Managed Validation and Translation Services (MVTS)
SPECIFICATION

Business Owner:	Federation Operations
Creation Date:	02/05/07
Last Updated:	10/25/07
Version:	EA-DD-0127-1.0-F
Audience:	Public

Document History

Status	Release	Date	Comment	Audience
Release Draft	0.1.0	2/5/07	Initial draft of version 0.1.0	Limited
Release Draft	0.1.1	2/23/07	Update with Monitoring, Edits from Design Review	Limited
Release Draft	0.1.2	5/21/07	Version release, Updates per PMO comment	PMO
Release	0.1.3	06/14/07	Version release, Updates per PMO comment	PMO
Final	1.0		Updates per PMO comment	Public
Final	1.0	06/18/07	Approved	Public

Editors

Denise Finnance	Richard Webb	Ken Pillow
Terry McBride	Doug Hansen	

TABLE OF CONTENTS

1 Introduction

The Federal Acquisition Service (FAS), Integrated Technology Services (ITS), E-Authentication Solution Program Management Office (PMO) has an ongoing requirement for E-Authentication solutions that encompass identity Credential Services, Integration and Technical Support Services, and Identity Software Products that enable public access to Internet-based government services.

As a key component of the President's Management Agenda, the U.S. E-Authentication Identity Federation (Federation) enables trust and confidence in E-Government transactions via integration of policy and technical infrastructure for electronic authentication.

After careful analysis and proofs-of-concept, the E-Authentication Program Management Office (PMO) decided to implement E-Authentication infrastructure as a federated architecture called the Authentication Service Component (ASC). The ASC leverages credentials from multiple credential providers through certifications, guidelines, standards, and policies. The ASC accommodates assertion-based authentication and certificate-based authentication. Assertion-based authentication uses passwords and PINs. Certificate-based authentication uses Public Key Infrastructure (PKI) certificates.

The ASC is not reliant on a single identity assurance scheme or a single identity assurance commercial product. Rather, the ASC is an architectural framework that (a) supports multiple identity assurance schemes concurrently, and (b) allows any commercial identity product conformant with Federation implementation requirements. Over time, the ASC may support additional schemes as they emerge from identity management standards bodies such as OASIS (e.g., SAML), Liberty Alliance (e.g., Identity Federation Framework), and Internet2 (e.g., Shibboleth).

The Federal Enterprise Architecture (FEA) uses the ASC as its government-wide authentication component. The ASC aligns with Office of Management and Budget (OMB) M-04-04, which provides policy guidance for identity authentication. It also aligns with National Institute for Standards and Technology (NIST) Special Publication 800-63, which is the technical companion document to OMB M-04-04. While the ASC architecture addresses authenticating end users to applications, authorization privileges at the application are beyond the scope of the ASC architecture and this document.

1.1 Problem Statement

In order to implement PKI-based identity authentication, it is necessary for the software application that authenticates users with digital certificates to be able to determine that the credentials presented to it are valid and of the minimum required Level of Assurance. The Federal PKI Architecture provides the basic infrastructure to allow certificate validation to occur but the software to enable end users, servers, etc. to use the infrastructure is not generally available natively in desktop Operating Systems. That is, they have demonstrated the ability to discover and validate paths to the issuing PKI certification authority, determine the validity of the digital certificate in question, and ascertain the level of assurance of the certificate as well.

While the Federal PKI Architecture has the infrastructure to support path discovery and validation, it does not have the tools to provide these services to relying parties that are members of the Federation.

To satisfy this requirement, the GSA U.S. E-Authentication Identity Federation PMO has established a Managed Validation and Translation Service (MVTS).

