Wells Fargo PKI Certification Practice Statement

Issued by Wells Fargo Bank, N.A.

Version 13.1

Approved by the Wells Fargo PKI Management:7-27-15
Effective: 7-30-15

Wells Fargo Proprietary Information

Document Version	Document Date	Revision Details
Version 12	July 2009	Removed detailed physical and logical security information, copied implementation level details from WF CP, consistency with WF 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 WF CPS was skipped to achieve consistency between the WF CP and WF CPS. Version 12.1 of this WF 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 - 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 - Remove references to High Assurance and EV SSL certificate support
Version 13.0	April 2013	- This CPS will now be called Wells Fargo CPS, or WF CPS.
Version 13.1	May 2015	- 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. - 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 Definition, Suspension Definition, Wells Fargo PKI Management Definition. - Removed the requirement in section 3.1.2 that names need to be meaningful.

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Overview

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

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

1.1.1 Relationship Between A Certificate Policy And A Certification Practice Statement

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

In the event of any conflicts between the Wells Fargo CPS and any other applicable PKI Document, this Wells Fargo CPS will take precedence.

1.2 Document Name And Identification

This WF CPS is referred to as the "Wells Fargo Certification Practice Statement", "Wells Fargo CPS" or "WF CPS". It corresponds with Version 13.1 of the "Wells Fargo Certificate Policy" or "Wells Fargo CP" or "WF 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 Wells Fargo PKI will identify the Wells Fargo 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 Wells Fargo PKI supports multiple Certificate types. The types of Certificates supported by the WF 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 Wells Fargo PKI will identify the Wells Fargo 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 Wells Fargo PKI issues multiple types of Certificates at multiple Assurance Levels. The Assurance Levels supported by the WF 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 WF 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 Wells Fargo CPS, available upon request to the Wells Fargo PKI Contact (see Section 1.5.2).

1.2.4 Other PKI Documents

1.2.4.1 Sub-CA Agreements

The Wells Fargo Public Root CA and the Wells Fargo 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 Wells Fargo Sub-CAs. In such an event, the Organization or WF Affiliate Organization Unit seeking to become a Wells Fargo 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 WF CP, this WF 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 Wells Fargo Sub-CA.

1.2.4.2 RA Agreements

The Wells Fargo 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 Wells Fargo 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 WF CP, this WF 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo PKI. Nothing in this WF CPS or any other PKI Document will prevent the Wells Fargo 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 Wells Fargo 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 WF CP and this WF CPS. For Certificates issued at a Low level of assurance, a Customer Agreement may not be required.

For Certificates issued from the Wells Fargo 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 WF CP and this WF CPS, as well as specify such other terms and conditions applicable to the Subscribing Customer's role within the Wells Fargo 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 Wells Fargo PKI is not currently cross-certified.

