IT Security Procedural Guide: Key Management CIO-IT Security-09-43

Revision 4

April 13, 2020

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Revision 1 – November 19, 2008		
1	Eric Hummel	Additional References to x.509 Common Framework	Response to comments	1,6,16
		Revision 2 – February 25, 2016		
1	Salamon	Updated Policy and NIST references	Updated to current versions of CIO 2100.1, NIST SP 800-53, and NIST SP 800-57	Throughout
2	Wilson, Klemens	Updated GSA Logo, formatting, style changes	Updated GSA Logo, formatting and style.	Throughout
		Revision 3 – March 6, 2018		
1	Salamon	Removed NIST SP 800-21 and updated Policy references	NIST SP 800-21 withdrawn, updated to current CIO 2100.1	2, 7, 17
2	Salamon	Updated Procedural Guide links	Updated Procedural Guides	8
3	Dean	Changes throughout the document to correspond with current guide structure and formatting.	Updated to current guide structure, style, and formatting	Throughout
		Revision 4 – April 13, 2020		
1	Richards	Updated references and minor language clarifications	Scheduled update	Throughout
2	Salamon	Updated Section 2 to include specific requirements for key management	Operational feedback	7
3	Salamon	Scope updated in Section 1.2	Operational feedback	3

Approval

IT Security Procedural Guide: Key Management, CIO-IT Security-09-43, Revision 4 is hereby approved for distribution.

X DocuSigned by: Bo Berlas FD71792616154 4F...

Bo Berlas
Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Security Engineering Division (ISE) at SecEng@gsa.gov

Table of Contents

1 Introduction

Encryption is an important tool used to meet security control requirements in the Federal Information Security Modernization Act (FISMA) of 2014, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations",* and the General Services Administration (GSA) Order CIO 2100.1, "GSA *Information Technology (IT) Security Policy*". When used to protect sensitive information, Federal systems must use encryption that meets the requirements of the Federal Information Processing Standards (FIPS) 140-2, "*Security Requirements for Cryptographic Modules*." Once a system has been designed and deployed using FIPS compliant technologies it must be operated following documented procedures to ensure keys are created, stored, retired, revoked and otherwise managed in a consistent and secure manner.

The NIST promulgated FIPS 140-2 to ensure that encryption technology meets minimum standards when protecting sensitive data on Federal networks and systems. All cryptographic modules used in Federal systems must meet the standards in FIPS 140-2. FIPS 140-2 provides a certification path for vendors of cryptographic modules. Certification ensures that the standards are met in the specific vendor implementation. FIPS does not specify procedures and processes for management of these systems. General guidance is provided in NIST SP 800-57, "*Recommendation for Key Management*", Part 1, Part 2, and Part 3. Appendix A contains a glossary to clarify terms used throughout this guide.

Encryption is used in IT systems to meet several security requirements. These include confidentiality of information in storage or in transit, integrity of files, authentication of people and systems, signatures to establish the pedigree of information, and many other applications. Encryption is often used as a small component of a larger application. There are various types of encryption. This guide focuses upon encryption that uses keys. Encryption algorithms and their associated keys are either symmetric or asymmetric. In symmetric key cryptography, the same key is used for both encryption and decryption. In asymmetric key cryptography, pairs of keys are used together; one to encrypt and the other to decrypt the content. Symmetric keys are faster and more suited to bulk encryption. Asymmetric keys are slower but are the foundation for public, private key systems including public key infrastructure (PKI). In both types of cryptography, access to keys must be carefully controlled. The confidentiality and integrity of key material is at least as important as the confidentiality and integrity of the data that it protects.

PKI systems should comply with the Federal Public Key Infrastructure Policy Authority (FPKIPA) X.509 Version 1.31, "*Certificate Policy For The U.S. Federal PKI Common Policy Framework*" standards for the creation, distribution and management of signed digital certificates. These certificates incorporate public keys and other information to ensure the authenticity of the digital signature and the contents of the certificate.

