusted Identity Entities may also use these Dispute Resolution Procedures, but only if the parties expressly agree.

(a) Upon the demand of any Participant, any Dispute with respect to the Wells Fargo Trusted Identity Entities' compliance with this WellsSecure CPS, or with respect to CA operations and Certificates issued pursuant to this WellsSecure CPS and other applicable PKI Documents, shall be resolved by binding arbitration in accordance with the terms of this Section 9.13. A "Dispute" shall mean any action, dispute, claim or controversy of any kind, whether in contract or tort, statutory or common law, legal or equitable, now existing or hereafter arising under or in connection with, or in any way pertaining to the WellsSecure PKI or the action or inaction of the Wells Fargo Trusted Identity Entities. Any party may, by summary proceedings, bring an action in court to compel arbitration of a Dispute. Any party who fails or refuses to submit to arbitration following a lawful demand by any other party shall bear all costs and expenses incurred by such other party in compelling arbitration of any Dispute.

(b) Arbitration proceedings shall be administered by the American Arbitration Association ("AAA") or such other administrator as the parties shall mutually agree upon. Arbitration shall be conducted in accordance with the AAA Commercial Arbitration Rules. If there is any inconsistency between the terms hereof and any such rules, the terms and procedures set forth herein shall control. All Disputes submitted to arbitration shall be resolved in accordance with the Federal Arbitration Act (Title 9 of the United States Code). The arbitration shall be conducted at a location in Minnesota selected by the AAA or other administrator. All statutes of limitation applicable to any Dispute shall apply to any arbitration proceeding. All discovery activities shall be expressly limited to matters directly relevant to the Dispute being arbitrated. Judgment upon any award rendered in an arbitration may be entered in any court having jurisdiction, provided however, that nothing contained herein shall be deemed to be a waiver, by any party that is a bank, of the protections afforded to it under 12 U.S.C. § 91 or any similar applicable federal or state law.

(c) Arbitrators must be active members of the Minnesota State Bar or retired judges of the state or federal judiciary of Minnesota, with expertise in the substantive laws applicable to the subject matter of the Dispute. Arbitrators are empowered to resolve Disputes by summary rulings in response to motions filed prior to the final arbitration hearing. Arbitrators (i) shall resolve all Disputes in accordance with the substantive law of the state of Minnesota, (ii) may grant any remedy or relief that a court of the state of Minnesota could order or grant within the scope hereof and such ancillary relief as is necessary to make effective any award, and (iii) shall have the power to award recovery of all costs and fees, to impose sanctions and to take such other actions as they deem necessary to the same extent a judge could pursuant to the Federal Rules of Civil Procedure, the Minnesota Rules of Civil Procedure or other applicable law. Any Dispute in which the amount in controversy, as stated in the demand for arbitration, is $5,000,000 or less shall be decided by a single arbitrator who shall not render an award of greater than $5,000,000 (including damages, costs, fees and expenses). By submission to a single arbitrator, each party expressly waives any right or claim to recover more than $5,000,000. Any Dispute in which the amount in controversy exceeds, $5,000,000 shall be decided by majority vote of a panel of three arbitrators, provided however, that all three arbitrators must actively participate in all hearings and deliberations.

(d) Notwithstanding anything herein to the contrary, in any arbitration in which the amount in controversy exceeds $5,000,000, the arbitrators shall be required to make specific, written findings of fact and conclusions of law. In an arbitration where the award exceeds $5,000,000: (i) the arbitrators shall not have the power to make any award which is not supported by substantial evidence or which is based on legal error, (ii) an award shall not be binding upon the parties unless the findings of fact are supported

by substantial evidence and the conclusions of law are not erroneous under the substantive law of the state of Minnesota, and (iii) the parties shall have the right to judicial review (A) of whether the findings of fact rendered by the arbitrators are supported by substantial evidence in the record, and (B) of whether the conclusions of law are erroneous under the substantive law of the state of Minnesota. A party seeking judicial review under this provision shall be responsible for the attorney fees and costs of the other party in the event the party seeking such review is unsuccessful. Judgment confirming an award in such a proceeding may be entered only if a court determines that the award is supported by substantial evidence, was not based on legal error under the substantive law of the state of Minnesota and should not be vacated.

