



**OPEN ACCESS TECHNOLOGY INTERNATIONAL, INC.**

INDEPENDENT SERVICE AUDITOR'S REPORT ON THE WEBTRUST® FOR  
CERTIFICATION AUTHORITIES – SSL BASELINE REQUIREMENTS

NOVEMBER 15, 2014

Attestation and Compliance Services

**Schellman & Company, LLC**

*Certified Public Accountants*

**Proprietary & Confidential**

Unauthorized use, reproduction or distribution of this report, in whole or in part, is strictly prohibited.

This report is intended solely for use by the management of Open Access Technology International, Inc., its user entities (i.e., customers) that utilized the services covered by this report during the specified time period, and the independent financial statement auditors of those user entities (each referred to herein as a "specified user").

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction or distribution of this report, in whole or in part, is strictly prohibited.

# TABLE OF CONTENTS

SECTION 1	INDEPENDENT SERVICE AUDITOR'S REPORT .....	1
SECTION 2	MANAGEMENT'S ASSERTION .....	3
SECTION 3	DESCRIPTION OF THE SYSTEM .....	5

# SECTION I

## **INDEPENDENT SERVICE AUDITOR'S REPORT**

## INDEPENDENT SERVICE AUDITOR'S REPORT

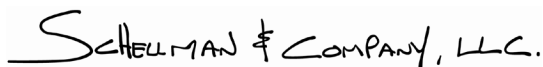
We have examined management's assertion that Open Access Technology International, Inc. ("OATI" or the "service organization") controls over its Certification Authority (CA) services ("OATI webCARES CA") were suitably designed to meet the WebTrust® for Certification Authorities - SSL Baseline Requirements Audit Criteria (the "SSL Baseline Requirements") ("the Description") as of November 15, 2014. OATI's management is responsible for compliance with the SSL Baseline Requirements and for the assertion, including the completeness, accuracy, and method of presentation of the Description and the assertion, providing the services covered by the Description, specifying the compliance requirements and stating them in the Description, identifying the risks that threaten the achievement of the compliance requirements, selecting the criteria, and designing and implementing the internal controls to meet the related compliance requirements stated in the Description.

Our responsibility is to express an opinion on management's assertion about OATI's compliance with the SSL Baseline Requirements 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 examining, on a test basis, evidence supporting management's assertion and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Our examination does not provide a legal determination of OATI's compliance with the SSL Baseline Requirements; however, this report may be useful to legal counsel or others in making such determinations.

In our opinion, management's assertion referred to above is fairly stated, in all material respects, based on the criteria described in OATI's assertion.

This report is intended solely for the information and use of OATI, and user entities of OATI's services as of November 15, 2014. This report is not intended to be and should not be used by anyone other than these specified parties.

SCHHELLMAN & COMPANY, LLC.

Tampa, Florida  
December 12, 2014

## **SECTION 2**

### **MANAGEMENT'S ASSERTION**



## MANAGEMENT'S ASSERTION

We have prepared the description of Open Access Technology International, Inc.'s ("OATI") controls over its Certification Authority (CA) services ("OATI webCARES CA") relevant to the WebTrust® for Certification Authorities - SSL Baseline Requirements Audit Criteria ("SSL Baseline Requirements") (the "Description") for user entities of the system as of November 15, 2014. We confirm, to the best of our knowledge and belief, that

- a. Management's Description fairly presents the controls supporting the SSL Baseline Requirements as of November 15, 2014. The criteria we used in making this assertion were that the Description
  - i. presents how the controls were designed and implemented; and,
  - ii. does not omit or distort information relevant to the scope of the controls supporting the SSL Baseline Requirements.
- b. The controls related to the applicable SSL Baseline Requirements Audit Criteria stated in the Description were suitably designed as of November 15, 2014, to achieve the criteria, if operating effectively. The criteria we used in making this assertion were that
  - i. the risks that threaten the achievement of the criteria stated in the Description have been identified by OATI; and
  - ii. the controls identified in the Description would, if operating as described, provide reasonable assurance that those risks would not prevent the criteria stated in the Description from being achieved.

Section 3 of this report includes OATI's Description of the controls supporting the SSL Baseline Requirements that is covered by this assertion.

# SECTION 3

## DESCRIPTION OF THE SYSTEM



---

## OVERVIEW OF OPERATIONS

### Company Background

Open Access Technology International, Inc. (OATI), a privately held Minnesota corporation, provides solutions to the web-connected world. OATI overall staffing now exceeds 930 including power systems and industry experts, information technology (IT) and cyber security experts, Smart Grid and green energy experts, as well as help desk and support. OATI's corporate headquarters and Data Centers are located in and around Minneapolis, Minnesota. OATI also has an office in Redwood City, California, and regional employees located throughout North America.

Key aspects of OATI services focus on data/transaction management, warehousing, and retrieval in real-time. Critical in its delivery of these services are OATI's Data Centers, which provide a secure production application environment, with multiple redundant systems and networks.

### Description of Services Provided

OATI webCARES is OATI's proprietary and wholly managed Public Key Infrastructure (PKI) and Certificate Authority (CA). OATI webCARES is hosted in the OATI Private Cloud Infrastructure, where it benefits from system availability and redundancy. OATI webCARES undergoes third party audits/assessments on an annual basis.

The OATI Private Cloud Infrastructure provides redundancy, ensuring the system availability, including, but not limited to:

- Geographically diverse sites, with full load balancing and synchronous data replication
- Monthly inter-site transfer drills to ensure business continuity
- Information compartmentalized for increased security and reliability

Security of the PKI, both physical and virtual, is critical for both the reliability and trust inherent in CA operations. OATI employs a layered and comprehensive security approach with no single point of protection.

### Scope Definition

The scope of this examination was limited to the OATI webCARES CA operations and related controls supported by the Minneapolis, Minnesota, and Plymouth, Minnesota, facilities relevant to the WebTrust® for Certification Authorities - SSL Baseline Requirements Audit Criteria.

No subservice organizations were included in the scope of this assessment.

