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

28 February 2024

Mark Ruchie
Chief Information Security Officer
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 Managed Service PKI Federal Root Certification Authority & Federal Shared Service Provider Certification Authority, Version 3.1
- X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.5
- Entrust Managed Services Non-Federal Public Key InfrastructureX.509 Certification Practice Statement, Version 2.1
- Entrust Managed Services Non-Federal Public Key Infrastructure X.509 Certificate Policy, Version 2.1
- X.509 Certification Practices Statement for Entrust Managed Service PKI Derived PIV Credential Federal Shared Service Provider Certification Authorities, 15 November, 2017, Version 1.1
- Delta Certification Practices Statement for the Entrust Managed Service PKI Department of Energy Shared Service Provider Certification Authority, 4 May, 2012, Version 1.5
- Delta Certification Practices Statement for the Entrust Managed Service PKI Department of Health and Human Services Certification Authority, 13 May, 2013, Version 0.3

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 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 during January 2024. This audit covers the following period.

- Audit Period Start: December 15, 2022
- Audit Period Finish: January 15, 2024

Findings from the previous year were reviewed. Findings related to updating CPs and other posted materials, CRL reasons, audit configuration, physical log management had not been addressed.

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.

- Disparate – 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 Managed Service PKI Federal Root Certification Authority & Federal Shared Service Provider Certification Authority, Version 3.1

- X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.5
- Entrust Managed Services Non-Federal Public Key InfrastructureX.509 Certification Practice Statement, Version 2.1
- 
- Entrust Managed Services Non-Federal Public Key Infrastructure X.509 Certificate Policy, Version 2.1
- X.509 Certification Practices Statement for Entrust Managed Service PKI Derived PIV Credential Federal Shared Service Provider Certification Authorities, 15 November, 2017, Version 1.1
- Delta Certification Practices Statement for the Entrust Managed Service PKI Department of Energy Shared Service Provider Certification Authority, 4 May, 2012, Version 1.5
- Delta Certification Practices Statement for the Entrust Managed Service PKI Department of Health and Human Services Certification Authority, 13 May, 2013, Version 0.3
- Memorandum of Agreement between the United States Federal Public Key Infrastructure Policy Authority and. Entrust Corporation [Non-Federal Identity], May 2024
- Council of the Inspectors General on Integrity and Efficiency (CIGIE) Registration Authority (RA) Auditor Letter of Compliance 2023
- Certificate Request Form – Federal Common Policy Certification Authority (FCPCA) 6/5/2023
- Configuration Management Plan (Version 9.0) Entrust Managed Services Public Key Infrastructure (EMS PKI) July 17, 2023Z
- Entrust Security Incident Response Plan, Published Date May 10, 2023
- U.S. General Services Administration HSPD-12 Managed Service Office (MSO) Third-party Key Recovery Request Form (example)
- Decision for a Standard Assessment & Authorization for Entrust Public Key Infrastructure Shared Service Provider DATE: November 17, 2022, EXPIRATION DATE: November 16, 2025
- Entrust: Appointment of EMS PKI Federal CA Trusted Personnel, 10-January-2024
- US Federal Managed PKI (MPKI) Disaster Recovery Plan - Appendix E, Document Version 0.5, Date 06/28/2023
- United States Department of Agriculture (USDA) Derived Personal Identity Verification PKI Compliance Audit Report 2023 Date: September 28, 2023
- Entrust Federal Managed PKI Information System Contingency Plan Test Plan, June 22, 2023
- Employment Screening Package
- SIR01-Security Incident Response Plan Overview v7.1 2021Security Incident Response Plan, Published Date: 2021-05-20
- Memorandum: 10-January-2024, Reference: Appointment of EMS PKI Federal CA Trusted Personnel

It is noted that the NFI and SSP CAs are operated using primarily the same practices; consideration could be given to combining the SSP and NFI CPS. The combined CPS would need to satisfy both the NFI CP and the Common CP.

The Entrust Key Recovery Practice Statement has been incorporated into the SSP CPS. The Delta CPSs for the Derived, HHS and Energy CAs have not been updated recently.

A direct CP-to-CPS traceability analysis evaluated the following Certificate Practices Statements:

- *The Combined X.509 Certification Practices Statement for the Entrust Managed Service PKI Federal Root Certification Authority & Federal Shared Service Provider Certification Authority, Version 3.1*

for compliance with the following policy:

- *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.5*

Twenty four disparate items were identified.

A direct CP-to-CPS traceability analysis evaluated the following Certificate Practices Statements:

- *X.509 Certification Practices Statement for Entrust Managed Service PKI Derived PIV Credential Federal Shared Service Provider Certification Authorities, 15 November, 2017, Version 1.1*

for compliance with the following policy:

- *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.5*

The Derived CPS is written as a "delta" CPS indicating differences between the Managed Service CPS and the Derived CPS. Eighteen recommendations were made to the document.

A direct CP-to-CPS traceability analysis evaluated the following Certificate Practices Statements:

- *Entrust Managed Services Non -Federal Public Key Infrastructure X.509 Certification Practice Statement, Version 2.1*

for compliance with the following policy:

- *Entrust Managed Services Non-Federal Public Key Infrastructure X.509 Certificate Policy, Version 2.1*

Nine disparate items were 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*

Nineteen (19) issues in operational compliance were identified.

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*

Seventeen (17) issues in operational compliance 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.

2/28/2024

X James Walker Jung DIGITALLY SIGNED The Slandala Company

James Jung
Lead Auditor
Signed by: Jung.James.W.ORC3011047256.ID

James Walker Jung DIGITALLY SIGNED The Slandala Company

Date: 2024.02.28 20:11:33 -05'00'