(e) No provision hereof shall limit the right of any party to obtain provisional or ancillary remedies, including without limitation injunctive relief, attachment or the appointment of a receiver, from a court of competent jurisdiction before, after, or during the pendency of any arbitration or other proceeding. The exercise of any such remedy shall not waive the right of any party to compel arbitration or reference hereunder.

(f) The arbitrator(s) will have no authority to award damages in excess of those allowed by this WellsSecure CPS. Any award in an arbitration under this Section shall be limited to monetary damages and shall include no injunction or direction to any party other than the direction to pay a monetary amount. The prevailing party in the arbitration shall be entitled to reasonable attorney fees and costs incurred in the arbitration proceedings.

(g) To the maximum extent practicable, the AAA, the arbitrator, and the parties shall take all action required to conclude any arbitration proceeding within 180 days of the filing of the Dispute with the AAA. No arbitrator or other party to an arbitration proceeding may disclose the existence, content or results thereof, except for disclosures of information by a party required in the ordinary course of its business, by applicable law or regulation, or to the extent necessary to exercise any judicial review rights set forth herein. This arbitration provision shall survive termination, amendment or Expiration of all PKI Documents that are applicable to the dispute or any relationship between the parties.

9.14 Governing law

This WellsSecure CPS is governed by the laws of the State of Minnesota of the United States of America, excluding its “Choice of Law” principles, and all Participants hereby submit to the exclusive jurisdiction and venue of the federal or state courts of that State.

9.15 Compliance with applicable law

This WellsSecure CPS may be subject to national, state, and local laws, rules, regulations, ordinances, decrees and orders applicable to the issuance of Certificates.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

This WellsSecure CPS, the applicable Sub-CA Agreement, RA Agreement (for business units not within WFBNA), Repository Agreement, Customer Agreements or other agreement between WFBNA and a non-Wells Fargo Participant, and other applicable PKI Documents, as periodically amended, constitute the entire agreement with respect to the rights, obligations, and responsibilities of the Participants. The headings preceding the text of the various provisions of this WellsSecure CPS are inserted solely for reference and shall not constitute a part of this WellsSecure CPS or affect its meaning, construction or effect.

9.16.2 Assignment

Relying Parties and Subscribers may not assign or delegate, in whole or part, by operation of law or otherwise, including in the event of a reorganization, merger, acquisition, divestiture, other deemed transfer or change of control, any of their rights or obligations under this WellsSecure CPS without Wells Fargo’s prior written consent. Any actual or attempted assignment or delegation contrary is null and void.

This WellsSecure CPS shall be binding upon and inure to the benefit of the parties hereto, their successors and any permitted assignees.

9.16.3 Severability

If part of any provision in this WellsSecure CPS is held to be illegal, invalid, or unenforceable by a court or other decision-making authority of competent jurisdiction, then the remainder of the provision shall be enforced so as to effect the intentions of the WellsSecure Issuing CA, and the validity and enforceability of all other provisions in this WellsSecure CP/CPS shall not be affected or impaired.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

See sections 9.9 and 9.13. Waiver of any one default of any provisions herein by the WellsSecure Issuing CA shall not waive subsequent defaults of the same or different kind.

9.16.5 Force Majeure

Wells Fargo shall not be liable for any default or delay in the performance of any of its obligations hereunder to the extent and while such default or delay is caused, directly or indirectly, by a cause outside the reasonable control of Wells Fargo, including but not limited to, fire, flood, earthquake, elements of nature or acts of God, acts of war, terrorism, riots, civil disorders, rebellions, or revolutions, strikes, lockouts, or labor difficulties.

