pennsylvania
JUSTICE NETWORK

JNET Public Key Infrastructure (PKI) Background

FEDERATION ORGANIZATION OVERVIEW

March 22, 2013, Version 1.1

Revision History

Version	Date	Author(s)	Revision Notes
1.0	11/14/01	John Davenport	Initial version.
1.1	03/22/13	James Dyche	Updated version.

Table of Contents

1 JNET Public Key Infrastructure (PKI)

JNET has a mature Public Key Infrastructure (PKI), which is used by Pennsylvania justice agencies to issue and assign digital second factor credentials. These credentials are used to provide a greater level of assurance and enforce access rights to specific agency staff. The procedures and practices are defined by a Certificate Policy (CP), Certification Practice Statement (CPS), and various forms and procedures available on the JNET intranet website.

1.1 Certificate Generation, Storage and Maintenance

Symantec's (private) Managed Public Key Infrastructure (MPKI) solution is used to support JNET user and server certificates. The JNET PKI also provides key recovery to support non-repudiation. JNET requires the capability to download and install these certificates either by the end-user or by an authorized agency enroller. The capability also exists to install these certificates on the workstation, on a smart-card, on a hardware token, or on a virtual smart card. All four of these capabilities are in use by various justice agencies. Some of the justice agencies are using advanced smart-cards or hardware tokens.

1.2 Existing Certificates and Certificate Path

JNET currently issues X.509 version 3 certificates with 2048 bit keys. JNET issued the user certificates by a single Certificate Authority (CA) with a Common Name (CN) =Commonwealth of Pennsylvania JNET CA O = JNET. The JNET CA certificate was issued by CN = Commonwealth of Pennsylvania JNET Root CA O = JNET. JNET has retained the capability to add additional intermediary Certificate Authorities under the Commonwealth of Pennsylvania CA so that individual justice agencies may eventually become their own Certificate Authorities as required.

The JNET PKI currently generates two client certificates. One client certificate can be used for e-mail encryption and file encryption. The second client certificate can be used for client identification, authentication and signing of e-mail. To date JNET has issued approximately 35,000 certificates to 17,000 end users.

2 Agency Responsibilities

Each agency has at least one trained registrar who uses a web based administrative application built by JNET to process requests for JNET user access which have been previously approved by the users sponsor. The sponsor knows the end user and the sponsor knows the agency registrar.

The information on the access request form is stored in the JNET LDAP directory server during the registration phase. The most important piece of this information is the JNET user role which is used by all JNET agencies and applications to grant or deny access when a specific user presents their JNET digital credentials to a JNET agency website. Any new system must provide this registration information to the JNET LDAP directory.

3 Digital Certificates for Servers

All JNET servers have JNET issued digital certificates which are used to enable encrypted sessions. These certificates provided for secured communication between user, servers and appliances. The JNET service and message infrastructure connections use digital certificates to ensure the highest security level technically possible when data is in motion. All JNET traffic is encrypted from end to end.

4 Client Digital Certificates

New JNET user accounts created in the automated registration system do not, by default, include the downloading of digital certificates. JNET user accounts are created using a username and password and are automatically set to the appropriate user role depending on the nature of work being performed by the user.

4.1 Fixed Users

In contrast, the issuance of user digital certificates is a part of a more secured role approval process. These entitlements may be granted to any legally authorized JNET system user. For the user to be authorized they must have a role in supporting a criminal justice organization as defined by the Pennsylvania Criminal History Records Information Act (CHRIA). The user, sponsor, and registrar are administrative roles which can be granted to any JNET system user. An organization’s more security privileged users are required to obtain JNET PKI digital certificates for two-factor authentication. This authentication requirement meets the Federal Bureau of Investigation (FBI) Criminal Justice Information Systems (CJIS) Security Policy, which governs access to federal National Crime Information Center (NCIC) and Interstate Identification Index (III) records and databases. The JNET digital certificates are necessary to authenticate and verify a user’s identity within the JNET portal for access to resources that require a higher level of identity and authorization assurance.

User identity validation, vetting and enrollment requirements are increased at the more secured access levels to provide for higher-level of user assurance. When a more secured role request is submitted by the user, it is forwarded to the sponsor of the user organization for an initial approval. Once the Agency sponsor has approved the request, it is routed for additional approvals. Upon all approvals, the more secured users are then required to download their digital certificate. Registrars manage the digital certificate process upon user deactivation, non-compliance, suspension or termination.

JNET users with a more secured role will be required to present their digital certificate, in addition to their JNET user ID and password to satisfy the CJIS two-factor authentication requirements. All other users of JNET are required to present only their JNET user ID and password for single sign on access.

4.2 Roaming Users

Many JNET users are not assigned to a fixed desktop computer. JNET requires a number of methods to be available for storage of user certificates including hardware tokens, smart cards, and virtual smart cards. Currently, virtual smart cards are stored on an RSA Keon Web Passport server protected by an RSA ACE server using SecurID tokens for access. The JNET PKI environment is capable of integrating to and providing digital certificates to roaming end-users from a secured server.

4.3 Service Clients

The JNET PKI is used to provide client certificates to selected high-assurance web service client identities. JNET has infrastructure installed to support the certificate creation, installation, maintenance and management processes. The JNET infrastructure communicates with the Symantec infrastructure for the generation of certificates.

5 Cross Certification and Bridging

JNET is not currently cross certified or bridged with any other certificate authority. The JNET PKI is a stand-alone private CA owned and operated by the commonwealth.

JNET and the Commonwealth have considered a connection with the Federal Bridge Certification Authority (FBCA) as a participating state and a shared service provider, including mapping of JNET access levels with federal levels. JNET has made no formal commitments at this time. But, JNET recognizes the importance of providing a more unified credential to its user community. A large portion of JNET’s user base are also first responders which will need Personal Identification Verification Interoperable (PIV-I) credentials in order to participate in a national emergency.