# AUDITOR LETTER OF COMPLIANCE

## Compliance Audit Requirements

## October 28, 2009

**These requirements apply to all cross-certified entities under the FBCA CP or through the Common Policy (other than the C4CA).**

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 cross-certification MOAs executed by the Entity PKI with other entities. If there are no MOAs or other comparable agreements, this requirement does not apply.
- Report the findings of the evaluation of the Principal CA CPS conformance to the requirements of all cross-certification MOAs executed by the Entity PKI. If there are no MOAs or other comparable agreements, this requirement does not apply.

**Auditing New CAs**

Where the Entity PKI being audited is new and some procedures have only been performed in test environments, the report must include the following:

1. State which procedures have been performed using the operational system and could be fully evaluated for conformance to the requirements of the entity PKI CPS;
2. Report the findings of the evaluation in "1." above;
3. State which procedures have not been performed on the operational system and were evaluated for conformance to the requirements of the entity PKI CPS, but only with respect to training and procedures;
4. Report the findings of the evaluation in "3." above;
5. State that the entity PKI's CPS was evaluated for conformance to the supported certificate policies;
6. Report the findings of the evaluation in "5." above.

**Note:** These requirements are separate and distinct from the certification and accreditation requirements imposed by the Designated Approving Authority (DAA).

Since the FBCA/Common Policy CPs are neutral as to audit methodology, and do not prefer one methodology over another, any audit approach is acceptable provided that these points are addressed.

At the present time, a default WebTrust for CA audit will not satisfy the requirements set forth above. To meet FBCA/Common Policy requirements, the

management assertions of the entity being audited would need to include the substance of the following 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 of the Entity-CPS are in place and operational.
    - Procedures defined in Section 2 of the Entity-CPS are in place and operational.
    - Procedures defined in Section 3 of the Entity-CPS are in place and operational.
    - Procedures defined in Section 4 of the Entity-CPS are in place and operational.
    - Procedures defined in Section 5 of the Entity-CPS are in place and operational.
    - Procedures defined in Section 6 of the Entity-CPS are in place and operational.
    - Procedures defined in Section 7 of the Entity-CPS are in place and operational.
    - Procedures defined in Section 8 of the Entity-CPS are in place and operational.
    - Procedures defined in Section 9 subsections 9.4.4 and 9.6.3 are in place and operational.
4. The Entity-CA is operated in conformance with the requirements of all cross-certification MOAs executed by the Entity-CA. If there are no MOAs or other comparable agreements, this requirement does not apply.

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