Authorization to Operate Letter

U.S. General Services Administration

MEMORANDUM FOR	Mark Rucchi Vice President, Chief Information Security Officer Entrust Datacard System Owner
FROM:	Dominic K. Sale Authorizing Official Deputy Associate Administrator Authorizing Official
THRU:	Kurt Garbars Chief Information Security Officer General Services Administration
THRU:	Joseph Hoyt Information System Security Manager General Services Administration
SUBJECT:	Decision for Standard Assessment & Authorization Entrust Managed Services PKI
DATE:	July 17, 2017

A security controls assessment of the Entrust environment has been conducted at the Federal Information Processing Standards (FIPS) 199 Moderate Impact level in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* and General Services Administration (GSA) IT Security Procedural Guide: Managing Enterprise Risk Security Assessment and Authorization, Planning, and Risk Assessment (CA, PL, & RA), CIO-IT Security-06-30. This security controls assessment focused on the integration of the Non-Federated Credentialing (NFI) system to include supporting assets and functionalities into the Entrust Managed Services PKI system boundary.

The security controls listed in the System Security Plan (SSP) have been assessed by Dalethes Inc. using the assessment methods and procedures described in the Security Assessment Report (SAR) to determine the extent the controls are implemented correctly, operating as intended, and producing the desired outcome for meeting the security requirements of the system. A Plan of Action and Milestones (POA&M) has been developed describing the corrective measures implemented or planned to address any deficiencies in the security controls for the information system and to reduce or eliminate known vulnerabilities.

Based on the security configuration defined in the SSP, and the planned actions in the POA&M, I recommend authorization of the Entrust information system.

RECOMMEND AUTHORIZATION:

7/17/2017

X Joseph Hoyt

Joseph Hoyt
Information System Security Manager
Signed by: JOSEPH HOYT

After reviewing the results in the SAR, and the supporting evidence provided in the security authorization package, I have determined the risk to GSA's Federal systems, data, and/or assets resulting from the operation of the information system is acceptable.

Accordingly, I am issuing an Authorization to Operate (ATO) for the Office of Government wide Policy (OGP) Entrust information system in its current environment and configuration. This authorization is valid for Three (3) years from November 3rd, 2016 or until a significant change in the system or threat/risk environment, as described in CIO-IT Security 06-30, necessitates re-assessment and re-authorization. This security authorization is my formal declaration that adequate security controls have been implemented in the information system and that a satisfactory level of security is present in the system.

The security authorization of the information system will remain in effect for three (3) years from November 3rd, 2016 under the following conditions:

1) The Entrust Program Manager shall mitigate all open POA&M action items identified during the security assessment process, per the schedule defined in the POA&M in accordance with GSA policy and guidance, unless an exception is made by the AO.
2) Submit one populated, representative sample card for each PIV issuer configuration used to the FIPS 201 Evaluation Program for testing. Within six months (4/30/2017) of receipt of this signed ATO letter, Entrust shall work with their issuers to correct all errors identified from testing. In addition, Entrust and their associated issuers shall work with the agencies to issue the correct updated PIV cards to the federal agencies.
3) Submit sample production end-entity certificates currently in use for all types of certificates issued from the Entrust PKI. Resolve all issues identified within three months of receipt of feedback.
4) Provide all audits from their RA and CMS components under COMMON and Certificate Authorities cross certified with the Federal Bridge and abiding by all requirements outlined in the FPKI Annual Review, Federal COMMON Certificate Policy, and Federal Bridge Certificate Policy. Resolve all issues within three months from receipt of feedback from GSA.

5) Adhere to the Memorandum of Agreement established between the FPKIPA and Entrust.

APPROVED:

7/17/2017

X Dominic K. Sale

Dominic Sale
Authorizing Official
Signed by: DOMINIC SALE

CONCURRENCE:

7/17/2017

X Kurt Garbars

Kurt Garbars
Chief Information Security Officer
Signed by: KURT GARBARS

Copies of the authorization package are available for review at the GSA facilities in the Washington, D.C. metropolitan area. If you have any questions or comments regarding this authorization to operate, please contact the ISP Division, at ispcompliance@gsa.gov.