Non-Federal Identity (NFI) Public Key Infrastructure Certification Practices Statement [REDACTED]

Version 2.2

12 November, 2025

Non-Federal Identity (NFI) Public Key Infrastructure Certification Practices Statement [REDACTED]

Version: 2.2

Signature Page

Jim Trovato

Entrust Federal mPKI Policy Authority (Print Name)

Signed by:
Jim Trovato
89D32B44D9C945B...

Entrust Federal mPKI

Policy Authority

12 November, 2025

Date

CONTENTS

Revision History

Document Version	Document Date	Revision Details
1.0	April 24, 2009	Initial draft.
1.1	May 15, 2009	Align document more closely with FBCA [CP]
1.1.1	May 26, 2009	Align Section 5.3.1 with the FBCA [CP] and other minor corrections
1.1.2	June 09, 2009	Updates based upon comments from the FBCA CPWG mapping review.
1.2	March 5, 2010	Revised to incorporate requirements for SAFE and align with version 1.2 of the EMS NF PKI X.509 [CP]
1.3	September 30, 2010	Revised to incorporate requirements for PIV-I for the US Federal Government
1.4	March 20, 2011	Revised to clarify sections that were identified as unclear during annual audit
1.5	August 15, 2011	Revised Section 6.1.4.2 to clarify key update certificate issuance for Issuing CAs
1.6	June 10, 2016	Update for current policy and practices
1.7	July 20, 2018	Updated to reflect the changes to Version 1.7 of the Certificate Policy.
1.8	April 17, 2020	Updated to reflect the changes to Version 1.8 of the Certificate Policy and mapping commends from the audit
1.9	October 7th, 2021	Updated to align document more closely with FBCA [CP]
2.0	October 27th, 2022	Updated to align with NFI CP 2.0 updates
2.1	January 3rd, 2024	Updated to align with NFI CP 2.1 updates
2.2	November 12th, 2025	Major update to address service updates and compliance requirements

1 INTRODUCTION

Entrust Corporation (Entrust)) has implemented a comprehensive, outsourced Public Key Infrastructure (PKI) to provide the services necessary to support Non-Federal entities. The Entrust Non-Federal Identity (NFI) PKI, referred to as EMS NFI, is a Shared Service Provider (SSP) PKI.

The EMS NFI is compliant with the *Entrust Managed Services Non-Federal Identity Public Key Infrastructure Certificate Policy Version 2.2*, [CP]. The EMS NFI consists of products and services that provide and manage X.509 public key certificates. Certification Authorities (CAs) are part of this PKI and generate and manage (revoke, suspend, restore) X.509 public key certificates, and bind the subscribers to their public/private key pairs through the issuance of these X.509 certificates. These CAs are hereafter referred to as NFI CAs.

The EMS NFI consists of multiple CAs; a self-signed Root Certification Authority, hereafter referred to as the Root CA, and one or more Subordinate CAs, hereafter referred to as Issuing CAs. The EMS NFI was instantiated for interoperation with Federal PKIs, through cross certification with the Federal Bridge Certificate Authority (FBCA). The EMS NFI consists of the NFI Root CA and NFI Subordinate/Issuing CA(s) known as the as the NFI Shared Service Provider (SSP) CA(s).

This CPS covers sixteen (16) policies defined in the [CP]. The policies represent five different assurance levels (Rudimentary, Basic, Medium, PIV-I Card Authentication, and Medium Hardware) for public key certificates. The level of assurance refers to the strength of the binding between the public key and the individual whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.

Personal Identity Verification Interoperable (PIV-I) policies for PIV-I Hardware, PIV-I Card Authentication, and PIV-I Content Signing are for use with PIV-I smart cards (see Appendix A for more information).

This Certification Practices Statement CPS is applicable for NFI CA issued certificates, to support access to systems that have not been designated as national security systems. Certificates are issued to state and local governments, commercial employees, contractors, and other affiliated personnel for the purposes of authentication, signature, and confidentiality.

This CPS defines the practices under which the NFI CAs operate. This CPS is subject to review and approval by the Entrust Managed Services Policy Authority (Entrust PA).

This CPS is applicable to all entities with relationships with the NFI CAs, including Trusted Role users. No end user certificates are issued from the Root CA. All individual certificates issued from the NFI Root CA are to those entities filling Trusted Roles. This CPS provides these entities with a clear statement of the practices and responsibilities of the NFI CAs, as well as the responsibilities of each entity in dealing with the NFI CAs.

Security management services provided by the NFI CAs include the following:

- Key Generation/Storage/Recovery
- Certificate and Certificate Revocation List (CRL) generation and distribution
- Certificate Update, Renewal, and Re-key

- Certificate token initialization/programming/management
- System Management Functions (e.g., security audit, certificate tracking, archive, etc.)

The security and trustworthiness of the EMS NFI depends on the security of the hardware, software, facilities, personnel, and procedures used in the operation of the NFI CAs.

This CPS is consistent with Internet Engineering Task Force (IETF) Request for Comment (RFC) 3647: *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework*.

The remaining sections of this document have been redacted and are not included in this version. For additional information regarding the NFI PKI and related Certification Authorities, please refer to:

https://www.entrust.com/legal-compliance/federal-pki

Please contact your representative for any further information regarding this document.