1.2 Document References

[CAF, CAP]	Credential Assessment Framework & Credential Assessment Profiles, http://www.cio.gov/eauthentication/CredSuite.htm
[FMD]	Federation Membership Documents http://www.cio.gov/eauthentication
[HSPD-12]	Homeland Security Presidential Directive/HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors;* August 27, 2004 http://csrc.ncsl.nist.gov/policies/Presidential-Directive-Hspd-12.html
[NIST SP 800-63]	Electronic Authentication Guideline, National Institute of Science and Technology (NIST Special Publication 800-63) http://csrc.nist.gov/publications/nistpubs/
[OMB M-04-04]	E-Authentication Guidance for Federal Agencies, Office of Management and Budget (OMB) Memorandum M-04-04 http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
[OMB M-03-22]	OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Office of Management and Budget (OMB) Memorandum M-03-22 http://www.whitehouse.gov/omb/memoranda/m03-22.html

Additional U.S. E-Authentication Identity Federation Resources

http://www.cio.gov/eauthentication/documents/ApprovedProviders.htm

http://www.cio.gov/eauthentication

http://www.cio.gov/eauthentication/library.htm

1.3 Operational Environment

The MVTS shall perform certificate validation and provide validation functionality at an enterprise level and perform certificate authentication services and provide translated security token assertions to U.S. E-Authentication Identity Federation Relying Parties; where security experts can control the trust settings and ensure correct operation and auditing of authentication transactions with U.S. U.S. E-Authentication Identity Federation digital certificate users. See Appendix B for the MVTS Context Diagram. The MVTS is operated in a secure network operations center.

1.3.1 Subscribers

A subscriber is an End-Entity (EE) named as the subject in a certificate, and who asserts that it uses its key and certificate in accordance with a Federal Compliant Certificate Policy (CP). Subscribers are limited to the following categories of entities:

1.3.1.1 Unaffiliated Individuals - citizens of the United States, conducting personal business with an U.S. E-Authentication Identity Federation Relying Party.

1.3.1.2 Employees of Businesses – individuals acting in the capacity of an employee to conduct business with an U.S. E-Authentication Identity Federation Relying Party.

1.3.1.3 State and Local Government Employees - individuals acting in the capacity of a Government representative with an U.S. E-Authentication Identity Federation Relying Party.

1.3.2 Relying Party

Relying Parties are those entities authorized to accept and rely upon U.S. E-Authentication Identity Federation services (including: workstations, firewalls, routers, trusted servers, and other infrastructure components within the U.S. E-Authentication Identity Federation).

Note: Relying Parties are those eligible Federal agencies and entities that enter into an agreement with GSA to be bound by the terms of the U.S. E-Authentication Identity Federation. Other eligible federal agencies and entities under the Federal PKI Common Policy Framework (FPCPF) may include all federal agencies, authorized federal contractors, agency-sponsored universities and laboratories, other organizations, and, if authorized by law, state, local, and tribal governments.

1.3.3 U.S. E-Authentication Identity Federation Levels

1.3.3.1 The MVTS shall support Relying Parties operating at U.S. E-Authentication Identity Federation Levels 1, 2, 3, and 4.

1.4 Related Systems

The MVTS operates consistent with the policies set forth by the Federal PKI Policy Authority and Operational Authority and coexist under the Systems Security Plan.

1.5 Key Stakeholders

The Key Stakeholders are identified as:

1. Relying Party Applications – applications needing to obtain revocation status and translation services for their user community.

2. Certificate Authorities – all Federal Bridge certified certificate authorities that issue digital certificates to their user community.

3. User community – individuals who have obtained digital certificates from certificate authorities and are trying to access certain relying party applications.

4. U.S. E-Authentication Identity Federation PMO and Federation – members of the Federation who are required to meet the goals of the E-Government initiatives and have authorized funding for the MVTS capability.

2 Functional Requirements

Functional requirements define the specific functions that the software system performs, along with the data operated on by the functions. The functional requirements are presented in scenarios that depict the operational system from the perspective of its end users.

2.1 User Interface Overview

The MVTS system supports entities transacting electronic business with or business for Federal Government entities. Users may include Unaffiliated Individuals, Business Representatives, and members of Federal, State, and Local Government agencies who are members of the U.S. E-Authentication Identity Federation.

2.1.1 U.S. E-Authentication Identity Federation relying parties shall interface with the MVTS using http, OCSP (RFC 2560), SCVP (ITF draft) and/or PDVAL (RFC 3379) protocols.

2.1.2 The MVTS shall be configured to accept/read CRLs and/or signed OCSP, SCVP and/or PDVAL responses.

2.1.3 Relying Parties shall be responsible for archiving CRLs and/or signed OCSP, SCVP and/or PDVAL responses, as necessary to satisfy internal auditing requirements.