---

## CONTROL ENVIRONMENT

Management, under the leadership of the Chief Executive Officer (CEO), has established a program in support of OATI controls. The OATI Compliance Program manages controls and implements policies, procedures, and processes, and is monitored by OATI management to provide discipline, structure, efficiency, and continuity of operations.

OATI executive management coordinates aspects of operations, identifies areas requiring controls, implements controls, performs application planning and implementation, reviews network and system operations, and oversees business continuity and resiliency planning. Executive management approves controls, policies, procedures, and processes through a structured corporate approval process. Executive management also reviews reports from internal audits, external auditors, and staff to verify that the control environment is functioning as intended.

Corporate objectives and performance standards are understood and followed by OATI personnel. Expectations of employee conduct are set out in an Employee Handbook that is given to a new employee on the first day of employment. New employees are required to read, study, and ask questions about the Employee Handbook. In addition, new employees undergo a new employee orientation program. New employees also sign the Confidentiality Agreement that is designed to protect the confidentiality of OATI proprietary information and customers' applications and data. Management uses a variety of means to support ethical standards. These include supervision, periodic meetings, annual performance reviews, e-mail communications, and the actions of management.

OATI seeks to employ qualified technical personnel to support its operations. College degrees are required for specific work positions. Technical competence is promoted by project team meetings so that OATI staff, who are involved in developing and supporting software applications, understand the industry requirements that drive OATI applications and also understand new and existing functionality of OATI applications.

OATI maintains a Help Desk 24x7x365 to support customers in their use of the software applications, including research and resolution of identified problems. The CEO and other senior management periodically visit and meet with customers to understand their needs and objectives in using OATI products and services. A project manager oversees the launch of a software application for a new customer, and remains assigned to the customer for the lifecycle of the application to provide customer support, including training, to support the customer's use of the application. Project managers are required by the CEO to periodically visit their respective customers to maintain a working relationship.

Corporate controls require the use of the OATI Software Development Methodology, which is the main method used for the development of new OATI products and services and for software changes made to existing OATI products and services. The same overall process is used at OATI when planning, implementing, and deploying a large new project, or managing a project change order that may develop a new application or an enhancement to an existing production system.

The key organizational roles and responsibilities for projects are as follows:

- President - The president has general oversight responsibility for OATI projects and services.
- Executive Management - Executive management is responsible to set strategy, and oversee and guide the implementation of OATI's projects and services.
- Product Manager - The product manager sets the overall direction for the product and interacts with OATI sales and marketing department on product marketing. This person is assigned responsibility for overseeing activities that concern a particular product. OATI products are assigned a product manager.
- Technical Consultant - Technical consultants are designated OATI personnel who share responsibility for guiding overall system architecture decisions and high level direction of OATI products and solutions for complex integration issues. They also propose new solutions for ever-changing industry requirements.
- Project Manager - A project manager is engaged with a project from its inception through the lifecycle of the project. OATI utilizes third party software project tools to assist in project planning and project control throughout the life of the project. The allocation of resources to maintain customer implementation schedules is continuously monitored with the help of these tools. Project activities and tasks are utilized to provide various checkpoints throughout the project. The OATI project manager manages the development, implementation, and operation of the assigned project using the OATI Project Management Methodology. This methodology is a systematic approach to managing the initiatives, scope, priorities, risk, and resources necessary for executing the project plan and meeting the delivery milestones. The project manager is responsible to address problems to mitigate the impact of unforeseeable problems.

This document contains confidential and proprietary information of OATI.  
Do not copy or distribute without express written consent of OATI.

This includes schedule related issues, potential scope issues and possible budget impacts. The project manager facilitates the management of risk, scope, and quality, as well as the transfer of knowledge across teams to further diminish the risk of issues.

- **Software Developers** - Software developers are individuals who design, write, unit test, and maintain OATI software.
- **Product Lead** - A product lead is responsible for the overall technical product direction. A product lead works closely with technical leads to maintain leadership for the overall product design and requirement definitions and to maintain consistency and general technical quality.
- **Technical Lead** - A technical lead is responsible for a specific technical aspect of a product.
- **Project Engineer** - The project engineer is a member of the OATI IT department and is the primary resource for project-related systems and network issues and activities.
- **Integrator** - An integrator is assigned to perform specific tasks for customer systems, including, but not necessarily limited to, staging application on hardware; working with IT to configure applications; assisting the customer in initial system configuration and testing; deploying corrections and new changes/releases of project systems; and initially reviewing and investigating customer problems and issues. An integrator may do software development. An integrator is responsible for testing changes implemented by software developers when the changes involve project-specific changes.
- **Product Team** - A group of individuals assigned to the design, development, and maintenance of a common product. The team is comprised of a product manager, a product owner, a product lead, a technical consultant, and a team of software developers. A product team may also include a project team.
- **Project Team** - A group of individuals assigned to the design, development, and maintenance of a customer's system. The team is comprised of a project manager, product owners, an integrator, a project engineer, and a team of software developers. The project team may also include a product team or certain product team members.
- **Testing Team** - A testing team (designated by the product manager) is created for the short term purpose of performing testing activities for changes, releases, or patches. This team may be made up of developers, independent testers, support staff, sales and marketing staff, or other technical management members.
- **Training Team** - A group of individuals assigned to provide specific training for OATI customers.
- **IT Management** - IT staff members at the senior management level or executive level and their delegates for specific IT-related tasks as recorded in webSupport. IT management is responsible for managing the physical and cyber infrastructure which includes 24x7 monitoring, hardware installation and maintenance, database administration, outage management, and system upgrades.

---

## RISK ASSESSMENT

OATI considers risk management and risk mitigation critical functions. OATI management monitors the quality of internal control performance as part of their management responsibilities. Continuous monitoring and assessment of the performance and effectiveness are performed using automated monitoring, audits, and reviews of process implementation and effectiveness.

OATI has automated systems to monitor activity and assess risk concerns. Policies and procedures are reviewed and updated regularly, incorporating new standards and policies as needed to meet changing markets and technology.

