Wells Fargo Bank N.A.

WellsSecure® PKI Certificate Policy

Issued by Wells Fargo Bank NA.

Version 12.2

Approved by the Wells Fargo Identity Assurance Policy Approval Committee on 10 September, 2010.

Wells Fargo Proprietary Information

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

Document Version	Document Date	Revision Details
12.0	30 November 2008	This version of the Wells Fargo CP replaces version 11, dated 20 April 2007. Memo of changes is available upon request.
12.1	30 November 2008	Added change tracking chart and edited typos.
12.1.1	01 April 2009	Modification of section 3.1.5 and footer. Memo of changes is available upon request.
12.1.2	30 May 2009	Memo of changes is available upon request.
12.2	10 September, 2010	- Phased migration of 1024 bit keys and SHA1, - Changes in requirements for RA Agreements, - Termination of Federal Bridge Cross Certification, - Carry over changes from CPS - CA Hierarchy, CA Names and other corrections,

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

TABLE OF CONTENTS

1 INTRODUCTION 12
1.1 Overview 12
1.1.1 Relationship between a Certificate Policy and a Certification Practice Statement 12
1.2 Document name and identification 12
1.2.1 Certificates issued on or before August 1, 2006 12
1.2.2 Certificates Issued Subsequent to August 1, 2006 13
1.2.3 Certificate Policy Identifications Previously Used 14
1.2.4 Other PKI Documents 14
1.3 PKI participants 16
1.3.1 Certification Authorities (CAs) 16
1.3.2 Registration Authorities 19
1.3.4 Subscribers 19
1.3.7 Relying Parties 21
1.3.8 Other participants 21
1.4 Certificate usage 21
1.4.1 Appropriate Certificate uses 21
1.4.2 Prohibited Certificate uses 23
1.5 Policy administration 24
1.5.1 Organization administering the document 24
1.5.2 Contact person 24
1.5.3 Persons determining CPS suitability for the policy 24
1.5.4 CPS approval procedures 24
1.6 Definitions and acronyms 25
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 25
2.1 Repositories 25
2.2 Publication of certain PKI Documents and Certificate status information 25
2.3 Time or frequency of publication 25
2.3.1 Certificate status information 25
2.3.2 Changes to PKI Documents 25
2.4 Access controls on Repositories 26
3 IDENTIFICATION AND AUTHENTICATION 26
3.1 Naming 26

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

3.1.1 Types of names 26
3.1.2 Need for names to be meaningful 26
3.1.3 Anonymity or pseudonymity of Subscribers 26
3.1.4 Rules for interpreting various name forms 26
3.1.5 Uniqueness of names 26
3.1.6 Recognition, authentication, and role of trademarks 27
3.2 Initial identity validation 27
3.2.1 Method to prove possession of Private Key 27
3.2.2 Authentication of Organization Identity 27
3.2.2.4 Authentication of Organizations for CA certificates 28
3.2.3 Authentication of Individual Identity 28
3.2.6 Non-verified Subscriber information 30
3.2.7 Validation of authority 30
3.2.8 Criteria for interoperation 30
3.3 Identification and authentication for re-key requests 30
3.3.1 Identification and authentication for routine issuance on upon renewal 30
3.3.2 Identification and authentication for re-issuance upon Revocation 31
3.4 Identification and authentication for Revocation request 31
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 31
4.1 Certificate Application 31
4.1.1 Who can submit a Certificate application 31
4.1.2 Enrollment process and responsibilities 31
4.2 Certificate application processing 33
4.2.1 Performing identification and authentication functions 33
4.2.2 Approval or rejection of Certificate applications 33
4.2.3 Time to process Certificate applications 34
4.3 Certificate issuance 34
4.3.1 CA actions during Certificate issuance 34
4.3.2 Shared Key Issuance 34
4.3.3 Notification to Subscriber by the CA of issuance of Certificate 34
4.4 Certificate acceptance 35
4.4.1 Conduct constituting Certificate acceptance 35
4.4.2 Publication of the Certificate by the CA 35
4.4.3 Notification of Certificate issuance by the CA to other entities 35
4.5 Key pair and Certificate usage 35
4.5.1 Subscriber Private Key and Certificate usage 35

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

4.5.2 Relying Party Public Key and Certificate usage 37
4.6 Certificate renewal 38
4.6.1 Circumstance for Certificate renewal 38
4.6.2 Who may request renewal 38
4.6.3 Processing Certificate renewal requests 38
4.6.4 Notification of new Certificate issuance to Subscriber 38
4.6.5 Conduct constituting acceptance of a renewal Certificate 38
4.6.6 Publication of the renewal Certificate by the CA 38
4.6.7 Notification of Certificate issuance by the CA to other entities 38
4.7 Certificate re-key 38
4.7.1 Circumstance for Certificate re-key 38
4.7.2 Who may request certification of a new Public Key 38
4.7.3 Processing Certificate re-keying requests 38
4.7.4 Notification of new Certificate issuance to Subscriber 38
4.7.5 Conduct constituting acceptance of a re-keyed Certificate 38
4.7.6 Publication of the re-keyed Certificate by the CA 39
4.7.7 Notification of Certificate issuance by the CA to other entities 39
4.8 Certificate modification 39
4.8.1 Circumstance for Certificate modification 39
4.8.2 Who may request Certificate modification 39
4.8.3 Processing Certificate modification requests 39
4.8.4 Notification of new Certificate issuance to Subscriber 39
4.8.5 Conduct constituting acceptance of modified Certificate 39
4.8.6 Publication of the modified Certificate by the CA 39
4.8.7 Notification of Certificate issuance by the CA to other entities 39
4.9 Certificate Revocation and Suspension 39
4.9.1 Circumstances for Revocation 39
4.9.2 Who can request Revocation 40
4.9.3 Procedure for Revocation request 40
4.9.4 Revocation request grace period 41
4.9.5 Time within which CA must process the Revocation request 41
4.9.6 Revocation checking requirement for Relying Parties 41
4.9.7 CRL issuance frequency 41
4.9.8 Maximum latency for CRLs 42
4.9.9 On-line Revocation/status checking availability 42
4.9.10 On-line Revocation checking requirements 42

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

4.9.11 Other forms of Revocation advertisements available 42
4.9.12 Special requirements regarding key compromise 42
4.9.13 Circumstances for Suspension 43
4.9.14 Who can request Suspension 43
4.9.15 Procedure for Suspension request 43
4.9.16 Limits on Suspension period 43
4.10 Certificate status services 43
4.10.1 Operational characteristics 43
4.10.2 Service availability 43
4.10.3 Optional features 43
4.11 End of subscription 43
4.12 Key escrow and recovery 44
4.12.1 Key escrow and recovery policy and practices 44
4.12.2 Session key encapsulation and recovery policy and practices 44
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 44
5.1 Physical controls 44
5.1.1 Site location and construction 44
5.1.2 Physical access 44
5.1.3 Power and air conditioning 45
5.1.4 Water exposures 45
5.1.5 Fire prevention and protection 45
5.1.6 Media storage 45
5.1.7 Waste disposal 45
5.1.8 Off-site backup 45
5.2 Procedural controls 46
5.2.1 Trusted roles 46
5.2.2 Number of Individuals Required per Task 46
5.2.3 Identification and Authentication for Each Role 47
5.3 Personnel controls 47
5.3.1 Qualifications, experience, and clearance requirements 47
5.3.2 Background check procedures 48
5.3.3 Training requirements 48
5.3.4 Retraining frequency and requirements 48
5.3.5 Job rotation frequency and sequence 48
5.3.6 Sanctions for unauthorized actions 48
5.3.7 Independent contractor requirements 48

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

5.3.8 Documentation supplied to personnel 49
5.4 Audit logging procedures 49
5.4.1 Types of events recorded 49
5.4.2 Frequency of processing log 52
5.4.3 Retention period for audit log 52
5.4.4 Protection of audit log 52
5.4.5 Audit log backup procedures 52
5.4.6 Audit collection System (internal vs. external) 52
5.4.7 Notification to event-causing subject 53
5.4.8 Vulnerability assessments 53
5.5 Records archival 53
5.5.1 Types of records archived 53
5.5.2 Retention period for archive 54
5.5.3 Protection of archive 54
5.5.4 Backup Procedures 54
5.5.5 Requirements for time-stamping of records 54
5.5.6 Archive collection system (internal or external) 54
5.5.7 Procedures to obtain and verify archive information 54
5.6 Key Pair changeover / Reissuance 55
5.6.1 WellsSecure Sub-CA Certificate Reissuance 55
5.6.2 Subscribing Customer or Subject Certificate Reissuance (Individual Certificates, Basic and Medium Assurance only) 55
5.6.3 Root Key Reissuance 56
5.7 Compromise and disaster recovery 56
5.7.1 Incident and compromise handling procedures 56
5.7.2 Computing resources, software, and/or data are corrupted 57
5.7.3 WellsSecure Issuing CA Private Key compromise procedures 57
5.7.4 Business continuity capabilities after a disaster 57
5.8 CA or RA termination 57
5.8.1 WellsSecure Issuing CA Termination 57
5.8.2 RA Termination 58
6 TECHNICAL SECURITY CONTROLS 58
6.1 Key Pair generation and installation 58
6.1.1 Key Pair generation 58
6.1.2 Private Key delivery 59
6.1.3 Public Key delivery to Certificate issuer 60

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

6.1.4 CA Public Key delivery to Relying Parties 60
6.1.5 Key sizes 60
6.1.6 Public Key parameters generation and quality checking 60
6.1.7 Key usage purposes 61
6.2 Private Key Protection and Cryptographic Module Engineering Controls 61
6.2.1 Cryptographic module standards and controls 61
6.2.2 Private Key (n out of m) multi-person control 61
6.2.3 Private Key escrow 61
6.2.4 Private Key backup 62
6.2.5 Private Key archival 62
6.2.6 Private Key transfer into or from a cryptographic module 62
6.2.7 Private Key storage on cryptographic module 62
6.2.8 Method of activating Private Key 62
6.2.9 Method of deactivating Private Key 62
6.2.10 Method of destroying Private Key 62
6.2.11 Cryptographic Module Rating 63
6.3 Other aspects of Key Pair management 63
6.3.1 Public Key archival 63
6.3.2 Certificate Operational Periods and Key Pair usage periods 63
6.4 Activation Data 64
6.4.1 Activation Data generation and installation 64
6.4.2 Activation Data protection 64
6.4.3 Other aspects of Activation Data 64
6.5 Computer security controls 64
6.5.1 Specific computer security technical requirements 64
6.5.2 Computer security rating 65
6.6 Life cycle technical controls 65
6.6.1 System development controls 65
6.6.2 Security management controls 65
6.6.3 Life cycle security controls 65
6.7 Network security controls 66
6.8 Time-stamping 66
7 CERTIFICATE, CRL, AND OCSP PROFILES 66
7.1 Certificate profile 66
7.1.1 Version number(s) 66
7.1.2 Certificate extensions 66

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

7.1.3 Algorithm object identifiers 66
7.1.4 Name forms 67
7.1.5 Name constraints 67
7.1.6 Certificate policy object identifier 67
7.1.7 Usage of Policy Constraints extension 67
7.1.8 Policy qualifiers syntax and semantics 67
7.1.9 Processing semantics for the critical Certificate policies extension 67
7.2 CRL profile 67
7.2.1 Version number(s) 67
7.2.2 CRL and CRL entry extensions 67
7.3 OCSP profile 67
7.3.1 Version number(s) 68
7.3.2 OCSP extensions 68
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 68
8.1 Frequency or circumstances of assessment 68
8.2 Identity/qualifications of assessor 68
8.3 Assessor's relationship to assessed Organization or Organization Unit 68
8.4 Topics covered by assessment 68
8.5 Actions taken as a result of deficiency 68
8.6 Communication of results 68
9 OTHER BUSINESS AND LEGAL MATTERS 69
9.1 Fees 69
9.1.1 Certificate issuance or renewal fees 69
9.1.2 Certificate access fees 69
9.1.3 Revocation or status information access fees 69
9.1.4 Fees for other services 69
9.1.5 Refund policy 69
9.2 Financial responsibility 69
9.2.1 Insurance coverage 69
9.2.2 Other assets 69
9.2.3 Insurance or warranty coverage for end-entities 69
9.3 Confidentiality of business information 69
9.3.1 Scope of Confidential Information 69
9.3.2 Information not within the scope of Confidential Information 70
9.3.3 Responsibility to protect Confidential Information 70
9.4 Privacy of personally identifiable information 71

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

9.4.1 Privacy plan ... 71
9.4.2 Information treated as private ... 71
9.4.3 Information not deemed private ... 72
9.4.4 Responsibility to protect private information ... 72
9.4.5 Notice and consent to use private information ... 72
9.4.6 Disclosure pursuant to judicial or administrative process ... 72
9.4.7 Other information disclosure circumstances ... 72
9.5 Intellectual property rights ... 72
9.5.1 Reservation of Rights ... 72
9.5.2 License ... 72
9.5.3 Termination ... 72
9.5.4 Modifications ... 73
9.6 Representations and warranties ... 73
9.6.1 CA representations and warranties ... 73
9.6.2 RA representations and warranties ... 73
9.6.3 Subscriber and Subject representations and warranties ... 73
9.6.5 Relying Party representations and warranties ... 74
9.6.6 Representations and warranties of other Participants ... 74
9.7 Disclaimers of Warranties ... 74
9.7.1 No Fiduciary Relationships ... 74
9.8 Limitations of liability ... 74
9.8.1 Limitations on Amount and Type ... 74
9.8.2 Exclusions of Certain Damages ... 74
9.9 Indemnities ... 76
9.9.1 Indemnification by RAs and Repositories ... 76
9.9.2 Indemnification by Subscribing Customers ... 76
9.9.3 Indemnification by the Relying Party ... 77
9.10 Term and termination ... 77
9.10.1 Term ... 77
9.10.2 Termination ... 77
9.10.3 Effect of termination and survival ... 77
9.11 Individual notices and communications with participants ... 78
9.12 Amendments ... 78
9.12.1 Procedure for amendment ... 78
9.12.2 Notification mechanism and period ... 78
9.12.3 Circumstances under which OID must be changed ... 78

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

9.13 Dispute resolution provisions 78
9.14 Governing law 80
9.15 Compliance with applicable law 80
9.16 Miscellaneous provisions 80
9.16.1 Entire agreement 80
9.16.2 Assignment 80
9.16.3 Severability 80
9.16.4 Enforcement (attorneys' fees and waiver of rights) 80
9.16.5 Force Majeure 80
9.17 Other provisions 80
10 DEFINITIONS AND ACRONYMS 80
11 BIBLIOGRAPHY 86

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

1 INTRODUCTION

1.1 Overview

The WellsSecure® Public Key Infrastructure ("WellsSecure PKI"), established under the authority of the Wells Fargo Identity Assurance Policy Approval Committee ("IAPAC") and managed by the Wells Fargo Organization Unit known as Technology Operations Group/Information Security Technology ("TOG/IST"), has been created to enable reliable and secure authentication of identities, and to facilitate the confidentiality and integrity of certain internal and external electronic transactions.