To prevent misuse or exploitation, keys should expire after a carefully chosen period of time. The time from creation to expiration is called the "cryptoperiod" of the key. Although the key

may be revoked before its expiration, the cryptoperiod is the longest that a key should remain valid.

In some applications, keys are generated frequently and used for a very short duration. In other cases, the keys are "persistent". Persistent keys are usually "bound" to a process, device, person or data set, and are used for an extended period. Persistent keys may be used to authenticate, encrypt data for extended periods, distribute other keys, and/or provide digital signatures. With the exception of bulk data encryption, most persistent keys are asymmetric where one key is designated as a generally available public key and the other is a carefully guarded private key.

Although all keys must be managed securely, persistent keys are of particular importance. This is because persistent keys exist over an extended period of time during which different people may manage them.

There are many ways of assigning roles and responsibilities for Key Management. FIPS 140-2 suggests, at minimum, a framework that includes a user role, a crypto-officer role, and a maintenance role. A separate audit role may also be appropriate.

1.1 Purpose

This guide will provide a framework to document operating procedures and processes that are required by GSA IT Security Policies, FISMA and FIPS 140-2[1]. These policies set general standards that must be adhered to. Other documents such as NIST 800-57 provide detailed recommendations for creating these procedures and processes. The Key Management guide recommends a consistent documentation framework that will help each project meet the policy requirements. The details of processes vary from system to system; however, basic roles, responsibilities, and task categories are common enough to benefit from standardized documentation. The purpose of this guide is to introduce a template for documenting the following set of common Key Management tasks:

- Setting Roles and Responsibilities
- Creating Keys
- Managing the Storage of Keys
- Distribution of Keys
- Changing Keys
- Archiving Keys
- Destruction of Keys

[1] Please note that while FIPS 140-3 has been released, implementing guidance is still in progress and FIPS 140-2 certificates will continue to be issued.

For information on designing or improving the procedures used in Key Management systems, see NIST SP 800-57, Part 2.

1.2 Scope

This guide is applicable to all systems that create, manage, and revoke persistent keys used to protect sensitive information. For the purpose of this guide, "persistent" keys have a cryptoperiod of more than three (3) months, and "sensitive" information includes the following:

- Personally Identifiable Information (PII) as defined by GSA policy
- Sensitive financial data including Payment Card Industry (PCI) data
- Data categorized as Controlled Unclassified Information (CUI), Sensitive But Unclassified (SBU), or For Official Use Only (FOUO)
- Authenticator data
- Any other information designated as sensitive by the data owner, GSA policy or federal regulation.

This guide is NOT applicable to systems that manage only the following:

- Keys that are created and managed automatically by software without operator intervention;
- Keys that are not a part of GSA systems;
- Keys that are not "persistent";
- Keys that are not used in the storage, transfer or authentication of "sensitive" information;
- Keys that are used in classified systems.
- Keys used for authenticating devices for actions that are low impact as defined in Section 3.2 of NIST SP 800-60 Volume 1, "*Guide for Mapping Types of Information and Information Systems to Security Categories."*

1.3 Policy

Selected governing policy statements from NIST/FIPS and GSA CIO 2100.1 applicable to Key Management procedures are listed in the following sections.

1.3.1 GSA IT Security Policy, CIO 2100.1

CIO Order 2100.1 Chapter 4, Policy for Protect Function, states the following:

Paragraph 3, Data security

a. All PII and PCI data, and business sensitive data as determined by the AO, and authenticators, including but not limited to passwords, keys, and tokens must be encrypted in storage.

c. All agency data on portable storage devices (e.g., USB flash drives, SD cards, external hard drives), must be encrypted with a FIPS 140-2 certified encryption module.

d. If it is a business requirement to store PII on GSA user workstations or mobile devices including, but not limited to notebook computers, USB drives, CD-ROMs/DVDs, personal digital assistants, PII must be encrypted using a FIPS 140-2 certified encryption module.