9.16.6 Order of precedence.

In the event of a conflict between the most current version of this WellsSecure CP/CPS, and the respective version of such document that was in effect on the date of a Certificate issuance, the version in effect on the date of issuance prevails with regard to issuance of that Certificate and the most current version prevails with regards to the use, management, and Revocation of that Certificate, as well as to all other matters relating to the Certificate.

9.17 Other provisions

9.17.1 No Fiduciary Relationships

All non-Wells Fargo Participants agree that the participation of a WF Affiliate Organization or WF Affiliate Organization Unit in the WellsSecure PKI, the creation and operation of any WellsSecure Issuing CA, the issuance of Certificates by the WellsSecure Issuing CA, and assistance in that issuance by an RA, does not make any WF Affiliate Organization or WF Affiliate Organization Unit an agent, partner, joint venture, fiduciary, trustee, or other representative of any Subscribing Customer, Subject, or Applicant.

10 DEFINITIONS AND ACRONYMS

Activation Data: Data, other than keys, that is required to access or operate cryptographic modules (e.g., a passphrase or a Personal Identification Number or "PIN").

Applicant: An Individual authorized by an Organization to undertake the Registration Process for the purpose of having a Certificate issued to that Organization as a Wells Fargo Subscribing Customer.

Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, Government official, or other reliable third party customarily relied upon for such information.

Authentication Policy: A document issued by the WellsSecure PKI - specifying the I & A procedures to be used in connection with the Registration Process and with requests for Certificate Reissuance, Suspension, Unsuspension, and Revocation for all Certificates issued by any WellsSecure PKI's CA as well as with any specific PKI Implementation approved by the WellsSecure PKI.

Authority Revocation List (ARL): A list of Revoked CA Certificates. An ARL is a CRL for CA Cross-Certificates.

Basic Assurance Level: This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious.

Bridge CA: A Certificate Authority that establishes peer-to-peer trust relationships with different user communities by cross certifying with a Root or sub CA that allows the users to keep their natural trust points, while having the ability to interact and trust users whose Certificates are issued from a different CA

CA: See Certificate Authority

CA Services: Services specified in the WellsSecure CP and this WS CPS and provided by the WellsSecure PKI relating to the creation, issuance, or management of Certificates.

Certificate: A digitally-signed electronic record issued within a PKI that: (i) identifies the Organization issuing the Certificate as the "Organization (o)" in the Certificate's "Issuer Distinguished Name (idn)" field; (ii) identifies the Organization to which the Certificate is issued as the "Organization (o)" in the Certificate's "Subject" field; (iii) uniquely identifies the Subject as the "Common Name (cn)" in the "Subject" field of the Certificate; (iv) contains the Public Key associated with the Subject; and (v) states the Certificate's Operational Period.

Certificate Authority (CA): An authority possessing a valid Issuer Certificate and trusted by one or more users to issue and manage X.509 Public Key Certificates.

Certificate Policy (CP): A set of rules governing the operation, applicability, and use of a named set of Certificates for a defined set of users.

Certification Authority: See Certificate Authority

Certificate Revocation List (CRL): A regularly updated list of Invalid Certificates and Compromised Users that is created and digitally signed by the Organization (e.g., The WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2 or a Sub-CA) that issued the Certificates listed in such CRL.

Certificate Subscriber Agreement for Digital Certificates: A document that sets forth the terms and conditions of use which the Certificate Subscriber must accept after having had a reasonable opportunity to review in order to apply for, receive or use a Certificate.

Compromised Users: Those Subjects that have had their Certificates Revoked for reasons relating to key compromise or that, in the WellsSecure Issuing CA or RA's opinion, should undergo a full I & A before receiving any new Certificates.

CP: See Certificate Policy.

Cross-Certificate A Certificate used to establish a trust relationship between two Certification Authorities.

CR/EIS Executive Manager: Executive Manager of Wells Fargo Information Security Technology Organization.

