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

24 September 2018

Justin Page
Senior Security Compliance Analyst
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, 9 March 2018, version 2.8.1
- X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 1.28 April 4, 2018
- Entrust Managed Services Non-Federal Public Key InfrastructureX.509 Certification Practice Statement, Version 1.7 July 20, 2018
- Entrust Managed Services Non-Federal Public Key Infrastructure X.509 Certificate Policy, Version,1.6.4, December 8, 2016
- 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

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.

The compliance audit evaluated the PKI systems and was performed via interviews, documentation reviews and site visits performed between 31 July and 8 August 2018. Audit site visits were performed at sites in Northern Virginia, and Dallas Texas. The compliance audit meets the requirements of the Federal Public Key Infrastructure (FPKI) Annual Review Requirements, Version v1.0, April 11, 2017. The audit addresses the annual period of operation from 24 August 2017 to the dates of the site visit. 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 June 2011 was reviewed. Entrust is operating in accordance with this MOA.

Results from certificate testing were not available. NFI sample certificates were submitted to GSA in November 2017. SSP sample certificates were submitted to GSA in January 2018. Registration Authority Agreements (RAAs) are being developed with the agency and client organizations. Entrust reports that the RAAs were sent to clients in mid-August and are awaiting signatures. Findings from the previous year were reviewed. Some findings from the previous year have not yet been addressed as indicated in the report.

The system operated with a primary site in Washington, DC and a secondary site in Dallas, Texas. The system has migrated and now operates with the primary site in Dallas. All CAs are now operating out of Dallas, with the exception of the HHS CA, which will migrate in the future. Washington currently acts as the secondary site, but disaster recovery functions are being migrated to Denver, Colorado. The migration to Dallas was performed as a failover (and constituted a failover test). This migration is considered a system change and was reviewed, especially with regard to updated system configurations.

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 29 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, 9 March 2018, version 2.8.1
- X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 1.28 April 4, 2018
- Entrust Managed Services Non-Federal Public Key InfrastructureX.509 Certification Practice Statement, Version 1.7 July 20, 2018

- Entrust Managed Services Non-Federal Public Key Infrastructure X.509 Certificate Policy, Version,1.6.4, December 8, 2016,
- 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
- Memorandum of Agreement between the United States Federal Public Key Infrastructure (PKI) Policy Authority (Federal PKI Policy Authority) and Entrust Inc., signed in June 2011,
- Orangetree Employment Screening Current Screening Packages
- Incident Response Plan Overview v5.2 April 2017
- Memorandum: Appointment of EMS PKI Federal CA Trusted Personnel, August 7, 2017
- Entrust Datacard US Cloud Services OS & Application Patching Process.
- 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
- System and Organization Controls 2 Type II Report, ViaWest, Inc.'s Decription of Its Colocation, Managed Service and Client Center Cloud System for the Period October 1, 2016 to September 2017
- Century Communications, LLC SOC 2 Report for Managed Network and Hosting Services a Type 2 Independent Service auditors's Report on Controls Relevant to Security, Availability and Confidentiality, October 1, 2016 to September 2017
- Report on Cyrusone, LLCs Description of its Systems and on the Suitability of the Design and Operating Effectiveness of its Controls Relevant to Security and Availability and Hitrust Control Specifications, pursuant to reporting on Service Organization Controls 2 (SOC 2) Type 2 + Hitrust examination performed under AT- 105 and AT-C 205 July 1, 2016 through June 30, 2017

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, 9 March 2018, version 2.8.1

for compliance with the following policy:

X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 1. 28 April 4, 2018

5 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 1. 28 April 4, 2018

The Derived CPS is written as a “delta” CPS indicating differences between the Managed Service CPS and the Derived CPS. No disparate items were identified.

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

Entrust Managed-Federal Public Key Infrastructure X.509 Certification Practice Statement, Version 1. 7 July 20, 2018

for compliance with the following policy:

Entrust Managed Services Non-Federal Public Key Infrastructure X.509 Certificate Policy, Version,1.6.4, December 8, 2016,

14 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, 9 March 2018, version 2.8.1

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

17 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, Version 1. 7 July 20, 2018

15 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.

9/24/2018

X 

James Jung
Lead Auditor
Signed by: Jung.James.W.ORC3010006689.ID

Jung.James.W.ORC3010006689.ID
Digitally signed by Jung.James.W.ORC3010006689.ID
Date: 2018.09.24 16:57:46 -04'00'