This Certificate Policy (the "CP") is issued by Wells Fargo as one of several "PKI Documents" (hereinafter defined) that taken together define and govern the WellsSecure PKI. These documents provide the framework under which all Certificates in the WellsSecure PKI will be created, issued, managed and/or used by Participants.

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

1.1.1 Relationship between a Certificate Policy and a Certification Practice Statement

This CP states what assurance can be placed in a Certificate issued by the Wells Fargo Root CA, WellsSecure Public Root CA or any WellsSecure Sub-CA. The WellsSecure Certification Practice Statement (the "WellsSecure CPS" or "CPS") is also included in the PKI Documents and states how the Wells Fargo Root CA, WellsSecure Public Root CA and/or WellsSecure Sub-CAs establish that assurance.

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

1.2 Document name and identification

This CP may be referred to as the "WellsSecure Certificate Policy" or "WellsSecure CP".

All Certificates issued by the WellsSecure PKI are issued pursuant to this CP. The OID for this CP is: 2.16.840.1.114171.500.0.0.

This CP governs both Certificates that were issued prior to the date of this CP as well as those issued subsequent to such date. Therefore, the following Object Identifier (OID) information is broken into two general sections. The first section sets forth the OIDs that are found in all Certificates that were issued on or before August 1, 2006; the next section sets forth the OIDs that will be included in all Certificates that are issued subsequent to August 1, 2006.

1.2.1 Certificates issued on or before August 1, 2006

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

1.2.1.1 Certificate Types

(a) The WellsSecure PKI supports multiple Certificate types. The types of Certificates supported by this CP 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 Infrastructure 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:

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

(i) “0” will signify a standard software key,

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

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

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

1.2.2 Certificates Issued Subsequent to August 1, 2006

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

1.2.2.1 Certificate Assurance Levels

The WellsSecure PKI issues multiple types of Certificates at multiple Assurance Levels. The Assurance Levels supported by this CP 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) High

High Assurance = 2.16.840.1.114171.500.5

Company High Assurance = 2.16.840.1.114171.500.8

TEST High Assurance = 2.16.840.1.114171.501.5

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

TEST Company High Assurance = 2.16.840.1.114171.501.8

(e) Extended Validation

Company EV Assurance = 2.16.840.1.114171.500.9

(f) 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 this CP 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 WellsSecure PKI Contact (see Section 1.5.2).

1.2.4 Other PKI Documents

1.2.4.1 Sub-CA Agreements

The Wells Fargo Root CA and WellsSecure Public Root CA may issue Issuer Certificates to one or more Organizations or WF Organization Units for the purpose of establishing such Organizations as WellsSecure Sub-CAs. In such an event, the Organization or WF Organization Unit seeking to become a WellsSecure Sub-CA must enter into a Sub-CA Agreement with WFNA and must be approved through a WFNA PKI Governance Signoff (see Section 1.5.1.1). The Sub-CA Agreement must bind such Organization or WF Organization Unit to the terms and conditions of this CP and other applicable PKI Documents. The Sub-CA Agreement must also specify such other terms and conditions applicable to the Organization or WF Organization Unit's role as a WellsSecure Sub-CA.

1.2.4.2 RA Agreements

The WellsSecure PKI may delegate its obligations to one or more qualified Organizations or WF 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.

In the event the WellsSecure PKI seeks to delegate these RA functions, the intended Organization , or WF Organization Unit (unless the WF Organization Unit is a unit under WFNA, in which case no RA Agreement is required) must enter into an RA Agreement with WFNA and must be approved through a WFNA PKI Governance Signoff (see Section 1.5.1.1);. The RA Agreement must bind the Organization or such WF Organization Unit to the terms and conditions of this CP and 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 Organization or WF Organization Unit "Know Your Customer Guidelines" and the appropriate authentication policies. These authentication policies include, but may not be limited to the WellsSecure Authentication Policy and the EV SSL Authentication Policy.

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

1.2.4.3 Customer Agreements and Terms of Use

(a) Customer Agreements

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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

For Certificates issued from the WellsSecure PKI to a Subscribing Customer at a Basic, Medium, or High level of assurance, the Subscribing Customer must enter into an applicable Customer Agreement. The Customer Agreement will bind such Subscribing Customer to the terms and conditions of this CP, as well as specify such other terms and conditions applicable to the Subscribing Customer's role within the WellsSecure PKI.

All Subscribing Customers to EV SSL Certificates shall sign an EV SSL Customer Agreement and the rights and responsibilities of said Subscribing Customers shall be to the extent provided in the EV SSL Customer Agreement and all PKI Documents incorporated therein by reference.

(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 Repository Agreement

The WellsSecure PKI may delegate its obligations to perform Repository functions to one or more qualified Organizations or WF Organization Units. In the event that the WellsSecure PKI seeks to delegate these functions, the intended Organization, or WF Organization Unit, must enter into a Repository Agreement with WFNA and must be approved through a WFNA PKI Governance Signoff (see Section 1.5.1.1). The Repository Agreement must bind the Organization or WF Organization Unit to the terms and conditions of this CP and other applicable PKI Documents. The Repository Agreement must also specify such other terms and conditions applicable to the Organization or WF Organization Unit's role as a Repository.

1.2.4.5 Cross-Certification Agreements

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

Currently, WFNA's Wells Fargo CA 01 is cross certified as follows:

1) Federal Bridge Certificate Authority (FBCA)

   a) Basic Assurance cross-certified at FBCA Basic.

By 31 December, 2010, this Cross-Certificate, along with any remaining valid End-entity Certificates issued under this Cross-Certificate, will be revoked.

2) GTE CyberTrust has issued a Cross-Certificate to WellsSecure Public Root CA. See Section 1.3.1.5 for details.

1.2.4.6 Accrediting Parties

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

Currently, WFNA has been approved as follows:

1) Secure Identity Services Accreditation Corporation (SISAC)

   a. Commercial Medium Assurance approved for use by SISAC

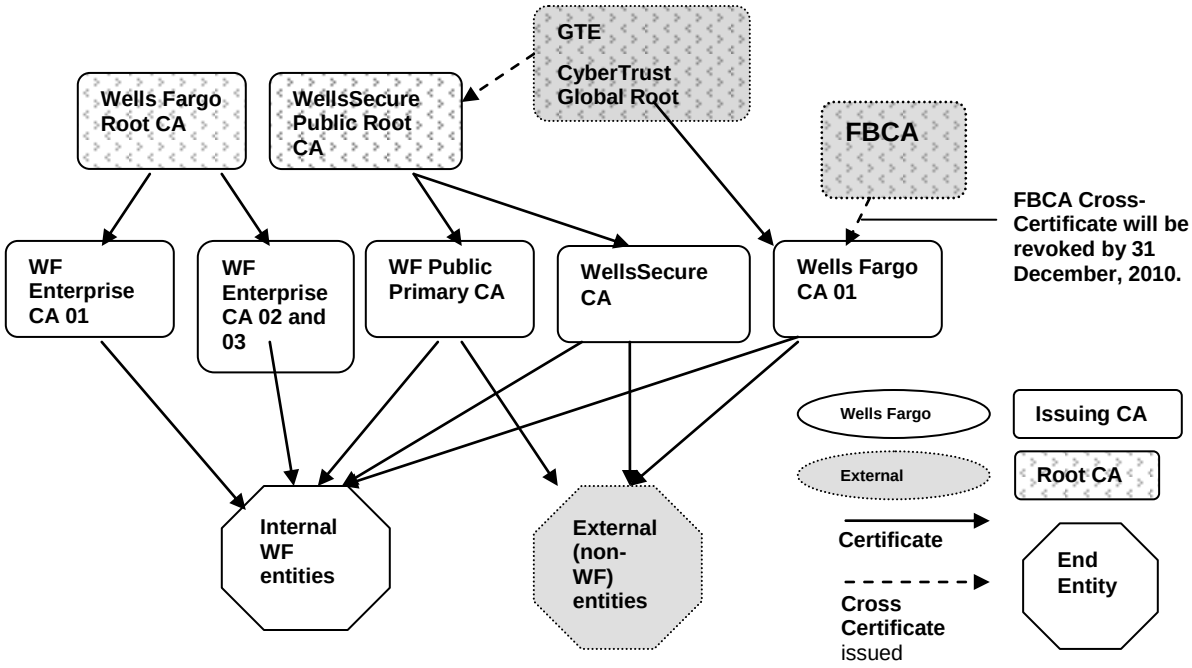
   b. Company Medium Assurance level approved for use SISAC

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

1.3 PKI participants

1.3.1 Certification Authorities (CAs)

The following diagram outlines all of the Certification Authorities which are part of the WellsSecure PKI, as well as related external Certification Authorities:



The Wells Fargo Root CA, WellsSecure Public Root CA, and all Subordinate CAs ("Sub-CAs") in the WellsSecure PKI are operated by a WF Organization or WF Organization Unit. Nothing in this CP, however, will prevent the approval of other WF Entities to act as Sub-CAs in the future, provided that such WF Entities (i) adhere to the requirements of this CP and the applicable PKI Documents, (ii) are approved through a WFNA PKI Governance Signoff, and (iii) adhere to any other requirements as the IAPAC (see Section 1.5.1) may establish.

The WellsSecure Public Root CA and the Wells Fargo CA 01 both have been issued Certificates signed by the GTE CyberTrust Global Root Certificate ("CyberTrust OmniRoot") that is maintained within CyberTrust's PKI. The CyberTrust OmniRoot and the CyberTrust PKI are not owned, operated or maintained by any WF Organization or WF Organization Unit and are not part of the WellsSecure PKI.

The Wells Fargo CA 01 has also been issued a Cross Certificate signed by the Federal Bridge Certification Authority (FBCA) that is maintained by the U.S. Federal Government. The FBCA issued Cross-Certificate and any remaining valid End-entity Certificates issued under this Cross-Certificate will be revoked by 31

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

December, 2010. The FBCA is not owned, operated, or maintained by any WF Organization or WF Organization Unit and is not part of the WellsSecure PKI.

1.3.1.1 Wells Fargo Root CA

The Wells Fargo Root CA Certificate is the highest level CA for the WellsSecure PKI and is operated by an internal WF Organization Unit approved by the IAPAC and approved through a WFNA PKI Governance Signoff to perform CA Services. The Wells Fargo Root CA provides a self-signed Root Certificate and is generally accepted in the PKI and identity verification industries as a Trusted Root.

1.3.1.2 WellsSecure Public Root CA

The WellsSecure Public Root CA is also at the highest level CA for the WellsSecure PKI. It is intended to be for public consumption and is not signed by the Wells Fargo Root. The WellsSecure Public Root CA provides a self-signed Root Certificate and is generally accepted in the PKI and identity verification industries as a Trusted Root. It has been issued a Cross-Certificate signed by the GTE CyberTrust Global Root (see Section 1.3.1.6). This CA is operated by the WF Organization Unit known as the Technology Operations Group (TOG), on behalf of WFNA, and only issues Certificates to CAs that are subordinate to itself.

1.3.1.3 Wells Fargo Enterprise CAs

The Wells Fargo Enterprise CA's Certificates are signed by the Wells Fargo Root CA. These CAs are considered Subordinate CAs within the WellsSecure PKI. These CAs are operated by the WF Organization Unit known as the Technology Operations Group (TOG), on behalf of WFNA, and issue Certificates to other WF Organization Units (as the Subscriber) that identify:

(a) Wells Fargo Personnel,

(b) Internal Wells Fargo Systems,

(c) Wells Fargo Devices, or

(d) Infrastructure Components.

1.3.1.4 Wells Fargo Public Primary CA

The Wells Fargo Public Primary Certificate Authority is part of the WellsSecure PKI, but it has been issued a Certificate with the following field identifiers: *subject name CN=WellsSecure Public Primary Certificate Authority, OU=Wells Fargo Certificate Authorities, O=Wells Fargo, C=US*, signed by the WellsSecure Public Root. This CA is operated by TOG, on behalf of WFNA, and may issue EV SSL Certificates to either Organizations or WF Organization Units that identify the Systems of such Organizations or WF Organization Units.