OATI has established certain broad categories including:

- Strategic objectives - these pertain to the high-level organizational goals and the alignment of those goals to support the overall mission
- Operations objectives - these pertain to effectiveness and efficiency of the entity's operations, including performance and profitability goals and safeguarding of resources against loss
- Reporting objectives - these pertain to the preparation of reliable reporting
- Compliance objectives - these pertain to adherence to laws and regulations to which the entity is subject

## **Risk Identification**

In order to identify the risk associated with each control area, a risk level assessment is performed on the control activities found within the respective control areas. For example, a control area such as application development and change management is comprised of individual control activities. Each control activity is reviewed by management and departmental personnel to determine whether OATI's ability to adhere to the control activity as stated exists and the probability that OATI will maintain adherence using a grading system of high, medium, and low. The factors considered in the risk level process include the following:

### *External Factors*

- Natural catastrophes
- Major connectivity disruptions including loss of communication links
- Power failures
- Code hacks and other external attacks
- Changing customer needs or expectations
- Technological developments
- New accounting pronouncements
- Changes in local, regional and national industry regulations

### *Internal Factors*

- A disruption in information systems, including simultaneous losses of core pieces of hardware
- Incompetent personnel
- Unethical personnel with access to confidential data
- Loss or leaks of customer data
- Rapid growth
- Changes in operating environment
- New business models, products, or activities
- Corporate restructurings
- Loss of code and other intellectual property

## Risk Analysis

OATI's methodology for analyzing risks varies, largely because many risks are difficult to quantify. The process includes:

- Estimating the significance of a risk
- Assessing the likelihood (or frequency) of the risk occurring
- Considering how the risk should be managed, including an assessment of what actions need to be taken

---

## MONITORING

OATI management monitors the quality of internal control performance as a routine part of their activities. OATI IT monitoring is the direct responsibility of the IT management team. The OATI compliance program team is responsible for overseeing the documentation of processes and controls. This team periodically audits processes to verify policies are being enforced. Discrepancies are brought to the attention of senior management and resolved.

---

## INFORMATION AND COMMUNICATION SYSTEMS

### Information Systems

Production information systems are located in the OATI Data Centers located in Minneapolis and Plymouth, Minnesota. The OATI Data Centers include over 20,000 square feet of production data center space with additional capacity for expansion and are managed solely by OATI. Each Data Center is a mirror of the other. The two Data Centers actively share and balance load between one another. In the event of unexpected downtime or planned maintenance at one Data Center, the other is capable of hosting all systems independently. A real-time active copy of the data resides at each Data Center simultaneously, so the data resides in two geographically diverse sites.

Network connectivity between the two Data Centers is provisioned over redundant, dedicated and secure fiber optic connectivity. The two Data Centers, and secure redundant network connectivity, form the backbone of the OATI Private Cloud. Each individual Data Center production environment is served by redundant power and heating, ventilation, and air conditioning (HVAC), along with backup generators. Systems are tested and maintained at regular intervals.

Additionally, multiple diverse connections are used for Internet connectivity. OATI also offers managed communication solutions to customers for security and management purposes and maintains redundant telecom connectivity.

OATI provides many of its products and services over the public Internet, accessed through secure communication paths to OATI's Data Centers as hosted web-based applications. Many entities utilize private network connections, like OATInet, which OATI networking professionals may manage on behalf of customers. These applications are hosted and maintained by OATI staff. Other applications are custom-designed and implemented for clients and are delivered to the customer sites. Regardless of how customers access the applications, critical data is secured with digital certificates that are also provided and secured by OATI. Additionally, OATI hosted applications can be integrated with the customer site-resident software through defined and documented application program interfaces (APIs).

This document contains confidential and proprietary information of OATI.  
Do not copy or distribute without express written consent of OATI.

To protect critical customer data, OATI has detailed physical and cyber security policies to provide direction and to establish policies for employees of OATI and other persons entering an OATI Data Center, the production environment, and selected restricted access areas. Additionally, physical and cyber security policies control access to customer data and customer application software residing at an OATI Data Center.

The OATI Data Centers have multiple zones of security with logging of access activities. These sites are controlled and monitored on a 24x7x365 basis.

Physical site security measures include:

- Access control throughout the Data Center
- Motion detection throughout the Data Center
- Role-based access control
- Video surveillance
- 24x7x365 alarm system monitoring
- Concrete reinforced structure within an exterior building
- Site redundancy
- Site sign in and out logs
- Tracking logs

Cyber security and data protection measures in place in the OATI Data Centers include:

- Local and remote backup of critical systems
- Network protection through redundant firewalls
- Intrusion detection software, including pattern matching, intrusion mitigation, and usage reporting
- Antivirus tools to perform constant scanning, periodic scanning, and e-mail scanning
- Logging of successful and failed system logons
- Encryption to provide data security and login security
- Traffic filtering to protect against known hackers and known hacks
- Restricted network access
- Redundancy of network connectivity and infrastructure
- Internal and external auditing
- Application-level passwords and user roles

OATI employs a role-based Access Control System (ACS) at its Data Centers. This system, provided by a national provider of access control systems, consists of the following components:

- Perimeter entrances and Data Center entrances are locked 24x7
- An access control system and biometric scanners are maintained for production environment
- Role-based security policy
- Access to a Data Center within an OATI facility is restricted to authorized personnel and visitor access is by escort
- Alarm system monitored 24x7x365
- Electronic entry audit system for entrances and exits to/from a Data Center

OATI-hosted and delivered applications support the flow of data and transactions between customer business processes and third party entities, such as regulatory entities, reliability organizations, utilities, or other organizations. Regardless of the applications used by OATI customers, the customer initiates transactions and enters transaction details in the respective application. Customers are required to define their own internal control procedures to initiate and approve transactions. The customer decides how specific applications in its accounting processes will be utilized. Accordingly, OATI applications can provide the customer with a summary of transactions processed.