2.1.4 Entities interface to the MVTS via (at a minimum) a FIPS 140-1/2 Level 1 cryptographic module.

2.2 System-Specific Requirements

The MVTS consists of two major subsystems: a digital certificate Validation Service (VS) and an authentication step-down Translation Service (TS).

2.2.1 MVTS

The MVTS supports multiple trust models and multiple online validation status check protocols.

2.2.1.1 The MVTS shall maintain a trust list of all Federal Bridge certified certificate authorities that issue digital certificates to their user community.

2.2.1.2 The MVTS shall ensure that certificate validation occurs only from Federal Bridge certified certificate authorities that issue digital certificates to their user community.

2.2.1.3 The MVTS shall maintain evidence that due diligence was exercised in validating the U.S. E-Authentication Identity Federation CA credentials and its translated assertions.

2.2.1.4 The MVTS shall be capable of protecting communications using RSA 1024-bit and 2048-bit keys and/or the Advanced Encryption Standard (AES). The MVTS server(s) shall obtain certificates from an approved U.S. E-Authentication Identity Federation CA to protect communications.

2.2.1.5 The MVTS shall include a FIPS 140-2 validated cryptographic module to support protected communications with U.S. E-Authentication Identity Federation users and Relying Parties.

2.2.1.6 The MVTS shall be capable of building certification paths in the Federal PKI environment and validating certification paths in compliance with X.509 and RFC 3280.

2.2.1.7 The MVTS shall, at a minimum, recognize and process the following cryptographic features:

2.2.1.7.1 Certificates that contain 1024-bit and 2048-bit RSA public keys.

2.2.1.7.2 Certificates signed using 1024-bit and 2048-bit RSA keys.

2.2.1.7.3 Certificate signatures generated using SHA-1.

2.2.1.7.4 Certificate signatures generated using SHA-256.

2.2.1.7.5 Certificates with RSA PKCS#1 v1.5 formatted digital signatures.

2.2.1.8 The MVTS shall recognize and process the following cryptographic features no later than January 1, 2009:

2.2.1.8.1 Certificates containing elliptic curve public keys for curve P-256 in certificates.

2.2.1.8.2 Certificates with RSA PSS formatted digital signatures generated with 2048-bit keys and the SHA-256 hash algorithm.

2.2.1.8.3 Certificates with ECDSA signatures generated over curve P-256 with the SHA-256 hash algorithm.

2.2.1.9 At Level 3 and above, the MVTS shall use the FIPS 140-2 validated hardware cryptographic module for digital signature generation.

2.2.1.9.1 Digital signatures shall be generated using a 2048-bit RSA private key. Services shall be capable of generating PKCS #1 v1.5 digital signatures (i.e., the RSASSA-PKCS1-v1_5 signature format) using both SHA-1 and SHA-256.[FIPS 186-3][FIPS 180-2].

2.2.1.9.2 The service shall use SHA-1 to sign assertions through 12/31/2008.

2.2.1.9.3 Assertions shall be signed using SHA-256 after 12/31/2008.

2.2.1.10 The MVTS shall not require user installation of software or reconfiguration of end user systems.

2.2.1.10.1 The MVTS may offer services that require downloading software (e.g., JAVA applets or ActiveX controls) onto user systems, but solutions that do not impose such requirements are preferred.

2.2.1.10.2 Any applets or ActiveX controls downloaded to user systems shall be signed by the MVTS.

2.2.1.10.3 Where downloading software is required, the software shall be compatible, at a minimum, with the latest two supported versions of the following Internet browsers:

2.2.1.10.3.1 Internet Explorer.
2.2.1.10.3.2 Mozilla/Firefox.
2.2.1.10.3.3 Safari.
2.2.1.10.3.4 Opera.

2.2.2 Validation Service

The VS offloads the task of performing certificate validations and provides validation functionality at an enterprise level.

2.2.2.1 The VS shall ensure that certificate and revocation information is accepted only from valid U.S. E-Authentication Identity Federation CAs.

2.2.2.2 The VS shall perform certificate and CRL retrieval using LDAP and may support the following optional mechanisms for obtaining CA certificates and certificate status:

2.2.2.2.1 http-based certificate and CRL retrieval.