1.3.1.5 Wells Fargo CA 01

The Wells Fargo CA 01 is part of the WellsSecure PKI, but it has been issued a Certificate with the following field identifiers: *subject name CN=Wells Fargo Certificate Authority 01, OU=Wells Fargo Certification Authority, O=Wells Fargo, C=US*, signed by the CyberTrust OmniRoot. The Wells Fargo CA 01 is considered a Subordinate CA within the WellsSecure PKI, even though it does not have a Certificate that is signed by the Wells Fargo Root CA. The Wells Fargo CA 01 is operated by TOG,, on behalf of WFNA, and currently issues Certificates to Subscribers that identify:

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

(b) Organizations or Organization Units,

(c) Systems, or

(d) Devices.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

The Wells Fargo CA 01 is an Issuing CA only. There will be no CAs that are subordinate to the Wells Fargo CA 01. This CA has been issued a Cross Certificate signed by the FBCA (see Section 1.3.1.8). The FBCA issued Cross-Certificate and any remaining valid End-entity Certificates issued under this Cross-Certificate will be revoked by 31 December, 2010.

1.3.1.6 WellsSecure CA

The WellsSecure CA is part of the WellsSecure PKI, but it has been issued a Certificate with the following field identifiers: *subject name CN=WellsSecure CA, OU=Wells Fargo Bank NA, O=Wells Fargo WellsSecure, C=US*, signed by the WellsSecure Public Root CA. The WellsSecure CA is considered a Subordinate CA within the WellsSecure PKI. The WellsSecure CA is operated byTOG, on behalf of WFNA, and currently issues Certificates to Subscribers that identify:

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

(b) Organizations or Organization Units,

(c) Systems, or

(d) Devices.

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

1.3.1.7 GTE CyberTrust Global Root

The GTE CyberTrust Global Root ("CyberTrust OmniRoot") is a third-party Root Certificate Authority, with the following field identifiers: *subject name CN=GTE CyberTrust Global Root, OU=GTE CyberTrust Solutions, Inc., O=GTE Corporation, C=US*. The Root CA associated with this Root Certificate is not owned, operated or maintained by any WF Organization or WF Organization Unit and is not part of the WellsSecure PKI. The CyberTrust OmniRoot is owned, operated and maintained by CyberTrust and is part of the CyberTrust PKI. The CyberTrust OmniRoot is the Root Certificate to which the Wells Fargo CA 01 is chained. As such, the CyberTrust OmniRoot is responsible for signing the Wells Fargo CA 01 Certificate. GTE CyberTrust has also issued a Cross-Certificate to WellsSecure Public Root CA. The operations and procedures associated with the CyberTrust OmniRoot, for signing the Certificate issued to the Wells Fargo CA 01 and for issuing the Cross-Certificate to the Wells Secure Public Root CA donot fall within this CPS. The CPS for the CyberTrust OmniRoot may be found at the following URL:

http://cybertrust.omniroot.com/repository.cfm

1.3.1.8 Federal Bridge Certification Authority

The Federal Bridge Certification Authority (FBCA) is a third-party Bridge Certificate Authority, with the following field identifiers: *subject name OU=Entrust, OU=FBCA, O=U.S. Government, C=US*. The CA associated with this Bridge Certificate is not owned, operated or maintained by any WF Organization or WF Organization Unit and is not part of the WellsSecure PKI. The FBCA is owned, operated and maintained by the U.S. Federal Government. The FBCA has issued a Cross Certificate to the Wells Fargo CA 01. The operations and procedures associated with the FBCA for signing the Cross Certificate issued to the Wells Fargo CA 01 do not fall within this CP. The Certificate Policy for the FBCA may be found at the following URL:

http://www.cio.gov/fpkipa/

The FBCA issued Cross-Certificate and any remaining valid End-entity Certificates issued under this Cross-Certificate will be revoked by 31 December, 2010.

1.3.1.9 Additional Subordinate CAs

Nothing in this CP or any other applicable PKI Document will prevent the Wells Fargo Root CA or WellsSecure Public Root CA from issuing Issuer Certificates to an Organization or WF Organization Unit for the purpose of establishing that Organization or WF Organization Unit as a WellsSecure Sub-CA. To be appointed a WellsSecure Sub-CA, an Organization or WF Organization Unit must: (i) be authorized through

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

a WFNA PKI Governance Signoff; (ii) execute a Sub-CA Agreement with WFNA; and (iii) agree to be bound by the terms and conditions of this CP, other applicable PKI Documents, and any other requirements as the IAPAC or the WellsSecure PKI may periodically establish.

1.3.2 Registration Authorities

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

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

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

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

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

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

1.3.3 Trusted Registrars

A Trusted Registrar 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.

In the event the Subscribing Customer has obtained its Certificates from an RA that has been authorized by the WellsSecure PKI to perform RA Functions, Trusted Registrars will only be permitted if the RA has specifically granted permission to such Subscribing Customer to use Trusted Registrars. TRs must have been issued a Certificate at the same or higher Assurance Level than that of the Certificate that they are requesting.

1.3.4 Subscribers

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

(a) Organizations

Organizations eligible to become Subscribing Customers are limited to those that: (i) have an existing business relationship with a WF Organization or WF Organization Unit; (ii) have an existing business relationship with a customer of a WF Organization or WF Organization Unit; or (iii) in the sole discretion of Wells Fargo, are considered to have a potential business relationship. The WellsSecure PKI retains the sole and exclusive right to reject any Organization's application to become a Subscribing Customer. In all events, any Organization seeking to become a Subscribing Customer must execute an applicable Customer Agreement authorizing the WellsSecure Sub-CA to issue Certificates to it. Once an Organization has become a Subscribing Customer, the Organization can authorize one or more Applicants who can request Certificates from the WellsSecure Sub-CA. For each Certificate it requests, the Applicant must successfully complete the applicable Registration Process.

(b) Individuals

(i) Generally

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

Individuals eligible to become Subscribing Customers are limited to those that: (A) will use the Certificate in connection with his or her business or professional purposes and not for consumer purposes; (B) have an existing business relationship with a WF Organization or WF Organization Unit; (C) have an existing business relationship with a customer of a WF Organization or WF Organization Unit; or (D) in the sole discretion of Wells Fargo, are considered to have a potential business relationship. In all events, any Individual seeking to become a Subscribing Customer must execute an applicable Customer Agreement authorizing the WellsSecure Sub-CA to issue Certificates to him or her. Once an Individual has become a Subscribing Customer, the Individual is the only person who is authorized to request Certificates from the WellsSecure Sub-CA. The Individual Subscribing Customer cannot designate any other Individual to request Certificates on the Individual Subscribing Customer's behalf. For each Certificate he or she requests, the Individual must successfully complete the applicable Registration Process.

(ii) For Low Assurance Level Certificates

For Certificates issued with the Low Assurance level the Subscribing Customer may be an Individual based on his or her, or his or her Organization's, existing business relationship with a WF Organization, WF Organization Unit, or the RA that is requesting the Certificate. The WF Organization, WF 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 Organization Unit or RA, so long as the minimum language requirements as agreed between WFNA 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 CP, (ii) the Customer Agreement (including any documents referenced therein, including, but not limited to: the Trusted Registrar Manual, the User Guide, the Roaming Activation Guide. the Smart Card Activation Guide, and in the case of EV SSL Customer's, the Guidelines for EV SSL Certificates) signed by such Subscribing Customer, and (ii) the Terms of Use.

1.3.5 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 Organization or WF Organization Unit that has an existing business relationship with the Subscribing Customer, to undertake the Registration Process for Certificate Issuance for such Subscribing Customer.

1.3.6 Subjects

An Applicant may 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 must be 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.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

1.3.7 Relying Parties

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

1.3.8 Other participants

No stipulation.

1.4 Certificate usage

The CAs within the WellsSecure PKI issue Certificates at the Assurance Levels described in Section 1.2.2.1. These Certificates are issued pursuant to different practices and procedures and are suitable for different purposes based on the Assurance Levels. Policies governing the appropriate issuance of these Certificates are set forth below. Each Certificate issued will contain 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.

1.4.1 Appropriate Certificate uses

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

1.4.1.1 Low Assurance Level

This level provides the lowest degree of assurance. One of the primary functions of this level is to provide data integrity to the information being signed. This level is relevant to environments in which the risk of malicious activity is considered to be low. It may be used for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used where Certificates having higher levels of assurance are unavailable, or where the Relying Party has determined that it is sufficient. It cannot be used for transactions requiring non-repudiation. Low Assurance Level Certificates are issued to Individual end users and not to Organizations, Systems or Devices.

1.4.1.2 Basic Assurance Level

This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious. This level of assurance meets the requirements of E-Authentication Level 3 as defined in [SP800-63] and [OMB04-04]. . 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. This level of assurance meets the requirements of E-Authentication Level 3 as defined in [SP800-63] and [OMB04-04]. 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. This level of assurance meets the requirements of E-Authentication Level 3 as defined in [SP800-63] and [OMB04-04].

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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. This level requires that all persons who participate in Trusted Roles (see Section 5.2.1) related to the issuance of Certificates at this Assurance Level shall be citizens of the United States of America. This level of assurance meets the requirements of E-Authentication Level 3 as defined in [SP800-63] and [OMB04-04]. 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. This level requires that all persons who participate in Trusted Roles (see Section 5.2.1) related to the issuance of Certificates at this Assurance Level shall be citizens of the United States of America. This level of assurance meets the requirements of E-Authentication Level 3 as defined in [SP800-63] and [OMB04-04]. 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 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. Certificates with this Assurance Level can only be issued for use in level 2 of [FIPS140] certified, or higher, cryptographic containers. Currently, the WellsSecure Sub-CAs do not issue Certificates at this level. Additional protections and requirements for Certificates issued under this Assurance Level may be added prior to the WellsSecure Sub-CAs issuing Certificates at this level. High Assurance Level Certificates are issued to Individual end users and not to Organizations, Systems or Devices.

1.4.1.8 Test Assurance Levels

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

1.4.1.9 Infrastructure Component

Infrastructure Component Certificates shall be issued only to components of the Public Key Infrastructure and may be used only by the Infrastructure Component that is named in the "Common Name (cn)" section of the "Subject" field of such Certificate. Infrastructure 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. Infrastructure Component Certificates that are issued from the Wells Fargo Root CA will only be used within the WellsSecure PKI.

1.4.1.10 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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

further described in Sections 3.2.4 and 6.1.2 may be performed by a systems administrator for the Subscribing Customer.

1.4.1.11 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.

1.4.1.12 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.

1.4.1.13 Company 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. Company High Certificates are issued to Systems or Devices and not to Individual end users. Certificates with this Assurance Level can only be issued for use in level 2 of [FIPS140] certified, or higher, cryptographic containers. Currently, the WellsSecure Sub-CAs do not issue Certificates at this level. Additional protections and requirements for Certificates issued under this Assurance Level may be added prior to the WellsSecure Sub-CAs issuing Certificates at this level. In the event a Company High Certificate is issued to an Organization, the Applicant is responsible for the Certificate.

1.4.1.14 Company EV SSL Assurance Level

This level is reserved only for Systems that the Wells Fargo Public Primary CA has certified in conformance with the Guidelines for EV SSL Certificates.

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.

Subscribers shall not, nor shall Subscribers allow any of their Certificate Holders, to use the CA Service or the Validation Service, or Certificates in fraudulent manner, including in any of the following: manipulating the client clock to reflect anything other than the correct, current, regional time, and/or damaging, investigating, re-engineering, or otherwise interfering with the token, clock, Certificate, smart card chip, or other element of the WellsSecure PKI.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

1.5 Policy administration

1.5.1 Organization administering the document

The Identity Assurance Policy Approval Committee ("IAPAC") is responsible for overseeing various aspects of the WellsSecure PKI's functions. These responsibilities currently include: (a) approving the content of this CP and other applicable PKI Documents; and (b) developing and approving the Standard Operating Procedures ("SOPs") which direct the WFNA PKI Governance Signoffs.

The IAPAC will be comprised of at least three (3) members, with at least one (1) representative from the WFNA Law Department and WFNA Risk / Compliance. Optional members may include WFNA Human Resources and business representatives, for example: Retail/Consumer, Lending, Wholesale and WellsSecure.

The IAPAC will review proposals and policies drafted for approval by the Identity Assurance Working Group ("IAWG"), an ad-hoc working group currently managed by IST. The policies and proposals brought before the IAPAC will be practice statements and policies associated with digital Certificates, biometrics, and other identity assurance related technologies as required by Wells Fargo and constructed by the IAWG. The IAWG is open to all Wells Fargo lines of business. The IAWG may be split into sub-groups as appropriate.

Certain approvals for documents and operational activities require a WFNA PKI Governance Signoff in addition to IAPAC approval. The WFNA PKI Governance Signoff is described in Section 1.5.1.1 below.

1.5.1.1 WFNA PKI Governance Signoffs

Wells Fargo SOPs have been developed by the IAPAC which contain distinct sign-off requirements to manage regular PKI governance as documented in this CP. Where WFNA PKI Governance Signoff is required, approval must be obtained from assigned representatives of the following WF Organization Units: Legal, Business-line, TOG/IST, and Enterprise Architecture.

1.5.1.2 Wells Fargo PKI Review Board

The Wells Fargo PKI Review Board was the organization responsible for governance of the WellsSecure PKI until April, 2007. Information about the PKI Review Board was published in earlier versions of the Wells Fargo CPS, available upon request to the WellsSecure PKI contact persons (see Section 1.5.2).

