AUDITOR LETTER OF COMPLIANCE

Compliance Audit Requirements

October 2, 2008

In order to evaluate a compliance audit, the following background information is required.

- Identity of the Auditor and the individuals performing the audit;
- Competence of the Auditor to perform audits;
- Experience of the individuals performing the audit in auditing PKI systems;
- Relationship of the Auditor to the entity that owns the PKI being audited. This relationship must clearly demonstrate the independence of the auditor from the entity operating or managing the PKI.

The following information regarding the audit itself is required.

- The date the audit was performed.
- Whether a particular methodology was used, and if so, what methodology.
- Which documents were reviewed as a part of the audit, including document dates and version numbers.

In addition to this background, the entity should ensure that, as part of the audit, an audit summary is prepared, signed by the auditor, reporting on the following elements after conducting the compliance audit:

- State that the operations of the entity PKI's Principal CA were evaluated for conformance to the requirements of its CPS.
- Report the findings of the evaluation of operational conformance to the Principal CA CPS.
- State that the entity PKI's Principal CA CPS was evaluated for conformance to the entity PKI's CP.

- Report the findings of the evaluation of the Principal CA CPS conformance to the entity PKI CP.
- For PKIs with multiple CAs, state whether audit reports showing compliance were on file for any additional CA components of the entity PKI
- State that the operations of the Entity PKI's Principal CA were evaluated for conformance to the requirements of all current cross-certification MOAs executed by the Entity PKI with other entities.
- Report the findings of the evaluation of the Principal CA CPS conformance to the requirements of all current cross-certification MOAs executed by the Entity PKI.

As the FBCA CP is neutral as to audit methodology, and does not prefer one methodology over another, any audit approach is acceptable to it provided that these points are addressed.

Audit methodologies that focus on validating specific management assertions (such as WebTrust for Certification Authorities) should include the substance of the following in the management assertions:

1. The Entity-CPS conforms to the requirements of the Entity-CP
2. The Entity-CA is operated in conformance with the requirements of the Entity-CPS;
3. The Entity-CA has maintained effective controls to provide reasonable assurance that:
    - Procedures defined in Section 1 (Introduction) of the Entity-CPS are in place and operational.
    - Procedures defined in Section 2 (Publication and Repository Responsibilities) of the Entity-CPS are in place and operational.
    - Procedures defined in Section 3 (Identification and Authentication) of the Entity-CPS are in place and operational.

- Procedures defined in Section 4 (Certificate Life Cycle) of the Entity-CPS are in place and operational.
- Procedures defined in Section 5 (Facility Management and Operations Controls) of the Entity-CPS are in place and operational.
- Procedures defined in Section 6 (Technical Security Controls) of the Entity-CPS are in place and operational.
- Procedures defined in Section 7 (Certificate, CARL/CRL and OCSP Profiles Format) of the Entity-CPS are in place and operational.
- Procedures defined in Section 8 (Compliance Audit and other Assessments) of the Entity-CPS are in place and operational.
- Procedures defined in Section 9 subsections 9.4.4 (Privacy of Personal Information – Responsibility to Protect Private Information) and 9.6.3 (Representations and Warranties – Subscriber Representations and Warranties) are in place and operational.

4. The Entity-CA is operated in conformance with the requirements of all current cross-certification MOAs executed by the Entity-CA.

Note: *The FBCA does not require and will not consider any statements with respect to the entity PKI's suitability for cross certification with the FBCA or conformance to the FBCA certificate policies. Such a determination is exclusively the purview of the FPKIPA and its working groups.*