Standard OATI graphical user interfaces for certain OATI products allow customers to export summary screens to Microsoft® Excel spreadsheets. Additionally, with certain OATI applications, customers have the flexibility to create ad-hoc reports to meet their specific needs and requirements.

## Communication Systems

OATI has implemented communications to inform staff members of/about individual roles and responsibilities regarding customer service and the handling of customer confidential applications and data. Communications include orientation and training for newly hired personnel and the use of e-mail to communicate time-sensitive messages and information, including, but not limited to cyber security awareness and business continuity. Management holds daily staff meetings to communicate information as it relates to the employees' job functions and implementation of OATI control procedures. Staff are required to review and accept OATI's security policies as a condition of employment.

The OATI Help Desk provides ongoing communication with the customer. The Help Desk maintains records on relevant customer communications and tracks issues.

## WEBTRUST® FOR CERTIFICATION AUTHORITIES – SSL BASELINE REQUIREMENTS

OATI's management is responsible for compliance with the following WebTrust® for Certification Authorities – SSL Baseline Requirements (SSL Baseline Requirements). OATI asserts that it meets the following criteria.

Ref #	SSL Baseline Requirements Audit Criteria
<b>Principle 1: Baseline Requirements Business Practices Disclosure</b> - The Certification Authority (CA) discloses its Certificate practices and procedures and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines.	
1	<p>The CA and its Root CA discloses on its website its:</p> <ul style="list-style-type: none"> <li>• Certificate practices, policies and procedures,</li> <li>• all Cross Certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue), and</li> <li>• its commitment to conform to the latest version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum.</li> </ul> <p>(See SSL Baseline Requirements Section 8.3 and 8.4)</p>



Ref #	SSL Baseline Requirements Audit Criteria
2	The Certificate Authority discloses in the Certificate Policy (CP) and/or Certification Practice Statement (CPS) that it includes its limitations on liability, if the CA chooses to limit its liability for Certificates that are not issued or managed in compliance with these Requirements or its Certificate Policy and/or Certification Practice Statement. (See SSL Baseline Requirements Section 18.1)
3	The issuing CA documents in its CP or CPS that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with the SSL Baseline Requirements. (See SSL Baseline Requirements 9.3.4)
4	The Certificate Authority has controls to provide reasonable assurance that the CA CP and/or CPS that describes how the CA implements the latest version of the Baseline Requirements are updated annually. (See SSL Baseline Requirements Section 8.2.1)
5	The CA and its Root has controls to provide reasonable assurance that there is public access to the CP and/or CPS on a 24x7 basis, and the content and structure of the CP and/or CPS are in accordance with either RFC 2527 or RFC 3647. (See SSL Baseline Requirements 8.2.2)
<b>Principle 2: Service Integrity</b> - The Certification Authority maintains effective controls to provide reasonable assurance that: <ul style="list-style-type: none"> <li>Subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;</li> <li>The integrity of keys and certificates it manages is established and protected throughout their life cycles.</li> </ul>	
	The following criteria apply to both new and renewed Certificates.
<b>1</b>	<b>KEY GENERATION CEREMONY</b>
1.1	The CA maintains controls to provide reasonable assurance that for Root CA Key Pairs created after the Effective Date of the Baseline Requirements that Baseline Requirements are followed. (See SSL Baseline Requirements Section 17.7)
<b>2</b>	<b>CERTIFICATE CONTENT AND PROFILE</b>
2.1	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 Baseline Requirements including the following: <ul style="list-style-type: none"> <li>Issuer Information (See SSL Baseline Requirements Section 9.1)</li> <li>Subject Information (See SSL Baseline Requirements Section 9.2)</li> <li>Certificate Policy Identification (See SSL Baseline Requirements Section 9.3)</li> <li>Validity Period (See SSL Baseline Requirements Section 9.4)</li> <li>Subscriber Public Key (See SSL Baseline Requirements Section 9.5)</li> <li>Certificate Serial Number (See SSL Baseline Requirements Section 9.6)</li> <li>Additional Technical Requirements (See SSL Baseline Requirements Section 9.7)</li> <li>Appendix A - Cryptographic Algorithm and Key Requirements</li> <li>Appendix B - Certificate Extensions.</li> </ul> (See SSL Baseline Requirements Section 9)



Ref #	SSL Baseline Requirements Audit Criteria
2.2	<p>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:</p> <ul style="list-style-type: none"> <li>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. (See SSL Baseline Requirements Section 9.2.1)</li> </ul>
2.3	<p>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:</p> <ul style="list-style-type: none"> <li>The CA shall implement a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with SSL Baseline Requirements Section 11.2 and the Certificate also contains subject:organizationName, subject:localityName, and subject:countryName attributes, also verified in accordance with SSL Baseline Requirements Section 11.2.</li> <li>Appendix C - User Agent Verification. (See SSL Baseline Requirements Section 9.2.6)</li> </ul>
2.4	<p>The CA maintains controls and procedures to provide reasonable assurance that Certificates are valid for a period not exceeding 60 months. (See SSL Baseline Requirements Section 9.4)</p>
2.5	<p>The CA maintains controls and procedures to provide reasonable assurance that Certificates are not issued if the requested Public Key does not meet the requirements set forth in Appendix A or if it has a known weak Private Key (such as a Debian weak key, see <a href="http://wiki.debian.org/SSLkeys">http://wiki.debian.org/SSLkeys</a>). (See SSL Baseline Requirements Section 9.5)</p>
<b>3</b>	<b>CERTIFICATE REQUEST REQUIREMENTS</b>
3.1	<p>The CA maintains controls and procedures to provide reasonable assurance that the CA, prior to the issuance of a Certificate obtains the following documentation from the Applicant:</p> <ol style="list-style-type: none"> <li>A certificate request, which may be electronic; and</li> <li>An executed Subscriber or Terms of Use Agreement, which may be electronic.</li> <li>Any additional documentation the CA determines necessary to meet the Baseline Requirements. (See SSL Baseline Requirements Section 10.1)</li> </ol>

