WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security

INDEPENDENT AUDITOR'S REPORT

Swedish Social Insurance Agency ("SSIA") (Swedish: "Försäkringskassan") Certification Authority, ("MCA"):

We have been engaged, in a reasonable assurance engagement, to report on SSIA's CA management's statement that for its Certification Authority (CA) operations at Sundsvall, Sweden, throughout the 30 May 2016 to 30 November 2016. For its services known as Swedish Government Root Authority v3 (Thumbprint 74 6f 88 f9 ac 16 3c 53 00 9e ef 92 0c 40 67 75 6a 15 71 7e) and Swedish Government HW CA v4, FK-CA has, with the exceptions mentioned below under the section "modified opinion":

- disclosed its SSL certificate lifecycle management business practices in its:
    - Swedish Social Insurance Agency Authentication X.509 Certification Practices Statement v2.2.0 dated 2016-10-31 and Swedish Social Insurance Agency Hardware X.509 Certification Practices Statement v4.3.0 dated 2016-10-31, and
    - Swedish Social Insurance Agency Authentication X.509 Certificate Policy v2.2.0 dated 2016-10-31 and Swedish Social Insurance Agency Hardware X.509 Certificate Policy v4.2.0 dated 2016-05-24.

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the SSIA's CA website, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
    - SSL subscriber information is properly authenticated (for the registration activities performed by SSIA)

- maintained effective controls to provide reasonable assurance that:
    - logical and physical access to CA systems and data is restricted to authorized individuals;
    - the continuity of key and certificate management operations is maintained; and
    - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.0.

Certification authority's responsibilities

SSIA's management is responsible for its statement, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.0.

Our independence and quality control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies International Standard on Quality Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on management's statement based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information,* issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's statement is fairly stated, and, accordingly, included:

(1) obtaining an understanding of SSIA's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of SSIA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
(2) selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management practices;
(3) testing and evaluating the operating effectiveness of the controls; and
(4) performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at SSIA 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.

Inherent limitations

Because of the nature and inherent limitations of controls, SSIA'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.

Modified Opinion

We noted the following issues below that resulted in a modification of our opinion for the (prior) testing period covering February 16 2016 to May 29 2016. SSIA's management have been remediating the issues noted during the current testing period 30 May 2016 to November 30 2016. Hence it is our opinion and SSIA's managements opinion as described in their statement issued 31 October 2017 that the issues noted below, are impacting/are relevant also for the current testing period while being remediated. We have however, noted that remediation has taken place as also evidenced by subsequent testing period covering 1 December 2016 to 29 May 2017 as covered by subsequent Independent Auditors Report issued 31 October 2017.

Principle Number	Impacted SSL Baseline with Network Security Principle	Issues Noted during testing period 16 February 2016 to 29 May 2016 as reported 26 September 2016. Issues below have been subject to remediating activities during current testing period 30 May 2016 to 30 November 2016.
2.2	The CA maintains controls to provide reasonable assurance that certificates issued meet the minimum requirements for Certificate Content and profile as established in section 9 of the SSL Baseline Requirements including the following: • As of the Effective Date of these Requirements, prior to the issuance of a Certificate with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name, the CA shall notify the Applicant that the use of such Certificates has been deprecated by the CA / Browser Forum and that the practice will be eliminated by October 2016. Also as of the Effective Date, the CA shall not issue a certificate with an Expiry Date later than 1 November 2015 with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name. Effective 1 October 2016, CAs shall revoke all unexpired Certificates whose subjectAlternativeName extension or Subject commonName field contains a Reserved IP Address or Internal Server Name.	It was noted that the (required) Subject Alternative Name extension was only present only on 2 of 5 certificates tested.
4.2	The CA maintains controls to provide reasonable assurance that: • A documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them is followed; • The responsibilities and tasks assigned to Trusted Roles are documented and "separation of duties" for such Trusted Roles based on the risk assessment of the functions to be performed is implemented; • Only personnel assigned to Trusted Roles have access to Secure Zones and High Security Zones; • Individuals in a Trusted Role acts only within the scope of such role when performing administrative tasks assigned to that role; • Employees and contractors observe the principle of "least privilege" when accessing, or when configuring access privileges on, Certificate Systems; • Trusted Role use a unique credential created by or assigned to that person for authentication to Certificate Systems; • Trusted Role using an username and password to authenticate shall configure accounts to include but not be limited to: o Passwords have at least twelve (12) characters for accounts not publicly accessible (accessible only within Secure Zones or High Security Zones); o Configure passwords for accounts that are accessible from outside a Secure Zone or High Security Zone to have at least eight (8) characters, be changed at least every 90 days, use a combination of at least numeric and alphabetic characters, and not be one of the user's previous four passwords; and implement account lockout for failed access attempts; OR	There is no documentation specifying rules for which roles/responsibilities that should not be combined (Segregation of Duties). IT personnel without a Trusted Role has access to the Secure Zones where CA support systems are hosted as this is a normal data center where other systems hosted. Access controls are utilized to ensure that an individual in a trusted role acts only within the scope of such role when performing administrative tasks assigned to that role. It has however been noted during the audit that access reviews are not performed every 90 days for all CA components. Password setting for system lockout on failed login attempts

