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

15 February 2021

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, 26 June 2019, version 2.9
- X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework Version 2.0, 1 September 2020
- Entrust Managed Services Non-Federal Public Key InfrastructureX.509 Certification Practice Statement, Version 1.8, 17 April 2020
- Entrust Managed Services Non-Federal Public Key Infrastructure X.509 Certificate Policy, Version,1.8, 17 April 2020
- 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
- Federal Public Key Infrastructure Key Recovery Policy, Version 1.0, October 6, 2017

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. 2020 FIPS 201/FICAM Testing Program Annual PIV and PIV-I Card Testing Report were reviewed. Issues identified by these reports are being reviewed by Entrust.

This audit covers the following period.

- Audit Period Start: August 15, 2019
- Audit Period Finish: October 22, 2020

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

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

The audit was performed in October of 2020, at which time precautions to protect against the Covid-19 virus were in place. The report identifies with notes where methods used to evaluate the practice were modified as part of these precautions. In general:

- Interviews were conducted remotely.
- The assessment of the physical protections was based on interviews with staff, log reviews and documentation.
- System configuration assessments were conducted using remote video or screen captures.

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.

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,
- Noted – Methods used to evaluate the practice were modified as part of the precautions to protect against the Covid-19 virus
- 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 35 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, 26 June 2019, version 2.9
- X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework Version 2.0, 1 September 2020
- Entrust Managed Services Non-Federal Public Key InfrastructureX.509 Certification Practice Statement, Version 1.8, 17 April 2020
- Entrust Managed Services Non-Federal Public Key Infrastructure X.509 Certificate Policy, Version,1.8, 17 April 2020
- 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
- Federal Public Key Infrastructure Key Recovery Policy, Version 1.0, October 6, 2017
- Memorandum of Agreement between the United States Federal Public Key Infrastructure Policy Authority and Entrust, Inc. [Non-Federal Identity], April 2020
- Memorandum of Agreement between the United States Federal Public Key Infrastructure Policy Authority and Entrust, Inc. [Entrust Federal Shared Service Provider], April 2020
- FIPS 201 / FICAM Testing Program Annual PIV-I Card Testing Report Version 1.1 Entrust Non-Federal Issuer (PKI) & GSA Managed Service Offering (Issuing Organization), April 24, 2020

- FIPS 201 / FICAM Testing Program Annual PIV Testing Report Version 1.1 Entrust Managed Services (PKI Shared Services Provider) & General Services Administration (GSA, Issuing Organization), April 16, 2020
- FIPS 201 / FICAM Testing Program Remote Annual PIV Testing Report Version 1.1 Entrust Federal Shared Service Provider (PKI Shared Service Provider) & XTec (Registration Authority) & U.S. Agency for Global Media (Issuing Organization), September 15, 2020
- Employment Screening Package
- Incident Response Plan Overview v5.2 April 2017
- Memorandum: Appointment of EMS PKI Federal CA Trusted Personnel, September 28, 2020
- Entrust DataCard US Cloud Services OS & Application Patching Process.
- Report on CyrusOne LLC's Description Of Its System And On The Suitability Of The Design And Operating Effectiveness Of Its Controls Relevant To Security And Availability; Pursuant To Reporting On Service Organization Controls 2 (SOC 2) Type 2 examination performed under AT-C 105 and AT-C 205 and ISAE 3000, July 1, 2018 through June 30 2019
- Bridge Letter for CyrusOne (Managed Services)-2019-Type 2 SOC 1 and ISAE 3402, September 30, 2019
- Report on Flexential's Description Of Its System And On The Suitability Of The Design And Operating Effectiveness Of Its Controls Relevant To Security And Availability; Pursuant To Reporting On Service Organization Controls 2 (SOC 2) Type 2 examination performed under AT-C 105 and AT-C 205 November 1, 2018 through October 31, 2019
- Flexential 2019 FISMA High Security Assessment Report (SAR) Version 1.2 Version November 8, 2019
- Flexential's SOC 2 Bridge Letter, 1 September 2020
- CyrusOne LLC 2018 FISMA High Security Assessment Report (SAR) Version 1.1, August 31, 2018
- FIPS 201 / FICAM Testing Program Annual PIV-I Card Testing Report Version 1.1 XTec, Inc. (First Data Configuration) February 19, 2019
- FIPS 201 / FICAM Testing Program Annual PIV Testing Report Version 1.1 Broadcasting Board of Governors (BBG) February 19, 2019
- Appointment of EMS PKI Federal CA Trusted Personnel, September 28, 2020 (Trusted Role List)
- Certificate Request Form – Federal Common Policy Certification Authority (FCPCA), 8 August 2019

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, 26 June 2019, version 2.9* for compliance with the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.0, 1 September 2020.* 21 disparate items were identified.

The Federal PKI Policy Authority has completed a substantial "clean-up" update of the Common Policy and is currently processing an update to incorporate the Key Recovery Policy into the Common Policy. These substantial changes are likely to be completed this year and should be considered in future CPS updates. It is noted that the incorporation of the Key Recovery Policy into the Common Policy still allows, but does not require, the Key Recovery Practice Statement to remain a separate document.

A direct CP-to-CPS traceability analysis evaluated the *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 *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.0, 1 September 2020.* 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 *Entrust Managed-Federal Public Key Infrastructure X.509 Certification Practice Statement, Version 1.8, 17 April 2020* for compliance with the *Entrust Managed Services Non-Federal Public Key Infrastructure X.509 Certificate Policy, Version, 1.8, 17 April 2020.* 14 disparate items were identified.

The Entrust "Key Recovery Practices Statement (KRPS) for the Entrust Managed Service, 20 June 2019, Version 1.1" addresses a separate key recovery system that has not been deployed. It does not address the Federal KRP. The Entrust SSP CPS and Entrust NFI CPS were reviewed against the Federal KRP. Findings from that analysis are included in their respective results.

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, 26 June 2019, version 2.9*
- *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*

Seven issues in operational compliance were identified. Five items were noted, where methods used to evaluate the practice were modified as part of the precautions to protect against the Covid-19 virus.

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 1.8, 17 April 2020*

Five issues in operational compliance were identified. Five items were noted, where methods used to evaluate the practice were modified as part of the precautions to protect against the Covid-19 virus.

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.

2/15/2021

X James Walker Jung DIGITALLY SIGNED

James Jung
Lead Auditor
Signed by: Jung.James.W.ORC3011018685.ID

Jung.James
.W.ORC301
1018685.ID

Digitally signed by
Jung.James.W.OR
C3011018685.ID
Date: 2021.02.15
15:47:23 -05'00'