DBA: Doing Business As

Device: A physically distinct hardware processing platform or set of software programs operated by a Subscribing Customer.

Digital Signature: The data produced by transforming an electronic record using Public Key Cryptography and the Private Key of the signer of the electronic record, allowing a recipient, having the original electronic record, the data produced by the transformation, and the signer's Public Key, to accurately determine: (i) whether the data produced by the transformation was generated using the signer's Private Key that corresponds to the signer's Public Key; and (ii) whether the original electronic record has been altered since such transformation.

Directory: An online, searchable database of Certificate status information (including CRLs, reasons for Revocation, and a list of Compromised Users)

Distinguished Name (DN): The Distinguished Name (DN) is used on Certificates and in the Repository to uniquely represent a Subject identified in a Certificate.

Domain Authorization Document: Documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in a Domain Name Registrar's WHOIS database as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

Domain Name: The label assigned to a node in the Doman Name System.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by a Domain Name Registrar's WHOIS database.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Domain Name System: A distributed hierarchical naming systems for computers, services, devices, or any resource connected to the Internet.

Employee: Any Individual employed by an Organization, whether full-time or part-time.

Encryption Certificate: A Certificate containing a Public Key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.

Expire: Means, with reference to any Certificate issued by a WellsSecure Issuing CA, that the date specified in the Certificate's "Validity" field (i.e., its Operational Period), has passed. See also Operational Period.

Good: An OCSP Responder-generated response to a Certificate status request, identifying that the Certificate in question is currently not Revoked or Suspended.

High Assurance Level: This level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

I & A: See Identification and Authentication.

Identification and Authentication (I & A): The process set forth in the Authentication Policy for ascertaining and confirming through appropriate inquiry and investigation the identity and authority of: (i) any Applicant undertaking the Registration Process, and the Wells Fargo Subscribing Customer and Subject designated by the Applicant to be named in the requested Certificate; or (ii) a Wells Fargo Subscribing Customer or Individual making a Reissuance, Suspension, UnSuspension, or Revocation request.

Individual: A living human being.

Invalid: Specifies that the Certificate is temporarily or permanently Revoked and is not valid.

IP Addresses: A unique string of numbers separated by periods that identifies each computer or device attached to the Internet.

Issuer Certificate: The Certificate issued to the WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2 and/or and WellsSecure Sub-CAs that contains the Public Key that corresponds to the Private Key an Organization uses to sign Certificates it issues. Although other Organizations may possess and issue Issuer Certificates, only the WellsSecure Public Root CA's Issuer Certificates, WellsSecure Public Root CA 01 G2's Issuer Certificates or Issuer Certificates it may issue to WellsSecure Sub-CAs are subject to the terms of the WellsSecure CP and this WS CPS.

Issuing CA: The CA that issued a Certificate and is identified in the "Issuer Distinguished Name" field of a particular Certificate.

Key Module: A hardware or software object that can be used securely to: (1) store one or more Private Keys; (2) create Digital Signatures or Authenticate data using a Private Key; and (3) generate Key Pairs or permit an externally generated Private Key to be inserted for storage and use. Key Modules can be implemented as Smart Cards, Hardware Security Modules or software-only Tokens.

Key Pair: Two mathematically related numbers, referred to as a Public Key and its corresponding Private Key, possessing properties such that: (i) the Public Key may be used to verify a Digital Signature generated by the corresponding Private Key; and/or (ii) the Public Key may be used to encrypt an electronic record that can be decrypted only by using the corresponding Private Key or vice versa.

Low Assurance Level: This level provides the lowest degree of assurance concerning identity of the Individual. One of the primary functions of this level is to provide data integrity to the information being signed. This level is relevant to environments in which the risk of malicious activity is considered to be low. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used for the latter where Certificates having higher levels of assurance are unavailable.

Medium Assurance level: This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.

Object Identifier (OID): A unique alphanumeric/numeric identifier registered under the International Standards Organization's applicable standard for a specific object or object class.