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

Figure 1: Wells Fargo PKI SHA-1 Hierarchy

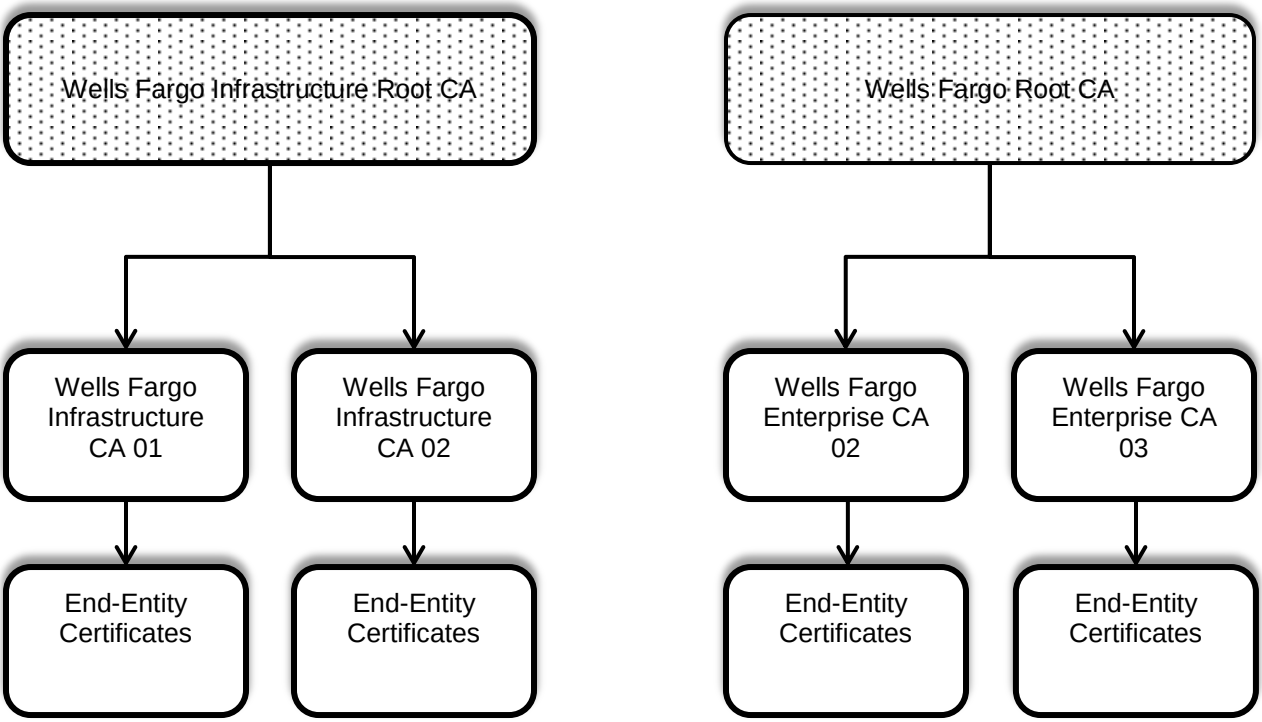
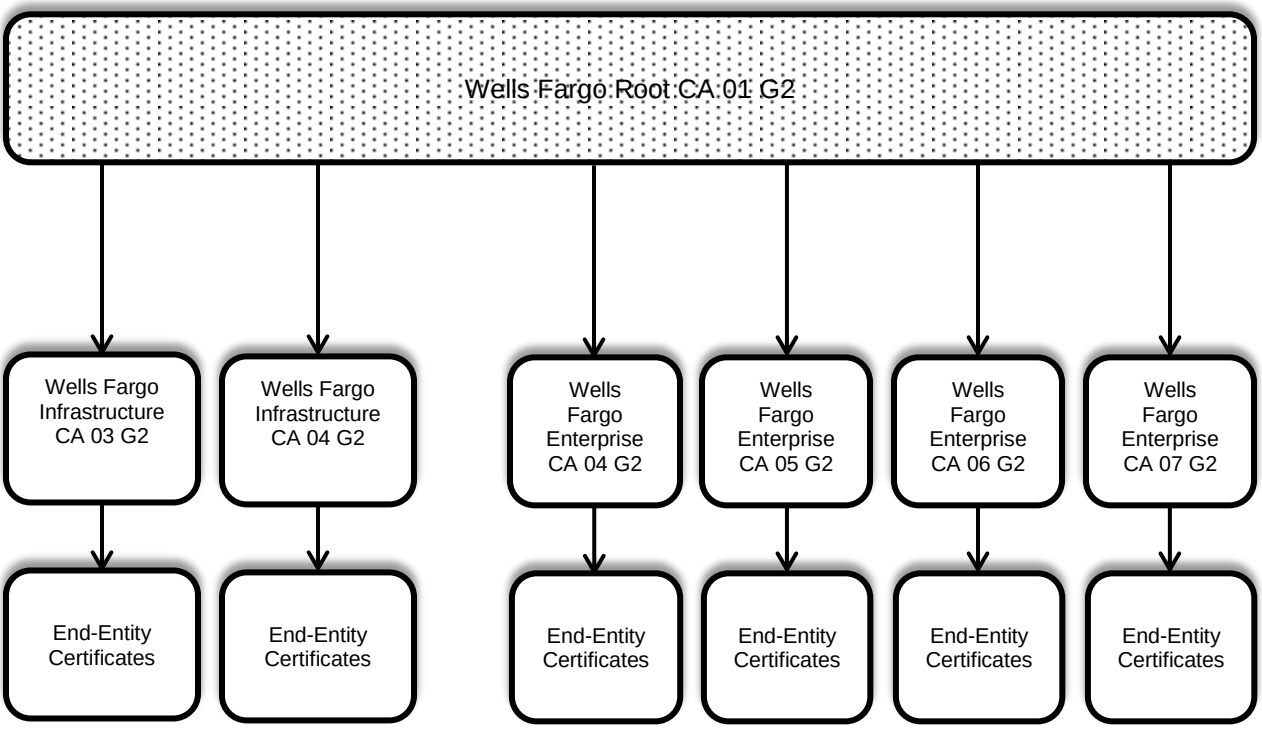


