The Slandala Company
203 North Lee Street
Falls Church, Virginia 22046

26 November 2025

Jim Trovato
Entrust Managed Services Policy Authority Chair
Director, Product Compliance
Entrust Datacard
1187 Park Place
Shakopee, Minnesota 55379

The Slandala Company conducted a compliance audit of the Entrust Federal Certification Authorities. The audit was conducted to verify that the system was being operated in accordance with the security practices and procedures described by the following Practices and Policies:

- The Combined X.509 Certification Practices Statement for the Entrust PKI SSP (ETPKISPP) Federal Root Certification Authority & Federal Shared Service Provider Certification Authority, Version 3.2.1, 17 November 2025
- X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.12, August 4, 2025
- Entrust Managed Services Non-Federal Public Key InfrastructureX.509 Certification Practice Statement, Version 2.2, 12 November 2025
- Entrust Managed Services Non-Federal Public Key Infrastructure X.509 Certificate Policy, Version 2.2, 18 November 2025

Entrust operates the following Federal Certification Authorities (CAs):

- OU = Entrust Managed Services Root CA
- OU = Entrust Managed Services SSP CA
- CN = HHS-FPKI-Intermediate-CA-E1
- CN = DoE SSP CA
- CN = Entrust Derived Credential SSP CA
- OU = Entrust Managed Services NFI Root CA
- OU = Entrust NFI Medium Assurance SSP CA

The DoE SSP CA was decommissioned during the audit period.

The compliance audit evaluated the Certificate Authority, repositories, certificate status servers and ancillaries associated with these CAs. Registration authority functions are not performed by Entrust and were not included in the audit. Card Management Systems (CMS) operated by SSP or other clients are also beyond the scope of this audit. As part of the audit, the Memorandum of Agreement between the United States Federal Public Key Infrastructure (PKI) Policy Authority (Federal PKI Policy Authority) and Entrust Inc., signed in April 2020 were reviewed. Entrust is operating in accordance with these MOAs.

The compliance audit was performed via interviews, documentation reviews and site visits performed during October 2025. This audit covers the following period.

- Audit Period Start: January 15, 2024
- Audit Period Finish: 1 October 2025

Findings from the previous year were reviewed and have been corrected.

The system operates with a primary site in Dallas, Texas and a secondary site in Colorado.

The compliance audit was performed using a requirements decomposition methodology and was initiated by first performing a direct CP-to-CPS traceability analysis. CPS practices found to not comply with or address the requirements of the applicable policies are categorized as Disparate.

- Disparity – CPS practices found to not comply or address the requirements of the applicable policies.

The CPS was then reviewed and decomposed into requirements, and the requirements were then evaluated to determine the general methodology for their evaluation and the activities that should be taken by the auditor to fulfill the audit of that requirement. Findings and data are recorded during these activities, and are categorized as follows:

- Complies – operations comply with the practices documented in the CPS,
- Discrepancy – operations do not comply with the practices documented in the CPS,
- Recommendation - operations comply with the practices documented in the CPS; however, improvements to the implementation could be considered.

The audit was performed by Mr. James Jung of The Slandala Company, who acted as the lead auditor. Mr. Jung has performed audits of PKI systems since 2001 and has over 39 years' experience in the design, implementation and certification of information assurance systems. He is certified by the International Information Systems Security Certification Consortium (ISC)² as a Certified Information Systems Security Professional (CISSP) and is certified by the Information Systems Audit and Control Association (ISACA) as Certified Information Systems Auditor (CISA).

Mr. Jung has not held an operational role or a trusted role on the Entrust Federal CA systems, nor has he had any responsibility for writing the Certificate Practices Statements. The Slandala Company and Mr. Jung are independent of Entrust and its operations and management.

Information from the following documents was used as part of the compliance audit.