OCSP Responder: An online software application operated under the authority of a PKI to process online Certificate status requests (including Validation Service requests). See also, Online Certificate Status Protocol.

OFAC: Office of Foreign Assets Control

OID: See Object Identifier.

Online Certificate Status Protocol (OCSP): An online Certificate-checking protocol that enables an OCSP Responder to determine the status of an identified Certificate by contacting the Repository. See also OCSP Responder.

Operational Period: A Certificate's intended term of validity, including beginning and ending dates, as indicated in the Certificate's "Validity" field. See also Expire.

Organization: A non-consumer entity, including, but not limited to, companies, corporations, limited liability companies, associations, government agencies, partnerships, limited partnerships, and sole proprietorships.

Organizational Certificate Officer: An appointee who maintains the Private Key of an organizational Certificate, which is a Certificate issued to several entities operating in one capacity.

PKI Component: Hardware and software components that make up the WellsSecure PKI.

PKI Component Certificate: A Certificate that is issued to a PKI Component.

PKI Documents: The following documents issued by the WellsSecure PKI:

(a) The [WellsSecure CP];

(b) This WS CPS;

(c) Authentication Policies;

(d) Registration Authority Agreements;

(e) Customer Agreements;

(f) Sub-CA Agreements; and

(g) Other agreements, manuals or procedures provided to Program Members by the WellsSecure PKI.

Not all PKI Documents will be applicable to every Program Member.

PKI Implementation: An application or other business implementation within Wells Fargo or between Wells Fargo and one or more outside parties involving the use of Public Key Cryptography and Certificates.

PKI Implementation Agreement: An agreement between Wells Fargo and an outside party, or between different WF Affiliate Organization Units, which may be entered into (in addition to those Subscribing Customer or Relying Party Agreements that are signed by Organizations who become Wells Fargo Subscribing or Relying Parties) to establish terms and conditions under which Certificates may be used for specific PKI Implementations.

PKI Manager: Manager of WellsSecure PKI operations.

Private Key: The key of a Key Pair that must be kept secret by the holder of the Key Pair, and that is used to generate Digital Signatures and/or to decrypt electronic records that were encrypted with the corresponding Public Key.

Program Members: This term includes the Wells Fargo PKI Management, the WellsSecure Root CA, one or more RAs, all WellsSecure Sub-CAs, Repositories, and Wells Fargo Subscribing Customers operating under the authority of the WellsSecure PKI or to whom the WellsSecure PKI has issued Certificates. It does not include any Organization or Individual to whom the WellsSecure PKI has not issued a Certificate.

Public Key: The key of a Key Pair that is intended to be publicly shared with recipients of digitally signed electronic records and that is used by such recipients to verify Digital Signatures created with the corresponding Private Key and/or to encrypt electronic records so that they can be decrypted only with the corresponding Private Key.

Public Key Cryptography: A type of cryptography, also known as asymmetric cryptography, that uses a unique Key Pair in a manner such that the Private Key of that Key Pair can decrypt an electronic record encrypted with the Public Key, or can generate a Digital Signature, and the corresponding Public Key, to encrypt that electronic record or verify that Digital Signature.

Public Key Infrastructure (PKI): A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

RA: See Registration Authority.

Registration Authority (RA): A role within the WellsSecure PKI, under the authority of the WellsSecure PKI, that administers the Registration Process and processes requests for Certificate Reissuance, Suspension, Unsuspension, and Revocation. The RA does not create or issue Certificates.

RA Application: An enrollment system that allows the management of the digital certificate lifecycle..

Registration Process: The process administered by an RA that a Wells Fargo Subscribing Customer uses to apply for and obtain a Certificate.

Reinstate, Reinstatement: The process of transforming a Certificate from temporarily Revoked to Good.

