



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

REPORT OF THE INDEPENDENT ACCOUNTANT

To the Management of Wells Fargo Bank N.A:

We have examined for Wells Fargo Bank N.A.'s ("Wells Fargo") Certification Authority (CA) operations at Shoreview, Minnesota; Tempe Arizona; Homewood, Alabama and Silas, North Carolina, Wells Fargo's 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 throughout the period September 1, 2015 through August 31, 2016, 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").

These disclosures and controls are the responsibility of Wells Fargo's management. Our responsibility is to express an opinion on the conformity of these disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Requirements Audit Criteria Version 2.0, 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 matters that resulted in a modification of our opinion:

No.	Impacted WebTrust Criteria	Matters Noted
1	<p>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.</p> <p>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.</p>	<p>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.</p> <p>As a result, we noted that Wells Fargo did not meet Principle 2 Criterion §7.3 for firewall activity logs during the examination period.</p>
2	<p>Principle 4 Criterion §4.0 requires that the CA maintains controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"> • A formal documented vulnerability correction process is followed and includes identification, review, response, and remediation of vulnerabilities; 	<p>Wells Fargo internal policies target high risk vulnerabilities to be addressed within 60 days from the third party vendor patch release date. However, KPMG identified 2 out of 25 high risk vulnerabilities that were not remediated timely (remediation occurred past 60 days from the patch release date).</p> <p>As a result, we noted that Wells Fargo did not meet Principle 4 Criterion §4.0 for vulnerability management during the examination period.</p>
3	<p>Principle 4 Criterion §1.0 requires that the CA maintains controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"> • Certificate Systems are segmented into networks or zones based on their functional, logical, and physical (including location) relationship; 	<p>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.</p> <p>As a result, we noted that Wells Fargo did not meet Principle 4 Criterion §1.0 during the examination period.</p>

In our opinion, except for the effects of the matters discussed in the preceding paragraphs, in providing its Wells Fargo SSL Certification Authority (CA) services at Shoreview, Minnesota; Tempe Arizona; Homewood, Alabama and Silas, North Carolina during the period September 1, 2015 through August 31, 2016, 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 Requirements 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

Santa Clara, California
November 29, 2016



**Assertion of Management as to
its Disclosure of its Business Practices and its Controls
over its Certification Authority Operations during the period
from September 1, 2015 through August 31, 2016**

November 29, 2016

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, 2015 through August 31, 2016, 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 Requirements 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.	Impacted WebTrust Criteria	Matters Noted
1	<p>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.</p> <p>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.</p>	<p>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.</p> <p>As a result, Wells Fargo did not meet Principle 2 Criterion §7.3 for firewall activity logs during the examination period.</p>



No.	Impacted WebTrust Criteria	Matters Noted
2	<p>Principle 4 Criterion §4.0 requires that the CA maintains controls to provide reasonable assurance that:</p> <ul style="list-style-type: none">• A formal documented vulnerability correction process is followed and includes identification, review, response, and remediation of vulnerabilities;	<p>Wells Fargo internal policies target high risk vulnerabilities to be addressed within 60 days from the third party vendor patch release date. However, KPMG identified 2 out of 25 high risk vulnerabilities that were not remediated timely (remediation occurred past 60 days from the patch release date).</p> <p>As a result, Wells Fargo did not meet Principle 4 Criterion §4.0 for vulnerability management during the examination period.</p>
3	<p>Principle 4 Criterion §1.0 requires that the CA maintains controls to provide reasonable assurance that:</p> <ul style="list-style-type: none">• Certificate Systems are segmented into networks or zones based on their functional, logical, and physical (including location) relationship;	<p>The PKI network is not physically or logically segregated from the Wells Fargo enterprise systems. The CAs are currently on the same corporate network and not segregated from the rest of the corporate systems.</p> <p>As a result, Wells Fargo did not meet Principle 4 Criterion §1.0 during the examination period.</p>

Wells Fargo Bank N.A:

Patricia S. O'Boyle
Executive Vice President