2.2.2.2.2 OCSP status checking.

2.2.2.3 The VS shall ensure provide certificate revocation status and/or complete certification path validation (including revocation checking) to U.S. E-Authentication Identity Federation Relying Parties.

2.2.2.4 The VS shall ensure that the status and validation responses contain authentication and integrity services commensurate with the assurance level of the certificate being checked.

2.2.2.5 Maintenance and secure distribution of the CA hints (trust) list. In the TLS protocol, when a mutually authenticated TLS session is to be established, the server sends a certificate request message to the client:

2.2.2.5.1 The MVTS must maintain a list of acceptable CAs for inclusion in the certificate request message that is sent to clients when mutually authenticated TLS sessions are established. The list of acceptable CAs must be sufficiently comprehensive so that any user who has been issued a certificate that can be validated as satisfying U.S. E-Authentication Identity Federation Level 2 or higher will be permitted by their browser to present their certificate to the server for validation. Requirements for PKI certificate-based authentication at U.S. E-Authentication Identity Federation Level 2 and higher are specified in [SP 800-63].

2.2.2.5.2 The MVTS must maintain the list of acceptable CAs, including adding new CAs to the list as they are added to the Federal PKI. The MVTS must also develop a method for securely distributing the list to PKI-aware web servers and must provide guidance to the operators of the web servers on how to install this list so that the list is sent to clients as part of the certificate request message of the TLS session establishment protocol.

2.2.2.5.3 Where the secure distribution method relies on cryptography, all cryptographic mechanisms shall use FIPS-Approved algorithms and provide at least 80 bits of security. Beginning on January 1, 2009, cryptographic mechanisms shall provide at least 112 bits of security. See Table 4.5-1, below, for a summary of FIPS-Approved algorithms that satisfy 80 and 112 bits of security. Cryptographic operations shall be performed in a CMVP Validated cryptographic module.

Bits of Security	Symmetric Encryption	Public Key Algorithms	Hash Algorithms in Signatures	Hash Algorithms in HMACs
80	2key TDEA, 3key TDEA			
AES (128, 192, and 256)	RSA, DSA, or Diffie-Hellman 1024 bits or greater			
Elliptic Curve Cryptography 161 bits or greater	SHA-1			
SHA-224, SHA-256, SHA-384, SHA-512	SHA-1			
SHA-224, SHA-256, SHA-384, SHA-512				
112	3key TDEA, AES (128,	RSA, DSA, or Diffie-		

	192, and 256)	Hellman 2048 bits or greater		
Elliptic Curve Cryptography 224 bits or greater	SHA-224, SHA-256, SHA-384, SHA-512	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		

Table 4.5- 1 Bits of Security of FIPS Approved Algorithms

2.2.2.6 The VS shall operate an online delegated path validation server performing path validation. This server must include the server functionality associated with the selected delegated path validation protocol.

2.2.2.7 The VS shall support Enhanced Local Validation. In general, certificate validation mechanisms associated with COTS web servers cannot be replaced, but may be augmented by supplemental mechanisms. With enhanced local validation, the supplemental mechanism is a comprehensive path discovery and validation module provided as a web server plug-in. In this scenario, the web server validates the user's certificate using the native path validation mechanism with respect to a trust list composed of leaf CAs and establishes a mutually authenticated TLS pipe. After establishing a secure connection, the user certificate is provided to the plug-in, which repeats path validation. If the plug-in authenticates the certificate successfully, then the user is permitted to access the desired application.

2.2.2.8 The VS shall provide web server plug-ins and configuration guidance for each of the web servers listed below. The plug-in shall provide client functionality for a delegated path validation protocol.

2.2.2.8.1 Web server applications running on IIS-based Web Servers;

2.2.2.8.2 Web server applications running on Apache Server; and

2.2.2.8.3 Web server applications running on the Domino Server.

2.2.3 Translation Service

An end user attempting to access an U.S. E-Authentication Identity Federation SAML-enabled application using an U.S. E-Authentication Identity Federation approved PKI credential shall be directed to the TS. Upon being presented with the PKI credential, the TS shall validate that credential via the VS. Once the digital certificate validation process is successfully completed, the TS shall generate a SAMLv1.0/2.0 U.S. E-Authentication Identity Federation assertion conforming to SAML 1.0 Artifact Profile v1.0.0. [ARTIFACT] or SAML 2.0 POST Profile [POST] as adopted/modified.