Reissuance: The process of acquiring a new Certificate and associated Key Pair to replace an existing Certificate and associated Key Pair, prior to the Expiration of the existing Certificate and associated Key Pair's Operational Period.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Relying Party: A person or Entity who has received information that includes a Certificate and a Digital Signature verifiable with reference to a Public Key listed in the Certificate, and is in a position to rely on said Certificate.

Repository: A database containing information and data relating to Certificates as specified in the WellsSecure CP and this WS CPS; may also be referred to as a Directory.

Revoke, Revocation: The process of transforming the status of a Certificate to “Revoked”.

Revocation and Suspension Request Page: An online location established by the WellsSecure Issuing CA for the exclusive use of Wells Fargo Subscribing Customers or Subjects, used to request Certificate Revocation or Suspension.

Revoked: A Certificate status designation that means the Certificate has been rendered permanently invalid. Revoked is also an OCSP Responder-generated response to a Certificate status request provided when the Certificate in question has been Revoked or Suspended.

Root Certificate: A Certificate identifying a Root CA and that is issued and self-signed by the same Root CA that is identified in the Certificate.

Secure Socket layer (SSL) - Secure Socket Layer is a security protocol that operates between a browser and a Web site. It provides confidentiality and data integrity by means of cryptographic techniques.

Signature Key: A Private Key used solely for performing Digital Signatures.

Signing Certificate: A Public Key Certificate that contains a Public Key intended for verifying Digital Signatures rather than encrypting data or performing any other cryptographic functions.

Signing and Encryption Certificate Pair: A pair of Public Key Certificates issued to the same Subject, one for verifying Digital Signatures, and the other for encrypting data (e.g. electronic messages, files, documents, or data transmissions) or to establish or exchange a session key for encryption purposes.

S/MIME: Secure MIME (Multipurpose Internet Mail Extensions)

Software Key Storage System (SKSS): A software-only system or service for the performance of the functions of a Key Module. An SKSS may be implemented in a distributed architecture or client-server systems which may involve a single server or multiple servers.

SSL – See Secure Socket Layer

Subject: The Individual, Organization, or Device named in the "Common Name (cn)" section of a Certificate's "Subject" field.

Sub-CA: In a hierarchical PKI, a CA whose Certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).

Subscribing Customer: An Organization that is identified as the "Organization (o)" in the "Subject" field of a Certificate.

Superior CA: In a hierarchical PKI, a CA who has certified the Certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).

Suspended: A Certificate status designation that means the Certificate has been rendered temporarily Invalid. Suspension does not apply to SSL Certificates.

Suspend, Suspension: The process of transforming a Certificate from Good to temporarily Invalid. Suspension does not apply to SSL Certificates.

System: A discrete set of software and/or hardware, characterized by set of states that define the relationship between the systems inputs and outputs, which is designed to allow an application or group of applications to run.

Token: A hardware Device (such as a smart card) used to store a Key Pair and associated Certificate and to perform cryptographic functions.

TR: See Trusted Registrar.

Trusted Registrar: An Individual employed and appointed by a Wells Fargo Subscribing Customer to perform I & A of potential Subjects for Certificates issued to such Wells Fargo Subscribing Customer.

Trusted Root: A certification authority that is absolutely trusted by a Relying Party and is used for validating Certificates in certification paths.

Unknown: An OCSP Responder-generated response to a Validation Service request indicating that the Certificate status information cannot be located in the Directory.

Validation Service: The framework that supports requests from Relying Parties seeking confirmation of the status of a specific Certificate.

Wells Fargo: Wells Fargo Bank, N.A. or Wells Fargo Bank, national association (also referred to as WFBNA).

Wells Fargo PKI Management: Individuals within CR/EIS that are responsible for overseeing various aspects of the WellsSecure PKI's functions.

WellsSecure Authentication Policy: A document that describes the policies for authenticating the information provided in connection with a request for a Certificate under the WellsSecure PKI. See Sections 3.2.2, 3.2.3, and 3.2.4.

