EFFECTIVE DATE

(11-03-2023)

PURPOSE

(1) This transmits revised Internal Revenue Manual (IRM) 10.8.52, *Information Technology (IT) Security, IRS Public Key Infrastructure (PKI) X.509 Certificate Policy*.

MATERIAL CHANGES

(1) Roles and responsibilities was moved from IRM 10.8.52.2 to IRM 10.8.52.1.5.

(2) Treasury Policy Management Authority (PMA) was moved from IRM 10.8.52.2.1 to IRM 10.8.52.1.5.1.

(3) IRS PKI Program Management Office (PMO) was moved from IRM 10.8.52.2.2 to IRM 10.8.52.1.5.2.

(4) PKI Operations Program Manager was moved from IRM 10.8.52.2.3 to IRM 10.8.52.1.5.3.

(5) Treasury PKI Operational Authority was moved from IRM 10.8.52.2.4 to IRM 10.8.52.1.5.4.

(6) PKI Operational Staff was moved from IRM 10.8.52.2.5 to IRM 10.8.52.1.5.5.

(7) Registration Authority/Local Registration Authority was moved from IRM 10.8.52.2.6 to IRM 10.8.52.1.5.6.

(8) IRS Subscribers was moved from IRM 108.52.2.7 to IRM 10.8.52.1.5.7

(9) Relying Parties was moved from 10.8.52.2.8 to IRM 10.8.52.1.5.8.

(10) Other Participants was moved from IRM 10.8.52.2.9 to IRM 10.8.52.1.5.9.

(11) Treasury Root Certification Authority (TRCA) was moved from IRM 10.8.52.2.10 to IRM 10.8.52.1.5.10.

(12) Subordinate Certification Authorities was moved from IRM 10.8.52.2.11 to IRM 10.8.52.1.5.11.

(13) Certificate Status Servers was moved from IRM 10.8.52.2.12 to IRM 10.8.52.1.5.12.

(14) Repositories was moved from IRM 10.8.52.2.13 to IRM 10.8.52.1.5.13.

(15) Trusted Roles was moved from IRM 10.8.52.2.14 to IRM 10.8.52.1.5.14.

(16) Administrator was moved from IRM 10.8.52.2.15 to IRM 10.8.52.1.5.15.

(17) Officer was moved from IRM 10.8.52.2.16 to IRM 10.8.52.1.5.16.

(18) Auditor was moved from IRM 10.8.52.2.17 to IRM 10.8.52.1.5.17.

(19) Operator was moved from IRM 10.8.52.2.18 to IRM 10.8.52.1.5.18.

(20) Scope was moved from IRM 10.8.52.1.2 to IRM 10.8.52.1.7 Program Control.

(21) Objectives was moved from IRM 10.8.52.1.3 to IRM 10.8.52.1.7 Program Control.

EFFECT ON OTHER DOCUMENTS

IRM 10.8.52 dated August 22, 2022 is superseded. This IRM supersedes all prior versions of IRM 10.8.52. This IRM supplements IRM 10.8.1, *Information Technology (IT) Security Policy and Guidance,* and IRM 10.8.2, *Information Technology Security Roles and Responsibilities.*
Also, this IRM augments IT security controls as defined in IRM 10.8.22, *Information Technology (IT) Security, Web Server Security Policy*.

AUDIENCE

IRM 10.8.52 shall be distributed to all personnel who install, use or operate PKI services, and who store, process, or transmit IRS data. This policy applies to all employees, contractors, and vendors of the IRS.

Kaschit Pandya
Acting, Chief Information Officer

10.8.52
IRS Public Key Infrastructure (PKI) X.509 Certificate Policy

Table of Contents

10.8.52.1
(11-03-2023)
Program Scope and Objectives

(1) **Overview:** This Internal Revenue Manual (IRM), lays the foundation to implement and manage security controls and guidance for the use of Public Key Infrastructure (PKI) implementation within the Internal Revenue Service (IRS).

a. This manual is subordinate to IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*, and augments the existing requirements identified within IRM 10.8.1, as they relate to IRS Public Key Infrastructure (PKI) implementation.

(2) **Purpose of the Program** Develop and publish policies to protect the IRS against potential IT threats and vulnerabilities and ensure compliance with federal mandates and legislation.

(3) **Audience:** The provisions within this manual apply to:

a. All offices and business, operating, and functional units within the IRS.
b. Individuals and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers, which use or operate systems that store, process, or transmit IRS Information or connect to an IRS network or system.

(4) **Policy Owner:** Chief Information Officer

(5) **Program Owner:** Cybersecurity Threat Response and Remediation (an organization within Cybersecurity)

(6) **Program Goals**: Cyber Security Policy is responsible for the development and maintenance of IRS's enterprise information technology security policies. The IRM 10.8.X Series provides the minimum-security requirements to protect the confidentiality, integrity, and availability of data processed on IRS systems. IRMs are developed in accordance with applicable laws, policies, federal regulations, Office of Management and Budget (OMB), Treasury Directives (TDs), National Institute of Standards and Technology (NIST) Publications, and National Archives and Records Administration (NARA).

10.8.52.1.1
(08-22-2022)
Background

(1) This Internal Revenue Manual (IRM) establishes the minimum controls for Internal Revenue Service (IRS) Public Key Infrastructure (PKI) implementation used to protect federal systems and data.

(2) IRM 10.8.52 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS Information Technology Cybersecurity.