Ref #	SSL Baseline Requirements Audit Criteria
3.2	<p>The CA maintains controls and procedures to provide reasonable assurance that the Certificate Request is:</p> <ul style="list-style-type: none"> <li>• obtained and complete prior to the issuance of Certificates (See Baseline Requirements Section 10.2.1),</li> <li>• signed by an authorized individual (Certificate Requester),</li> <li>• properly certified as to being correct by the applicant (See SSL Baseline Requirements Section 10.2.2), and</li> <li>• contains the information specified in Section 10.2.3 of the SSL Baseline Requirements.</li> </ul>
3.3	<p><b>Subscriber Private Keys</b>  Parties other than the Subscriber shall not archive the Subscriber Private Key:  If the CA or any of its designated RAs generated the Private Key on behalf of the Subscriber, then the CA shall encrypt the Private Key for transport to the Subscriber.  If the CA or any of its designated RAs become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then the CA shall revoke all certificates that include the Public Key corresponding to the communicated Private Key.  (See SSL Baseline Requirements Section 10.2.4)</p>
3.4	<p><b>Subscriber Agreement and Terms of Use</b>  The CA maintains controls and procedures to provide reasonable assurance that the CA, prior to the issuance of a Certificate, obtains a Subscriber and/or Terms of Use agreement in accordance with the SSL Baseline Requirements Section 10.3.1. That agreement contains provisions imposing obligations and warranties on the Application relating to:</p> <ul style="list-style-type: none"> <li>• the accuracy of information</li> <li>• protection of Private Key</li> <li>• acceptance of certificate</li> <li>• use of certificate</li> <li>• reporting and revocation</li> <li>• termination of use of certificate</li> <li>• responsiveness</li> <li>• acknowledgement and acceptance.</li> </ul> <p>(See SSL Baseline Requirements Section 10.3)</p>
<b>4</b>	<b>VERIFICATION PRACTICES</b>
	<b>Authorization by Domain Name Registrant</b>
4.1	<p>The CA maintains controls and procedures to provide reasonable assurance that as of the date the Certificate was issued, the CA obtains confirmation in accordance with the SSL Baseline Requirements Section 11.1 related to the Fully-Qualified Domain Name(s) and IP address(es) listed in the Certificate.  (SSL Baseline Requirements Section 11.1)</p>

Ref #	SSL Baseline Requirements Audit Criteria
	<b>Verification of Subject Identity Information</b>
4.2	<p>The CA maintains controls and procedures to provide reasonable assurance that the following information provided by the Applicant is verified directly by performing the steps established by the SSL Baseline Requirements Section 11.2:</p> <ul style="list-style-type: none"> <li>• Identity (SSL Baseline Requirements Section 11.2.1)</li> <li>• DBA/Tradename (SSL Baseline Requirements Section 11.2.2)</li> <li>• Authenticity of Certificate Request (SSL Baseline Requirements Section 11.2.3)</li> <li>• Verification of Individual Applicant (SSL Baseline Requirements Section 11.2.4)</li> <li>• Verification of Country (SSL Baseline Requirements Section 11.2.5)</li> </ul>
4.3	<p>The CA maintains controls and procedures to provide reasonable assurance that it inspects any document relied upon for identity confirmation for alteration or falsification. (See SSL Baseline Requirements Section 11.2)</p>
4.4	<p>The CA maintains controls and procedures to provide reasonable assurance that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then the CA shall not accept any certificate requests that are outside this specification. The CA shall provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request. (See SSL Baseline Requirements Section 11.2.3)</p>
4.5	<p>The CA maintains controls and procedures to provide reasonable assurance that it screens proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located, when the subjectcountryName field is present. (See SSL Baseline Requirements Section 11.2.5)</p>
4.6	<p>The CA maintains controls and procedures to provide reasonable assurance that the CA does not use any data or document from a source specified under Section 11 of SSL Baseline Requirements to validate a certificate request if the data or document was obtained more than thirty-nine (39) months prior to issuing the Certificate (See SSL Baseline Requirements Section 11.3)</p>
4.7	<p>The CA maintains controls and procedures to provide reasonable assurance that the CA uses an internal database of all previously revoked Certificates and previously rejected certificate requests to identify subsequent suspicious certificate requests. (See SSL Baseline Requirements Section 11.4)</p>
4.8	<p>The CA maintains controls and procedures to provide reasonable assurance that the CA identifies high risk certificate requests, and conduct additional verification activity in accordance with the SSL Baseline Requirements. (See SSL Baseline Requirements Section 11.5)</p>
4.9	<p>The CA maintains controls and procedures to provide reasonable assurance that, prior to using a data source, the CA evaluates the data source's accuracy and reliability in accordance with the requirements set forth in section 11.6 of the SSL Baseline Requirements.</p>
	<b>Certificate Issuance by a Root CA</b>
4.10	<p>The CA maintains controls to provide reasonable assurance that Certificate issuance by the Root CA shall require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation. (See Baseline Requirements Section 12)</p>

Ref #	SSL Baseline Requirements Audit Criteria
4.11	The CA maintains controls to provide reasonable assurance that Root CA Private Keys must not be used to sign Certificates except as permitted by the Baseline Requirements. (See SSL Baseline Requirements Section 12)
<b>5</b>	<b>CERTIFICATE REVOCATION AND STATUS CHECKING</b>
5.1	The CA maintains controls to provide reasonable assurance that a process is available 24x7 that the CA is able to accept and respond to revocation request and related inquiries. (See Baseline Requirements Section 13.1.1)
5.2	<p>The CA maintains controls to provide reasonable assurance that it:</p> <ul style="list-style-type: none"> <li>• has the capability to accept and acknowledge Certificate Problem Reports on a 24x7 basis;</li> <li>• identifies high priority Certificate Problem Reports;</li> <li>• begin investigation of Certificate Problem Reports within 24 hours;</li> <li>• decides whether revocation or other appropriate action is warranted; and</li> <li>• where appropriate, forwards such complaints to law enforcement.</li> </ul> <p>(See Baseline Requirements Section 13.1.2, 13.1.3 and 13.1.4)</p>