g. All sensitive information, such as PII, as deemed by the data owner, which is transmitted outside the GSA firewall, must be encrypted. Certified encryption modules must be used IAW FIPS 140-2, Security requirements for Cryptographic Modules.

h. An employee or contractor shall not physically take out PII from GSA facilities (including GSA managed programs housed at contractor facilities under contract), or access remotely (i.e., from locations other than GSA facilities), without written permission from the employee's supervisor, the data owner, and the IT system AO. Approvals shall be filed with the employee's supervisor. This applies to electronic media (e.g., laptops, USB drives), paper, and any other media (e.g., CDs/DVDs) that may contain PII.

q. When using password generated encryption keys, a password of at least 8 characters with a combination of letters, numbers, and special characters is required.

r. Systems implementing encryption must follow the Key Management procedures and processes documented in GSA CIO-IT Security-09-43: Key Management.

Paragraph 6, Protective technology

e. Protect digital media during transport outside of controlled areas using a certified FIPS 140-2 encryption module; non-digital media shall follow GSA personnel security procedures.

1.3.2 NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations

Control SC-12: Cryptographic Key Establishment and Management

Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with *NIST and FIPS requirements for key generation, distribution, storage, access, and destruction*.

Supplemental Guidance: Cryptographic Key Management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define Key Management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This

includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems. Related controls: SC-13, SC-17.

Control Enhancements: For high impact systems,

(1) *Cryptographic Key Establishment and Management | Availability*

The organization maintains availability of information in the event of the loss of cryptographic keys by users.

Supplemental Guidance: Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys (e.g., due to forgotten passphrase).

Control SC-13: Cryptographic Protection

Control: The information system implements *FIPS-validated or NSA-approved cryptography* in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Supplemental Guidance: Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.

Control SC-28 (1): Protection of Information at Rest | Cryptographic Protection

Control: The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of *(1) Personally identifiable information; (2) Payment Card Industry data; (3) Authenticators, including but not limited to passwords, keys, and tokens; (4) business sensitive data as determined by the data owner and approved by the AO* on *any system component, including databases (i.e., table, column, or field level) or applications*.

Supplemental Guidance: Selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category and/or classification of the

information. This control enhancement applies to significant concentrations of digital media in organizational areas designated for media storage and also to limited quantities of media generally associated with information system components in operational environments (e.g., portable storage devices, mobile devices). Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields). Organizations employing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions. Related controls: AC-19, SC-12.

1.3.3 FIPS 140-2, Security Requirements for Cryptographic Modules

Section 1.1, Security Level 1[2],

Security Level 1 provides the lowest level of security. Basic security requirements are specified for a cryptographic module (e.g., at least one Approved algorithm or Approved security function shall be used). No specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components. An example of a Security Level 1 cryptographic module is a personal computer (PC) encryption board.

Security Level 1 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an unevaluated operating system. Such implementations may be appropriate for some low-level security applications when other controls, such as physical security, network security, and administrative procedures are limited or nonexistent. The implementation of cryptographic software may be more cost-effective than corresponding hardware-based mechanisms, enabling organizations to select from alternative cryptographic solutions to meet lower-level security requirements.

Security Requirements (Security Level 1):	Description
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.
Roles, Services, and Authentication	Logical separation of required and optional roles and services. roles and services.
Operational	Single operator. Executable code. Approved integrity technique.

[2] Note that since GSA does not require cryptography higher than Security Level 1 for any of its applications, only Security Level 1 requirements are itemized here.

Security Requirements (Security Level 1):	Description
Environment	
Cryptographic Key Management	Key Management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization. Secret and private keys established using manual methods may be entered or output in plaintext form.