1.5.2 Contact person

The contact persons for this CP are as follows:

IAPAC Chairman
Wells Fargo Services
8901 E MOUNTAIN VIEW RD
SCOTTSDALE, AZ
85258-4422

General Counsel, Law Department
MAC A0194-27545
Fremont St
27th Floor
San Francisco, CA
94105-2204

1.5.3 Persons determining CPS suitability for the policy

The members of the IAPAC are responsible for asserting that the WellsSecure CPS conforms to this CP, and will determine the suitability of the WellsSecure CPS for any additional Certificate Policy.

1.5.4 CPS approval procedures

The IAPAC will determine the approval procedures for the WellsSecure CPS.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

1.6 Definitions and acronyms

See Section 10.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

2.1.1 Obligations

In accordance with this CP and other applicable PKI Documents, the Repository's obligations are:

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

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

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

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

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

(f) Making CA Certificates and CRLs publicly available for retrieval from the Repository 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year and scheduled down-time not to exceed 0.5% annually.

2.1.2 Purpose

The primary purpose of the Repository is to provide Certificate status. To fulfill this purpose,

The requirements and obligations of the repositories within the WellsSecure PKI shall be described within the WellsSecure CPS.

The WellsSecure PKI also makes Certificate status information available through an OCSP Responder; see Section 4.9.9 for more information.

2.2 Publication of certain PKI Documents and Certificate status information

The WellsSecure PKI will make this CP and selected PKI Documents available to authorized Participants. The WellsSecure Issuing CA will provide Certificate status information and Compromised User information to the Repository as set forth in this CP.

This CP can be found on the Internet in .pdf format at: http://www.wellsfargo.com/cp.

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 CP.

2.3.2 Changes to PKI Documents

2.3.2.1 In the event the IAPAC decides to make significant changes to this CP, as set forth in Section 9.12, the PKI manager will make an electronic copy of the modified CP publicly available to all Participants. The new version of the CP will become effective immediately for all Participants with which WFNA does not have a contractual relationship relating to the WellsSecure PKI.

2.3.2.2 In the event WFNA has a contractual relationship with a Participant that is a Relying Party, written notice of prospective CP changes shall be communicated via U.S. Mail or email. The modified CP will become effective twenty (20) days after the notice of the changes has been delivered to such Participants.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

After the twenty day notice period, the new CP will supersede all previous versions and will be binding on all such Participants from that point forward.

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

2.4 Access controls on Repositories

The WellsSecure PKI shall make publicly available through the Internet a Repository containing Certificate status information, CA certificates, CRLs and any other public and non-personal information Wells Fargo deems necessary to support: (a) the interoperation of the WellsSecure PKI with those PKIs for which a WellsSecure CA has been issued a Cross Certificate; and (b) Relying Parties.

3 IDENTIFICATION AND AUTHENTICATION

The following sections describe the procedures to be followed for the I & A of: (a) Applicants, (b) Individual Sponsors for Certificates issued to Devices or Systems, and (c) Subjects. These procedures are set forth in more detail in one or more applicable Authentication Policies.

3.1 Naming

3.1.1 Types of names

The WellsSecure Certificate Management System ("WSCMS") used by the WellsSecure Issuing CA will systematically create the DN in such a manner using the information that is gathered during the enrollment process to create the DN, and each DN will be unique within the WellsSecure PKI (see Section 3.1.5).

3.1.2 Need for names to be meaningful

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

3.1.3 Anonymity or pseudonymity of Subscribers

No stipulation.

3.1.4 Rules for interpreting various name forms

Names shall be interpreted according to the Certificate Profiles set forth in Section 7.1 of the WellsSecure CPS.

3.1.5 Uniqueness of names

The WellsSecure PKI will verify that all DNs used within its domain are unambiguous and unique (except as otherwise provided in Sections 3.1.5.1, 3.1.5.2, and 3.1.5.3, below) as provided in the Authentication Policies.

3.1.5.1 The Same DN for an Signing and Encryption Certificate Key Pair is Acceptable

The same DN may be used for a Signing and Encryption Certificate Key Pair, as defined within this CP.

3.1.5.2 The Same DN for Certificates Issued for Different Key Storage Systems is Acceptable

The same DN may be used for Certificates issued for different types of key storage systems.

3.1.5.3 A low assurance Domain Validated Certificate Issued for *.sub-domain.domain.com is Acceptable where supporting documentation is present

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

The same DN may be used for a Certificate issued to *.sub-site.domain.com form where the end-user has provided the RA: (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.

3.1.5.4 Assurance levels covered by this section

The uniqueness of names as stated in section 3.1.5 is applicable to the following assurance levels only. All

Low

Basic

Medium

Medium hardware

Medium US

Medium us hardware

Company medium

3.1.6 Recognition, authentication, and role of trademarks

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

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

3.2 Initial identity validation

A Subscriber seeking to obtain Certificates from a WellsSecure Issuing CA must have their identity validated before a certificate will be issued.

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

3.2.2.1 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 Organization or WF Organization Unit authorized Employees, in certain circumstances, the I & A may be performed by Trusted Registrars.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

3.2.2.2 Previously performed I & A of an Organization will satisfy the I & A requirements under this CP 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 Organization or WF Organization Unit, or (b) the Organization is an existing Subscribing Customer.

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

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

3.2.2.4 Authentication of Organizations for CA certificates

Requests for WellsSecure CA certificates in the name of an organization shall include the organization name, address, and documentation of the existence of the organization.

The WellsSecure RA shall verify 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 will be conducted in accordance with applicable Authentication Policies. Although I & A will generally be performed by the RA or by Wells Fargo or WF Organization or WF 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 shall not 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.

Assurance Level	**Applicable Authentication Policies**	**I&A performed by**
Basic, Medium Commercial, Medium Commercial (Hardware), Medium U.S., Medium U.S. (Hardware)	WellsSecure Authentication Policy (part of RA Policies and Procedures)	Trusted Registrars, RA, Wells Fargo, WF Organization or WF Organization Unit authorized Employees, an entity certified by a State or Federal Government as being authorized to confirm Individual identities

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

High	WellsSecure Authentication Policy (part of RA Policies and Procedures)	Trusted Registrars, RA, Wells Fargo, WF Organization or WF Organization Unit authorized Employees
Low, Test	None	n/a

3.2.4 Authentication of Devices or Systems

(a) Some Devices or Systems (including without limitation routers, firewalls, servers, and the like) will be named as Subjects in the Certificate. In such cases, the Device or System must have an Individual Sponsor. The Individual Sponsor is responsible for providing the following registration information:

(i) Equipment identification (e.g., serial number) or service name (e.g., DNS name);
(ii) Equipment Public Keys;
(iii) Equipment authorizations and attributes (if any are to be included in the Certificate); and
(iv) Contact information to enable the RA to communicate with the Individual Sponsor when required.

(b) The registration information shall be verified to an Assurance Level commensurate with the Certificate Assurance Level being requested. Certificates for Devices or Systems fall into one of the following Assurance Levels: Infrastructure, Company Low, Company Basic, Company Medium, Company High, Company EV and Test Assurance Levels. Acceptable methods for performing this I&A checking include, but are not limited to:

(i) Verification of digitally signed messages sent from the Individual Sponsor (using Certificates of equivalent or greater assurance than that being requested); or
(ii) Registration by the Individual Sponsor, with the identity of the Individual Sponsor confirmed in accordance with the requirements of Section 3.2.3.

(c) The table below outlines the minimum requirements for authentication of the identity of Devices or Systems for each Assurance Level, more stringent practices may be used.

Assurance Level	**Applicable Authentication Policies**	**I&A performed by**
Infrastructure	See Section 3.2.4(b) above	n/a
Company Low	None	n/a
Company Basic, Company Medium, Company High	WellsSecure Authentication Policy (part of RA Policies and Procedures)	Trusted Registrars, RA, Wells Fargo, WF Organization or WF Organization Unit authorized Employees, an entity certified by a State or Federal Government as being authorized to confirm Individual identities
Company EV SSL	EV SSL Authentication Policy	See WellsSecure EV Policy for authentication guidelines for authorized entities who are authorized to perform I&A
Company Low, Company Test	None	n/a

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

3.2.5 Authentication of Individuals for Organization Certificates

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

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

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

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

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

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

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

3.2.6 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), Company Medium, or Company EV Assurance Levels, information that is not verified shall not be included within the Certificate.

3.2.7 Validation of authority

No stipulation.

3.2.8 Criteria for interoperation

No stipulation.

3.3 Identification and authentication for re-key requests

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

The Wells Fargo Root CA, WellsSecure Public Root CA, Sub-CA, RA, and OCSP Responder Certificates are not re-keyed or rolled-over. The Wells Fargo Root CA, WellsSecure, Public Root CA, 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 issuance on upon renewal

Subscribing Customers may establish their identity through the use of a current 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.

Assurance Level	Routine issuance upon renewal requirements
Low	Identity may be established through the use of a current, valid Signature Key.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

Basic (all policies)	Identity may be established through the use of a current, valid Signature Key, except that the identity shall 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 shall be re-established through the Registration Process at least once every 9 years from the time of the initial Registration Process.
High	Identity may be established through the use of a current, valid Signature Key, except that the identity shall be re-established through the Registration Process at least once every 3 years from the time of the initial Registration Process.

3.3.2 Identification and authentication for re-issuance upon 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) This CP; and

(b) Any other applicable PKI Documents; and

(c) Any agreements in force between the WellsSecure Issuing CA and. any other Participant.

4.1 Certificate Application

To obtain a Certificate, a Subscribing Customer must 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 Certificate applications.

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 procedures specified by the RA;

(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;

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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

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

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

For all other Assurance Levels, consult the applicable authentication policy.

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

4.1.2.1 **Applicant Obligations**

Applicant obligations are set forth in this CP and other applicable PKI Documents. These include, but are not limited to: the Subscribing Customer Agreement, the Service Request Forms, and the 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.

(d) 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 EV SSL Applicant Obligations

EV SSL Applicant obligations are set forth in this CP and in the set of documents that govern issuance and Certificate management for EV SSL Certificates.

4.1.2.3 Trusted Registrar Obligations

Trusted Registrar obligations are set forth in this CP 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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

A Trusted Registrar is responsible for:

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

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

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

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

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

(vi) Any Trusted Registrar who has direct access to WSCMS must authenticate him or herself to WSCMS using his or her WellsSecure Digital ID 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.

4.1.2.4 RA Obligations

RA obligations are set forth in this CP, the CPS, the RA Policies and Procedures Manual 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;

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

(d) Any RA that has direct access to the WSCMS must authenticate themselves to the WSCMS using their WellsSecure Digital ID at the Basic Assurance Level or the Medium Assurance Level only.

4.1.2.5 Subject Obligations

Subject obligations are set forth in this CP 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.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

4.2.3 Time to process Certificate applications

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during Certificate issuance

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

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

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

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

(i) the Subscribing Customer; and

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

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

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

(f) Ensure that 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 CP, 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 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, Company Medium, or Company EV SSL as set forth in Section 1.2.2 above for situations that involve Shared Keys..

4.3.3 Notification to Subscriber by the CA of issuance of Certificate

See Section 4.3.1.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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 High, 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.

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 this CP 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 this CP, 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 this CP 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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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

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

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

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

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

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

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

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

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

(i) Otherwise complying fully with all terms and conditions of participating in the WellsSecure PKI as set forth in this CP 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.

4.5.1.2 EV SSL Subscribing Customers

EV SSL Subscribing Customer obligations are as follows:

(a) Accuracy of Information

An obligation to provide accurate and complete information at all times to the Wells Fargo Public Primary CA, both in the EV SSL Certificate Request and as otherwise requested by the Wells Fargo Public Primary CA in connection with the issuance of the EV SSL Certificate(s) to be supplied by the Wells Fargo Public Primary CA.

(b) Protection of Private Key

An obligation by the EV SSL Subscribing Customer or a subcontractor (e.g. hosting provider) to take all reasonable measures necessary to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested EV SSL Certificate(s) (and any associated access information or Device – e.g., password or Token).

(c) Acceptance of EV SSL Certificate

An obligation that the EV SSL Subscribing Customer will not install and use the EV SSL Certificate(s) until it has reviewed and verified the accuracy of the data in each EV SSL Certificate.

(d) Use of EV SSL Certificate

An obligation that the EV SSL Subscribing Customer shall only install the EV SSL Certificate on the server accessible at the domain name listed on the EV SSL Certificate, and to use the EV SSL Certificate solely in compliance with all applicable laws, solely for authorized company business, and solely in accordance with the EV SSL Customer Agreement.

(e) Reporting and Revocation upon Compromise

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

An obligation that the EV SSL Subscribing Customer promptly cease using an EV SSL Certificate and its associated Private Key, and promptly request the Wells Fargo Public Primary CA to Revoke the EV SSL Certificate, in the event that: (i) any information in the EV SSL Certificate is or becomes incorrect or inaccurate, or (ii) there is any misuse or compromise of the EV SSL Subscribing Customer's Private Key associated with the Public Key listed in the EV SSL Certificate.

(f) Termination of Use of EV SSL Certificate

An obligation that the EV SSL Subscribing Customer promptly cease all use of the Private Key corresponding to the Public Key listed in an EV SSL Certificate upon expiration or Revocation of that EV SSL 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 WFNA related to the WellsSecure PKI.

(b) Assumption of Risk and Liability

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

4.5.3 Obligations relating to Validation Service

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

(a) Validation Service Request

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

(b) OCSP Response

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

(c) Reliance

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

(d) CRL Request

In the case of a request to download the latest available CRL, the WellsSecure Repository will provide said CRL via a standard Internet communication protocol (typically http or ldap). The most current CRL available

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

for download may not necessarily reflect the most current status information for a given Subscribing Customer's Certificate, therefore a Relying Party is strongly encouraged to use OCSP instead of CRL validation wherever possible.