- The Combined X.509 Certification Practices Statement for the Entrust PKI SSP (ETPKISPP) Federal Root Certification Authority & Federal Shared Service Provider Certification Authority, Version 3.2.1, 17 November 2025
- X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.12, August 4, 2025
- Entrust Managed Services Non-Federal Public Key InfrastructureX.509 Certification Practice Statement, Version 2.2, 12 November 2025
- Entrust Managed Services Non-Federal Public Key Infrastructure X.509 Certificate Policy, Version 2.2, 18 November 2025
- DRAFT Entrust PKI Shared Service Provider Registration Practices Statement Template Version 1.0-rc1, 20 August, 2025
- Memorandum of Agreement between the United States Federal Public Key Infrastructure Policy Authority and Entrust, Inc. [Non-Federal Identity], May 2023
- Memorandum of Agreement between the United States Federal Public Key Infrastructure Policy Authority and Entrust, Inc. [Entrust Federal Shared Service Provider], May 2023
- Entrust Federal Managed PKI Information System Contingency Plan Test Plan
- Employment Screening Package
- SIR01-Security Incident Response Plan Overview v7.1 2021Security Incident Response Plan
- Memorandum: 23 October 2025, Reference: Appointment of EMS PKI Federal CA Trusted Personnel
- Entrust DataCard US Cloud Services OS & Application Patching Process.
- US Federal Managed PKI (MPKI) Disaster Recovery Plan - Appendix E
- Entrust Federal Managed PKI Information System Contingency Plan Test Plan, July 6, 2022
- FedSSP CRLs Service Availability Report from 2024-01-01 00:00:00 to 2025-01-01 00:00:00
- Sample Trusted Role Training (Jason McKenzie )
- Registration Authority (RA) & Local Registration Authority (LRA) Guidelines, October 28, 2020
- Sample Entrust - DFW / DEN Trusted Role Responsibility Form
- Sample U.S. General Services Administration HSPD-12 Managed Service Office (MSO) Third-party Key Recovery Request Form
- Incident Report Incident Index: 2025-MPKI-001
- Sample Dallas Datacenter Cage Access List
- Sample GSA-MSO 3rd-party Key Recovery Request Form
- Sample Entrust - DFW / DEN Trusted Role Responsibility Form
- Sample Entrust Managed Services Subscriber Agreement

A direct CP-to-CPS traceability analysis evaluated "*The Combined X.509 Certification Practices Statement for the Entrust Managed Service PKI Federal Root Certification Authority & Federal Shared Service Provider Certification Authority"* for compliance with the "*X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework."* One 1 disparate item was identified.

A direct CP-to-CPS traceability analysis evaluated the "*Entrust Managed Services Non-Federal Public Key Infrastructure X.509 Certification Practice Statement"* for compliance with the "*Entrust Managed Services Non-Federal Public Key Infrastructure X.509 Certificate Policy."* One disparate item was identified .

The practices of the Entrust Managed Services CAs were evaluated for compliance with the following certification practice statements:

- *The Combined X.509 Certification Practices Statement for the Entrust Managed Service PKI Federal Root Certification Authority & Federal Shared Service Provider Certification Authority*
- *X.509 Certification Practices Statement for Entrust Managed Service PKI Derived PIV Credential Federal Shared Service Provider Certification Authorities*

Four issues in operational compliance were identified. One issue was corrected during the audit.

The practices of the Entrust Managed Services NFI CAs were evaluated for compliance with the following certification practice statements:

- *Entrust Managed Services Non-Federal Public Key InfrastructureX.509 Certification Practice Statement*

Three issues in operational compliance were identified. One issue was corrected during the audit.

Registration Authority practices and operations were evaluated for conformance to the applicable Practice Statements.

In this audit, the following RA sites were audited:

- CIGIE, operating under the NFI CA. Three discrepancies were identified during the audit, and three recommendations were made,
- House of Representatives, operating under the Common SSP CA. Four discrepancies were identified during the audit and three recommendations were made,
- Idaho National Labs (DOE INL), operating under the Common Derived CA. No discrepancies were identified,
- MITRE, operating under the NFI CA. Three discrepancies were identified during the audit and three recommendations were made,
- USAID, operating under the NFI CA. One discrepancy was identified during the audit
- The Department of Energy (DoE) PKI was decommissioned and the audit focused on archiving and termination procedures. No discrepancies were identified.

No failures were found that suggested that the system had been operated in an overtly insecure manner and it is the lead auditor's opinion that the Entrust PKI provided reasonable security control practices and has maintained effective controls providing reasonable assurance that the practices defined in the applicable certification practice statements are in place and operational. Discrepancies with the stated CPS practices are identified in the report.

11/26/2025

X James Walker Jung DIGITALLY SIGNED The Slandala Company

James Junq
Lead Auditor
Signed by: Slandala

James Walker Jung DIGITALLY SIGNED The Slandala Company

2025.11.26 16:13:04 -05'00'