pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Product Standards for Public Key Infrastructure

ITP Number STD-SEC014C	**Effective Date** November 20, 2006
Category Recommended Policy	**Supersedes**
Contact RA-ITCentral@pa.gov	**Scheduled Review** Annual

CURRENT STANDARDS

(These technologies meet the requirements of the current architecture and are recommended for use.)

Technology	Platforms	Technology Classification
Qualified vendors[1]	All Digital Certificates (Server, Personal)	Current
Microsoft Certificate Server[2]	Windows 2008 Digital Certificates (Server, Personal)	Current

[1] This standard is to be applied to the procurement and use of digital certificates which are intended to be presented (or to potentially be presented) to entities outside of the commonwealth enterprise. Such uses include, but are not limited to:

- Secure Socket Layer (SSL) to verify the identity of and to encrypt transmissions with Commonwealth and agency Web sites
- Digital Signatures
- Document encryption
- Use on Personal Identity Verification Interoperability (PIV-I) cards
- Two-factor authentication to non-Commonwealth systems (not necessarily including Commonwealth Virtual Private Networks (VPN) or wireless networking)
- Machine-to-machine authentication involving an outside entity

There are a number of vendors who now offer PKI and digital certificates that differ mainly in the details of their customer services. It is the intent of this ITB to enumerate vendor qualifications and certificate properties rather than to prescribe a

specific vendor. Agencies are encouraged to shop for the best pricing for these services.

To be qualified as an approved vendor, the vendor must be currently accredited as a shared service provider by the Federal PKI Bridge Authority. This certification provides some assurance as to the internal practices and viability of the vendor. The current list of such vendors can be found at the federal ID Management website.

Note: this requirement only pertains to the vendor's general qualifications. It does not require agencies to procure certificates that are cross-certified with the federal PKI bridge unless functionally necessary. These vendors offer other levels of services and digital certificates and the agency may purchase based upon their needs.

The certificates themselves must be at least 2048 bit. Requirements for issuance, escrow services, lifetime, etc. are determined by the type of certificate and its intended use; and should be reviewed and discussed with the agency business owner.

[2] Use of internally generated digital certificates (through an implementation of Microsoft Certificate Server) is permitted for applications internal to the commonwealth enterprise where two-factor authentication is the primary concern. Such applications would include enterprise and agency VPN and wireless networking. Refer to GEN-SEC013G, *Public Key Infrastructure* and the Commonwealth Certificate Policy.

Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication. Questions regarding this publication are to be directed to RA-itcentral@pa.gov.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision
Original	11/20/2006	Base Policy
Revision	6/22/2009	(Formerly SEC014F) Added Windows 2003 to Current Standards; update format
Revision	5/12/2012	Update the use of Windows 2008; expand the acceptable commercial PKI vendors
	4/2/2014	ITP Reformat
	9/4/2014	Updated ID Management URL