	○ Implement a documented password management and account lockout policy that the CA has determined provide at least the same amount of protection against password guessing as the foregoing controls. • Trusted Roles log out of or lock workstations when no longer in use; • Workstations are configured with inactivity time-outs that log the user off or lock the workstation after a set time of inactivity without input from the user; • Review all system accounts at least every 90 days and deactivate any accounts that are no longer necessary for operations; • Revoke account access to Certificate Systems after no more than five (5) failed access attempts, provided that this security measure is supported by the Certificate System and does not weaken the security of this authentication control; • Disable all privileged access of an individual to Certificate Systems within 24 hours upon termination of the individual's employment or contracting relationship with the CA or Delegated Third Party; • Enforce multi-factor authentication for administrator access to Issuing Systems and Certificate Management Systems; • Each Delegated Third Party, shall be: ○ Required to use multi-factor authentication prior to the Delegated Third Party approving issuance of a Certificate; or ○ Be technically constrained that restrict the Delegated Third Party's ability to approve certificate issuance for a limited set of domain names; and • Restrict remote administration or access to an Issuing System, Certificate Management System, or Security Support System except when: ○ The remote connection originates from a device owned or controlled by the CA or Delegated Third Party and from a pre-approved external IP address, ○ The remote connection is through a temporary, non-persistent encrypted channel that is supported by multi-factor authentication, and ○ The remote connection is made to a designated intermediary device meeting the following: ▪ Located within the CA's network, ▪ Secured in accordance with these Requirements, and ▪ Mediates the remote connection to the Issuing System.	has been configured to high (8 attempts).
4.3	The CA maintains controls to provide reasonable assurance that: • Security Support System under the control of CA or Delegated Third Party Trusted Roles are implemented to monitor, detect, and report any security-related configuration change to Certificate Systems; • Certificate Systems under the control of CA or Delegated Third Party Trusted Roles capable of monitoring and logging system activity and are configured to continuously monitor and log system activity; • Automated mechanisms under the control of CA or Delegated Third Party Trusted Roles are configured to process logged system activity and alert personnel, using notices provided to multiple destinations, of possible Critical Security Events; • Trusted Role personnel follows up on alerts of possible Critical Security Events; • A human review of application and system logs is performed at least every 30 days and includes: ○ Validating the integrity of logging processes ○ Testing the monitoring, logging, alerting, and log-integrity-verification functions are operating properly; and • Maintain, archive, and retain logs in accordance with disclosed business practices.	A human review of application and system logs is not performed at least every 30 days for; • validating the integrity of logging processes • testing the monitoring, logging, alerting, and log-integrity-verification functions are operating properly. Weekly vulnerability scans are performed on public IP addresses but there are no scans performed on internal CA IP addresses.
4.4	The CA maintains controls to provide reasonable assurance that: • Detection and prevention controls under the control of CA or Delegated Third Party Trusted Roles are implemented to protect Certificate Systems against viruses and malicious software; • A formal documented vulnerability correction process is followed and includes identification, review, response, and remediation of vulnerabilities; • Perform a Vulnerability Scan on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems based on the following:	Formalised procedures to perform a Penetration Tests have not yet been fully developed. A contract has been signed with a 3rd party firm for penetration tests of the CA systems/environment. Procedures for handling a Critical Vulnerability exists in form of the

	○ Within one week of receiving a request from the CA/Browser Forum, ○ After any system or network changes that the CA determines are significant, and ○ At least once per quarter; • Perform a Penetration Test on the CA's and each Delegated Third Party's Certificate Systems on at least an annual basis and after infrastructure or application upgrades or modifications that the CA determines are significant; • Document that Vulnerability Scan and Penetration Test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test; and • Perform one of the following within 96 hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process: ○ Remediate the Critical Vulnerability; ○ 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; or ○ 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.	incident, problem and change management procedures. These are not CA specific and do not clearly specify how to address the Network Security Requirements for handling of a Critical Vulnerability within 96 hours of discovery.

In our opinion, considering the matters described in the preceding paragraphs, SSIA's management's statement, as referred to above, is fairly stated, in all material respects, throughout the period throughout the 30 May 2016 to 30 November 2016 in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.0.

This report does not include any representation as to the quality of SSIA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.0, nor the suitability of any of SSIA's services for any customer's intended purpose.

31 October 2017

Deloitte AB

Marcus Sörlander
Stockholm, Sweden