Certificate Validation for PIV across the Federal Bridge using the Server-based Certificate Validation Protocol (SCVP) – RFC 5055

Nabil A. Ghadiali
Electrosoft Services
11417 Sunset Hills Road, Suite 228
Reston, VA 20190
+001 (703)-437-9541 x15

nabil@electrosoft-inc.com

ABSTRACT

In this paper, we describe the challenges and a potential solution for validating public key (PKI) certificates associated with issued Personal Identity Verification (PIV) cards and PIV-Interoperable (PIV-I) cards.

The current federal PKI landscape is complex, and unique requirements for trust makes certificate path validation extremely tedious for relying parties. This paper identifies the need, discusses the complexities and proposes an approach in an attempt to use the credentials on a PIV Card as the interoperable, federated identity credential envisioned by Homeland Security Presidential Directive 12 (HSPD-12) - *Policy for a Common Identification Standard for Federal Employees and Contractors* [1].

Categories and Subject Descriptors

K.6.5 [Management of Computing and Information Systems]: Security and Protection; authentication

General Terms

Management, Security, Standardization

Keywords

Personal Identity Verification, SCVP, Authentication, Smart cards, PKI, Federal Bridge Certification Authority, Validation

1. AUDIENCE

This paper is intended for the government officials responsible for authenticating PIV credentials. It will also aid senior government executives to evaluate business cases and develop authentication strategies for their departments or agencies – both in the area of physical and logical access. Information in this document is also useful to the contractors, security industry vendors and integrators implementing HSPD-12 related products, systems and services.

2. VALIDATION IN HSPD-12

On August 27, 2004, the Homeland Security Presidential Directive (HSPD) -12 was issued. The goals of this Directive were to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors.

Once agencies issue these expensive PIV Cards to their employees and contractors, it only makes sense to utilize the credentials it houses for identification, authentication and authorization such that the true intent of HSPD-12 is recognized.

2.1 FIPS 201 Authentication Mechanisms

Section 6 of FIPS 201 - *Personal Identity Verification (PIV) of Federal Employees and Contractors* [2] defines a suite of identity authentication mechanisms that are supported by the PIV Card, and their applicability in meeting the requirements for graduated levels of identity assurance based on the different credentials (PIV data objects) loaded on it. Government stakeholders responsible for controlling access to Federal resources (both physical and logical) determine the appropriate level of identity assurance required for access, based on the harm and impact to individuals and organizations as a result of errors in the authentication of the identity of the PIV cardholder.

Given that the PIV specifications are standardized and accessible to the general public, a PIV system protects the trustworthiness of PIV data objects through smart card access rules and digital signatures. That being said, it is imperative that these digital signatures be verified at the time of authentication in order to establish trust in the card, cardholder and the authentication action.

The most commonly used authentication mechanisms as identified in FIPS 201 and SP 800-116 - *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)* [3] are discussed below. For each discussed mechanism, a brief description on how a forged credential may be accepted as genuine, unless validation is performed, is explained.

2.1.1 CHUID Authentication

The CHUID is a PIV data object specified in *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems (TIG-SCEPACS)* [4] and further refined in FIPS 201. The CHUID data object can be counterfeited extremely easily with the exception of the issuer signature. If signature verification is performed, the relying party can be assured that the CHUID came from a valid issuer and that it was not altered post-issuance.

2.1.2 Biometric Authentication

Biometric authentication is performed using fingerprint information stored on the PIV Card. A rogue can easily generate a fingerprint biometric data object on a fake PIV Card, or modify the biometric within a valid PIV Card such that the 1:1 biometric match succeeds. Relying parties should always verify the digital signature on the fingerprint biometric template data object, and perform path validation before performing a match. Otherwise, the result of the match should not be trusted.

2.1.3 PIV Authentication

This authentication mechanism uses the PIV authentication key and certificate to authenticate the cardholder. As part of the process, a cryptographic challenge-response is performed with the relying party application and the PIV authentication certificate validated.