2.2.3.1 The TS shall rely only on FPKI-compliant certificates (see National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63) X.509 certificates.

2.2.3.2 The TS shall provide a U.S. E-Authentication Identity Federation compliant security token to U.S. E-Authentication Identity Federation relying parties, based on a certificate authentication (functioning as a compliant U.S. E-Authentication Identity Federation Credential Service (CS) by authenticating a user based on a PKI credential, then generating a SAML assertion that indicates the claimant has successfully been authenticated.

2.2.3.3 The MVTS shall support U.S. E-Authentication Identity Federation Relying Parties that rely on SAML assertions for user authentication and shall use a TLS session for confidentiality and integrity services .

2.2.3.4 The MVTS shall support U.S. E-Authentication Identity Federation SAML 1.0 Relying Parties that rely on a mutually authenticated TLS session between the server and the user's system for authentication, confidentiality, and integrity services.

Note: To support applications that rely on SAML assertions for user authentication, the TS operates one or more translation servers.

2.2.3.4.1 At Level 2, the TS must generate SAML assertions that conform to the profile specified in U.S. E-Authentication Identity Federation Requirements Specification for the SAML 1.0 Artifact Profile v1.0.0. [ARTIFACT] or SAML 2.0 POST Profile as adopted/modified .

2.2.3.4.2 At Level 3, the TS must generate digitally signed and encrypted assertions conforming to SAML 2.0.

2.2.3.5 The TS shall support path discovery and be capable of passing directory-based tests from the Path Discovery Test Suite at both the Rudimentary and Basic levels.

2.2.3.5.1 The path validation capabilities must include those specified for a Bridge-enabled path validation module in the NIST Recommendation for X.509 Path Validation.

2.2.3.5.2 Products that appear on the Path Discovery and Validation Working Group's Qualified Validation List are considered to satisfy the path discovery and validation requirements.

2.2.3.6 The MVTS shall include a SAML profile for the Level 3 digitally signed and encrypted assertions conforming to SAML 2.0.

2.2.3.6.1 The profile shall be consistent with the SAML 1.0 Artifact Profile v1.0.0. [ARTIFACT] or SAML 2.0 POST Profile as adopted/modified ..

2.2.3.6.2 The Government shall approve the profile before system deployment.

2.2.4 Managed monitoring and reporting

The MVTS shall provide managed monitoring and reporting of U.S. E-Authentication Identity Federation trusted CAs/CRLs.

2.2.4.1 Federation Monitoring Management to include:

2.2.4.1.1 Management processes and reports that support the monitoring of the new and existing U.S. E-Authentication Identity Federation trusted CA sites.

2.2.4.1.2 Monitoring U.S. E-Authentication Identity Federation system certificate components and trusted CAs/CRLs through periodic polling

2.2.4.1.3 Performing various automatic test probes to ensure that CA's directories are stable and operating properly, and that CRL's are issued in accordance with their respective certificate policy.

2.2.4.1.4 Providing advice to the U.S. E-Authentication Identity Federation PMO of each site's ability to meet the U.S. E-Authentication Identity Federation approved service levels.

2.2.4.2 Maintain and configure new and existing U.S. E-Authentication Identity Federation trusted CA sites as directed by the U.S. E-Authentication Identity Federation PMO for performance monitoring. Monitoring shall be conducted using an agent-less software monitoring tool(s) sufficient enough to collect performance metrics and monitor the performance of U.S. E-Authentication Identity Federation trusted CA sites and U.S. E-Authentication Identity Federation certificate components.

2.2.4.3 Maintain an activity report, which shall include but is not limited to:

2.2.4.3.1 CAs/CRLs monitoring.

2.2.4.3.2 Availability /Uptime test.

2.2.4.3.3 Average Response Time.

2.2.4.3.4 Benchmark test (12 times per hour per member)

2.2.4.3.5 Transactional Test (12 times per hour per member)

2.2.4.3.6 End-to-End Throughput.

2.2.4.4 The monitoring service shall operate in a manner that generates alerts when reasonable response times for processing Subscriber requests are not met. The MVTS shall monitor these response times to ensure that infrastructure supporting the U.S. E-Authentication Identity Federation certificate community are available and generate an alert when there are potential problems.