Figure 2: Wells Fargo PKI SHA-2 Hierarchy



1.3.1.1 SHA-1 CAs

1.3.1.1.1 Wells Fargo Public Root CA

The Wells Fargo Public Root CA is one of the highest level CAs for the Wells Fargo PKI. It is intended to be for public consumption. The Wells Fargo 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 Wells Fargo Infrastructure Root CA

The Wells Fargo Infrastructure Root CA is also one of the highest levels CA for the Wells Fargo PKI. 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. The Wells Fargo Infrastructure Root CA provides a self-signed Root Certificate.

1.3.1.1.3 Wells Fargo Enterprise CA 02 and Wells Fargo Enterprise CA 03

The Wells Fargo Enterprise CA's are considered Subordinate CAs within the Wells Fargo PKI. The Certificates for these CAs are signed by the Wells Fargo Root CA. These CAs are operated by the WF Affiliate Organization Unit known as CR/EIS, on behalf of WFBNA, and issue Certificates to other WF Affiliate Organization Units (as the Subscriber) that identify:

(a) Wells Fargo Personnel,

(b) Internal Wells Fargo Systems,

(c) Wells Fargo Devices, or

(d) PKI Components.

1.3.1.1.4 Wells Fargo Infrastructure CA 01 and Wells Fargo Infrastructure CA 02

The Wells Fargo Infrastructure CA 01 and Wells Fargo Infrastructure CA 02 are considered Subordinate CAs within the Wells Fargo PKI. The Certificate for each of these CAs is signed by the Wells Fargo Infrastructure Root CA. These CAs are operated by the WF Affiliate Organization Unit known as CR/EIS, on behalf of WFBNA. These CAs issue Certificates only to Wells Fargo Devices.

1.3.1.2 SHA-2 CAs

The following CAs use the SHA-2 hashing algorithm.

1.3.1.2.1 Wells Fargo Public Root CA 01 G2

The Wells Fargo Public Root CA 01 G2 is also one of the highest level CAs for the Wells Fargo PKI. It is intended to be for public consumption. The Wells Fargo 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 Wells Fargo Enterprise CA 04 G2, Wells Fargo Enterprise CA 05 G2 and Wells Fargo Enterprise CA 06 G2

The Wells Fargo Enterprise CA 04 G2, Wells Fargo Enterprise CA 05 G2, and Wells Fargo Enterprise CA 06 G2 are each considered a Subordinate CA within the Wells Fargo PKI. The Certificate for each of these CAs is signed by the Wells Fargo Root CA 01 G2. These CA are operated by the WF Affiliate Organization Unit known as CR/EIS, on behalf of WFBNA. These CAs issue Certificates to other WF Affiliate Organization Units (as the Subscriber) that identify:

(a) Wells Fargo Personnel,

(b) Internal Wells Fargo Systems,

(c) Wells Fargo Devices, or

(d) PKI Components.

1.3.1.2.3 Wells Fargo Infrastructure CA 03 G2 and Wells Fargo Infrastructure CA 04 G2

The Wells Fargo Infrastructure CA 03 G2 and Wells Fargo Infrastructure CA 04 G2 are considered Subordinate CAs within the Wells Fargo PKI. The Certificates for each of these CAs is signed by the Wells Fargo Root CA 01 G2. These CAs are operated by the WF Affiliate Organization Unit known as CR/EIS, on behalf of WFBNA. These CAs issues Certificates to Wells Fargo Devices.