2.1.4 Card Authentication

Similar to the PIV Authentication mechanism, the card authentication mechanism uses the card authentication key and certificate to authenticate the card rather than the cardholder. As part of the process, a cryptographic challenge-response is performed with the relying party application and the card authentication certificate validated.

3. VALIDATING CERTIFICATES THROUGH THE FEDERAL BRIDGE

There are a variety of applications (both in the area of physical and logical access) that can make use of public key certificates. However in order to accept and trust a PKI-based transaction, these applications are burdened with the overhead and complexity of constructing and validating the certification paths.

Within the context of PIV, depending on the credential selected for authentication, validation of a certificate (CHUID signer, biometric signer, PIV authentication or card authentication) needs to be performed.

For those security professionals who have been dealing with PKI and the validation of digital certificates within the Federal space, it comes as no surprise when mentioned that this task is extremely complex.

Figure 1 illustrates the numerous Certification Authorities (CAs) that are cross-certified through the Federal Bridge CA (FBCA) and the elaborate labyrinth of hierarchical PKI structures underneath each of these cross-certified entities. Path development through this maze is complicated for any relying party. Furthermore, distributed revocation checking using certificate revocation lists (CRLs) and the Online Certificate Status Protocol (OCSP) coupled with the validation requirements is process intensive and extremely cumbersome.

Adding fuel to the fire - continuously changing trust rules (e.g. trust anchors, validation policy parameters etc.) doesn't help either and only makes configuration updates to deployed applications a nightmare.

The Server-based Certificate Validation Protocol (SCVP), as explained in subsequent sections of this paper, can be used effectively to solve this long-lived validation problem that currently exists within the Federal Bridge PKI trust fabric.

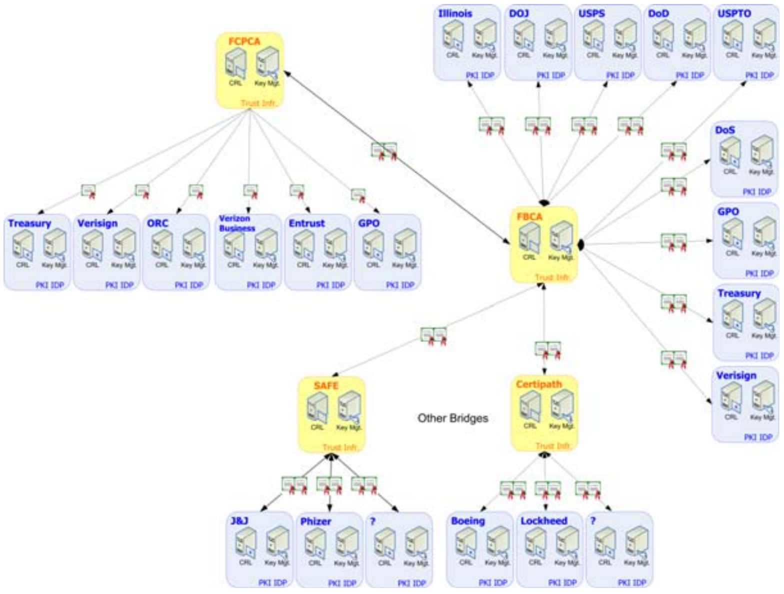

Figure 1 - Federal PKI Architecture

(Source: Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 1.0, Nov 10, 2009)

4. SERVER-BASED CERTIFICATE VALIDATION PROTOCOL

The Server-based Certificate Validation Protocol (SCVP) [5] is a standard developed by the Internet Engineering Task Force (IETF) Public- Key Infrastructure (PKIX) working group. It was finalized as RFC 5055 in December 2007.