Section 4.3: Roles, Services, and Authentication

A cryptographic module shall support authorized roles for operators and corresponding services within each role. Multiple roles may be assumed by a single operator. If a cryptographic module supports concurrent operators, then the module shall internally maintain the separation of the roles assumed by each operator and the corresponding services. An operator is not required to assume an authorized role to perform services where cryptographic keys and CSPs are not modified, disclosed, or substituted (e.g., show status, self-tests, or other services that do not affect the security of the module).

Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module, and to verify that the operator is authorized to assume the requested role and perform the services within the role.

Section 4.3.3: Operator Authentication

Documentation shall specify:

- the authentication mechanisms supported by a cryptographic module,
- the types of authentication data required by the module to implement the supported authentication mechanisms,
- the authorized methods used to control access to the module for the first time and initialize the authentication mechanisms, and
- the strength of the authentication mechanisms supported by the module.

1.4 References

Federal Laws and Regulations:

- FIPS 140-2, "*Security Requirements for Cryptographic Modules*"
- NIST SP 800-57 Part 1 Revision 4, "*Recommendation for Key Management, Part 1: General*"
- NIST SP 800-57 Part 2 Revision 1, "*Recommendation for Key Management: Part 2 - Best Practices for Key Management Organizations*"
- NIST SP 800-57 Part 3 Revision 1, "*Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance*"

- NIST SP 800-60 Revision 1 Volume 1, "*Guide for Mapping Types of Information and Information Systems to Security Categories.*"
- FPKIPA Version 1.31, *"X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework"*

GSA Directives, Policies, and Procedures:

- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- GSA Order CIO 2180.2, "*GSA Rules of Behavior for Handling Personally Identifiable Information (PII)*"

2 Procedures

2.1 GSA Requirements for Key Usage

For keys within the scope of this document (see Section 1.4), the following are GSA requirements for key usage:

- Keys shall never be stored in source code or configuration files.
- Keys must be stored separately from the data that they are used to encrypt, either physically or logically (e.g. AWS KMS, HSM, key vaults, or custom isolation means as approved by OCISO).
- The details of key management are clearly identified in Section 10 of the SSP narrative and applicable NIST SP 800-53 controls [e.g. SC-12, SC-13, SC-28(1)] in Section 13.

2.2 Documenting Key Management Systems

This guide presumes that the system has been properly designed using validated FIPS 140-2 cryptographic modules. In addition to FIPS compliance, the development of the system should follow NIST SP 800-57 guidelines. PKI implementations should conform to the guidance in the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework. The design should securely integrate the validated technology with processes and procedures that ensure secure Key Management throughout the system lifecycle.

The following section provides a line-by-line description of elements in the Key Management System Instructions & Template. The template is a form with two sections. A completed procedural document will have a Section 1 that describes the overall system and its cryptographic components as they relate to the data protection objectives and IT environment. The completed procedural documentation will have a copy of Section 2 from the template for each persistent key type in the system. For example, in a system that generates public/private key pairs for differing purposes (e.g. data transmission and storage) a separate Section 2 must document each of these key *uses*, but not each of the keys. This is necessary because different key uses will require different parameters such as cryptoperiod and may involve different roles and individuals in the Key Management processes. **The details should be clearly identified in**

Section 10 of the SSP narrative and applicable NIST SP 800-53 controls [e.g. SC-12, SC-13, SC-28(1)] in Section 13.

Where possible refer to the documentation provided by the vendor. In some cases, items in the template may be "not applicable" (N/A). In other cases, the template should be extended to document additional aspects of the Key Management system procedures.