4.6 Certificate renewal

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

4.6.1 Circumstance for Certificate renewal

No stipulation.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing Certificate renewal requests

No stipulation.

4.6.4 Notification of new Certificate issuance to Subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal Certificate

No stipulation.

4.6.6 Publication of the renewal Certificate by the CA

No stipulation.

4.6.7 Notification of Certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

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

4.7.1 Circumstance for Certificate re-key

No stipulation.

4.7.2 Who may request certification of a new Public Key

No stipulation.

4.7.3 Processing Certificate re-keying requests

No stipulation.

4.7.4 Notification of new Certificate issuance to Subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed Certificate

No stipulation.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

4.7.6 Publication of the re-keyed Certificate by the CA

No stipulation.

4.7.7 Notification of Certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

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

4.8.1 Circumstance for Certificate modification

No stipulation.

4.8.2 Who may request Certificate modification

No stipulation.

4.8.3 Processing Certificate modification requests

No stipulation.

4.8.4 Notification of new Certificate issuance to Subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified Certificate

No stipulation.

4.8.6 Publication of the modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 Request made by a WellsSecure PKI Organization or Organization Unit

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

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

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

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

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

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

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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

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

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

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

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

4.9.1.2 Request made by Subscribing Customer or Subject

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

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

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

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

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

4.9.1.3 Revocation of EV SSL Certificates

Revocation of EV SSL Certificates will be pursuant to the current WellsSecure EV SSL Revocation Policy.

4.9.2 Who can request Revocation

Certificate Revocation can be initiated by:

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

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

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

(d) The WellsSecure Issuing CA that issued the Certificate.

4.9.3 Procedure for Revocation request

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

(b) A Subscribing Customer may, depending on availability and implementation, submit its Revocation request by using the Revocation and Suspension Request Page, by phone, or e-mail. Specific procedures, including appropriate methods, for submitting Revocation requests will be described in materials distributed to the Subscribing Customer at the time of Certificate delivery.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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

(i) For all Revocation requests, the WellsSecure Issuing CA or RA will be required to perform I & A of the requestor. After performing appropriate I & A, as specified in the applicable authentication policy, the WellsSecure Issuing CA or RA may in its sole discretion and subject to the provisions of Section 4.9.5, immediately Revoke or Suspend the Certificate in question;

(ii) For all requests, regardless of method, and prior to confirming the identity or authority of the requestor, the WellsSecure Issuing CA or RA receiving such a request may, in its sole discretion, immediately Suspend the Certificate pending further investigation. In such event, the WellsSecure Issuing CA or RA will bear no liability for Suspending or refusing to Suspend the Certificate in question;

(iii) The WellsSecure Issuing CA or RA will send an acknowledgment to the requestor that the Revocation request has been received. Following delivery of this acknowledgement, the WellsSecure Issuing CA or RA will take reasonable steps to process the request before the next CRL is published, in no case will the Revocation request processing (including issuance and publication of CRL) take longer than eighteen (18) hours for Certificates issued to Individuals unless they are High Assurance level Certificates, in which case, the Revocation processing will take no longer than six (6) hours. If the request is validated within two (2) hours of CRL issuance, the request shall be processed before the following CRL is published;

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

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

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

4.9.4 Revocation request grace period

No stipulation.

4.9.5 Time within which CA must process the Revocation request

The WellsSecure Issuing CA will process requests from the RA for Revocation of Certificates it has issued as quickly as practical, but in no event longer than eighteen (18) hours from receipt of the Revocation request from the RA. Revocation requests shall be processed before the next CRL is published, excepting those requests validated within two (2) hours of CRL issuance. Revocation requests validated within two (2) hours prior to CRL issuance shall be processed as part of the next CRL to be published.

4.9.6 Revocation checking requirement for Relying Parties

A Relying Party must use the Validation Service prior to relying on any Certificate. Reliance without using the Validation Service will be considered an unreasonable reliance on the Certificate in question. Revocation checking of EV SSL Certificates will be pursuant to the current WellsSecure EV SSL Revocation Policy.

4.9.7 CRL issuance frequency

4.9.7.1 Wells Fargo Root CA CRLs

Information relating to the status of a Certificate issued by the Wells Fargo Root CA, as being Suspended or Revoked, will be published to the Repository a minimum of once every 365 days and within a commercially reasonable time whenever an Infrastructure Component Certificate is revoked.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

4.9.7.2 WellsSecure Public Root CA CRLs

Information relating to the status of a Certificate issued by the WellsSecure PublicRoot CA, as being Suspended or Revoked, will be published to the Repository a minimum of once every thirty (30) days and within a commercially reasonable time whenever an Infrastructure Component Certificate is revoked.

4.9.7.3 Subordinate CA CRLs

Information relating to the status of a Certificate issued by a WellsSecure Sub-CA, as being Suspended or Revoked, including the CRLs and ARLs created by any CA, will be published to the Repository a minimum of once every twenty four (24) hours unless otherwise specified with greater frequency in an applicable PKI Implementation Agreement. The WellsSecure Sub-CA shall publish a CRL no less than once every twenty four (24) hours and publish it to the Repository.

4.9.8 Maximum latency for CRLs

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

4.9.9 On-line Revocation/status checking availability

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

4.9.10 On-line Revocation checking requirements

See Section 4.9.6.

4.9.11 Other forms of Revocation advertisements available

No stipulation.

4.9.12 Special requirements regarding key compromise

If a Subscriber suspects that its Private Key has been compromised, that Subscriber must immediately initiate a Revocation or Suspension request as set forth in Section 4.9.3 of this CP. In such request, the Subscriber must specify that the reason for the request is suspected or known key compromise.

4.9.12.1 Emergency publication of WellsSecure Public Root CA CRL.

In the event of an issuing sub-CA private key is revoked for any reason, the WellsSecure Public Root CA shall:

i) Provide notice to any organizations with which the WellsSecure Public Root CA, or any Sub CA, is cross-certified as soon as possible and in no case in more than 6 hours from when the compromise is discovered.

ii) Generate a new CRL within 14 hours

iii) Publish the new CRL within 4 hours after generation.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

4.9.13 Circumstances for Suspension

(a) Certificate Suspension is used whenever a Certificate is under investigation or out of use for a certain “Grace Period” as set forth in Section 4.9.16. The Grace Period allows the WellsSecure Issuing CA to complete an investigation into whether a Certificate must be Revoked or to temporarily Suspend a Certificate's use at the Subscribing Customer's request.

(b) Certificates may be Suspend for any of the reasons listed in Section 4.9.1 or the following:

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

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

(iii) The Customer requests Suspension; or

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

(c) A Suspended Certificate will be Reinstated and removed from applicable CRLs upon request from an Organization or Individual authorized by Section 4.9.14 if, after appropriate I & A, the WellsSecure Issuing CA or the RA is satisfied of the identity and authority of the requestor and the validity of the reason for the Reinstatement request.

4.9.14 Who can request Suspension

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

4.9.15 Procedure for Suspension request

The procedures stated for Certificate Revocation in Section 4.9.3 of this CP must also be followed for Certificate Suspension. In all cases, the processing time for Suspension requests will be the same as for Revocation requests as set forth in Section 4.9.5.

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

4.9.16 Limits on Suspension period

Suspension of Certificates may not exceed sixty (60) days. During this Grace Period, a Suspended Certificate may be Reinstated or Revoked. Certificates that remain Suspended at the end of the Grace Period will be revoked.

4.10 Certificate status services

See Section 4.9.9.

4.10.1 Operational characteristics

No stipulation.

4.10.2 Service availability

No stipulation.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

No stipulation.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

4.12 Key escrow and recovery

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

4.12.1 Key escrow and recovery policy and practices

No stipulation.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

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

5.1 Physical controls

(a) The WellsSecure PKI has in place appropriate physical security controls to restrict access to all hardware and software (including the server, work stations, and any external cryptographic hardware modules or Tokens) used in connection with providing CA Services. Access to such hardware and software is limited to those personnel performing in a trusted role as described in Section 5.2.1. Specific controls shall be described within the WellsSecure CPS.

(b) The physical security requirements are designed to:

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

5.1.1 Site location and construction

Information on the site location, construction, and physical security of the WellsSecure PKI shall be described within the WellsSecure CPS.

5.1.2 Physical access

5.1.2.1 Wells Fargo Root CA, WellsSecure Public Root CA and Sub-CAs

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

5.1.2.2 Offsite Records Storage

Records that are generated pursuant to the operations, audit, etc, of the WellsSecure PKI are stored in a secure facility. Detailed security procedures shall be described within the WellsSecure CPS.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

5.1.2.3 Cryptographic Modules

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

5.1.2.4 Systems hosting RA Application

The Systems that host the WellsSecure RA Application and the workstations which allow administrator access to the WellsSecure RA Application are located in appropriate secured areas within the WellsSecure PKI's facility. The Systems that the RA uses to host any external applications and the workstations which allow administrator access to the WellsSecure RA Application are located in appropriate secured areas within the RA's facility, and are consistent with the physical security requirements that are set forth in the WellsSecure CP and CPS. Any RAs that are not under the direct control of the WellsSecure PKI are required to conform to the RA Agreement (for business units not within WFNA) and RA Policies and Procedures Manual that is consistent with this WellsSecure CP and the CPS.

5.1.2.5 Wells Fargo Repository

The Systems that host the Wells Fargo Repository are located in appropriate secured areas within the WellsSecure PKI's facility.

5.1.3 Power and air conditioning

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

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

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

5.1.7 Waste disposal

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

5.1.8 Off-site backup

The WellsSecure PKI has taken reasonable steps to ensure that its backup facility has equivalent security and controls to its primary facility. Back up of all data generated or received in performing the CA Services is performed on a daily basis. The backed up information is then stored off site on a weekly basis.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

5.2 Procedural controls

5.2.1 Trusted roles

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

(b) The requirements of this CP are defined in terms of four roles.

(i) Operator: authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate Component Keys.

(ii) Officer: authorized to request or approve Certificates or Certificate Revocations.

(iii) Auditor: authorized to maintain audit logs.

(iv) Administrator: authorized to perform system backup and recovery.

Some roles may be combined. The roles required for each level of assurance are identified in Section 5.2.4. The following subsections provide a detailed description of the responsibilities for each role.

5.2.1.1 Operator

An Operator is responsible for: (a) installation, configuration, and maintenance of the CA; (b) establishing and maintaining CA system accounts; (c) configuring Certificate profiles or templates and audit parameters, and (d) generating and backing up CA Keys. Operators may only issue Infrastructure Component Certificates.

5.2.1.2 Officer

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

5.2.1.3 Auditor

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

5.2.1.4 Administrator

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

5.2.2 Number of Individuals Required per Task

Only one Individual is required per task for CAs operating at the Low and Basic Levels of Assurance. Two or more Individuals are required for CAs operating at the Medium (all policies), or High Levels of Assurance for the following tasks: (a) CA Key generation; (b) CA Signing Key activation; and (c) CA Private Key backup. Where multiparty control for logical access is required, at least one of the Individuals shall be an Administrator. All Individuals must serve in a Trusted Role as defined in Section 5.2.1. Multiparty control for logical access shall not be achieved using Individuals that serve in the Auditor Trusted Role. Physical

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

access to the CAs does not constitute a task as identified in this Section**.** Therefore, two-person physical access control may be attained as required in this Section and Section 5.1(b)(v).

5.2.3 Identification and Authentication for Each Role

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

5.2.4 Separation of Roles

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

Assurance Level	Role Separation Rules
Low	No stipulation
Basic	Individuals shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role; however, no one Individual shall assume both the Officer and Administrator roles. This may be enforced procedurally. No Individual shall be assigned more than one identity.
Medium	Individuals shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may only assume one of the Officer, Administrator, Operator, and Auditor roles, The CA and RA Systems shall identify and authenticate their users and shall ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, nor assume both the Auditor and Officer roles. No Individual shall have more than one identity.
High	Individuals shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume only one of the Officer, Administrator, Operator, and Auditor roles. An Auditor may not assume any other role. The CA and RA Systems shall identify and authenticate their users and shall enforce these roles. No individual shall have more than one identity.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

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

For TRs and RAs that are authorized to issue Certificates at the Medium US and Medium US Hardware Assurance Levels, all trusted roles must be held by US citizens. For TRs and RAs that issue Certificates for any other Assurance Level, there is no citizenship requirement specified.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

5.3.2 Background check procedures

The WellsSecure PKI will implement background checks in accordance with Wells Fargo internal policies. Detailed background check procedures shall be described within the WellsSecure CPS.

5.3.2.1 For TRs and RAs that are authorized to issue Certificates (under the WellsSecure Public Root CA) at the Basic and Medium (All) Assurance levels, all individuals who hold trusted roles must undergo a background check that is consistent with the requirements that are set forth in the WellsSecure PKI CPS section

5.3.2.2. For TRs and RAs that issue Certificates for any other Assurance Level, there is no background check requirement specified.

5.3.3 Training requirements

Individuals performing duties in the operation of a WellsSecure CA or RA will receive appropriate training in:

(a) Basic PKI concepts;

(b) The use and operation of CA or RA Systems;

(c) Documented CA and RA procedures;

(d) Computer security awareness and procedures;

(e) How to explain the responsibilities adhering to the possession, use and operation of Key Pairs;

(f) How to explain to Subscribing Customers the responsibilities adhering to the possession, use and operation of the Subscribing Customers' Key Pairs;

(g) The general meaning of any legal contracts the WellsSecure PKI has signed sufficient to convey such meaning to other Participants;

(h) The meaning and effect of the WellsSecure CPS and/or any applicable Customer Agreements;

(i) PKI duties they are expected to perform; and

(j) Disaster recovery and business continuity procedures.