10.8.52.1.2
(08-22-2022)
Authority

(1) The IRS shall operate in accordance with the *Department of the Treasury (Treasury) Public Key Infrastructure (PKI) X.509 Certificate Policy* and *Treasury Only Locally Trusted (OLT) Public Key Infrastructure (PKI) X.509 Certificate Policy*. The Treasury Certificate Policy can be found at: *https://pki.treasury.gov/cert_policies.htm*

10.8.52.1.3
(11-03-2023)
Roles and Responsibilities

(1) IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*, defines IRS-wide roles and responsibilities related to IRS information and computer security, and is the authoritative source for such information.

(2) The supplemental roles provided below are derived from the Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy.

10.8.52.1.3.1
(11-03-2023)
Treasury Policy Management Authority (PMA)

(1) The Treasury Policy Management Authority (PMA) resides in the Office of the Chief Information Officer (OCIO) for Treasury. The Treasury PMA provides management authority over Treasury's PKI and Shared Service Programs. As such, the Treasury PMA ensures the conformity to central Department policy for PKI implementation and operation to ensure installation of one PKI solution throughout Treasury. The Treasury PMA is responsible for:

a. The Treasury PKI Certificate Policy (CP).
b. Review, approval, and compliance review of all Treasury Certification Practices Statement (CPS) issued and maintained in support of the Treasury Public Key Infrastructure(TPKI).
c. Approval of any subordinate or other certificate authorities created in support of other Agencies and Bureaus to support digital technologies for authentication, signing, encryption, access, or authorizations.
d. Oversight compliance management of the TPKI and all Treasury Certificate Authority (CA) assigned by the Treasury Root Certification Authority (TRCA).
e. Internal Auditing and compliance oversight of TPKI operations.
f. Determinations regarding CP and CPS compliance and assurance level with the Treasury CP.
g. Review and approval of Treasury or other Entities CPs and CPS pertaining to CAs being considered for cross certification with the TRCA.

(2) In the event the Treasury PMA makes the determination that other, non-Department of the Treasury Certificate Policies offer appropriately equivalent levels of assurance to the Treasury Certificate Policies, the TPKI may respond to such decisions by methods including, but not limited to the following:

a. Issuing cross certificates to other PKIs asserting other policies.
b. Including certificates issued by other PKIs and asserting other Certificate Policies, in Department of the Treasury Certificate Status Authorities (CSAs).
c. Recommending CAs asserting other Certificate Policies for inclusion in Department of the Treasury application trust lists.

(3) The PMA shall make information regarding such equivalency determinations widely available to Department of the Treasury Subscribers and Relying Parties.

(4) The PMA guidance in this section comes directly from Department of the Treasury PKI policy.

(5) The PMA for OLT PKIs is the Treasury PMA.

a. Each OLT PKI shall identify a person or organization as overall responsible for the implementation and operation of the OLT PKI – OLT Management Authority (MA).
b. The OLT MA is responsible for developing a certificate practice statement (CPS) for the OLT PKI and obtaining approval of the CPS from the Treasury PMA prior to beginning operation of the OLT PKI. The CPS will address all the applicable sections of the TREASURYCP.

c. An OLT PKI may be comprised of a single issuing CA (self-signed) or multiple issuing CAs with CA signing certificates issued by a locally implemented Root CA.

10.8.52.1.3.2 (11-03-2023)
IRS PKI Program Management Office (PMO)

(1) The IRS PKI Program Management Office (PMO) shall be established within the IRS Information Technology (IT) organization, ACIO Cybersecurity.

(2) The PMO shall enforce Department of the Treasury and IRS PKI policy. The PMO shall represent the interests of the PKI Program and the IRS in all internal and external matters relative to PKI technology. The PMO shall:

a. Provide oversight and coordination of the IRS CA on behalf of the IRS.
b. Create, publish, and maintain all CPS pertaining to the IRS PKI.
c. Participate in audit management activities (e.g., Government Accountability Office (GAO) and Treasury Inspector General Tax Administration (TIGTA) in accordance with the IRS IT organization Strategy and Planning, Risk Management organizational processes and procedures for audit management, reporting, and oversight.
d. Provide Bureau Registration Authority (RA) and Local Registration Authority (LRA) training.
e. Provide Bureau RA and LRA guidance.

(3) The PMO shall establish SOPs for the management and secure operation of the PKI program and assets per IRM 10.8.1.

(4) For additional information regarding the PKI PMO and SOPs, please email the Cybersecurity Front Door at *IT Cybersecurity Front Door or contact the PMO through the **IT PKI Management Solutions* mailbox.

10.8.52.1.3.3 (11-03-2023)
PKI Operations Program Manager

(1) The position of PKI Operations Program Manager shall be established within the IRS IT organization, Enterprise Operations (EOps).

(2) The PKI Operations Program Manager shall be responsible for the operation, control and management of all IRS subordinate CAs. In addition, the PKI Operations Program Manager shall:

a. Establish the operational requirements for the IRS subordinate CAs in the CPS.
b. Make recommendations to the PMO and PMA regarding corrective actions or other measures that might be appropriate for the IRS subordinate CAs.
c. Provide acquisition support to maintain PKI technology.
d. Provide costing support and seek funding as required to maintain technologically current hardware and software levels for IRS PKI.
e. Stay abreast of new PKI technology and requirements (i.e., Homeland Security Presidential Directive 12 (HSPD-12)) and participate in technology summits and meetings dealing with IRS PKI, including interdependencies with Department of the Treasury PKI.
f. Work with IRS IT organization communications to provide customer advisories in advance of any downtime or potential impact. Refer to IRM 10.8.1 for additional information regarding incident reporting requirements if applicable.

g. Coordinate PKI activities with the IRS IT organization, Enterprise Services and ensure that the IRS PKI complies with the IRS Enterprise Architecture.
h. Select the PKI operational staff to operate and maintain the IRS PKI CAs on behalf of the IRS, in coordination with the PKI PMO.