1. Section 1 - Key Management System
    a. System Description
        i. System Name
        ii. System Owner
        iii. Highest sensitivity level of data protected
        This information is part of the System Security Plan (SSP) on file with the ISSO.
        iv. Key Management Objectives
        Describe the data that is protected by keys in this system, the media where the data is encrypted and the duration of encryption.
        v. System description and operational environment
        Provide a brief description of the system, its business objectives and its operational environment (e.g. external facing, contractors, interconnection to other systems) or refer to a system design document.
        vi. FIPS 140-2 Validation Certificate
        The system must use a FIPS 140-2 compliant technology that has a valid certificate number listed in the NIST Cryptographic Module Validation Program. Certificate validation numbers are available at the Cryptographic Module Validation Program website.
        vii. Cryptographic system description
        Describe the functional components of the overall cryptographic system and explain how they work together to meet the Key Management Objectives. Include the vendor, a brief description of each component (Key stores, Certificate Authorities, algorithms, each hardware device and software used) and any cross certification agreements between systems. Use Vendor documentation as much as possible.
        viii. Constituent keys
        Give an appropriate name to each type of persistent key (or key pair) managed in the system. This name will identify documentation in Section 2. Only separate into unique key types that have different management procedures.
        ix. How are Key Management events audited?
            1. Who audits key creation, changes and retirement events?
            2. What parameters are audited?
            3. How are audit events stored?
            4. How often are audits performed?

The following sections are used to document the key lifecycle processes of each type of persistent encryption key in the system.

2. Section 2 - Key Management Lifecycle Processes
   a. Constituent Key Name
      The name given to a particular key named in Section 1(a)(viii).
   b. Key Creation Procedures
      i. Roles: Who initiates the creation of a key?
         Give the role of the person charged with creating keys.
      ii. What entity is "bound" to the key?
         Each key is associated with a particular entity. These might be the system, sub-system, data element of any size, person, a device or a link between any of these.
      iii. How is the "bound" entity authenticated?
         When a key is created, how is the identity of the "bound" entity (e.g. a person or device) established and authenticated?
      iv. What Algorithm is used?
         Search the Cryptographic Module Validation Program website for approved FIPS 140-2 cryptographic modules.
      v. Are new keys signed?
         If keys are signed, give the entity that provides the digital signature.
      vi. What is the "Cryptoperiod" of the key?
   c. Key Management Procedures
      i. Roles: Who has the right to send, store, change or update keys?
         Describe the roles that have permission to send, store, change or update keys handled by the module.
      ii. How are keys distributed?
         For example, are they transferred to users in encrypted messages, out-of-band (e.g. telephone message) or Key Server? How are they protected during distribution?
      iii. Where are keys stored?
         Include all locations where the persistent keys reside.
      iv. How are Secret keys protected from disclosure during storage?
         E.g., Key storage vault, Hardware Security Module, Encryption.
      v. How are keys changed or updated?
         Briefly describe the procedure for updating keys.
      vi. How is the change of keys authorized and authenticated?
         Which users can request a change of keys? How are they authenticated?
   d. Key Retirement Procedures
      i. Who has authority to revoke, destroy keys?
         Describe the roles that have permission to revoke, destroy keys handled by the module.
      ii. How and when are keys destroyed?
         Are they deleted from a key store or deactivated?
      iii. How are expired or revoked keys identified by the application?
         What procedures ensure that retired keys are not successfully used by the applications?

iv. How are key revocation lists distributed and accessed?
How are revocation lists distributed and how often? Are they accessed each time a key is used?
v. How and when are old keys archived?
Describe the archive process for keys.

The documentation of Key Management procedures is part of the system lifecycle. As a system is designed, procedures are required to ensure consistent and secure handling of keys. The identification of roles and designation of individuals to fill those roles is required. The ISSO of the system is responsible for ensuring these roles remain filled throughout the life of the system. Key Management procedural documentation for each system must be filed with both the ISSO and the System Administrator, and must be available to all individuals filling each role.

The Key Management System Instructions & Template offers one way of documenting recommended Key Management procedures. It is suggested that the template be utilized as a system is designed or to update existing documentation to improve audit compliance. Not all elements in the template are applicable to all Key Management systems.