1.3.1.2.4 Wells Fargo Enterprise CA 07 G2

The Wells Fargo Enterprise CA 07 G2 is considered a Subordinate CA within the Wells Fargo PKI. The Certificate for this CA is signed by the Wells Fargo Root CA 01 G2. This CA is operated by the WF Affiliate Organization Unit known as CR/EIS, on behalf of WFBNA. This CA issues Certificates to Wells Fargo Devices.

1.3.1.3 Additional Subordinate CAs

Nothing in this WF CPS or any other applicable PKI Document will prevent the Wells Fargo Public Root CA, or Wells Fargo 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 Wells Fargo Sub-CA.

To be appointed a Wells Fargo 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 WF CP, this WF CPS, other applicable PKI Documents, and any other requirements as the Wells Fargo PKI Management or the Wells Fargo 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 WF CPS and other applicable Wells Fargo PKI Documents.

The Wells Fargo PKI Management has authorized CR/EIS to act as an RA and perform RA Functions on behalf of the Wells Fargo PKI. Nothing in the Wells Fargo CP or any other PKI Document will prevent the Wells Fargo 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 Wells Fargo 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 WF CPS, other applicable Wells Fargo PKI Documents, and any other requirements as the Wells Fargo PKI Management or the Wells Fargo PKI may periodically establish.

The Wells Fargo PKI Documents applicable to an RA are: (i) the WF CP; (ii) this WF 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo 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 WF CPS, (ii) the WF 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo 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.

Wells Fargo 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo Public Root CA or Wells Fargo Public Root CA 01 G2 will only be used within the Wells Fargo 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 Wells Fargo 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 Wells Fargo CP conforms to this WF CPS.

1.5.4 CPS Approval Procedures

The Wells Fargo PKI Management is responsible for approving any changes to this WF 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 WF CP, this WF CPS and applicable PKI documents are:

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

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

(c) Operating and maintaining the Wells Fargo 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 Wells Fargo PKI and CRLs issued by any CA within the Wells Fargo 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 Wells Fargo PKI's behalf.

The PKI Documents applicable to the Repository are:

(i) this WF CPS;

(ii) the Wells Fargo CP;

(iii) the Repository Agreement, if applicable; and

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

The Directory provided by Wells Fargo is a fully compliant X.500 online and searchable database of Certificate status information. The Directory contains the then current CRL for each Wells Fargo Issuing CA, which is made available at the sole discretion of the Wells Fargo 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 Wells Fargo PKI will make this WF CPS and selected PKI Documents available to authorized Participants. The Wells Fargo Issuing CA will provide Certificate status information and Compromised User information to the Repository as set forth in this WF CPS. This WF 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 WF CPS.

2.3.2 Changes To PKI Documents

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

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

In the event WFBNA has a contractual relationship with a Participant that is a Relying Party, written notice of prospective WF CPS changes shall be communicated via U.S. Mail or email. The modified WF 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 WF 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 WF CPS, Subscribing Customers may revoke their Certificate(s) without obligating the Subscribing Customer to the terms of the new version of this WF CPS. A Subscribing Customer's decision not to Revoke its Certificate(s) within the twenty day notice period for the new version of this WF CPS constitutes acceptance of the terms of the new WF CPS.

The Wells Fargo 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 Wells Fargo PKI with those PKIs for which a Wells Fargo PKI's CA has been issued a Cross-Certificate; and
b) Relying Parties.