Ref #	SSL Baseline Requirements Audit Criteria
5.3	<p>The CA maintains controls to provide reasonable assurance that Certificates are revoked within 24 hours if any of the following events occurs:</p> <ul style="list-style-type: none"> <li>• The Subscriber requests in writing that the CA revoke the Certificate;</li> <li>• The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;</li> <li>• The CA obtains evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has suffered a Key Compromise, or that the Certificate has otherwise been misused (also See SSL Baseline Requirements Section 13.1.5);</li> <li>• The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber or Terms of Use Agreement;</li> <li>• The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);</li> <li>• The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;</li> <li>• The CA is made aware of a material change in the information contained in the Certificate;</li> <li>• 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;</li> <li>• The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;</li> <li>• The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;</li> <li>• The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;</li> <li>• The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate;</li> <li>• Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or</li> <li>• The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).</li> </ul> <p>(See SSL Baseline Requirements Section 13.1.5)</p>
5.4	<p>The CA maintains controls to provide reasonable assurance that the CA;</p> <ul style="list-style-type: none"> <li>• makes revocation information for Subordinate Certificates and Subscriber Certificates available in accordance with the Baseline Requirements Appendix B</li> <li>• For high-traffic FQDN, distribute its OCSP responses in accordance with Baseline Requirements.</li> </ul> <p>(See SSL Baseline Requirements Section 13.2.1)</p>

Ref #	SSL Baseline Requirements Audit Criteria
5.5	<p>The CA maintains controls to provide reasonable assurance that an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA:</p> <p><b>for Subscriber Certificates</b></p> <ul style="list-style-type: none"> <li>• CRLs are updated and reissued at least every seven (7) days, and the nextUpdate field value is not more than ten (10) days, or</li> <li>• if the CA provides revocation of information via an Online Certificate Status Protocol (OCSP) service, the OCSP service is updated at least every four (4) days, and OCSP responses from this service must have a maximum expiration time of ten (10) days.</li> </ul> <p><b>for subordinate CA Certificates</b></p> <ul style="list-style-type: none"> <li>• CRLs are updated and reissued at least (i) once every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the nextUpdate field is not more than twelve (12) months; or</li> <li>• if the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, the OCSP service is updated at least every twelve (12) months, and within 24 hours after revoking the Subordinate CA Certificate.</li> </ul> <p>effective 1 January 2013, the CA makes revocation information available through the OCSP capability using the GET method for Certificates issued in accordance with these Requirements (See Baseline Requirements Section 13.2.2)</p>
5.6	<p>The CA maintains controls to provide reasonable assurance that the CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions (See SSL Baseline Requirements Section 13.2.3)</p>
5.7	<p>The CA maintains controls to provide reasonable assurance that the CA does not remove revocation entries on a CRL or CSP Response until after the Expiry Date of the revoked Certificate. (See SSL Baseline Requirements Section 13.2.4)</p>
5.8	<p>The CA maintains controls to provide reasonable assurance that OCSP responses conform to RFC2560 and/or RFC5019, and are signed either:</p> <ul style="list-style-type: none"> <li>• by the CA that issued the Certificates whose revocation status is being checked, or</li> <li>• by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked (the OCSP signing Certificate must contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC2560). (See SSL Baseline Requirements Section 13.2.5)</li> </ul>
5.9	<p>After the effective date set by the CA/B Forum guidelines, the CA maintains controls to provide reasonable assurance that OCSP responses do not respond with a “good” status for Certificates that have not been issued. (See SSL Baseline Requirements Section 13.2.6)</p>
<b>6</b>	<b>EMPLOYEE AND THIRD PARTIES</b>
6.1	<p>The CA maintains controls to verify the identity and trustworthiness of an employee, agent, or independent contractor prior to engagement of such persons in the Certificate Management Process. (See SSL Baseline Requirements Section 14.1.1)</p>

Ref #	SSL Baseline Requirements Audit Criteria
6.2	<p>The CA maintains controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"> <li>the CA provides all personnel performing information verification duties (Validation Specialists) with skills-training that covers basic Public Key Infrastructure (PKI) knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements.</li> <li>the CA maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.</li> <li>Validation Specialists engaged in Certificate issuance maintains skill levels consistent with the CA's training and performance programs.</li> <li>the CA documents each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.</li> <li>the CA requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the Baseline Requirements. (See SSL Baseline Requirements Section 14.1.2)</li> </ul>
6.3	<p>The CA maintains controls to provide reasonable assurance that before the CA authorizes a Delegated Third Party to perform a delegated function, the CA contractually require the Delegated party to:</p> <ul style="list-style-type: none"> <li>meet the qualification requirements of the Baseline Requirements Section 14.1, when applicable to the delegated function;</li> <li>retain documentation in accordance with the Baseline Requirements Section 15.3.2;</li> <li>abide by the other provisions of the Baseline Requirements that are applicable to the delegated function; and</li> <li>comply with (a) the CA's Certificate Policy/Certification Practice Statement or (b) the Delegated Third Party's practice statement that the CA has verified complies with these Requirements. (See SSL Baseline Requirements Section 14.2.1)</li> </ul>
6.4	<p>The CA maintains controls to provide reasonable assurance that the CA verifies that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 14 and the document retention and event logging requirements of Section 15. (See SSL Baseline Requirements Section 14.2.1)</p>
6.5	<p>For High Risk Certificate Requests, the CA maintains controls to provide reasonable assurance that the CA verifies that the Delegated Third Party's processes to identify and further verify High Risk Certificate Requests meets the requirements of the CA's own processes for High Risk Certificate Requests. (See SSL Baseline Requirements Section 14.2.1)</p>
6.6	<p>The CA maintains controls to provide reasonable assurance that the CA internally audits each Delegated Third Party's compliance with the Baseline Requirements on an annual basis. (See SSL Baseline Requirements Section 14.2.2)</p>
6.7	<p>The CA maintains controls to provide reasonable assurance that the CA does not accept certificate requests authorized by an Enterprise RA unless the Baseline Requirements are met, and the CA imposes these requirements on the Enterprise RA, and monitor compliance by the Enterprise RA. (See SSL Baseline Requirements Section 14.2.4)</p>