(3) The PKI Operations Program Manager can be contacted through the **PKI Program Office* mailbox.

10.8.52.1.3.4
(11-03-2023)
Treasury PKI Operational Authority

(1) The Treasury Chief Information Officer (CIO) has designated the Bureau of Public Debt, as the Treasury PKI Operational Authority (PKI OA).

(2) The PKI OA is responsible for the operation, and control of the TRCA and the operation, control and management of all subordinate CAs.

(3) The PKI OA is responsible for the following:

a. Establishing the operational requirements for the subordinate CAs in the CPS.
b. Making recommendations to the PMO and PMA regarding corrective actions or other measures that might be appropriate for the TPKI.

(4) The PKI OA established the PKI Program Team.

a. The PKI Program Team is the organization that operates and maintains the Treasury PKI CAs on behalf of the Treasury, subject to the direction of the PMA.

Note: The PKI OA guidance stated above comes directly from the Treasury PKI policy.

10.8.52.1.3.5
(11-03-2023)
PKI Operational Staff

(1) The PKI operational staff shall be established within the IRS IT organization, EOPs. The PKI operational staff shall administer the IRS's PKI from an operation perspective and shall:

a. Administer PKI and IRS PKI CAs.
b. Publish certificates.
c. Perform issuance and revocation of certificates to subordinate CAs, and to Subscribers from those CAs.
d. Manage certificate repositories and certificate and authority revocation lists.
e. Ensure that all aspects of CA services, security/access controls, operations and infrastructure related to certificates issued under the CP are performed in accordance with the requirements, representations, and warranties of the CP, the appropriate CPS, IRS policy, and Department of the Treasury policy.
f. Manage technical operational issues, including:

- Set up and administer subordinate CAs
- Implement the PKI and components
- Coordinate installation
- Administer the IRS's PKI from a key management perspective, including rekey of CA signing material in cooperation with the PMO

- Security Assessment and Authorization activities, in accordance with IRM 10.8.1

g. Shall support the PMO/PMA with the creation and revision of Certification Practices Statements, including evaluation of changes at the requested of the PMA or PMO, and recommendation for approval/disapproval to the PMA, to maintain the level of assurance and operational practicality.

h. Establish operational guidance and procedures for subordinate CAs.

i. Perform Certification and Accreditation activities, including:

- Preparation of system security plans
- Conduct annual system security self-assessment reviews and prepare Plans of Action and Milestones (POA&M)

j. Perform Backup and Contingency planning, including:

- System backup
- Key recovery
- Key escrow
- Disaster recovery planning
- Perform contingency planning to ensure continuity of operations

k. Participate in the Federal PKI Policy Authority Share Service Program working group to ensure compliance to the Federal model.

l. Conduct liaison with other government agencies concerning SSP PKI matters.

m. Act as a focal point for IRS participation in the Federal PKI Policy Authority Share Service Program.

10.8.52.1.3.6 (11-03-2023)
Registration Authority/Local Registration Authority

(1) The IRS RA and LRA are entities recognized as authorized to collect and verify users' identity and information that is to be entered into the Subscriber's public key certificates. The key difference between RAs and LRAs is the nature and degree of their respective access to the IRS and treasury PKI CAs.

(2) RA functions as the Officer trusted role of the TPKI and IRS PKI CA.

(3) The EOps Program Manager(PM) appoints all RA and LRA for TPKI and IRS CA from members of the PKI operational staff, or other IRS personnel as necessary.

(4) The EOps PM shall maintain a current active list of all RAs and provide that list to the PMO when requested.

(5) Both Certification Authorities and Registration Authorities are termed "Certificate Management Authorities (CMA)." This policy uses the term "CMA" when a function may be assigned to either a CA or an RA, or when a requirement applies to both CAs and RAs. The term "Registration Authority" includes entities such as Local Registration Authorities (a.k.a. Trusted), unless otherwise specified.

(6) The division of Subscriber registration responsibilities between the CA and RA may vary among implementations of this CP, as outlined in the appropriate CPS. All CMAs shall protect personal information from unauthorized disclosure as mandated by the Privacy Act of 1974, as amended.

10.8.52.1.3.7
(11-03-2023)
IRS Subscribers

(1) A Subscriber is the entity (the user to whom, or device to which, a certificate is issued) whose Distinguished Name (DN) appears as the subject in a certificate, and who asserts that they use the key and certificate in accordance with this policy. Although CAs can be considered as PKI subjects, the term "Subscriber" as used in this document refers only to entities who request certificates for uses other than signing and issuing certificates or certificate status information.

(2) PKI Subscribers include but are not limited to the following categories of entities that may wish to conduct official Department business:

a. IRS personnel: Direct Hire, Part-time/Intermittent/Temporary (PIT) employees, contractors, commercial vendors, and agents.
b. Federal Government departments and agency personnel, and their contractors and agents.
c. Non-Person Entities (NPE) such as, workstations, guards and firewalls, routers, trusted servers (e.g., database, domain controller, File Transfer Protocol (FTP), and World Wide Web (WWW)), and other infrastructure components. These components shall be under the cognizance of humans, who accept the certificate and are responsible for the correct protection and use of the associated private key.

Note: For the Automated Certificate Issuance and Life-Cycle Management (ACM) process, the NPE Sponsor is not responsible for protecting the NPE's private key or ensuring proper use of each sponsored NPE's key and certificate.