5.3.4 Retraining frequency and requirements

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

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Independent contractor requirements

The WellsSecure PKI may employ independent third party contractors to perform services associated with the operation and management of the WellsSecure PKI entities. Such contractors will enter into written agreements defining their roles and responsibilities, and ensuring that they comply with rules applicable to WellsSecure PKI Employees and are bound to security and confidentiality requirements at least as restrictive as those applicable to WellsSecure PKI Employees.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

5.3.8 Documentation supplied to personnel

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

(a) This CP;

(b) The WellsSecure CPS as appropriate;

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

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

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

(f) Appropriate other documents as necessary.

5.4 Audit logging procedures

5.4.1 Types of events recorded

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

(a) Auditable Events

(i) Security Audit

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

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

(ii) Identification and Authentication

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

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

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

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

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

(iii) Private Key load and storage

(A) The loading of Component Private Keys.

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

(iv) Trusted Public Key entry, deletion and storage

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

(v) Private Key export

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

(vi) Certificate Status change approval

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

The approval or rejection of a Certificate status change request.

(vii) Account administration

(A) Roles and users are added or deleted.

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

(C) Successful and unsuccessful attempts to assume a role

(viii) Certificate profile management

All changes to the Certificate profile.

(ix) Revocation profile management

All changes to the Revocation profile.

(x) Certificate Revocation List profile management

All changes to the Certificate Revocation list profile.

(xi) Miscellaneous

(A) Installing hardware cryptographic modules.

(B) Removing hardware cryptographic modules.

(C) Destruction of cryptographic modules.

(D) Receipt of Hardware / Software.

(E) Attempts to set passwords.

(F) Attempts to modify passwords.

(G) Backing up CA internal database.

(H) Restoring CA internal database.

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

(J) Posting of any material to a Repository.

(K) Access to CA internal 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 confidential and 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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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

(Z) Appointment of an Individual to a trusted role

(AA) Designation of personnel for multi-party control

(BB) Installation of the operating system

(CC) Installation of the CA

(DD) System start up

(EE) Logon attempts to CA applications

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

(i) Hardware

(ii) Software

(iii) Operating System

(iv) Patches

(v) Security profiles

(xii) Physical access / site security

(A) Personnel access to room housing CA.

(B) Access to the CA server.

(C) Known or suspected violations of physical security.

(xiii) Anomalies

(A) Software error conditions.

(B) Software check integrity failures.

(C) Receipt of improper messages.

(D) Misrouted messages.

(E) Network attacks (suspected or confirmed).

(F) Equipment failure.

(G) Electrical power outages.

(H) Uninterruptible Power Supply (UPS) failure.

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

(J) Violations of Certificate Policy.

(K) Violations of Certification Practice Statement.

(L) Resetting Operating System clock.

(b) Additional information requirements

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

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

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

5.4.2 Frequency of processing log

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

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

5.4.3 Retention period for audit log

Audit logs will be kept for a period of at least ten and one-half (10 ½) years, or longer if required by law. Audit logs shall be retained onsite until reviewed.

5.4.4 Protection of audit log

Audit logs will be: (a) protected from unauthorized access, modification, or deletion by appropriate operating system and security mechanisms, (b) protected from deletion or destruction prior to the end of the audit log retention period, and (c) moved to a safe, secure storage location separate from the WellsSecure CA equipment. The Individual who removes audit logs from a WellsSecure Issuing CA shall be an official different from the Individuals who, in combination, command the WellsSecure Issuing CA Signature Key.

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection System (internal vs. external)

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

5.4.7 Notification to event-causing subject

There is no notification requirement when an event is audited. The determination of which events require notification is not covered in this CP. However, the WellsSecure PKI must be notified when a process or action causes a critical security event or discrepancy. The WellsSecure PKI will investigate the event or discrepancy and will notify the affected Participants if, in its sole discretion, notification is warranted by the circumstances.

5.4.8 Vulnerability assessments

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

5.5 Records archival

5.5.1 Types of records archived

Records to be archived are those specified in Section 5.4.1 including, without limitation, all records of:

(a) Certificate application records, including application rejections. These records include, but are not limited to:

(i) The initial application for Certificate issuance, including all Customer Agreements;

(ii) The identity of the Individual performing the identification;

(iii) A signed declaration by that Individual that he or she verified the identity of the Applicant (under penalty of perjury);

(iv) If in-person identity proofing is done, a unique identifying number(s) from the ID(s) of the Applicant, or a facsimile of the ID(s);

(v) The date of the verification; and

(vi) A declaration of identity signed by the Applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, (under penalty of perjury).

(b) Registration records, including rejected applications;

(c) Success or failure of any Key Pair generations;

(d) Success or failure of any Certificate generations;

(e) Certificate issuance records, including CRLs;

(f) Certificates, including Public Keys

(g) Audit records, including all security related events;

(h) CA accreditation (if applicable);

(i) This CP and the WellsSecure CPS;

(j) Contractual obligations, including other agreements concerning operations of the CA;

(k) System and equipment configuration;

(l) Modifications and updates to System or configuration;

(m) Other data or applications to verify archive contents;

(n) Documentation required by compliance Auditors; and.

(o) Certificate Requests, which shall include without limitation the following:

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

(i) Revocations Requests;

(ii) Subscriber identity authentication data;

(iii) Documentation of receipt and acceptance of Certificates;

(iv) Documentation of receipt of Tokens; and

(v) Record of any WellsSecure PKI CA Re-key or Reissuance.

5.5.2 Retention period for archive

Archived records must be retained for at least ten and one-half (10 ½) years, or longer as required by law. Archived records will be made available for compliance audits.

5.5.3 Protection of archive

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

5.5.4 Backup Procedures

(a) Backup

Backup and recovery procedures are utilized so that a complete set of backup copies will be available in the event of the loss or destruction of the primary archives.

(b) Maintenance

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Alternatively, a WF Organization or WF Organization Unit in operational control of a CA may retain data using whatever approved procedures for that category of documents. Applications required to process the archive data shall also be maintained for a period determined by the WF Organization or WF Organization Unit for the CA it controls.

5.5.5 Requirements for time-stamping of records

Each WellsSecure Issuing CA is required to use a synchronized reliable time source to time-stamp all transmissions and records. Detailed information about the use of a synchronized time source is described within the WellsSecure CPS.

5.5.6 Archive collection system (internal or external)

The archive collection system is internal to the WellsSecure Issuing CA.

5.5.7 Procedures to obtain and verify archive information

(a) Procedures detailing how to create, verify, package, transmit, and store archive information shall be set forth in the WellsSecure PKI Operations Manual. The contents of the archive shall not be released except as determined by the WellsSecure Issuing CA or as required by law. Records of individual transactions may be released upon request of any Subscribing Customers involved in the transaction or their legally recognized agents.

(b) The integrity of archived records is verified:

(i) At the time the archive is prepared;

(ii) During an annual security audit; and

(ii) At any other time deemed necessary by the WellsSecure Issuing CA in its sole discretion.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

5.6 Key Pair changeover / Reissuance

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

5.6.1 WellsSecure Sub-CA Certificate Reissuance

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

Notwithstanding the foregoing, the WellsSecure Sub-CA will not be required to apply for Reissuance of its Issuer Certificate or otherwise bear any liability or responsibility to any Participants for the Expiration of its Issuer Certificate or for any lapse or termination in CA Services that may occur. Upon Expiration of all of the WellsSecure Sub-CA's Issuer Certificates the Wells Fargo Root CA and WellsSecure Public Root CA will comply with all provisions of Sections 5.7.1 and 5.8 of this CP.

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

5.6.2 Subscribing Customer or Subject Certificate Reissuance (Individual Certificates, Basic and Medium Assurance only)

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

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

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

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

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

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

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

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

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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

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

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

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

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

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

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

5.6.3 Root Key Reissuance

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

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

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

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

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

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

(a) Immediately cease using its Certificate;

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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

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

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

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

5.7.2 Computing resources, software, and/or data are corrupted

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

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

5.7.3 WellsSecure Issuing CA Private Key compromise procedures

In the event that a WellsSecure Issuing CA's Private Key is compromised, the Wells Fargo Root CA or WellsSecure Public Root CA, as appropriate, will immediately Revoke the Issuer Certificate and follow the procedures set forth in Section 5.7.1. If the WellsSecure CA continues to operate, it will:

(a) Generate a new WellsSecure Issuing CA Key Pair in accordance with procedures set forth by the applicable Root CA (either Wells Fargo Root CA, WellsSecure Public Root CA or CyberTrust OmniRoot, depending on the Certificate) and those in this CP; and

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

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

5.7.4 Business continuity capabilities after a disaster

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

5.8 CA or RA termination

5.8.1 WellsSecure Issuing CA Termination

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

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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

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

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

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

5.8.2 RA Termination

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

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair generation and installation

6.1.1 Key Pair generation

6.1.1.1 WellsSecure CA and RA Key Pairs

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

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

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

6.1.1.2 Subscribing Customer Key Pairs

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

(i) Low Assurance

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

(ii) Basic Assurance

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

(iii) Medium Assurance

Private Keys for a Subscribing Customer who requests Keys Pairs be stored in Medium Commercial or Medium US (non-hardware) Assurance Level Key Modules are generated using a [FIPS140] approved method in a FIPS 140 Validated module, as set forth in Section 6.2.1, below, and stored a FIPS 140 Level 1 validated module, or better. Once the Private Key is loaded into the FIPS validated module, all other copies are destroyed. Key Pairs are generated by the WellsSecure Sub-CA, not by Subject, Individual Sponsor or RAs. Private Keys for a Subscribing Customer who requests Key Pairs be stored in Medium Commercial or Medium US Hardware Assurance level Key Modules are generated using a [FIPS140] approved method and stored in an encrypted form. After a Private Key is either generated on a Token or loaded onto a Token all other copies are destroyed. The hardware cryptographic Devices used by Subscribing Customers must meet Level 2 of [FIPS140].according to the Assurance level of the Certificate that is requested.

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

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

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

6.1.2 Private Key delivery

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

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

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

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

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

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

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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

6.1.3 Public Key delivery to Certificate issuer

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

6.1.4 CA Public Key delivery to Relying Parties

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

6.1.5 Key sizes

The WellsSecure Public Root CA and the WellsSecure Issuing CA Private Keys are a minimum of 2048 bit RSA keys. All OCSP Responders within the WellsSecure PKI use a minimum of 1024 bit RSA keys. OCSP Responders that validate certificates with an assurance level of Basic (all) and Medium (all) will migrate to use a minimum of 2048 bit RSA keys on or before December 31, 2008. All Certificates issued under the WellsSecure PKI must use a minimum of 1024 bit RSA keys. Certificates Issued by the WellsSecure PKI that expire before December 31, 2010 shall contain Public Keys that are at least 1024 bit for RSA. After December 31st, 2010, WellsSecure PKI will only issue Certificates against 2048-bit RSA key pairs or Diffie-Hellman, or 224 bit for Elliptic Curve Algorithms, unless a security exception is granted through the Wells Fargo security risk assessment process for the issuance of Certificates against 1024-bit RSA Key Pairs. All Certificates that expire after December 31, 2013 shall be against key lengths of 2048 bits for RSA or Diffie Hellman, or 224 bits for Elliptic Curve Algorithms.

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA for the asymmetric keys through 31 December, 2010. For TLS or another protocol providing similar security, WellsSecure PKI will only issue Certificates against 2048-bit RSA key pairs or Diffie-Hellman, or 224 bit for Elliptic Curve Algorithms, unless a security exception is granted through the Wells Fargo security risk assessment process for the issuance of Certificates against 1024-bit RSA key pairs. All Certificates for TLS or another protocol providing similar security that expire after December 31, 2013 shall be against key lengths of 2048 bit**s for** RSA or Diffie Hellman, or 224 bits for Elliptic Curve Algorithms.

CAs that generate Certificates and CRLs under this policy shall use at a minimum SHA-1 hash algorithms when generating Digital Signatures. WellsSecure PKI will continue to issue Certificates and CRLs that are digitally signed using SHA-1 hashing algorithm until the use of SHA-2 is widely supported and adopted by the industry.

6.1.6 Public Key parameters generation and quality checking

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

6.1.7 Key usage purposes

6.1.7.1 Subscriber Key Usage Purposes

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

(a) Signing

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

(b) Encryption

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

(c) Agreement

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

6.1.7.2 Sub-CA Key Usage Purposes

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

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

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

6.2.2 Private Key (n out of m) multi-person control

The Root CA is operated in offline mode. The participation of multiple trusted individuals is required to perform sensitive CA private key operations such as HSM activation, Sub-CA certificate signing, CRL signing, CA key backup, and CA key recovery.
The Issuing CA is operated in online mode. The participation of multiple trusted individuals is required to perform sensitive CA private key operations such as HSM activation, CA key backup, and CA key recovery.

6.2.3 Private Key escrow

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

6.2.4 Private Key backup

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

6.2.5 Private Key archival

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

6.2.6 Private Key transfer into or from a cryptographic module

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

6.2.7 Private Key storage on cryptographic module

Private Keys for the Wells Fargo Root CA, WellsSecure Public Root CA, WellsSecure Sub-CAs, RAs and WellsSecure OCSP Responders, are generated, stored in an encrypted form, and backed up on an industry-standard cryptographic module, per Section 6.2.11, below.

6.2.8 Method of activating Private Key

6.2.8.1 WellsSecure Issuing CA Private Keys

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

6.2.8.2 Subscribing Customer Private Keys

A Subscribing Customer's Private Key may only be activated after:

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

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

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

See also 6.4.

