KPMG LLP
Mission Towers I
Suite 100
3975 Freedom Circle Drive
Santa Clara, CA 95054

Independent Accountants' Report

To the Management of
Wells Fargo Bank N.A:

We have examined the assertion by the management of Wells Fargo Bank N.A ("Wells Fargo") regarding the disclosure of its key and certificate life cycle management business practices, and the effectiveness of its controls over key and SSL certificate integrity, the authenticity of subscriber information, logical and physical access to CA systems and data, the continuity of key and certificate life cycle management operations, and development, maintenance and operation of systems integrity, based on the WebTrust® Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.0 criteria, during the period September 1, 2014 through August 31, 2015, for the WellsSecure Public Root Certificate Authority, WellsSecure Certificate Authority, WellsSecure Public Root Certification Authority 01 G2, and WellsSecure Certification Authority 01 G2 (collectively referred to as the "Wells Fargo SSL CAs").

Wells Fargo's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and accordingly, included (1) obtaining an understanding of Wells Fargo's key and SSL certificate life cycle management business practices and its controls over key and SSL certificate integrity, over the continuity of key and certificate life cycle management operations, and over the development, maintenance, and operation of systems integrity; (2) selectively testing transactions executed in accordance with disclosed SSL certificate life cycle management business practices; (3) testing and evaluating the design and effectiveness of controls; and (4) performing such other procedures as we considered necessary in the circumstances.

We believe that our examination provides a reasonable basis for our opinion.

The relative effectiveness and significance of specific controls at Wells Fargo and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Because of the nature and inherent limitations of controls, Wells Fargo's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

We noted the following issues that resulted in a modification of our opinion:

No.	Requirements	Issues Noted
1	Principle 2 Criterion §2.1 requires the CA to maintain controls to provide reasonable assurance that certificates issued meet the minimum requirements for certificate content and profile as established in section 9 of the Baseline Requirements including the following: • Subject Information (See SSL Baseline Requirements Section 9.2)	We noted that 60 of the 3085 SSL certificates issued by Wells Fargo during the examination period to Wells Fargo owned domains did not meet the minimum subject information requirements for certificate content and profile as specified in section 9.2 of the SSL Baseline requirements. As a result, we noted that Wells Fargo did not meet Principle 2 Criterion §2.1 – sub bullet 2 "Subject Information (SSL Baseline Requirements Section 9.2)" during the examination period.
2	Principle 2 Criterion §5.3 required the CA to maintain controls to provide reasonable assurance that Certificates are revoked within 24 hours if any of the following events occurs: • The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;	Although the SSL certificates noted in issue 1 above have since been revoked or have expired, this was not completed within 24 hours for 16 certificates in accordance with Principle 2 Criterion §5.3 due to business needs. As a result, Wells Fargo did not meet Principle 2 Criterion §5.3 during the examination period.
3	Principle 2 Criterion §7.2 requires that the CA maintains controls to provide reasonable assurance that security events are logged including firewall and router activities. Furthermore, Principle 2 Criterion §7.3 requires that the CA has a policy and maintains controls to provide reasonable assurance that audit logs generated after the effective date of the Baseline Requirements are retained for at least seven years.	We noted that even though firewall activities are logged in accordance with Principle 2 Criterion §7.2, audit logs for these events are not required to be retained for at least seven years in accordance with Principle 2 Criterion §7.3. As a result, we noted that Wells Fargo did not meet Principle 2 Criterion §7.3 for firewall activity logs during the examination period.

No.	Requirements	Issues Noted
4	Principle 4 Criterion §4.0 requires to perform one of the following within 96 hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process: • If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to the following: - Vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0); and - Systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; • Document the factual basis for the CA's determination that the vulnerability does not require remediation because of one of the following: - The CA disagrees with the NVD rating; - The identification is a false positive; - The exploit of the vulnerability is prevented by compensating controls or an absence of threats; or - Other similar reasons.	Wells Fargo internal policies target critical vulnerabilities to be addressed within 30 days of discovery not 96 hours as required by WTBR 2.0 criteria 4-4. Furthermore, the average number of days to remediate vulnerabilities was approximately 60 days. As a result, we noted that Wells Fargo did not meet Principle 4 Criterion §4.0 for vulnerability management during the examination period.
5	Principle 4 Criterion §1.0 requires that the CA maintains controls to provide reasonable assurance that: • Certificate Systems are segmented into networks or zones based on their functional, logical, and physical (including location) relationship;	KPMG noted that the PKI network is not physically or logically segregated from the Wells Fargo enterprise systems. The CAs are currently on the corporate network and not segregated from the rest of the corporate systems. As a result, we noted that Wells Fargo did not meet Principle 4 Criterion §1.0 during the examination period. KPMG noted that the corporate network houses other critical systems and has incorporated stringent network security controls.

In our opinion, except for the effects of the matter(s) discussed in the preceding paragraphs, in providing its SSL Certification Authority (CA) services at Shoreview, Minnesota; Tempe Arizona; Homewood, Alabama and Silas, North Carolina during the period September 1, 2014 through August 31, 2015, Wells Fargo has in all material respects —

- disclosed its Certificate practices and procedures in WellsSecure PKI Certification Practice Statement version 13.3, August 2015 on the Wells Fargo website, and WellsSecure PKI Certificate Policy version 13.3, August 2015 (restricted to authorized users and provided upon request), including its commitment to provide SSL Certificates in conformity with the applicable

CA/Browser Forum Guidelines and provided such services in accordance with its disclosed practices and

- maintained effective controls to provide reasonable assurance that:
  - subscriber information was properly collected, authenticated (for the registration activities performed by Wells Fargo) and verified;
  - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
  - logical and physical access to CA systems and data was restricted to authorized individuals;
  - the continuity of key and certificate management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

based on the WebTrust® Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.0 for the Wells Fargo SSL CAs.