(3) A PKI Sponsor fills the role of a Subscriber for groups, organizations, disabled personnel, and non-human system components named as public key certificate subjects.

a. The PKI Sponsor works with the CMAs to register the above elements.
b. The PKI Sponsor is responsible for meeting the obligations of Subscribers as defined throughout this document.

(4) TRCA Subscribers include only PMA, PMO or other PKI Program Team personnel and, when determined by the PMA, PKI network or hardware devices.

(5) The Treasury may issue certificates to Subscribers other than employees of the U.S. Government, such as commercial vendors and agents, at the convenience of the Government and without fee, when those Subscribers have a bona fide need to possess a certificate issued by a Treasury CAs.

10.8.52.1.3.8
(11-03-2023)
Relying Parties

(1) A Relying Party uses a Subscriber's certificate to verify or establish the identity and status of an individual, the integrity of a digitally signed message, the identity of the creator of a message, and confidential communications with the Subscriber.

(2) The Relying Party relies on the validity of the binding between the Subscriber's name and public key.

a. A Relying Party may use information in the certificate (such as CP Identifiers) to determine the suitability of the certificate for a particular use.

(3) The Relying Party shall be responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information.

a. For a Certificate Policy, the relying party may be any Entity that wishes to validate the binding of a public key to the name of a federal employee, contractor, other affiliated personnel or device.

(4) This CP makes no assumptions or limitations regarding the identity of Relying Parties. While Relying Parties may be Subscribers, Relying Parties are not required to have an established relationship with the IRS PKI CA, Treasury PKI CA, Federal Bridge Certification Authority (FBCA) or another Entity CA.

10.8.52.1.3.9
(11-03-2023)
Other Participants

(1) All IRS CAs operating under this policy require the services of other security and application authorities, such as compliance auditors and attribute authorities.

a. Each IRS CA shall identify, in its CPS, the parties responsible for providing such services and the mechanisms used to support these services.

10.8.52.1.3.10
(11-03-2023)
Treasury Root Certification Authority (TRCA)

(1) TRCA shall not be part of an OLT PKI. Where an OLT PKI only supports a single Treasury Bureau, the root (if separate from the issuing CA) shall be operated to meet the requirements of this addendum. If there is a need for an OLT PKI to span multiple Treasury organizations, the organizations requiring the PKI shall work with the Treasury PMA to determine the appropriate place to operate the Root. A Root operated in support of multiple organizations shall be operated offline and conform to the requirements for Treasury Medium. In the future, it is anticipated that all Treasury OLT PKIs will be consolidated into a single PKI operated under a single Treasury Root CA.

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional requirements.

10.8.52.1.3.11
(11-03-2023)
Subordinate Certification Authorities

(1) Treasury's Subordinate Certification Authorities are responsible for all aspects of the issuance and management of certificates to users and devices, including control over the enrollment process, the identification and authentication process, the certificate manufacturing process, publication of certificates, revocation of certificates, and rekey.

(2) A CA, which issues certificates that assert the policies defined within the Treasury's CP, shall conform to the stipulations of the Treasury's CP and this document, including the following:

a. Providing to the appropriate authorities a CPS, as well as any subsequent changes, for conformance assessment.
b. Maintaining its operations in conformance to the stipulations of the approved CPS.
c. Ensuring that registration information is accepted only from RAs/LRAs who understand and are obligated to comply with this policy, and operating under an approved CPS.

d. Including only valid and appropriate information in the certificate, and to maintaining evidence that due diligence was exercised in validating the information contained in the certificate.
e. Ensuring that all Subscribers (government and non-government) are informed of their obligations, including the consequences of not complying with those obligations, and revoking the certificates of Subscribers found to have acted in a manner counter to those obligations.
f. Operating or obtaining the services of an online repository that satisfies the obligations defined within the Treasury's CP and this document, and informing the repository service provider of those obligations if applicable.

10.8.52.1.3.12
(11-03-2023)
Certificate Status Servers

(1) The IRS CA may optionally include an authority that provides status information about certificates on behalf of the IRS PKI CAs through online transactions. Examples include Online Certificate Status Protocol (OCSP) responders, termed Certificate Status Servers (CSS).

(2) Where certificates identify CSS as an authoritative source for revocation information, the operations of that authority shall be within the scope of this policy. This policy does not cover OCSP servers that are locally trusted.

a. A CSS shall assert all the policy Object Identifiers (OIDs) for which it is authoritative.

10.8.52.1.3.13
(11-03-2023)
Repositories

(1) The Department of Treasury (Treasury) PKI CA infrastructure shall serve as the primary repository of information for Subscribers and Relying Parties.

a. For all Treasury PKI CAs, this repository is the Treasury directory infrastructure.
b. The PKI Program Team web site (*https://pki.treas.gov*) serves as the primary repository to publish public information.
c. Network directories and all other repositories used to disseminate relevant information will:

- Maintain availability necessary to distribute current certificate information in a manner consistent with the posting and retrieval stipulations defined within the Treasury's CP and this policy.
- Implement access controls on all CA repositories to provide sufficient protection as described within the Treasury's CP and this policy.

(2) The PKI Program Team may use a variety of mechanisms for posting information into a repository as required by the Treasury's CP. These mechanisms at a minimum include:

a. A Directory Server System that is also accessible through the Lightweight Directory Access Protocol (LDAP).
b. Availability of the information as required by the certificate information posting and retrieval stipulations of this CP.
c. Access control mechanisms when needed to protect repository information as described in later sections.