The primary goal of SCVP is to make it easier to deploy Public Key Infrastructure (PKI)-enabled applications by delegating path discovery and/or validation processing to a server. The path construction is performed by dynamically discovering the next certificate (issuer certificate) in the chain using the Authority Information Access (AIA) extension present in the certificate until the specified trust anchor is reached. Validation involves making sure that none of the certificates in the path is expired or revoked and it has been issued under the appropriate certificate policy.

The SCVP protocol uses a simple request-response model. That is, a client creates a request and sends it to the SCVP server, and then the SCVP server creates a single response and sends it back to the client. The typical use of SCVP is over HTTP.

In general, SCVP can be useful in two kinds of scenarios:

1. Relying parties completely delegate certification path construction and validation to an SCVP server. This is often referred to as delegated path validation (DPV).
2. Relying parties delegate only the certification path construction to the SCVP server, but not validation of the returned certification path. This is referred to as delegated path discovery (DPD).

Neither mode (DPV or DPD) is better than the other. Both are equally relevant and environmental/architectural circumstances dictate when one is preferred over the other. For example, if the relying party has the capability to perform certification path validation, but lacks a reliable or efficient method of constructing a valid certification path, DPD might be an acceptable option. Moreover, if the relying party is using the services of SCVP server(s) that is outside its Enterprise and that it does not trust, DPD is extremely useful. On the other hand, if the relying party has complete trust in the SCVP Server, the work of certification path construction and validation can be delegated to the authoritative and trusted SCVP Server. Since validation is performed by the server, operating in DPV mode ensures that policies are consistently enforced throughout the organization.

For the remainder of this document, it is assumed that SCVP is used in the DPV mode unless explicitly stated otherwise.

5. APPLICABILITY OF SCVP IN PIV CERTIFICATE VALIDATION

Given that SCVP is a protocol for validating a public key certificate, its applicability spans across any application that uses PKI and requires certificate validation. Therefore, this includes both Physical Access Control (PACS) and Logical Access Control (LACS).

Figure 2 illustrates the use of an SCVP Server within the PACS architecture to obtain certificate revocation status information in the Federal-Bridged environment. Network accessible readers or head-end (host) systems can perform certificate validation prior to the access control system making the authorization decision. An intelligent, network-accessible reader may perform certain initial checks (e.g., CHUID expiration, correct agency code etc.) prior to sending a request (Step 1) to the SCVP server. Alternately, the host system could be responsible for performing the validation in legacy PACS where readers are not TCP/IP enabled. If certificate validation (Step 2) succeeds and trust is established, the controller can then grant or deny access (Step 3) based on the access authorizations for the individual requesting entry.

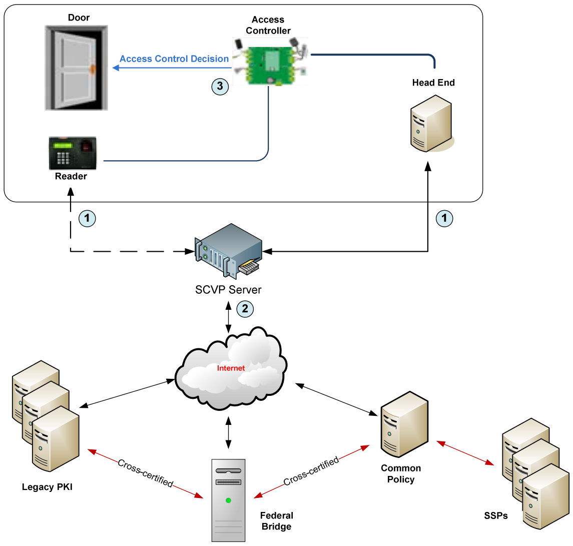

Figure 2 – SCVP within PACS

Similar to physical access, SCVP can be leveraged by several applications within the logical access domain. This includes Windows smart card logon, signed emails, certificate-based VPN and authentication to web servers (e.g. mutual authenticated TLS/SSL).