Note: Response times may be also be dependent upon on other factors such as speed and type of networking connections, and physical dispersion of networked Subscribers.

2.3 System Non-Functional Requirements

2.3.1 Interoperability

The MVTS service shall interoperate with each U.S. E-Authentication Identity Federation compliant PKI domain that is cross-certified with the FBCA to provide capability to authenticate certificates from issuing CA(s) recognized by the U.S. E-Authentication Identity Federation PMO.

2.3.2 Scalability

Approximately 24+ Government agency applications could make use of the MVTS service for validation of PKI credentials in the next three years. Some of these Relying Parties may process high volumes of certificate validations during certain time periods, such as IRS Relying Parties during federal tax deadlines.

2.3.2.1 The MVTS service shall be scalable, and provide architectural flexibility for validation solutions.

2.3.2.2 The performance of the validation system must not degrade as the number of Relying Parties increases significantly.

2.3.2.3 Deployment and the expansion of the system shall put the least burden on the participating relying parties.

2.3.2.4 The cost of system expansion shall be part of the architectural design.

2.3.2.5 Configuration Management, Recovery, Change Management, and Fault Tolerance capabilities shall be maintained during all expansions.

2.3.3 Security and Privacy Policy

The MVTS shall maintain a system of records on behalf of the Government under a written Privacy Policies and Procedures (PPP) designed to ensure compliance with the requirements of 5 U.S.C. 552a, Appendix I to OMB Circular A-130, and the ACES Contract. These policies and procedures are incorporated into this CPS.

2.3.4 Laws and Regulations

2.3.4.1 The MVTS service shall comply with all appropriate laws and regulations for Federal Government information systems and the additional specific security requirements for information systems deployed by or on behalf of the U.S. General Services Administration.

2.3.4.2 Security of federal information systems is controlled by the Federal Information Security Management Act of 2002 (FISMA). Under FISMA, the Director of OMB is tasked with implementing policy guidance for information security standards for Federal information systems. Technical guidance for Federal information systems security is provided by NIST through both mandatory guidance and voluntary guidelines.

2.3.5 FISMA, OMB regulations, and NIST guidance

2.3.5.1 The MVTS shall comply with FISMA, OMB regulations, and NIST guidance materials.

2.3.5.2 Privacy of Federal information systems is controlled by the Privacy Act of 1974, the Paperwork Reduction Act of 1995, and the E-Government Act of 2002. Under these laws the Director of OMB is tasked with implementing policy guidance for the protection of privacy.

2.3.6 Privacy Act of 1974, Paperwork Reduction Act of 1995, and the E Government Act of 2002

2.3.6.1 The MVTS shall implement any privacy affecting components of the MVTS service using Fair Information Practices as identified by the Organization for Economic Cooperation and Development (OECD).

2.3.6.2 The MVTS shall comply with these laws and regulations by invoking appropriate procedures, conducting compliance tests, and performing annual compliance audits.

2.3.6.2.1 The MVTS shall implement and maintain comprehensive security, continuity, and privacy policies.

2.3.6.3 The MVTS shall provide security and protection of MVTS service privacy information as follows:

2.3.6.3.1 Any GSA or Government information shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract and in accordance with in accordance with the Privacy Act of 1974, and Appendix III to Office of Management and Budget (OMB) Circular A-130;

2.3.6.3.2 In performance of this contract, the MVTS shall assume responsibility for protecting the confidentiality of Government records and for ensuring that all work is performed under the supervision of the responsible employees;

2.3.7 Record Maintenance and Privacy/Security

The MVTS service will provide a vital service to Relying Parties that are part of the nation's critical infrastructure.

2.3.7.1 Application access decisions will be based on the results of MVTS service processing.

2.3.7.2 MVTS service audit trails shall be Government System of Records, requiring archival, protection against unauthorized access, and provision for access and correction by the individuals to whom the individual records pertain in accordance with The Privacy Act of 1974, The Federal Information Security Management Act of 2002, Appendix I and III, Office of Management and Budget Circular A-130.

2.3.8 Security Certification, Accreditation, and Re-Accreditation

The MVTS shall gain Security Certification and Accreditation (C&A) in accordance with NIST Special Publication 800-37, Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems, prior to initial operation, and subsequently on an annual basis and at the time of any major change.