Ref #	SSL Baseline Requirements Audit Criteria
<b>7</b>	<b>DATA RECORDS</b>
7.1	The CA maintains controls to provide reasonable assurance that the CA records details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. (See SSL Baseline Requirements Section 15.1)
7.2	<p>The CA maintains controls to provide reasonable assurance that the following events are recorded:</p> <p><b>CA key lifecycle management events, including:</b></p> <ul style="list-style-type: none"> <li>• key generation, backup, storage, recovery, archival, and destruction</li> <li>• cryptographic device lifecycle management events.</li> </ul> <p><b>CA and Subscriber Certificate lifecycle management events, including:</b></p> <ul style="list-style-type: none"> <li>• Certificate Requests, renewal and re-key requests, and revocation</li> <li>• all verification activities stipulated in the Baseline Requirements and the CA's Certification Practice Statement</li> <li>• date, time, phone number used, persons spoken to, and end results of verification telephone calls</li> <li>• acceptance and rejection of certificate requests</li> <li>• issuance of Certificates</li> <li>• generation of Certificate Revocation Lists (CRLs) and OCSP entries.</li> </ul> <p><b>security events, including:</b></p> <ul style="list-style-type: none"> <li>• successful and unsuccessful PKI system access attempts</li> <li>• PKI and security system actions performed</li> <li>• security profile changes</li> <li>• system crashes, hardware failures, and other anomalies</li> <li>• firewall and router activities</li> <li>• entries to and exits from CA facility.</li> </ul> <p><b>Log entries must include the following elements:</b></p> <ul style="list-style-type: none"> <li>• Date and time of entry</li> <li>• Identity of the person making the journal entry</li> <li>• Description of entry</li> </ul> <p>(See SSL Baseline Requirements Section 15.2)</p>
7.3	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. (See SSL Baseline Requirements Section 15.3.1)
7.4	The CA has a policy and maintains controls to provide reasonable assurance that all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, is retained for at least seven years after any Certificate based on that documentation ceases to be valid. (See SSL Baseline Requirements Section 15.3.2)



Ref #	SSL Baseline Requirements Audit Criteria
8	<b>AUDIT</b>
8.1	<p>The CA maintains controls to provide reasonable assurance that prior to certificate issuance if the CA uses a non-Enterprise RA Designated Third Party the following requirements are followed:</p> <p><b>if the Designated Third Party is not currently audited</b></p> <ul style="list-style-type: none"> <li>the CA uses an out-of-band mechanism involving at least one human who is acting on either on behalf of the CA or on behalf of the Delegated Third Party to confirm the authenticity of the certificate request or the information supporting the certificate request, or</li> <li>the CA performs the domain control validation process itself. (See SSL Baseline Requirements Section 17.5 but note that the second bullet is not being considered for audit)</li> </ul>
8.2	<p>The CA maintains controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"> <li>it performs ongoing self assessments on at least a quarterly basis against a randomly selected sample of at least three percent (3%) of the Certificates issued during the period commencing immediately after the previous self assessment samples was taken,</li> <li>Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in the Baseline Requirements, the CA performs ongoing quarterly assessments against a randomly selected sample of at least three percent (3%) of the Certificates verified by the Delegated Third Party in the period beginning immediately after the last samples was taken</li> <li>The CA reviews each Delegated Third Party's practices and procedures to assess that the Delegated Third Party is in compliance with these Requirements and the relevant Certificate Policy and/or Certification Practice Statement. (See SSL Baseline Requirements Section 17.8)</li> </ul>
8.3	<p>The CA maintains controls to provide reasonable assurance that it complies with:</p> <ul style="list-style-type: none"> <li>laws applicable to its business and the certificates it issues in each jurisdiction where it operates, and</li> <li>licensing requirements in each jurisdiction where it issues SSL certificates. (See SSL Baseline Requirements Section 8.1)</li> </ul>

Ref #	SSL Baseline Requirements Audit Criteria
	<p><b>Principle 3: CA Environmental Security</b> - The Certification Authority maintains effective controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"> <li>• Logical and physical access to CA systems and data is restricted to authorized individuals;</li> <li>• The continuity of key and certificate management operations is maintained; and</li> <li>• CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity.</li> </ul>
1	<p>The CA develops, implement, and maintain a comprehensive security program designed to:</p> <ul style="list-style-type: none"> <li>• protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;</li> <li>• protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;</li> <li>• protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;</li> <li>• protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and</li> <li>• comply with all other security requirements applicable to the CA by law. (See SSL Baseline Requirements Section 16.1)</li> </ul>
2	<p>The CA performs a risk assessment at least annually that:</p> <ul style="list-style-type: none"> <li>• Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;</li> <li>• Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats. (See SSL Baseline Requirements Section 16.2)</li> </ul>
3	<p>The CA develops, implement, and maintain a Security Plan consisting of security procedures, measures, and products designed to reasonably manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan:</p> <ul style="list-style-type: none"> <li>• includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes.</li> <li>• takes into account then-available technology and the cost of implementing the specific measures, and</li> <li>• is designed to implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected. (See SSL Baseline Requirements Section 16.3)</li> </ul>