10.8.52.1.3.14
(11-03-2023)
Trusted Roles

(1) A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles shall be extraordinarily responsible and above reproach or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust in the entire PKI.

a. There are two approaches to increase the likelihood of successfully carrying out these roles:

- The first approach is to ensure that the person filling the role is trustworthy and properly trained
- The second is to distribute the functions of the role among several people, so that any malicious activity requires collusion.

(2) The requirements of this policy are defined in terms of four roles. (Note: the information derives from the Certificate Issuing and Management Components (CIMC) Protection Profile.)

a. Each CA shall maintain lists, including names, organizations, contact information, and copies of appointment memoranda of those who act in these trusted roles, and shall make them available during compliance audits.
b. The CA will make this information a part of the permanent records of the CA. However, the CA shall not maintain personnel or investigative records requiring protection under the Privacy Act.

- Administrator – authorized to install, configure, and maintain the CA; establish and maintain Subscriber accounts; configure profiles and audit parameters; and generate component keys
- Officer – authorized to request or approve certificates or certificate revocations
- Auditor – authorized to maintain audit logs
- Operator – authorized to perform system backup and recovery

(3) Each CA within an OLT PKI shall have specific individuals identified to perform the Officer, Administrator, and Auditor roles. The Officer and Administrator roles are referred to collectively as CA Operators. (Treasury OLT PKI Policy)

(4) The following subsections provide a detailed description of the responsibilities for each.

10.8.52.1.3.15
(11-03-2023)
Administrator

(1) The Administrator role is responsible for the following:

a. Installation, configuration, and maintenance of the CA,
b. Establishing and maintaining CA system accounts,
c. Configuring certificate profiles or templates and audit parameters,
d. Generating and backing up CA keys.

(2) Administrators do not issue certificates to Subscribers

10.8.52.1.3.16
(11-03-2023)
Officer

(1) The Officer (a.k.a. Security Officer, Registration Authority) role is responsible for issuing certificates, that is:

a. Registering new Subscribers and securely requesting the issuance of certificates,
b. Verifying the identity of Subscribers, validity of documentation, and accuracy of information included in certificates,
c. Approving and executing the issuance of certificates,
d. Requesting, approving and executing the revocation of certificates,
e. Receiving, controlling, and distributing Subscriber certificates on FIPS 140 Level 2 compliant hardware tokens (cryptographic modules containing the CA private key), as specified in this CP and the applicable CPS.

(2) The Officer also performs the administration and operation of the RA workstation.

10.8.52.1.3.17
(11-03-2023)
Auditor

(1) The Auditor role is responsible for the following:

a. Reviewing, maintaining, and archiving audit logs,
b. Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS.

10.8.52.1.3.18
(11-03-2023)
Operator

(1) The Operator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

10.8.52.1.4
(11-03-2023)
Program Management and Review

(1) The IRS Security Policy Program establishes a framework of security controls to ensure the inclusion of security in the daily operations and management of IRS IT resources. This framework of security controls is provided through the issuance of security policies via the IRM 10.8.x series and the development of technology specific security requirement checklists. Stakeholders are notified when revisions to the security policies and security requirement checklists are made.

(2) It is the policy of the IRS:

a. To establish and manage an Information Security Program within all its offices. This policy provides uniform policies and guidance to be used by each office.
b. To protect all IT resources belonging to, or used by, the IRS at a level commensurate with the risk and magnitude of harm that could result from loss, misuse, or unauthorized access to that IT resource.
c. To protect its information resources and allow the use, access, disposition, and disclosure of information in accordance with applicable laws, policies, federal regulations, Office of Management and Budget (OMB) guidance, Treasury Directives (TDs), NIST Publications, National Archives and Records Administration (NARA) guidance, other regulatory guidance, and best practice methodologies.
d. To use best practices methodologies (such as Capability Maturity Model Integration (CMMI), Enterprise Life Cycle (ELC), Information Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS)) to document and improve IRS IT process and service efficiency and effectiveness.

10.8.52.1.5
(11-03-2023)
Program Controls

(1) This IRM applies to all IRS information and systems, which include IRS production, development, test, and contractor systems. For systems that store, process, or transmit classified national security information, refer to IRM 10.9.1, *Classified National Security Information (NSI)*, for additional procedures for protecting classified information.

(2) The IRS shall ensure that:

a. The product (e.g., software, hardware) and version selected are in accordance with IRS Enterprise Architecture (EA) Enterprise Standards Profile (ESP) that dictates the official products and versions within the IRS; and
b. The application or system version is a version for which the vendor still offers standardized technical support.

(3) This IRM establishes the minimum baseline security policy and requirements for all IRS IT assets in order to:

a. Protect the critical infrastructure and assets of the IRS against attacks that exploit IRS assets.
b. Prevent unauthorized access to IRS assets.
c. Enable IRS IT computing environments that meet the security requirements of this policy and support the business needs of the organization.

(4) It is acceptable to configure settings to be more restrictive than those defined in this IRM.

(5) To configure less restrictive requirements requires a risk-based decision (RBD). Refer to the Risk Acceptance and Risk-Based Decisions section within this IRM for additional guidance.

(6) In the event there is a discrepancy between this policy and IRM 10.8.1, IRM 10.8.1 has precedence, unless the controls/requirements in this policy are more restrictive, or otherwise noted.

(7) To configure less restrictive requirements requires a risk-based decision (RBD). Refer to the Risk Acceptance and Risk-Based Decisions section within this IRM for additional guidance.

10.8.52.1.6
(11-03-2023)
Terms and Acronyms

(1) Refer to Exhibit 10.8.52-2 for a list of terms, acronyms, and definitions.

10.8.52.1.7
(11-03-2023)
Related Resources

(1) Refer to Exhibit 10.8.52-3 for a list of related resources and references.