WellsSecure Issuing CA: For a given Certificate or CRL, the CA within the WellsSecure PKI (WellsSecure Public Root CA, WellsSecure Public Root CA 01 G2 or any of the WellsSecure Sub-CAs) that acts as the issuer.

WellsSecure OCSP Responder: An OCSP responder operated under the authority of the WellsSecure PKI and connected to the Repository to process Certificate status requests for Certificates issued by WellsSecure Issuing CAs. See also, OCSP Responder, Online Certificate Status Protocol.

WellsSecure PKI: The PKI System (including hardware, software, people, procedures, rules, policies, and obligations), which is governed by this Certificate Policy.

WellsSecure Public Root Certification Authority 01 G2 (WellsSecure Public Root CA 01 G2): One of the highest or top-level Certificate Authorities in the WellsSecure PKI. This CA uses SHA-2 algorithm for signing Certificates and CRLs.

WellsSecure Root Certificate Authority (WellsSecure Root CA): The highest or top-level Certificate Authority in the WellsSecure PKI.

WellsSecure Sub-CA: A Sub-CA who's Issuer Certificate identifies Wells Fargo as the "Organization (o)" in the Certificate's "Issuer Distinguished Name" field.

WF Entities: Means Wells Fargo & Company and any present or future subsidiary thereof as defined under 12 U.S.C. §1841 (d).

WFBNA PKI Governance Signoff: A Wells Fargo Standard Operating Procedure containing distinct sign-off requirements to manage regular PKI governance and approvals.

WF Affiliate Organization Unit: A sub-group or unit operated by or under the authority Wells Fargo or a WF Entity. In certain circumstances, WF Entities may be considered to be WF Affiliate Organization Units of Wells Fargo.

WHOIS: WHOIS is a database of all registered domains, and supports a query and response protocol used to query the registered owners, users or assignees of a Domain Name.

11 BIBLIOGRAPHY

The following documents were used in part to develop this WS CPS:

CAB Forum Guidelines	CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (the "CA/B Forum") July 2013: https://www.cabforum.org/Baseline_Requirements_V1_1_6.pdf
FIPS112	Password Usage, May 1985. http://csrc.nist.gov/publications/fips/index.html
FIPS140	Security Requirements for Cryptographic Modules, June 2001. http://csrc.nist.gov/publications/fips/index.html
FIPS186	Digital Signature Standard, January 2000. http://csrc.nist.gov/publications/fips/index.html
OMB04-04	OMB Memorandum M-04-04, E-Authentication Guidance for Federal agencies, December 2003, http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
PG2177	Wells Fargo Internal Business Continuity Plan "AC Wells Fargo PKI/PG2177"
PKI02-026	WellsSecure PKI Internal Policy "PKI Operations Manual"
PSPRF	Wells Fargo Internal Policy "Physical Security Polices for Restricted Facilities"
RFC2560	Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP, Myers, Ankney, Malpani, Galperin, Adams, June 1999. http://www.ietf.org/rfc/rfc2560.txt
RFC3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Housley, Polk, Ford and Solo, April 2002. http://www.ietf.org/rfc/rfc3280.txt
RFC5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Cooper, Santessan, Farrell, et al. May 2008 www.**ietf**.org/**rfc/rfc5280**.txt
RFC3647	Certificate Policy and Certification Practices Framework, Chokhani, Ford, Sabett, Merrill and Wu, October 2003. http://www.ietf.org/rfc/rfc3647.txt
SP800-63	Electronic Authentication Guideline, NIST Special Publication 800-63, Version 1.0.2, Burr, Dodson, and Polk, April 2006. http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
SP800-131A	Recommendations for the Transitioning of Cryptographic Algorithms and Key Lengths, NIST Special Publication 800-131A. Elaine Barker and Allen Roginsky. January 2011. http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf
WellsSecure CP	WellsSecure® PKI Certificate Policy Version 13.1. Dated January 2014. https://www.wellsfargo.com/com/cp

LAST PAGE