Additional useful information is available in the following GSA IT Security Procedural Guides, located on the IT Security Procedural Guides website:

- CIO-IT Security-01-02, "*Incident Response*"
- CIO-IT Security-01-07, "*Access Control*"
- CIO-IT Security-01-08, "*Audit and Accountability*"
- CIO-IT Security-03-23, "*Termination and Transfer*"
- CIO-IT Security-14-69, "*SSL/TLS Implementation*"

3 Summary

Encryption is a required technical control for protecting moderate and high sensitivity data. Secure implementation of a cryptographic module that meets FIPS 140-2 standards must include documented procedures for creation, management and destruction of keys. This guide provides a framework for the documentation of these procedures. It is designed to be flexible enough to address the documentation requirements despite the diversity of uses of encryption in systems throughout GSA. The Cryptographic Module Validation Program website identifies compliant systems and operational procedures. FIPS 140-2 validation ensures that the vendor can supply appropriate procedural documentation.

Appendix A – Glossary and Acronyms

Asymmetric Key Algorithm

A cryptographic algorithm that uses two related keys - a public key and a private key. The secure characteristic of the key pair is that determining the private key from the public key is computationally infeasible. (Also known as Public Key algorithm)

Authentication

A process that establishes the origin of information, or vouches for an entity's identity. In a general information security context: Verifying the identity of a user, process, or device, often is a prerequisite to allowing access to resources in an information system [SP 800-53].

"Bound" entity

A key is generally created to identify, protect, authenticate or otherwise refer to specific entities. This may be a one-to-one or a one-to-many binding. Entities can include people, files, messages, systems, data or any other identifiable unit that requires cryptographic services.

Certificate Authority (CA)

The entity in a Public Key Infrastructure (PKI) that is responsible for issuing certificates and exacting compliance to a PKI policy.

Certificate Revocation List (CRL)

A list of certificates that have been issued by a Certification Authority (CA) but have been revoked prior to their stated expiration date.

Cryptoperiod

The time span during which a specific key is authorized for use or in which the keys for a given system or application may remain in effect.

Digital Signature

The result of a cryptographic transformation of data that, when properly implemented, provides the services of:

1. origin authentication,
2. data integrity, and
3. signer non-repudiation.

Key Distribution

The transport of a key and other keying material from an entity that either owns the key or generates the key to another entity that is intended to use the key.

Key Management

The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs, passwords) during the entire lifecycle of the keys, including their generation, storage, establishment, entry and output, and destruction.

Key Recovery

Mechanisms and processes that allow authorized entities to retrieve keying material from a key backup or archive.

Key Revocation

A process whereby a notice is made available to affected entities that keying material **should** be removed from operational use prior to the end of the originally established cryptoperiod of that keying material. (See Certificate Revocation List)

Personally Identifiable Information (PII)

Information about a person that contains some unique identifier, including but not limited to name or Social Security Number, from which the identity of the person can be determined. OMB Memorandum M-10-23 (June 25, 2010), updated the term "PII": "The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual."

See GSA Order CIO 2180.2, "*GSA Rules of Behavior for Handling Personally Identifiable Information (PII)"*

Private Key

A cryptographic key, used with a public key cryptographic algorithm that is uniquely associated with an entity and is not made public. In an asymmetric (public) cryptosystem, the private key is associated with a public key. The private key is known only by the owner of the key pair and is used to:

1. Compute the corresponding public key,
2. Compute a digital signature that may be verified by the corresponding public key,
3. Decrypt data that was encrypted by the corresponding public key, or
4. Compute a piece of common, shared data together with other information.

Public Key

A cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public. In an asymmetric (public) cryptosystem, the public key is associated with a private key. The public key may be known by anyone and is used to:

1. Verify a digital signature that is signed by the corresponding private key,
2. Encrypt data that can be decrypted by the corresponding private key, or
3. Compute a piece of shared data.

Symmetric Key

A single cryptographic key that is shared by both originator and recipient.

Symmetric key algorithm

A cryptographic algorithm that employs one shared key - a secret key. This key is used for both encryption and decryption.