10.8.52.2
(11-03-2023)
Risk Acceptance and Risk-Based Decision

(1) Any exception to this policy requires that the Authorizing Official (AO) make a Risk-Based Decision.

#
#
#

#
#

#
#

(3) Refer to IRM 10.8.1 for additional guidance about risk acceptance.

10.8.52.3
(02-09-2015)
IRS PKI Infrastructure

(1) The IRS shall use a dual PKI structure: external and internal. The IRS external certification services shall be provided by the Treasury PKI, and the internal certification services shall be provided by the internal IRS PKI. (IRS Defined)

10.8.52.4
(08-22-2022)
Certificate Usage

(1) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.4.1
(08-22-2022)
Appropriate Certificate Usage

(1) NPE Certificates issued by an OLT PKI support PK-enabled application with a locally defined environment. Examples include: (Treasury OLT PKI Policy)

- Performing device authentication to the local domain
- Signing and key encypherment of data retained locally
- A web server only accessed from within the local domain
- Device-to-device authentication internal to the domain

(2) OLT certificates are only issued by an OLT PKI to individuals for use cases specifically approved by the OLT PMA. The OLT MA provides the details of the specific use case to the OLT PMA. Examples of use cases include: (Treasury OLT PKI Policy)

- Certificates for people who perform administrative functions
- Signing of code that is only intended for local use

(3) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.4.2
(08-22-2022)
Prohibited Certificate Usage

(1) Certificates issued by an OLT PKI shall not be used in any circumstance where the certificate needs to be trusted outside the local environment for which the PKI is established. Examples include: (Treasury OLT PKI Policy)

- A PK-enabled web server accessed from outside the local domain

(2) Certificates issued by an OLT PKI to individuals shall not be used for any purpose not specifically approved by the OLT PMA. (Treasury OLT PKI Policy)

(3) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.5
(08-22-2022)
Identification and Authentication

(1) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.5.1 (08-22-2022) **Naming**

(1) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.5.1.1 (08-22-2022) **Types of Names**

(1) In order to ensure uniqueness of the names across OTL PKIs, each OLT MA shall obtain approval for the OLT PKI namespace from the Treasury PMA. This approval shall consider both the PKI namespace and Domain Name Service (DNS) names. (Treasury OLT PKI Policy)

(2) OLT PKIs may use either Domain component or X.500 Domain Names. (Treasury OLT PKI Policy)

(3) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.5.1.2 (08-22-2022) **Need for Names to Be Meaningful**

(1) No further stipulations beyond the Treasury Basic Policy. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.5.1.3 (08-22-2022) **Anonymity or Pseudonymity of Subscribers**

(1) No further stipulations beyond the Treasury Basic Policy. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.5.1.4 (08-22-2022) **Rules for Interpreting Various Name Forms**

(1) No further stipulations beyond the Treasury Basic Policy. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.5.1.5 (08-22-2022) **Uniqueness of Names**

(1) Name uniqueness for NPE certificates is enforced within the OLT PKI's approved CA namespace by use of approved DNS names for end entities. Name uniqueness for individuals is enforced by the RA by verifying that there are no name collisions for previously issued certificates issued within the OLT PKI to another individual. (Treasury OLT PKI Policy)

(2) Uniqueness across Treasury is enforced by separation of namespaces among OLT PKIs. (Treasury OLT PKI Policy)

(3) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.5.2 (08-22-2022) **Initial Identity Validation**

(1) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.5.2.1
(08-22-2022)
Method to Prove Possession of Private Key

(1) No further stipulations beyond the Treasury Basic Policy. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.5.2.2
(08-22-2022)
Authentication of Organization Identity

(1) No further stipulations beyond the Treasury Basic Policy. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.5.2.3
(08-22-2022)
Authentication of Individual Identity

(1) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.5.2.3.1
(08-22-2022)
Authentication of Human Subscribers

(1) A CA Operator authenticates an individual to receive a PKI certificate from an OLT PKI; by (Treasury OLT PKI Policy)

a. Receiving an email, digitally signed by the individual using a signing certificate issued by the Treasury PKI,
b. Performing face-to-face identity proofing (directly, or through an approved Trusted Agent or Notary) as required for Basic Assurance in Section 3.2.3.1 of the Treasury CP.

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.5.2.3.2
(08-22-2022)
Authentication of Devices

(1) OLT certificates may be issued on the basis of electronically authenticated entity subscriber requests using Certificate enrollment protocols that support automated and semi-automated mechanisms for authenticating these requests. (Treasury OLT PKI Policy)

- PKI Sponsor may request enrollment using digitally-signed e-mail using a Personal Identity Verification (PIV) certificate.
- Microsoft's auto-enrollment protocol includes limited support for authenticating requests from devices. This authentication is deemed sufficient for issuance of Internet Protocol Security(IPSec), Domain Controller, and workstation device certificates.
- Network Device Enrollment Services (NDES) enrollment shall be authenticated using credentials of the subscribing device submitting its request for a certificate to the NDES Server.
- Web Enrollment shall be authenticated using the PIV credentials of the administrator submitting the request for device certificates to the Web Enrollment Server.

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.5.3 (08-22-2022) **Identification and Authentication For Re-key Request**

(1) Refer to Treasury PKI X.509 Certificate Policy for guidance on Identification and Authentication for Re-key Request.