6.2.9 Method of deactivating Private Key

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

6.2.10 Method of destroying Private Key

All CA and RA Private Keys will be securely destroyed upon Revocation or expiration of their Operational Period. However, Private Keys cannot be deleted from the Token. In order to destroy the Private Key, the

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

Token is reinitialized, which effectively reformats the Token and overwrites the Private Key in the process. To reinitialize the Token, the Enterprise Security Officer uses the Initialize option of the Token manager application.

Subscribing Customers who receive their Private Keys and Certificates on Tokens are instructed to either return the Token to Wells Fargo or the RA from which they received the Keys upon Revocation or expiration or to physically destroy the Token (e.g. cut up a smart card). Subscribing Customers who access their Private Keys and Certificates via the SKSS are prevented from accessing the SKSS once the Certificates are Revoked or Expired. No one other than the end user has access to the SKSS, therefore, once the Certificates are Revoked or Expired, no one has access to the SKSS.

6.2.11 Cryptographic Module Rating

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

The cryptographic Devices used by RAs meet level 2 of [FIPS140].

6.3 Other aspects of Key Pair management

6.3.1 Public Key archival

See section 5.5.1

6.3.2 Certificate Operational Periods and Key Pair usage periods

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

(b) Certificates shall be valid for the Operational Period specified within the Certificate itself. Certificates, other than CA Certificates and the Certificates set forth below, shall have an Operational Period of not more than fifteen (15) years from the date of issuance. CA Certificates shall have an Operational Period not more than twenty (20) years and ninety (90) days. The Wells Fargo CA 01 shall limit the use of its Private Keys to a maximum of four (4) years for issuing Subscriber Certificates and a maximum of ten (10) years for CRL signing OCSP responder Certificates for issuance of Certificates that assert the OIDs listed below.

(i) Basic Assurance = 2.16.840.1.114171.500.10

(ii) Medium Commercial Assurance = 2.16.840.1.114171.500.3

(iii) Medium Commercial Assurance (Hardware) = 2.16.840.1.114171.500.4

(iv) Medium U.S. Assurance = 2.16.840.1.114171.500.11

(v) Medium U.S. Assurance (Hardware) = 2.16.840.1.114171.500.12

(vi) Company Medium Assurance = 2.16.840.1.114171.500.7

(c) Private Keys for any issuing CA that is under the WellsSecure Public Root CA will be used for no more than four (4) years for issuance of Certificates with the OIDs listed in the preceding Sub-section).

(d) Certificates issued to Subscribing Customers will have no more than a three (3) year Operational Period. CRL signing and OCSP responder Certificates shall have an Operational Period not more than ten (10) years. The Operational Periods for each Certificate issued at the request of an RA shall be in accordance with the terms of the applicable RA Agreement (for business units not within WFNA) with WFNA. Specific Operational Periods shall in every case be set to Expire no later than the expiration of the issuing CA's Certificate.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

6.4 Activation Data

The Private Keys of all Participants should be stored in encrypted form, and require the entrance of Activation Data to unlock. Activation Data will be provided to all Subscribing Customers separately from the Key Pair.

6.4.1 Activation Data generation and installation

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

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

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

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

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

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

6.4.2 Activation Data protection

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

6.4.3 Other aspects of Activation Data

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

6.5 Computer security controls

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

6.5.1 Specific computer security technical requirements

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

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

(a) Require authenticated logins;

(b) Provide Discretionary Access Control;

(c) Provide a security audit capability;

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

(e) Enforce separation of duties for PKI roles;

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

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

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

(i) Archive CA history and audit data;

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

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

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

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

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

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

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

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

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

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

6.6.2 Security management controls

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

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

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

6.6.3 Life cycle security controls

No stipulation.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

6.7 Network security controls

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

6.8 Time-stamping

No stipulation.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

Profiles for each Certificate type issued by a WellsSecure Issuing CA pursuant to Section 1.4.1 are included within the WellsSecure CPS. They are incorporated by this reference into this CP and available upon request (see Section 1.5.2). All CA's operating under the WellsSecure Public Root CA shall issue certificates according to the Profiles set forth in the WellsSecure CPS section 7.1.2.

7.1.1 Version number(s)

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

7.1.2 Certificate extensions

Recommended Certificate extensions for each Certificate type specified in Section 1.4.1 are detailed in the applicable Certificate profile that is available upon request (see Section 1.5.2). All use of standard Certificate extensions shall comply with [RFC3280]. CA Certificates shall not include critical private extensions.

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

7.1.3 Algorithm object identifiers

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

Certificates issued by any issuing CA that chains up to the WellsSecure Public Root CA shall identify the signature algorithm using one of the following OIDs:

id-dsa-with-sha1	1.2.840.10040.4.3
sha-1WithRSAEncryption	1.2.840.113549.1.1.5
sha256WithRSAEncryption	1.2.840.113549.1.1.11
ecdsa-with-SHA1	1.2.840.10045.4.1
ecdsa-with-SHA224	1.2.840.10045.4.3.1
ecdsa-with-SH256	1.2.840.10045.4.3.2
ecdsa-with-SHA384	1.2.840.10045.4.3.3
ecdsa-with-SHA512	1.2.840.10045.4.3.4

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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

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

7.1.4 Name forms

Names for the “Issuer” and “Subject” fields of each Certificate type specified in Section 1.4.1 are of the X.500 DN form. Distinguished names shall be composed of standard attribute types, such as those identified in [RFC3280].

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy object identifier

Each Certificate issued by a WellsSecure Issuing CA contains the OID of this CP in the Certificate policy extension. Each Certificate also contains an OID from Section 1.2.2 in the Certificate policy extension.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate policies extension

No stipulation.

7.2 *CRL profile*

The profile for the CRL issued by a WellsSecure Issuing CA conforms to the standards as described in [RFC3280]; the CRL profile is x509 v2.

7.2.1 Version number(s)

The WellsSecure PKI issues and uses X.509 version 2 CRLs.

7.2.2 CRL and CRL entry extensions

Recommended CRL and CRL entry extensions are detailed in the WellsSecure CPS and applicable CRL profile that is available upon request (see Section 1.5.2). All use of standard CRL and CRL entry extensions shall comply with [RFC3280].

7.3 *OCSP profile*

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

7.3.1 Version number(s)

The WellsSecure OCSP Responder expects OCSP version 1 requests and issues OCSP version 1 responses.

7.3.2 OCSP extensions

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

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

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

8.2 Identity/qualifications of assessor

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

8.3 Assessor's relationship to assessed Organization or Organization Unit

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

8.4 Topics covered by assessment

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

8.5 Actions taken as a result of deficiency

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

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

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

8.6 Communication of results

The results of all compliance audits will be communicated by the PKI manager to the IAPAC. Other Participants have no right to access the compliance audit results. If the audit is one that is engaged into in order to obtain industry certification or approval to provide a public assurance of compliance with this CP,

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

(such as a WebTrust Audit) Wells Fargo may, in its sole discretion, make the summary of such audit's results available on the same web page as this CP is accessed.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Fees related to the performance of services within the WellsSecure PKI are outside the scope of this CP.

9.1.1 Certificate issuance or renewal fees

See Section 9.1.

9.1.2 Certificate access fees

See Section 9.1.

9.1.3 Revocation or status information access fees

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

9.1.4 Fees for other services

See Section 9.1.

9.1.5 Refund policy

See Section 9.1.

9.2 Financial responsibility

No stipulation.

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of Confidential Information

The following categories of information are considered to be "Confidential Information". These categories of information are subject to the provisions of Section 9.3.2.

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

(b) All PKI Documents;

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

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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

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 WellsSecure PKI; provided, however, that references in a publicly available PKI Document to another PKI Document that is not made publicly available shall not cause the latter to be outside the scope of Confidential Information as defined in this CP;

(c) Revocation or Suspension information; and

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

9.3.3 Responsibility to protect Confidential Information

(a) Permitted Disclosures

The WellsSecure Issuing CAs and WellsSecure RAs will be entitled to disclose Confidential Information on a "need-to-know" basis to any of their Personnel, and WF Entities and their Personnel, that are assisting in the verification of information supplied in Certificate applications or that are assisting in the operation of the WellsSecure Issuing CAs or RAs. The WellsSecure Issuing CAs and RAs will also be entitled to disclose Confidential Information to third parties, such as legal and financial advisors, assisting in connection with any legal, judicial, administrative, or other proceedings required by law or by this CP, and to legal counsel, accountants, banks and financing sources and their advisors in connection with mergers, acquisitions, or reorganizations. Any such disclosures will be permissible provided that the WellsSecure Issuing CAs and RAs use reasonable efforts to ensure that all such third parties will protect the Confidential Information at the same level as such Confidential Information is protected in this CP.

(b) Safeguards

The WellsSecure Issuing CAs and their RAs will take reasonable steps to protect the confidentiality of Confidential Information (as defined in Sections 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 necessary to provide the CA Services and the Validation Services associated with the WellsSecure PKI.

(c) Legal Proceedings

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.

(d) Third Parties

(i) Permitted Disclosure

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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.

(ii) Indemnification Obligations

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

(e) Subscribing Parties

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 Organization or WF 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 personally identifiable information

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

- Procedural controls
- Ensuring that staff are aware of their responsibilities for safeguarding personal information,
- Physical security including locked filing cabinets and locked rooms,
- Logical security such as passwords and access control lists,
- Ensuring that personal information is accessible only to the staff who will require it to fulfil their duties,
- 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.

Personal information held by Wells Fargo will not be disclosed to outside organizations other than:

- To meet legal requirements, for example to law enforcement agencies under a properly drawn up warrant,
- The data subject themselves in response to a properly authenticated request,
- At the specific request of or with the permission of the data subject,
- To a contractor 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.

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.

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

See Section 9.3.1.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

9.4.3 Information not deemed private

See Section 9.3.2.

9.4.4 Responsibility to protect private information

See Section 9.3.3.

9.4.5 Notice and consent to use private information

See Section 9.3.3.

9.4.6 Disclosure pursuant to judicial or administrative process

See Section 9.3.3.

9.4.7 Other information disclosure circumstances

See Section 9.3.3.

9.5 Intellectual property rights

9.5.1 Reservation of Rights

Participants agree and acknowledge that the Wells Fargo Trusted Identity Entities own and shall retain all respective rights, title and interest in and to, and all intellectual property rights embodied in or associated with the WellsSecure PKI and the issuance, delivery and use of any Certificate, OIDs, Token(s), SKSS, Key Pairs, trademarks or other intellectual property and PKI Documents. Such right, title and interest shall extend without limitation to any content, software, graphics, design materials, technology, methods, architecture, publications, business plans and other tangible or intangible intellectual property-based assets of any kind in machine readable, printed or other form and all revisions, enhancements, improvements, technical know-how, patents, copyrights, moral rights and trade secrets associated with any Certificate, OIDs, Token(s), SKSS, Key Pairs, trademarks or other intellectual property, and/or PKI Documents. Except as expressly stated in this CP 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 CP, and any rights not expressly granted under this CP 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 WFNA), Repository Agreement, or Customer Agreements, the WellsSecure Issuing CA may grant Participants a revocable, nontransferable, non-sublicensable license to use their Certificates and Private Keys in accordance with this CP 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 CP, the applicable Sub-CA Agreement, RA Agreement (for business units not within WFNA), Repository Agreement, or Customer Agreement, and other applicable PKI Documents. Any use not in compliance with the foregoing is explicitly prohibited.

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

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

9.5.3 Termination

On termination of the Subscribing Customer's participation in the WellsSecure PKI or the Sub-CA Agreement, RA Agreement (for business units not within WFNA), Repository Agreement, or Customer Agreement, all

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

uses of any Wells Fargo or WellsSecure trademarks or other intellectual property will immediately cease and any Wells Fargo or WellsSecure intellectual property in the possession of the Participant who was party to such Agreement at the time of termination will either be returned to Wells Fargo or WellsSecure or will be destroyed.

9.5.4 Modifications

The terms and conditions of this Section 9.5 may be supplemented or altered by applicable Sub-CA Agreement, RA Agreement (for business units not within WFNA), Repository Agreement, or Customer Agreements between Wells Fargo, WellsSecure and Subscribing Customers.

9.6 Representations and warranties

9.6.1 CA representations and warranties

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

9.6.2 RA representations and warranties

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

9.6.3 Subscriber and Subject representations and warranties

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

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

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

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

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

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

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

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

(h) Subscriber will perform the obligations set forth in Sections 4.5.1.2 and, in the case where the Subscriber has been issued an EV SSL Certificate, the obligations set forth in Sections 4.5.1(d), (e) and (f).

9.6.4 Applicant representations and warranties

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

An Applicant, by participating in the Registration Process, warrants that he or she has full authority and permission to provide the requested information on behalf of the Subscribing Customer or Subscriber. At the WellsSecure Issuing CA's request, the Applicant may be required to produce evidence of such authority.

9.6.5 Relying Party representations and warranties

No stipulation.

9.6.6 Representations and warranties of other Participants

No stipulation.