2.4 Access Controls On Repositories

The Wells Fargo 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 Wells Fargo PKI with those PKIs for which a Wells Fargo 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
CN = Wells Fargo Root Certificate Authority	http://crl.pki.wellsfargo.com/root.crl	http://ocsp-root.pki.wellsfargo.com/
CN = Wells Fargo Enterprise CA 02	http://crl.pki.wellsfargo.com/ent02.crl	http://validator.wellsfargo.com/
CN = Wells Fargo Enterprise CA 03	http://crl.pki.wellsfargo.com/ent03.crl	http://validator.wellsfargo.com/
CN = Wells Fargo Infrastructure Root CA	http://crl.pki.wellsfargo.com/infroot.crl	http://validator.wellsfargo.com/
CN = Wells Fargo Infrastructure CA 01	http://crl.pki.wellsfargo.com/inf01.crl	http://validator.wellsfargo.com/
CN = Wells Fargo Infrastructure CA 02	http://crl.pki.wellsfargo.com/inf02.crl	http://validator.wellsfargo.com/

Table 2.2: CRL and OCSP: SHA-2 CAs

CA Common Name	CRL Distribution Point	OCSP URL
CN = Wells Fargo Root Certification Authority 01 G2	http://crl.pki.wellsfargo.com/root01G2.crl	http://validator.wellsfargo.com/
CN=Wells Fargo Enterprise Certification Authority 04 G2	http://crl.pki.wellsfargo.com/ent04G2.crl	http://validator.wellsfargo.com/
CN=Wells Fargo Enterprise Certification Authority 05 G2	http://crl.pki.wellsfargo.com/ent05G2.crl	http://validator.wellsfargo.com/
CN=Wells Fargo Enterprise Certification Authority 06 G2	http://crl.pki.wellsfargo.com/ent06G2.crl	http://validator.wellsfargo.com/
CN = Wells Fargo Infrastructure CA 03 G2	http://crl.pki.wellsfargo.com/inf03G2.crl	http://validator.wellsfargo.com/
CN = Wells Fargo Infrastructure CA 04 G2	http://crl.pki.wellsfargo.com/inf04G2.crl	http://validator.wellsfargo.com/

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types Of Names

The Wells Fargo 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 Wells Fargo 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

No stipulation.

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 Wells Fargo 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 WF CP and this WF 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo PKI may take steps to honor private trademark rights, the Wells Fargo Issuing CA makes no guarantee that it will at any point honor such rights.

Under no circumstances is the Wells Fargo Issuing CA obligated to seek evidence of trademark ownership or court orders. Where the Wells Fargo 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 Wells Fargo 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 WF CP, and this WF 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)	Wells Fargo 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	Wells Fargo 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 Wells Fargo 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 Wells Fargo 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)	Wells Fargo 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.

3.3 Identification And Authentication For Re-Key Requests

Certificates issued by the Wells Fargo Public Root CA, Wells Fargo Public Root CA 01 G2 and Wells Fargo 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 Wells Fargo Public Root CA, Wells Fargo Public Root CA 01 G2, Wells Fargo Sub-CA, RA, and OCSP Responder Certificates are not re-keyed or rolled-over. The Wells Fargo Public Root CA, Wells Fargo Public Root CA 01 G2, Wells Fargo 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 WF CP;
(b) This WF CPS;
(c) Any other applicable PKI Documents; and
(d) Any agreements in force between the Wells Fargo 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 Wells Fargo 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 WF CP and this WF 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 Wells Fargo 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 WF CP, this WF 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 WF CP, this WF 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 Wells Fargo 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 WF CP, this WF 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 Wells Fargo 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 WF CP, this WF 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo 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 WF 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 Wells Fargo 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 WF CP, this WF 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 WF CP, this WF 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 WF CP, this WF 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo Issuing CA;

(i) Otherwise complying fully with all terms and conditions of participating in the Wells Fargo PKI as set forth in the WF CP, this WF 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 Wells Fargo 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 Wells Fargo PKI. A Validation Service request could be either an OCSP request to the appropriate Wells Fargo 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo PKI Entity
The Wells Fargo Issuing CA must Revoke a Certificate it has issued, and its RA must request Revocation of any Certificate it has requested the Wells Fargo 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 Wells Fargo Issuing CA that issued the Certificate has ceased operations for any reason;

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

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

(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

processes, that is not published as part of a Certificate, in the Directory or CRL, or in this Wells Fargo CPS.

9.3.2 Information not within the scope of confidential information

Notwithstanding Section 9.3.1, 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo Issuing CAs and Wells Fargo 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 Wells Fargo Issuing CAs or RAs. The Wells Fargo 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo Issuing CAs and their RAs will take reasonable steps to protect the confidentiality of Confidential Information (as defined in Section 9.3.1) 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo CPS section 9.3.1.