10.8.52.5.3.1 (08-22-2022) **Identification and Authentication for Routine Re-key**

(1) OLT end entity certificates may be rekeyed through use of the current private key or via the initial enrollment method. (Treasury OLT PKI Policy)

(2) OLT maximum end entity certificate and key life is three (3) years. (Treasury OLT PKI Policy)

(3) OLT end entity certificates may be re-keyed indefinitely. (Treasury OLT PKI Policy)

(4) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.6 (08-22-2022) **Certificate Lifecycle**

(1) No further stipulations beyond the Treasury basic policy. (Treasury OLT PKI Policy)

10.8.52.7 (08-22-2022) **Facility, Management, and Operations Controls**

(1) Refer to Treasury PKI X.509 Certificate Policy for guidance on Facility, Management, and Operational Controls.

10.8.52.7.1 (08-22-2022) **Physical Controlsyesyes**

(1) Refer to Treasury PKI X.509 Certificate Policy for guidance.

10.8.52.7.1.1 (08-22-2022) **Site Location and Construction**

(1) The location and construction of the facility housing OLT PKI CA equipment shall be consistent with the security provided to the servers that provide network security and administration support (e.g., Microsoft Domain Controller) to the local environment. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.1.2 (08-22-2022) **Physical Access**

(1) Refer to Treasury PKI X.509 Certificate Policy for guidance on Physical Access.

10.8.52.7.1.2.1 (08-22-2022) **Physical Access for CA Equipment**

(1) OLT CAs shall be physically protected to be consistent with the security provided to the servers that provide network security and administration support (e.g., Microsoft Domain Controller) to the local environment. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.1.3
(08-22-2022)
Power and Air Conditioning

(1) OLT CAs shall have environmental controls (e.g., air, power) equivalent to that provided to the servers that provide network security and administration support (e.g., Microsoft Domain Controller) to the local environment. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.1.4
(08-22-2022)
Water Exposures

(1) OLT CAs shall have environmental controls (e.g., air, power) equivalent to that provided to the servers that provide network security and administration support (e.g., Microsoft Domain Controller) to the local environment. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.1.5
(08-22-2022)
Fire Prevention and Protection

(1) OLT CAs shall have environmental controls (e.g., air, power) equivalent to that provided to the servers that provide network security and administration support (e.g., Microsoft Domain Controller) to the local environment. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.1.6
(08-22-2022)
Media Storage

(1) OLT CAs shall have environmental controls (e.g., air, power) equivalent to that provided to the servers that provide network security and administration support (e.g., Microsoft Domain Controller) to the local environment. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.1.7
(08-22-2022)
Waste Disposal

(1) OLT CAs shall have environmental controls (e.g., air, power) equivalent to that provided to the servers that provide network security and administration support (e.g., Microsoft Domain Controller) to the local environment. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.1.8
(08-22-2022)
Off-Site Backup

(1) OLT CAs shall have environmental controls (e.g., air, power) equivalent to that provided to the servers that provide network security and administration support (e.g., Microsoft Domain Controller) to the local environment. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.2
(07-05-2019)
Procedural Controls

(1) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.2.1
(08-22-2022)
Number of Persons Required per Task

(1) There are no tasks associated with the OLT PKI that require multi-person control. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.2.2
(08-22-2022)
Identification and Authentication for Each Role

(1) Trusted roles are required to authenticate to the CA prior to performing any tasks on the CA. No individual shall have more than one identity on the CA. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.2.3
(08-22-2022)
Separation of Roles

(1) A single individual may assume both the Officer and Administrator roles. No one individual shall assume both a CA Operator role and an Auditor role. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.3
(07-05-2019)
Personnel Controls

(1) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.3.1
(08-22-2022)
Background, Qualifications, Experience, and Security Clearance Requirements

(1) Persons filling trusted roles in an OLT PKI are selected on the basis of loyalty, trustworthiness, and integrity. Trusted persons may be Department of the Treasury direct-hire personnel or contractors. Only U.S. Citizens may fill trusted roles. Persons filling trusted roles shall: (Treasury OLT PKI Policy)

- Be employees of the Department of the Treasury, GS-5 (equivalent) or above, or equivalent contractor/vendor position of responsibility.
- Have not been previously relieved of CA-related duties for reasons of negligence or non- performance of duties.
- Have not been denied a security clearance or had a security clearance revoked.
- Have not been convicted of a felony offense.
- Be appointed in writing by the OLT MA.

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.3.2
(08-22-2022)
Background Check Controls

(1) OLT Trusted Roles shall pass, at a minimum, a background investigation covering the following areas: (Treasury OLT PKI Policy)

- Employment
- Education
- Place of Residence
- Law Enforcement
- References

(2) The period of investigation must cover at least the last five years for each area, excepting the residence check, which must cover at least the last three

years. Regardless of the date of award, the investigation shall verify the highest educational degree obtained. (Treasury OLT PKI Policy)

(3) A competent adjudication authority shall perform adjudication of the background investigation. (Treasury OLT PKI Policy)

(4) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.4
(07-05-2019)
Audit Logging Requirements

(1) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.4.1
(08-22-2022)
Types of Events Recorded

(1) Table: Auditable Event Requirements (Treasury OLT PKI Policy)

Auditable Events (Logged either electronically or manually)	**OLT**	**PMA Auditor/or Script Required**
SECURITY AUDIT		
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X	
Any attempt to delete or modify the Audit logs	X	
Obtaining a third-party time-stamp	X	
IDENTIFICATION AND AUTHENTICATION		
Successful and unsuccessful attempts to assume a role	X	
The value of maximum authentication attempts is changed	X	
Maximum authentication attempts unsuccessful authentication attempts occur during user login	X	
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	
An Administrator changes the type of authenticator, e.g., from password to biometrics	X	
LOCAL DATA ENTRY		
All security-relevant data that is entered in the system	X	X
REMOTE DATA ENTRY		
All security-relevant messages that are received by the system	X	

