November 28, 2022

To whom it may concern,

This is a letter for Entrust customers describing how the Entrust secure issuance software suite complies with Payment Card Industry – Data Security Standards (PCI-DSS).

Entrust CardWizard instant issuance software is not a payment application as defined by the PCI SSC. However, Entrust engages with a PCI Approved Scanning Vendor (ASV) on a regular basis to assess the security of our internal implementation of CardWizard and the compliance of CardWizard to PCI Standards Council (PCI SSC) Payment Application Data Security Standards (PA-DSS) requirements. We run assessments with each major new release or update.

The Entrust Software Security Assurance program is tightly integrated into our software development process. This process has defined milestones, process artifacts and checkpoints, which allow for oversight and approval from key stakeholders. program defines a structured and managed approach to ensure that our products deliver a consistent, repeatable level of security to our customers. Every release of the Entrust secure issuance software suite follows this secure development lifecycle. Software security assessment includes both penetration testing and automated scanning (DAST, SAST, and Open Source Compliance).

Entrust's software development lifecycle (SDLC) includes a robust Security Assurance process which is audited annually under PCI-CP and ISO-27001. Management of 3rd party components bundled inside Entrust software applications are an integral part of the Security Assurance process. This includes regular monitoring of all supported products for CVEs using an industry-leading Software Composition Analysis tool. Any CVEs found are either upgraded to a safe version, or manually analyzed to verify that the application is not affected by the described vulnerability in any of its supported modes of operation.

In addition to the published CVSS score of a CVE, Entrust will perform in-context analysis of the issue and assign our own risk classification. Issues are then handled as follows:

- If a specific CVE is classified as critical or high risk, Entrust will propose a workaround or software patch with a level of urgency appropriate to the details of the issue.
- We will analyze the impact to already deployed systems and publish an Entrust Security Bulletin if customers are required to take action to protect their deployments.

- If a specific CVE is classified as medium or low risk, Entrust will include a workaround or software patch to the affected component as part of a scheduled software release.

As stated above, Entrust leverages Optiv, a PCI Approved ASV to conduct penetration testing on our secure issuance software platform. The latest versions available are penetration tested annually within our financial instant issuance hosted environment as part of our ongoing PCI CP (card production) certification that is validated by Visa and MasterCard annually.

Latest Penetration Tests by ASV	
Date	**Software Version**
October 2022	CardWizard 6.5.1 Adaptive Issuance Key Manager 6.5.2 Adaptive Issuance EMV Data Prep and Perso 6.5.2 Remote Monitoring and Management 6.7.1 Adaptive Issuance™ Instant Financial Issuance 8.2.1 Adaptive Issuance™ EMV Data Prep and Perso 8.2.1 Adaptive Issuance™ Device Management Software 8.2.1

If you have further questions, please contact Entrust Customer Service at 1-800-568-4598.

Best Regards,

Mark J. Ruchie

Mark J. Ruchie
Vice President, Chief Information Security Officer
Entrust