2.3.8.1 The MVTS shall follow FIPS PUB 199 - Standards for Security Categorization of Federal Information and Information Systems.

2.3.9 Annual Independent Quality Assurance and Inspection Requirements

2.3.9.1 The MVTS shall submit to Government-conducted quality assurance inspections, with notice, and shall schedule, submit to, and pay for an annual quality assurance inspection by an independent organization agreeable to the Government in accordance with NIST Special Publication 800-37.

2.3.9.2 The TS shall reside on a publicly accessible Internet site device that allows end users to access the TS via a General Services Administration (GSA) approved web portal.

2.4 Process-Related Non-Functional Requirements

Project Deliverables are provided in the fully executed contract.

2.5 Personnel-Related Non-Functional Requirements

Non-functional personnel requirements include applicable licensing and certification documentation.

Appendix A - Glossary

Appendix B: Acronyms

Reference U.S. E-Authentication Identity Federation Glossary

Appendix C – MVTS Context Diagram

Level 0 Context Diagram

The following Level 0 Context Diagram presents a system level view of the MVTS system (red rectangle) and the external entities (blue ovals) and external data sources (green rectangle) providing input/output (lines with arrows) to and from the system.

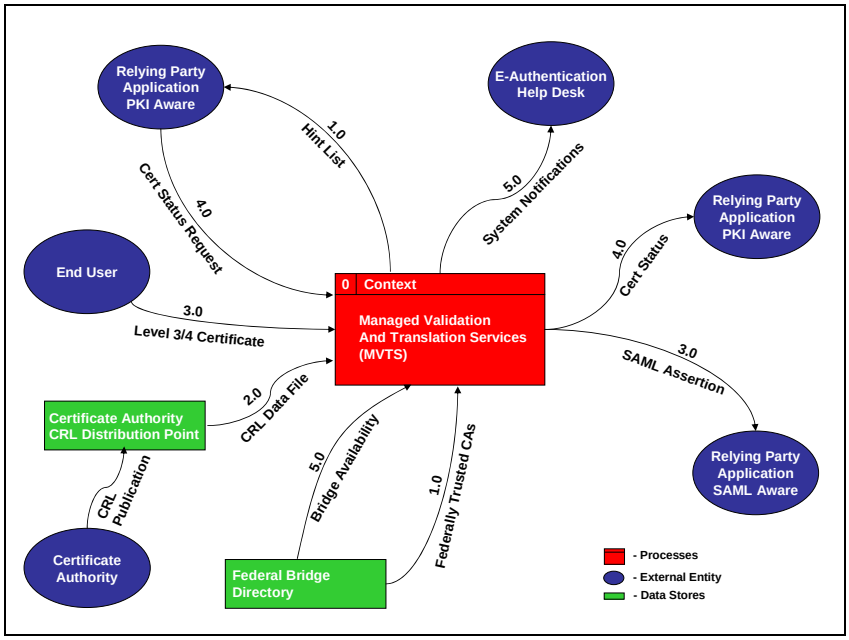

Figure 1 – Level 0 Context Diagram for the MVTS system

WBS 1.0 Hint List Management – describes the process flow of Hint List Management and its distribution to PKI-aware Relying Parties. The Hint List is managed by monitoring of the Federal Bridge Directory for the most current status and this list is passed onto the PKI-aware Application when updates occur.

WBS 2.0 Data Management – describes the process flow for the MVTS system to obtain Certificate Revocation List data from the various Certificate Authorities that are cross-certified with the Federal Bridge.

WBS 3.0 Translation Services – describes the process where a user with a Level 3 or Level 4 credential presents their certificate to the MVTS system to acquire an assertion for SAML-aware Relying Parties that do not accept certificates.

WBS 4.0 Validation Services – describes the process where PKI-aware Relying Parties request and receive revocation status on a certificate being presented to their website.

WBS 5.0 Monitoring – describes the process where the MVTS system monitors the availability of the Federal Bridge, CRLs from cross-certified Certificate Authorities and the maintenance of the Hint List previously described for timely updated distribution to all PKI-aware Relying Parties that are interacting with the MVTS system.