9.4.3 Information not deemed private

See this Wells Fargo CPS section 9.3.2.

9.4.4 Responsibility to protect private information

See this Wells Fargo CPS section 9.3.3.

9.4.5 Notice and consent to use private information

See this Wells Fargo CPS section 9.3.3.

9.4.6 Disclosure pursuant to judicial or administrative process

See this Wells Fargo CPS section 9.3.3.

9.4.7 Other information disclosure circumstances

See this Wells Fargo 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo CPS, and any rights not expressly granted under this Wells Fargo 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 Wells Fargo Issuing CA may grant Participants a revocable, nontransferable, non-sublicensable license to use their Certificates and Private Keys in accordance with this Wells Fargo 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo trademarks or other intellectual property will immediately cease and any Wells Fargo or Wells Fargo 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 Wells Fargo or will be destroyed.

9.5.4 Modifications

The terms and conditions of this Section 9.5 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, Wells Fargo 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 Wells Fargo 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 Wells Fargo RA or a third party RA authorized by the Wells Fargo 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 Wells Fargo 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 WF CP and other applicable PKI Documents;

(e) Subscriber and Subject consent to allow the Wells Fargo 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 Wells Fargo Issuing CA or RA has the authority to Revoke or Suspend the Certificate as set forth in this Wells Fargo 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 WELLS FARGO PKI, INCLUDING USE OF KEY PAIRS, CERTIFICATES, THE CA SERVICE, THE VALIDATION SERVICE OR ANY OTHER GOODS OR SERVICES PROVIDED BY THE WELLS FARGO PKI. THE WELLS FARGO TRUSTED IDENTITY ENTITIES FURTHER DISCLAIMS ANY AND ALL WARRANTIES, BOTH EXPRESS AND IMPLIED, THAT PARTICIPATION IN THE WELLS FARGO 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo Issuing CA is not acting either as principal or as agent for a principal that has been disclosed to the Wells Fargo 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 Wells Fargo Issuing CA and/or WF Entities;

(iv) Due to inadequate protection or safekeeping of a Certificate issued by The Wells Fargo Public Root CA, Wells Fargo Public Root CA 01 G2, Wells Fargo Sub-CA and/or WF Entities provided that such unauthorized use is by any Individual or Organization or Organization Unit other than the Wells Fargo 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 Wells Fargo Issuing CA; and/or

(vi) Due to any Individual or Organization or Organization Unit other than the Wells Fargo Issuing CA and/or WF Entities, causing an intrusion into, interference with, compromise, or destruction of the Wells Fargo PKI or any Wells Fargo Issuing CA, or any component or element thereof, or due to acts of God affecting the Wells Fargo PKI or any Wells Fargo Issuing CA, or any component or element thereof, unless any such events occur as a result of the Wells Fargo 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, HOWFOEVER 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 Wells Fargo Issuing CA Authorized RAs and Repositories

All liability for RAs and Repositories operating under the authority of a Wells Fargo Issuing CA is subsumed by the Wells Fargo Issuing CA and is subject to the limitations specified in Section 9.8. Despite the foregoing, nothing in this Section will prevent the Wells Fargo Issuing CA from pursuing its remedies against any Organization approved to undertake RA or Repository obligations on behalf of the Wells Fargo 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 Wells Fargo 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 9.9 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 Wells Fargo 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 9.9, 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 Wells Fargo 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 Wells Fargo CPS and other applicable PKI Documents; (vi) any unreasonable repudiation of a Certificate validated by any Wells Fargo Issuing CA; and (vii) the use of its Certificates in any transaction with a party that does not possess a Certificate issued by The Wells Fargo Public Root CA, Wells Fargo 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 Wells Fargo 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 9.9, 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 WF 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 Wells Fargo Public Root CA, Wells Fargo 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 Wells Fargo 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 Wells Fargo CPS is effective upon publication and remains in full force and effect until an updated version is published.