Figure 3 illustrates the use of SCVP at the time of authenticating to a website using the PIV authentication certificate. A web-client requests access to an organization's web portal by identifying itself to the web-server. The web server sends an SCVP request (Step 1) to the SCVP server which in turn performs path discovery and validation using the presented client certificate. If certificate validation (Step 2) succeeds and trust is established, the web server can then grant or deny access (Step 3) to the site based on the access authorizations for the individual requesting entry.

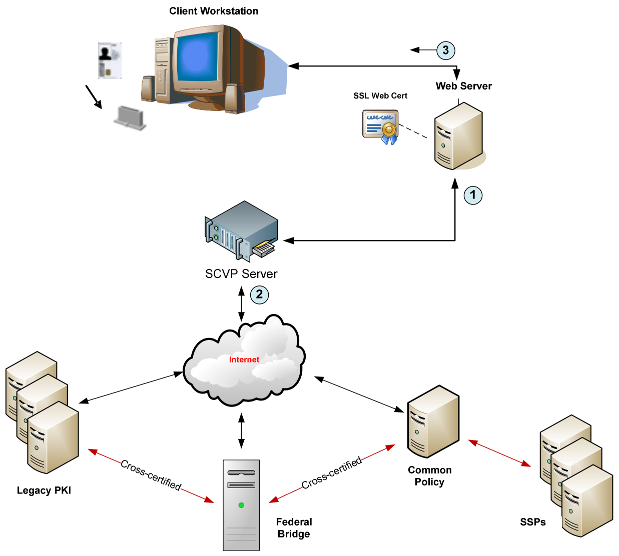

Figure 3 - Web Authentication using SCVP

5.1 Sample Validation Policy for PIV Authentication

As mentioned earlier, one of the advantages of using SCVP is the centralized configuration of the validation policy parameters. The following is an example of a policy configuration that can be set at an SCVP Server to validate the *PIV authentication certificate*.

- Trust Anchor – Common Policy Root CA
- Certificate Policy – id-fpki-common-authentication {2 16 840 1 101 3 2 1 3 13}
- initial-explicit-policy = true
- initial-policy-mapping-inhibit = false

By using the above configured policy, any certificate (issued under the Federal Shared Service Provider (SSP) Program or by a Legacy PKI) that chains up to the Common Policy Root CA and has a certificate issued under the policy corresponding to *id-fpki-common-authentication* or comparable (since policy mapping inhibit is set to false) will be accepted as trusted – provided obviously it isn't expired or revoked.

6. ADVANTAGES OF SCVP

There are several advantages of using SCVP within an organization to perform the path discovery and validation. Some of these include:

- **Simplification of the relying party application** - Applications do not need to incur the overhead of including complex certification path validation software (including configurations) and running it for each certificate it receives.
- **Centralized management of validation criteria** - Trust anchors and validation policy parameters are configured at the SCVP Server and not within each application. Updates/modifications can be made at one location (i.e., the Server) and the effects realized instantly across the Enterprise.
- **Higher performance** - Certificate revocation lists and intermediate CA certificates for known trust paths can be pre-fetched and cached by the SCVP Server. This results in efficient and quicker path building.
- **Lower load on network bandwidth** - Every relying party application performing validation does not have to download intermediate certificates and CRLs. Such PKI artifacts can be downloaded once at the SCVP Server and used repeatedly while providing responses. In general, typical signed SCVP requests and responses are ~3KB each.

7. DISADVANTAGES OF SCVP

As with any technology, advantages are always accompanied with certain disadvantages. For SCVP, these include:

- **Single point of failure** - Given that relying party applications use the SCVP Server to obtain certificate validity, any downtime in the service will have a significant impact on the client application and its ability to perform its function. Having failovers and redundant backups ensure that the SCVP service isn't the single point of failure for the application.
- **Server can get overloaded** - Peaks in the requests (potentially in the morning and shortly after lunch) received by the Server should be estimated and the ability of the server to support such loads analyzed. The use of load balancers will ensure the server does not get overloaded with requests and responses are received within an acceptable timeframe.
- **Expensive and difficult to set up initially** - Server-based products are generally more expensive than their client counterparts. Installation and configuration might be challenging early on, however once set up operations and maintenance should be fairly straightforward.