Ref #	SSL Baseline Requirements Audit Criteria
4	<p>The CA develops, implement, and maintain a Business Continuity Plan that includes at a minimum:</p> <ul style="list-style-type: none"> <li>• the conditions for activating the plan;</li> <li>• emergency procedures;</li> <li>• fallback procedures;</li> <li>• resumption procedures;</li> <li>• a maintenance schedule for the plan;</li> <li>• awareness and education requirements;</li> <li>• the responsibilities of the individuals;</li> <li>• recovery time objective (RTO);</li> <li>• regular testing of contingency plans;</li> <li>• the CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes;</li> <li>• a requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;</li> <li>• what constitutes an acceptable system outage and recovery time;</li> <li>• how frequently backup copies of essential business information and software are taken;</li> <li>• the distance of recovery facilities to the CA's main site; and</li> <li>• procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.</li> </ul> <p>The Business Continuity Plan is tested at least annually, reviewed, and updated. (See SSL Baseline Requirements Section 16.4) (For organizations that are undergoing a WebTrust for CA's examination, all of the above are required and already tested with the exception of the disclosure of the distance of recovery facilities to the CA's main site.)</p>
5	<p>The Certificate Management Process includes:</p> <ul style="list-style-type: none"> <li>• physical security and environmental controls (see WTCA 2.0* Section 3.4);</li> <li>• system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention (see WTCA 2.0 Section 3.7);</li> <li>• network security and firewall management, including port restrictions and IP address filtering (see WTCA 2.0 Section 3.6);</li> <li>• user management, separate trusted-role assignments, education, awareness, and training (see WTCA 2.0 Section 3.3); and</li> <li>• logical access controls, activity logging, and inactivity time-outs to provide individual accountability (see WTCA 2.0 Section 3.6).</li> </ul> <p>The CA implements multi-factor authentication for all user accounts capable of directly causing certificate issuance. (See SSL Baseline Requirements Section 16.5)</p>

Ref #	SSL Baseline Requirements Audit Criteria
6	<p>The CA maintains controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"> <li>• physical access to CA facilities and equipment is limited to authorized individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control;</li> <li>• CA facilities and equipment are protected from environmental hazards;</li> <li>• loss, damage or compromise of assets and interruption to business activities are prevented; and</li> <li>• compromise of information and information processing facilities is prevented.</li> </ul> <p>(WTCA 2.0 Section 3.4 in support of Section 16.5 of the SSL Baseline Requirements)</p>
7	<p>The CA maintains controls to provide reasonable assurance that CA systems development and maintenance activities are documented, tested, authorized, and properly implemented to maintain CA system integrity.</p> <p>(WTCA 2.0 Section 3.7 in support of Section 16.5 of the SSL Baseline Requirements)</p>
8	<p>The CA maintains controls to provide reasonable assurance that CA system access is limited to authorized individuals. Such controls provide reasonable assurance that:</p> <ul style="list-style-type: none"> <li>• operating system and database access is limited to authorized individuals with predetermined task privileges;</li> <li>• access to network segments housing CA systems is limited to authorized individuals, applications and services; and</li> <li>• CA application use is limited to authorized individuals.</li> </ul> <p>Such controls must include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• network security and firewall management, including port restrictions and IP address filtering;</li> <li>• logical access controls, activity logging (WTCA 2.0 Section 3.10), and inactivity time-outs to provide individual accountability.</li> </ul> <p>(WTCA 2.0 Section 3.6 in support of Section 16.5 of the SSL Baseline Requirements)</p>
9	<p>The CA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.</p> <p>(WTCA 2.0 Section 3.3 in support of Section 16.5 of the SSL Baseline Requirements)</p>
10	<p>The CA maintains controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"> <li>• significant CA environmental, key management, and certificate management events are accurately and appropriately logged;</li> <li>• the confidentiality and integrity of current and archived audit logs are maintained;</li> <li>• audit logs are completely and confidentially archived in accordance with disclosed business practices; and</li> <li>• audit logs are reviewed periodically by authorized personnel.</li> </ul> <p>(WTCA 2.0 Section 3.10 in support of Section 16.5 of the SSL Baseline Requirements)</p>

Ref #	SSL Baseline Requirements Audit Criteria
11	<p>The CA maintains controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"> <li>private keys are protected in a system or device that has been validated as meeting at least FIPS 140[-2] level 3 or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats;</li> <li>private keys outside the validated system or device specified above are protected with physical security, encryption, or a combination of both in a manner that prevents disclosure of the private keys;</li> <li>private keys are encrypted with an algorithm and key-length that meets current strength requirements (2048 bit minimum);</li> <li>private keys are backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment; and</li> <li>physical and logical safeguards to prevent unauthorized certificate issuance. (See SSL Baseline Requirements Section 16.6)</li> </ul>

The table below is a summary of OATI's compliance or applicability with the requirements noted above:

Requirement	In Place	N/A	Notes
<b>Principle 1</b>			
1	X		
2	X		
3	X		
4	X		
5	X		
<b>Principle 2</b>			
1.1	X		
2.1	X		
2.2	X		
2.3	X		
2.4	X		
2.5	X		
3.1	X		
3.2	X		
3.3		X	[A]
3.4	X		
4.1	X		
4.2	X		
4.3	X		
4.4	X		
4.5		X	[B]

Requirement	In Place	N/A	Notes
4.6	X		
4.7	X		
4.8	X		
4.9	X		
4.10	X		
4.11	X		
5.1	X		
5.2	X		
5.3	X		
5.4	X		
5.5	X		
5.6	X		
5.7	X		
5.8	X		
5.9	X		
6.1	X		
6.2	X		
6.3		X	[C]
6.4		X	[C]
6.5		X	[C]
6.6		X	[C]
6.7	X		

Requirement	In Place	N/A	Notes
<b>Principle 2 (cont)</b>			
7.1	X		
7.2	X		
7.3	X		
7.4	X		
8.1		X	[C]
8.2	X		
8.3	X		
<b>Principle 3</b>			
1	X		
2	X		

Requirement	In Place	N/A	Notes
3	X		
4	X		
5	X		
6	X		
7	X		
8	X		
9	X		
10	X		
11	X		

**Note [A]:** OATI does not provide subscriber private key generation services.

**Note [B]:** OATI does not allow Server certificates to be issued to IP addresses, only to FQDN's, and in no way relies on IP addresses as part of any verification or certificate issuance process.

**Note [C]:** OATI does not use Delegated Third Parties or delegate the performance or verification of all, or any part, of Section 11 of the SSL Baseline Requirements to a Delegated Third Party.