August 23, 2016

Darlene Gore
FPKI Management Authority Program Manager

Dear Darlene,

As requested, I've reviewed the recent FPKI audit ("Equivalent Audit") against the Microsoft Government CA Requirements and provide the additional information as requested by the Microsoft Trust Store Program.

Microsoft Requirement	Government Response
1. Attests that the audit is issued by an independent agency which is authorized by the Government CA's government to conduct the audit;	FPKI Auditor, James Jung of the Slandala Company, met the government requirements for competence, experience, and independence.
2. Lists the Government CA's government's criteria for auditor qualification, and certifies that the auditor meets this criteria;	The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CA's CP and CPS. The compliance auditor must perform such compliance audits as a regular ongoing business activity. In addition to the previous requirements, the auditor must be a certified information system auditor (CISA) or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices. The compliance auditor either shall be a private firm that is independent from the entities (CA and RAs) being audited, or it shall be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. An example of the latter situation may be an Agency inspector general. To insure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's CA Facility or certificate practices statement. The FPKIPA shall determine whether a compliance auditor meets this requirement.

3. Lists the particular statutes, rules, and/or regulations that the auditor assessed the Government CA's operations against;	See pages 2 – 3 of the Compliance Letter. The FPKI Audit Requirements are documented here: https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt0000000Sfx1
4. Certifies the Government CA's compliance with the requirements outlined in the named governing statutes, rules, and/or regulations;	The operations of the entity PKI Principal CA were evaluated for conformance to the requirements of the CPS and met the requirements.
5. Provides information that describes how the statute's requirements are equivalent to the appropriate WebTrust or ETSI audit(s) ;	Federal PKI audits are conducted against an entity's CP and CPS. The CP is in RFC 3647 format and has been evaluated to meet the requirements of the Federal Bridge CA CP. The audit tests all aspects of operation against all of the requirements of the CP and CPS, exceeding the requirements of a WebTrust of ETSI audit.
6. Lists Certificate Authorities and third parties authorized by the Government CA to issue certificates on the Government CA's behalf within a certificate chain;	Trust Anchor - Federal Common Policy CA Third Party CA – Betrusted Production SSP CA, Executive Office of the President CA-B8, GOVT-SSP-CA-B6, Veterans Affairs Device CA B2, Veterans Affairs User CA B1, Entrust Managed Services Root CA, DOE SSP CA, Entrust Managed Services SSP CA, HHS-FPKI-Intermediate-CA-E1, ORC SSP 3, ORC SSP 4, Symantec SSP Intermediate CA-G4, NRC SSP Agency CA G3, NRC SSP Device CA G3, U.S. Department of Transportation Agency CA G4, U.S. Department of Transportation Device CA G4, U.S. Department of State AD Root CA, U.S. Department of State AD High Assurance CA, U.S. Department of State AD Root CA, U.S. Department of State PIV CA, U.S. Treasury Root CA, Department of Veterans Affairs CA, DHS CA4, NASA Operational CA, Social Security Administration Certification Authority, US Treasury Fiscal Service, US Treasury OCIO CA, US Treasury Public CA, VeriSign SSP intermediate CA-G3, FDIC Agency CA, FDIC Device CA, Naval Reactors SSP Agency CA G2, Naval Reactors SSP Device CA G2, NRC SSP Agency CA G2, NRC SSP Device CA G2, RRB Device CA, U.S. Department of Education Agency CA – G3, U.S. Department of Education Device CA – G3, U.S. Department of Transportation SSP Agency CA G3, U.S. Department of Transportation SSP Device CA G3
7. Documents the full PKI hierarchy; and	See Attached Spreadsheet

8. Provides the start and end date of the audit period.	*May 2015 – June 2016*

Digitally signed by JOHN CORNELL
Date: 2016.09.27 18:59:06 -04'00'

John E Cornell
Senior Assistant General Counsel
Personal Property Division