8. SECURITY CONSIDERATIONS

Outside of the use of SCVP as a mechanism to obtain certificate validity and status information, it is equally important to secure the communications between the client (relying party) and the SCVP Server. Some of these security options that need to be considered by agencies and integrators are discussed below:

- **Use of SSL** - As mentioned earlier, SCVP uses a simple request-response model. Although the typical use of SCVP is expected to be over HTTP, especially in the case of especially the PIV authentication certificate, the use of SSL is highly recommended. This is due to the fact that the PIV authentication certificate contains the FASC-N which poses a major security concern if transmitted in the clear.
- **Signed requests** – This option should be exercised in the event that relying parties need to be authenticated by the SCVP Server prior to providing the validation result.
- **Signed responses** – In general SCVP responses are signed allowing the relying party to authenticate the Server that

provided the response. However in the event that the communication is protected using SSL or if the SCVP server is within a private network, response signing may be omitted thereby increasing throughput and reducing the payload.

9. ARCHITECTURAL CONSIDERATIONS

Given that SCVP is a client-server protocol, it can very easily be the single point of failure in the event that the SCVP Server goes down or if it isn't capable of supporting the load. Careful consideration needs to be given to the application and enterprise architecture within which SCVP is being deployed.

For high-throughput applications (e.g., the main door of a building), the host system may conduct validation (e.g., of the card authentication certificate) at off-peak hours for all certificates that are registered within the PACS system. In this case, the time taken to obtain a response will be minimal since the validation is performed previously and the status cached[1].

In certain scenarios, although an issued certificate complies with the specified validation policy requirements, only a subset of the Certification Authorities (CAs) issuing these certificates may need to be trusted. In such circumstances, functionality of SCVP Servers may be augmented to support disabling of dynamic discovery of certificates within the chain and only those intermediate CAs that need to be trusted be pre-populated within the SCVP Server trust stores. Alternatively, white-lists can be implemented whereby although certificate chains are built successfully, unless the chain contains a specific certificate, it will not be accepted as trusted.

10. CUSTOMIZATION

The SCVP specification is extremely rich in functionality. Agencies may consider developing request and response profiles suitable for use within their environment.

Through analysis of requirements for validation, network and architectural constraints, agencies should select and reject the optional elements within the SCVP specification that would simplify and streamline the use of SCVP while still maintaining the flexibility needed for potential future enhancements.

Development of such profiles supports vendor implementations to focus on those requirements within the specification that are deemed necessary by the agency. It also supports consistent and uniformly usage by all relying parties/applications within the agency.

11. CONCLUSION

In this paper, we discussed a number of path development and validation issues related to the use of PKI credentials within the Federal Government. We presented a number of use cases where validation of digital certificates is crucial in the context of PIV. Finally an open, standards-based solution was proposed in an attempt to solve this validation issue.

12. ACKNOWLEDGMENTS

My thanks to Dr. Sarbari Gupta on supporting the refinement of the thoughts presented in this paper.

13. REFERENCES

[1] The White House, August 2004. Homeland Security Presidential Directive 12 - Policy for a Common Identification Standard for Federal Employees and Contractors.

DOI=http://www.idmanagement.gov/documents/HSPD-12.htm

[2] National Institute of Standards and Technology, March 2006. FIPS 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors.

DOI=http://www.csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

[3] National Institute of Standards and Technology, March 2006. Special Publication 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)

DOI=http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf

[4] Physical Access Interagency Interoperability Working Group, July 2004. Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems, v2.2

[5] IETF, December 2007. RFC-5055 – Server-Based Certificate Validation Protocol

DOI=http://www.ietf.org/rfc/rfc5055.txt

[1] The component that performs this function is referred to as a Caching Status Proxy in SP 800-116.