9.7 Disclaimers of Warranties

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

9.7.1 No Fiduciary Relationships

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

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 WFNA), Repository Agreement, Customer Agreements or other agreement between a Participant and WFNA , the liability of the Wells Fargo Trusted Identity Entities to a Non-Wells Fargo Participant in connection with the performance of CA Services, the Validation Services, or any other obligations under the WellsSecure PKI, including negligence and misconduct and whether in contract, tort or otherwise, shall be exclusively limited to direct damages only, and shall not exceed the following:

(a) For EV SSL Certificates, $2,000 per EV SSL Certificate Subscribing Party, Relying Party of an EV SSL Certificate, or EV SSL Certificate; and

(b) For all other Certificates: (i) $15,000 per claim or transaction, or (ii) $750,000 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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

ENTITIES TO NON-WELLS FARGO PARTICIPANTS WHATSOEVER FOR ANY AND ALL LIABILITY, LOSSES, CLAIMS, DEMANDS, DISPUTES, DAMAGES OR COSTS OF ANY KIND, INCLUDING, WITHOUT LIMITATION, REASONABLE ATTORNEYS' FEES AND COSTS OF LITIGATION, (COLLECTIVELY, "LOSSES AND LIABILITIES"):

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

(ii) Relying on an EV SSL Certificate for any other purpose other than (A) identifying the legal entity that controls a web site, or (B) exchanging information in an encrypted format over the Internet with a web site;

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

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

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

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

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

(b) IN NO EVENT SHALL THE WELLS FARGO TRUSTED IDENTITY ENTITIES BE LIABLE FOR EXEMPLARY, PUNITIVE, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, ANY LOSS OF PROFITS, LOSS OF GOODWILL, LOSS OF BUSINESS, LOSS OF ANTICIPATED SAVINGS, LOSS OF DATA, COST OF PROCUREMENT OF SUBSTITUTE SERVICES AND/OR CERTIFICATES, OR ANY OTHER INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, HOWSOEVER CAUSED, AND ON ANY THEORY OF LIABILITY, WHETHER FOR BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY), OR OTHERWISE. THESE LIMITATIONS WILL APPLY WHETHER OR NOT THE WELLS FARGO TRUSTED IDENTITY ENTITIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER OR NOT THE WELLS FARGO TRUSTED IDENTITY ENTITIES COULD HAVE FORESEEN SUCH DAMAGES AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. SUBJECT TO THE FOREGOING, THE WELLS FARGO TRUSTED IDENTITY ENTITIES LIABILITY FOR DIRECT DAMAGES OF ANY KIND OR NATURE IN CONNECTION WITH THIS AGREEMENT SHALL IN NO EVENT EXCEED THE LIMITS SET FORTH IN SECTION 9.8.1 OR APPLICABLE SUB-CA AGREEMENT, RA AGREEMENT (for business units not within WFNA), REPOSITORY AGREEMENT, CUSTOMER AGREEMENTS OR OTHER AGREEMENT BETWEEN NON-

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

WELLS FARGO PARTICIPANT AND WFNA FOR ALL TRANSACTIONS ARISING OUT OF THE CERTIFICATE, CA SERVICE, OR VALIDATION SERVICE, AS APPLICABLE, WHICHEVER IS LESS. NON-WELLS FARGO PARTICIPANTS ALSO ACKNOWLEDGE AND AGREE THAT THEY HAVE REVIEWED AND FREELY CONSENTED TO THE LIMITATIONS OF LIABILITY IMPOSED IN THIS SECTION.

9.8.3 Liability for WellsSecure Issuing CA Authorized RAs and Repositories

All liability for RAs and Repositories operating under the authority of a WellsSecure Issuing CA is subsumed by the WellsSecure Issuing CA and is subject to the limitations specified in Section 9.8. Despite the foregoing, nothing in this Section will prevent the WellsSecure Issuing CA from pursuing its remedies against any Organization approved to undertake RA or Repository obligations on behalf of the WellsSecure Issuing CA, pursuant to the applicable RA Agreement (for business units not within WFNA) 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 CP 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 WFNA (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 CP 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 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”) resulting from or in any way connected with: (a) the Subscribing Customer’s breach of any representations and warranties and any obligations of the Subscribing Customer set forth in this CP and the PKI Documents; (ii) the actions or omissions of any Applicant authorized by the 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 CP and other applicable PKI Documents; (vi) any unreasonable repudiation of a Certificate validated by any WellsSecure Issuing CA; and (vii) the use of its

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

Certificates in any transaction with a party that does not possess a Certificate issued by the Wells Fargo Root CA, WellsSecure Public Root CA, 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 damages arising out of the WellsSecure Issuing CA's use of such name.

9.9.3 Indemnification by the Relying Party

Each Relying Party shall indemnify and hold harmless Participants, the Indemnified Parties as defined in this Section 9.9, and their directors, officers, Employees, agents, subsidiaries, parents and affiliates, irrespective of their active or passive negligence, against 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") 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 this 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 Root CA, WellsSecure Public Root CA, or Sub-CA.

9.9.4 Indemnification by Subject

The Subject agrees to indemnify and hold harmless all affected Participants for any losses or damages arising from: (a) reliance on incorrect representations made by the Subject, Individual Sponsor or by Applicant; (b) any failure to disclose material facts which if known, would have affected the decision to issue the Certificate or its continued validity; and (c) any other breach of the Subjects obligations under the WellsSecure PKI.

9.9.5 Indemnification by Applicant

The Applicant and either (a) the Subscribing Customer for which the Applicant is Personnel, or (b) the Subscriber, as applicable, shall indemnify and hold harmless all affected Participants for all loss, liability, damage, or expenses (including reasonable attorney's fees), 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

No stipulation.

9.10.2 Termination

No stipulation.

9.10.3 Effect of termination and survival

This CP, the CPS, the applicable Sub-CA Agreement, RA Agreement (for business units not within WFNA), Repository Agreement, Customer Agreements or other agreement between WFNA 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.

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

CP are inserted solely for reference and shall not constitute a part of the CP or affect its meaning, construction or effect. Waiver of any one default of any provisions herein by the WellsSecure Issuing CA shall not waive subsequent defaults of the same or different kind.

In the event of a conflict between the most current version of this CP or any 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.

All notices and requests in connection with this CP 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 within five (5) days after delivery.

The terms of this CP may be modified from time to time, with the approval of the IAPAC, in accordance with Section 9.12 of this CP.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

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

9.12.1 Procedure for amendment

Changes to this CP that, in the judgment of the IAPAC, will have no or only a minimal effect on Participants, may be made without requiring the issuance of a new version of the CP and without notification to Participants.

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

9.12.2 Notification mechanism and period

See Sections 2.2 and 2.3.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute resolution provisions

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

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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 California 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 California State Bar or retired judges of the state or federal judiciary of California, 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 California, (ii) may grant any remedy or relief that a court of the state of California 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 California 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 California, 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, (B) of whether the conclusions of law are erroneous under the substantive law of the state of California and (C) pursuant to Code of Civil Procedure Sections 1286, 1287-1287.4. 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 California and should not be vacated pursuant to California Code of Civil Procedure, Sections 1286, 1287 – 1287.4.

(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 CP. 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.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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

9.14 Governing law

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

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

No stipulation.

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 *Other provisions*

No stipulation.

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").

Administrator: See Section 5.2.1.1.

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 Subscribing Customer. If the Subscribing Customer is an Individual, the Applicant shall be the same as the Subscribing Customer.

Assurance Level: See Section 1.2.2.1.

Auditor: See Section 5.2.1.3.

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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 this CP and provided by the WellsSecure PKI relating to the creation, issuance, or management of Certificates.

Certificate: A digitally-signed electronic record issued within a PKI that:

(a) identifies the Organization issuing the Certificate as the "Organization (o)" in the Certificate's "Issuer Distinguished Name (idn)" field;

(b) identifies the Organization to which the Certificate is issued or with whom the Subject, who is also the Subscriber, has a relationship as a member of a professional association or other affiliation as the "Organization (o)" in the Certificate's "Subject" field;

(c) 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

(d) 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 Authority Certificate or CA Certificate: An infrastructure Certificate issued to a CA.

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

Certification Practice Statement (CPS): A statement of the practices that a Certificate Authority employs in issuing, managing, revoking, and renewing or re-keying Certificates

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

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

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

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: (a) whether the data produced by the transformation was generated using the signer's Private Key that corresponds to the signer's Public Key; and (b) 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.

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

EV SSL: See Extended Validation Secure Socket Layer.

EV SSL Customer: A Subscriber that has executed the applicable EV SSL Customer Agreement.

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

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

Extended Validation Secure Socket Layer (EV SSL): An extended validation secure socket layer Certificate (EV SSL Certificate) is a Certificate issued in conformance with the extended validation guidelines defined by the CA/Browser Forum.

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

Group: Several Individuals acting on behalf of a single Subscribing Customer acting in one capacity

Guidelines for EV SSL Certificates: The guidelines for issuing Extended Validation Secure Socket Layer Certificates as defined by the CA/Browser Forum and available at www.cabforum.org.

I & A: See Identification and Authentication.

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

Identity Assurance Policy Approval Committee (IAPAC): The IAPAC is responsible for approving Identity Assurance Policies for Wells Fargo and WellsSecure.

Identity Assurance Working Group (IAWG): An ad-hoc working group currently managed from the Information Security Technology (IST) group of Wells Fargo which provides technical input to the IAPAC.

Individual: A living human being. See also Sponsor, Individual Sponsor.

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

Infrastructure Component Certificate: A Certificate that is issued to an Infrastructure Component.

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

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

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: (a) store one or more Private Keys; (b) create Digital Signatures or Authenticate data using a Private Key; and (c) 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: (a) the Public Key may be used to verify a Digital Signature generated by the corresponding Private Key; and/or (b) the Public Key may be used to encrypt an electronic record that can be decrypted only by using the corresponding Private Key.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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.

Officer: See Section 5.2.1.2.

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.

Operator: See Section 5.2.1.4.

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

Organization Certificate: A Certificate issued to a Group

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

Organization Unit: A sub-group or unit operated by or under the authority of an Organization or group of Organizations.

Participants: See Section 1.3.8. This term also includes the IAPAC.

Personnel: Consists of Employees, contractors and agents of an Organization or Organization Unit.

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

(a) This CP;

(b) The WellsSecure CPS;

(c) The WellsSecure PKI Operations Manual

(d) The WellsSecure Authentication Policy;

(e) The EV SSL Authentication Policy;

(f) Registration Authority Agreements;

(g) Customer Agreements;

(h) Sub-CA Agreements; and

(i) Other agreements, manuals or procedures provided to non-Wells Fargo Participants by the WellsSecure PKI.

Not all PKI Documents will be applicable to every Participant.

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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.

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.

RA Application: A System that allows the RA to interface to the WellsSecure Certificate Management System (WSCMS).

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

Registration Process: The process administered by an RA that a 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.

Relying Party: An Individual or Organization 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 this CP; may also be referred to as a Directory.

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

Revocation and Suspension Request Page: An online location established by the WellsSecure Issuing CA for the exclusive use of 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.

Session Key: A temporary encryption key with a lifetime that is limited to the duration of a single login "session"

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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.

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.

Sponsor or Individual Sponsor: An Individual who is authorized to act for a System or Device, or, in the case of an Organization Certificate or Shared Certificate, has been authorized to act for all Individuals who may use such Certificate.

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).

Subordinate CA Certificate, Sub-CA Certificate: A Certificate issued to a Sub-CA.

Subscriber or Subscribing Customer: (a) The Organization that is identified as the “Organization (o)” in the “Subject” field of a Certificate, (b) the Individual named as the Subject in the case where the Certificate is issued to an Individual who is using the Certificate for business or professional purposes and not as an individual consumer. Such business or professional purposes may include as a member of a professional association established by the Organization identified in the Certificate or based on some other affiliation with such Organization; or (c) Personnel of an Organization that: (i) has an existing business relationship with a WF Organization or WF Organization Unit; (ii) has an existing business relationship with a customer of a WF Organization or WF Organization Unit; or (iii) in the sole discretion of Wells Fargo, is considered to have a potential business relationship.

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 Revoked.

Suspend, Suspension: The process of transforming a Certificate from Good to temporarily Revoked.

Symmetric Key: the key that is used to encrypt a file or message is the same key that is used to decrypt the file or message.

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.

Technology Operations Group (TIG): The group within Wells Fargo that operates the WellsSecure PKI.

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

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

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

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

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. (also referred to as WFNA).

Wells Fargo Trusted Identity Entities: Collectively includes Wells Fargo, the WellsSecure PKI, the Wells Fargo Root CA, WellsSecure Public Root CA, WellsSecure Issuing CA, WellsSecure Sub-CAs, WellsSecure RAs, WF Organizations, WF Organization Units and WF Affiliates.

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

WellsSecure Certificate Management System (WSCMS): The System used by Wells Fargo CAs to provide CA Services.

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

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

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

Wells Fargo Root Certificate Authority, Wells Fargo Root CA: One of the two highest or top-level Certificate Authorities in the WellsSecure PKI.

WellsSecure Public Root Certificate Authority, WellsSecure Public Root CA: One of the two highest or top-level Certificate Authorities in the WellsSecure PKI.

WellsSecure Sub-CA: A Sub-CA whose Certificate was issued by one (or more) of the two WellsSecure PKI Root Certificate Authorities.

Wells Fargo Affiliates, WF Affiliates: Means Wells Fargo & Company and any present or future subsidiary thereof as defined under 12 U.S.C. §1841 (d), which includes Wells Fargo Bank, N.A.

WFNA: See Wells Fargo.

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

11 BIBLIOGRAPHY

The following documents were used in part to develop this CP:

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
PKI02-026	WellsSecure PKI Internal Policy "Operations Manual"
RFC2560	Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP, Myers, Ankney, Malpani, Galperin, Adams, June 1999.

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.

	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
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
WellsSecure CPS	WellsSecure® PKI Certification Practices Statement, version 12.2

©Copyright, 2000-2010, Wells Fargo Bank, N.A. All rights reserved.
This document may not be reproduced without the express written permission of Wells Fargo.