9.10.2 Termination

See section 9.10.1. Subject to section 9.10.3, this Wells Fargo 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 Wells Fargo CPS shall survive and continue apply so long as a Certificate issued by the Wells Fargo Issuing CA remains active.

Individual notices and communications with participants

Unless otherwise specified in an agreement between the parties, all notices and requests in connection with this Wells Fargo 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.

9.11 Amendments

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

9.11.1 Procedure for amendment

Changes to this Wells Fargo 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 Wells Fargo 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.

9.11.2 Notification mechanism and period

Wells Fargo posts revisions of this Wells Fargo CPS to the Wells Fargo website, but does not guarantee or set a notice and comment period and may make changes to this Wells Fargo 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 Wells Fargo CPS. Wells Fargo is solely responsible for determining what constitutes a material change of this Wells Fargo CPS.

9.11.3 Circumstances under which OID must be changed

No stipulation.

9.12 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 Wells Fargo 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 Wells Fargo CPS, or with respect to CA operations and Certificates issued pursuant to this Wells Fargo 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 Wells Fargo 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 Wells Fargo 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.

9.13 Governing law

This Wells Fargo 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.

9.14 Compliance with applicable law

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

9.15 Miscellaneous provisions

9.15.1 Entire agreement

This Wells Fargo 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 Wells Fargo CPS are inserted solely for reference and shall not constitute a part of this Wells Fargo CPS or affect its meaning, construction or effect.

9.15.2 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 Wells Fargo CPS without Wells Fargo’s prior written consent. Any actual or attempted assignment or delegation contrary is null and void.

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

9.15.3 Severability

If part of any provision in this Wells Fargo 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 Wells Fargo Issuing CA, and the validity and enforceability of all other provisions in this Wells Fargo CPS shall not be affected or impaired.

9.15.4 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 Wells Fargo Issuing CA shall not waive subsequent defaults of the same or different kind.

9.15.5 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.

9.15.6 Order of precedence.

In the event of a conflict between the most current version of this Wells Fargo 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.

9.16 Other provisions

9.16.1 No Fiduciary Relationships

All non-Wells Fargo Participants agree that the participation of a WF Affiliate Organization or WF Affiliate Organization Unit in the Wells Fargo PKI, the creation and operation of any Wells Fargo Issuing CA, the issuance of Certificates by the Wells Fargo 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 Wells Fargo 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 Wells Fargo PKI's CA as well as with any specific PKI Implementation approved by the Wells Fargo 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 Wells Fargo CP and this WF CPS and provided by the Wells Fargo 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 Wells Fargo Public Root CA, Wells Fargo 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 Wells Fargo Issuing CA or RA's opinion, should undergo a full I & A before receiving any new Certificates.

Corporate Risk / Enterprise Information Security (CR/EIS): The group within Wells Fargo that operates the Wells Fargo PKI.

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

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 Wells Fargo 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 Wells Fargo Public Root CA, Wells Fargo Public Root CA 01 G2 and/or and Wells Fargo 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 Wells Fargo Public Root CA's Issuer Certificates, Wells Fargo Public Root CA 01 G2's Issuer Certificates or Issuer Certificates it may issue to Wells Fargo Sub-CAs are subject to the terms of the Wells Fargo CP and this WF 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 Wells Fargo PKI.

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

PKI Documents: The following documents issued by the Wells Fargo PKI:

(a) The [Wells Fargo CP];

(b) This WF 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 Wells Fargo 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 Wells Fargo 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 Wells Fargo Root CA, one or more RAs, all Wells Fargo Sub-CAs, Repositories, and Wells Fargo Subscribing Customers operating under the authority of the Wells Fargo PKI or to whom the Wells Fargo PKI has issued Certificates. It does not include any Organization or Individual to whom the Wells Fargo 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 Wells Fargo PKI, under the authority of the Wells Fargo 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 Wells Fargo CP and this WF 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 Wells Fargo 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 Wells Fargo PKI's functions.

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

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

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

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

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

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

Wells Fargo 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 WF CPS:

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	Wells Fargo 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
Wells Fargo CP	Wells Fargo PKI Certificate Policy Version 13.1 https://www.wellsfargo.com/com/cp

LAST PAGE