This report does not include any representation as to the quality of Wells Fargo's certification services beyond those covered by the *WebTrust® Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.0* criteria, nor the suitability of any of Wells Fargo's services for any customer's intended purpose.

KPMG LLP

December 21, 2015

Santa Clara, CA

Assertion of Management as to
its Disclosure of its Business Practices and its Controls
over its Certification Authority Operations during the period
from September 01, 2014 through August 31, 2015

December 21, 2015

Wells Fargo Bank N.A ("Wells Fargo") provides its SSL certification authority (CA) services through the WellsSecure Public Root Certificate Authority, WellsSecure Certificate Authority, WellsSecure Public Root Certification Authority 01 G2, and WellsSecure Certification Authority 01 G2 (collectively referred to as the "Wells Fargo SSL CAs").

The management of Wells Fargo has assessed the disclosure of its certificate practices and its controls over its SSL CA services. Based on that assessment, in Wells Fargo Management's opinion, in providing its SSL CA services at Shoreview, Minnesota; Tempe, Arizona; Homewood, Alabama; and Silas, North Carolina during the period from September 1, 2014 through August 31, 2015, Wells Fargo has:

- disclosed its Certificate practices and procedures in its WellsSecure PKI Certification Practice Statement version 13.3, August 2015 on the Wells Fargo website, and WellsSecure PKI Certificate Policy version 13.3, August 2015 (restricted to authorized users and provided upon request), including its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines and provided such services in accordance with its disclosed practices and

- maintained effective controls to provide reasonable assurance that:
  - subscriber information was properly collected, authenticated (for the registration activities performed by Wells Fargo) and verified;
  - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
  - logical and physical access to CA systems and data was restricted to authorized individuals;
  - the continuity of key and certificate management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

based on the WebTrust® Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.0 for the Wells Fargo SSL CAs except for the effects of the matters noted below:

No.	Requirements	Issues Noted
1	Principle 2 Criterion §2.1 requires the CA to maintain controls to provide reasonable assurance that certificates issued meet the minimum requirements for certificate content and profile as established in section 9 of the Baseline Requirements including the following: • Subject Information (See SSL Baseline Requirements Section 9.2)	60 of the 3085 SSL certificates issued by Wells Fargo during the examination period to Wells Fargo owned domains did not meet the minimum subject information requirements for certificate content and profile as specified in section 9.2 of the SSL Baseline requirements. As a result, Wells Fargo did not meet Principle 2 Criterion §2.1 – sub bullet 2 "Subject Information (SSL Baseline Requirements Section 9.2)" during the examination period.
2	Principle 2 Criterion §5.3 required the CA to maintain controls to provide reasonable assurance that Certificates are revoked within 24 hours if any of the following events occurs: • The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;	Although the SSL certificates noted in issue 1 above have since been revoked or have expired, this was not completed within 24 hours for 16 certificates in accordance with Principle 2 Criterion §5.3 in order to provide sufficient time to replace the certificates to meet business needs. As a result, Wells Fargo did not meet Principle 2 Criterion §5.3 during the examination period.
3	Principle 2 Criterion §7.2 requires that the CA maintains controls to provide reasonable assurance that security events are logged including firewall and router activities. Furthermore, Principle 2 Criterion §7.3 requires that the CA has a policy and maintains controls to provide reasonable assurance that audit logs generated after the effective date of the Baseline Requirements are retained for at least seven years.	Although firewall activities are logged in accordance with Principle 2 Criterion §7.2, audit logs for these events are not required to be retained for at least seven years in accordance with Principle 2 Criterion §7.3. As a result, Wells Fargo did not meet Principle 2 Criterion §7.3 for firewall activity logs during the examination period.
4	Principle 4 Criterion §4.0 requires to perform one of the following within 96 hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process: • If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to the following: - Vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0); and - Systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise;	Wells Fargo internal policies target critical vulnerabilities to be addressed within 30 days of discovery and not 96 hours as required by WTBR 2.0 criteria 4-4. Furthermore, the average number of days to remediate vulnerabilities was approximately 60 days. As a result, Wells Fargo did not meet Principle 4 Criterion §4.0 for vulnerability management during the examination period.

No.	Requirements	Issues Noted
	• Document the factual basis for the CA's determination that the vulnerability does not require remediation because of one of the following: - The CA disagrees with the NVD rating; - The identification is a false positive; - The exploit of the vulnerability is prevented by compensating controls or an absence of threats; or - Other similar reasons.	
5	Principle 4 Criterion §1.0 requires that the CA maintains controls to provide reasonable assurance that: • Certificate Systems are segmented into networks or zones based on their functional, logical, and physical (including location) relationship;	The PKI network is not physically or logically segregated from the Wells Fargo enterprise systems. The CAs are currently on the same corporate network that houses other critical enterprise systems and has incorporated stringent network security controls. As a result, Wells Fargo did not meet Principle 4 Criterion §1.0 during the examination period.

Wells Fargo Bank N.A:

Patty O'Boyle

Senior Vice President