



Public Key Infrastructure Policy

Policy Number:	OCTO – 2053.0	Creation Date:	4/22/2016
		Approval Date:	4/22/2016
Effective Date:	4/22/2016	Revised Date:	

1. **Scope/Applicability:** This policy applies to all District of Columbia Agencies that implement a Public Key Infrastructure (PKI) in conjunction with any District of Columbia Government information systems connected to the internal District of Columbia Wide Area Network.
2. **Authority:** DC Official Code § 1-1401 et seq.
3. **Purpose:** This policy establishes the responsibilities and measures for the implementation and usage of Public Key Infrastructure (PKI) Certification Authority (CA) by the District of Columbia Government and its Agencies.
4. **Definition:**
 - 4.1. Public Key Infrastructure (PKI) makes use of digital certificates to provide proof of identity for the individual.
 - 4.2. A trusted Certificate Authority (CA) creates the certificate and digitally signs it using the CA's private key, thereby authenticating the identity of the requestor. A person can use his or her certificate for authentication with different applications, and the applications then check the user's identity by verifying the digital signature with the issuing CA.
5. **Policy Requirements:**
 - 5.1. The agency Chief Information Officer (CIO) or his/her designee must ensure that each private key is protected and stored in a safe location, such as in a security token or smart card secured by a Personal Identification Number (PIN).
 - 5.2. The agency CIO or his/her designee must ensure that the password restrictions stated in OCTO Password Management Policy (OCTO-2003.2) are imposed on the PIN of the security token / smart card to prevent unauthorized access to the private key inside.
 - 5.3. The agency CIO or his/her designee must ensure that procedures are in place to handle key life-cycle management, issuing and revoking of certificates, storing and retrieving certificates and list of certificates that have been revoked or are otherwise inactive (Certificate Revocation Lists).
 - 5.4. The CIO or his/her designee must ensure that when any private key is lost, expired, or compromised, a new private key is issued.
6. **Policy Maintenance:** The Office of the Chief Technology Officer (OCTO) is responsible for the maintenance, administration, and publication of this policy. OCTO must annually review this policy and update as needed to ensure the policy's technical relevance and regulatory compliance.
7. **Policy Enforcement:** OCTO is responsible for the enforcement of this policy. Agencies must actively participate in the audit of this policy when requested by the OCTO.
8. **Exemptions:** None.



District of Columbia Government – Office of the Chief Technology Officer

9. **Sanctions:** If OCTO discovers non-compliance with this policy, OCTO will:
- 9.1. Advise the DC Agency CIO of the non-compliance and assist the DC Agency CIO in developing a corrective action plan and a reasonable timeframe for its implementation.
 - 9.2. If the DC Agency CIO does not implement the corrective action plan within the stated timeframe, OCTO will escalate the matter to the DC Agency Director for immediate action and resolution.
 - 9.3. If the DC Agency Director does not resolve the policy non-compliance within his/her DC Agency, OCTO will refer the matter to the DC City Administrator for immediate action and resolution.
10. **Supporting Laws and Regulations:**
- 10.1. E-Government Act, (P.L. 107-347), Title III, Federal Information Security Management Act (FISMA).
 - 10.2. Privacy Act of 1974, 5 U.S.C. § 552a, Public Law No. 93-579.
 - 10.3. HIPAA Security Rule, 45 C.F.R. Part 164, Subpart C.
11. **Reference Documents:**
- 11.1. NIST FIPS 140-2, “*Security Requirements for Cryptographic Modules*”, May 2001.
 - 11.2. NIST FIPS 200, “*Minimum Security Requirements for Federal Information and Information Systems*”, March 2006.
 - 11.3. NIST IR 7298 Revision 2, “*Glossary of Key Information Security Terms*”, May 2013.
 - 11.4. NIST SP 800-32, “*Introduction to Public Key Technology and the Federal PKI Infrastructure*”, February 2001.
 - 11.5. NIST SP 800-53 Revision 4, “*Security and Privacy Controls for Federal Information Systems and Organizations*”, April 2013.



OFFICE OF THE CHIEF TECHNOLOGY OFFICER

District of Columbia Government – Office of the Chief Technology Officer

12. Policy Review:

Document History

Policy Number	Action	Effective Date	Next Review Date
OCTO – 2053.0	Published	4/22/2016	4/22/2017



13. Policy Acceptance:

Public Key Infrastructure Policy

Effective April 22, 2016

Archana Vemulapalli

4/22/16

**Archana Vemulapalli
Chief Technology Officer
Government of the District of Columbia**

Date