Auditable Events (Logged either electronically or manually)	OLT	PMA Auditor/or Script Required
DATA EXPORT AND OUTPUT		
All successful and unsuccessful requests for confidential and security-relevant information	X	
KEY GENERATION		
Whenever the CA generates a key. (Not mandatory for single session or one-time symmetric keys)	X	X
PRIVATE KEY LOAD AND STORAGE		
The loading of Component private keys	X	X
All access to certificate subject private keys retained by the CA, RA, or LRA for key recovery purposes	X	
TRUSTED PUBLIC KEY ENTRY, DELETION, AND STORAGE		
All changes to the trusted public keys, including additions and deletions	X	
SECRET KEY STORAGE		
The manual entry of secret keys used for authentication		
PRIVATE AND SECRET KEY EXPORT		
The export of private and secret keys (keys used for a single session or message are excluded)	X	X
CERTIFICATE REGISTRATION		
All certificate requests and handling	X	
CERTIFICATE REVOCATION		
All certificate revocation requests and handling	X	
ESCROWED KEY RECOVERY REQUESTS		
All escrowed key recovery requests and handling′	X	
CERTIFICATE STATUS CHANGE APPROVAL		
The approval or rejection of a certificate status change request	X	
CA, RA or LRA CONFIGURATION		
Any security-relevant changes to the configuration of the CA or the RA	X	

Auditable Events (Logged either electronically or manually)	OLT	PMA Auditor/or Script Required
ACCOUNT ADMINISTRATION		
Roles and users are added or deleted The access control privileges of a user account or a role are modified	X	
The access control privileges of a user account or a role are modified	X	
CERTIFICATE PROFILE MANAGEMENT		
All changes to the certificate profile	X	
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT		
All changes to the certificate revocation list profile	X	
MISCELLANEOUS		
Appointment of an individual to a Trusted Role	X	
Installation of the Operating System	X	
Installation of CA, RA, or LRA Application	X	
Installing hardware cryptographic modules		
Removing hardware cryptographic modules		
Destruction of cryptographic modules	X	
System Startup	X	
Designation of personnel for multiparty control	X	
Logon Attempts on CA, RA, or LRA Applications	X	
Receipt of Hardware / Software		
Attempts to set passwords	X	
Attempts to modify passwords	X	
Backing up CA, RA. or LRA internal database	X	
Restoring* CA, RA, LRA internal database (*Auditor present with scripts for COOP Drills and Designated CA Disaster Recovery Events only. Auditor not required for high availability or normal switch over of services between facilities)	X	X
File manipulation (e.g., creation, renaming, moving)		
Posting of any material to a repository		
Access to CA, RA, or LRA internal database		
All certificate compromise notification requests	X	
Loading tokens with certificates		
Shipment of Tokens	X	

Auditable Events (Logged either electronically or manually)	OLT	PMA Auditor/or Script Required
Zeroize tokens	X	
Rekey of the CA	X	X
CONFIGURATION CHANGES TO THE CA SERVER, RA, OR LRA INVOLVING		
Hardware	X	
Software	X	
Operating System	X	
Patches	X	
Security Profiles		
PHYSICAL ACCESS/ SITE SECURITY		
Personnel Access to room housing CA		
Access to the CA server		
Known or suspected violations of physical security	X	
ANOMALIES		
Software Error conditions	X	
Software check integrity failures	X	
Receipt of improper messages		
Misrouted messages		
Network attacks (suspected or confirmed)	X	
Equipment failure	X	
Electrical Power Outages		
Uninterruptible Power Supply (UPS) failure		
Obvious and significant network service or access failures		
Violations of Certificate Policy	X	
Violations of Certification Practice Statement	X	
Resetting Operating System clock	X	

10.8.52.7.4.2
(08-22-2022)
Frequency of Processing Log

(1) OLT CA audit logs shall be reviewed for cause or as mandated by Treasury security policy. The review shall be performed by a security Auditor appointed by the OLT MA. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.5
(02-09-2015)
Records Archive

(1) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance. (Treasury OLT PKI Policy)

10.8.52.7.5.1
(07-05-2019)
Types of Records Archived

(1) Table: Data Archival Requirements. (Treasury OLT PKI Policy)

Data to be Archived	OLT
CA accreditation (if applicable)	X
Certificate Policy and Certification Practice Statement	X
Any contractual agreements (as appropriate) to which the CMA is bound, and other agreements concerning operations of the CA	X
System and equipment configuration	X
Modifications and updates to system, configuration, documentation (e.g., CPS), and contractual agreements	X
Certificate issuance, suspension, restoration and key recovery requests	X
Certificate Revocation requests	X
Documentation of receipt and acceptance of certificates	X
Documentation of receipt of tokens	X
All certificates issued or published	X
Record of CA Rekey and/or notification of cross-certified CA Rekey in accordance with applicable MOAs	X
All CRLs issued and/or published	X
All Audit Logs, and security audit data and reports	X
Other data or applications to verify archive contents	X
All CA operations communications and documentation to the PMA, PKI PA, other CMAs, and compliance auditors	X
Compliance Auditor reports	X

10.8.52.7.5.2
(08-22-2022)
Retention Period for Archive

(1) Archive records shall be retained as specified in the General Records Schedule established by the National Archives and Records Administration or an agency specific schedule as applicable. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.5.3
(08-22-2022)
Protection of Archive

(1) OLT Archive data shall be protected in accordance with Treasury records retention policies and procedures. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.6
(08-22-2022)
Key Changeover

(1) No further stipulations beyond the Treasury Basic policy. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.7
(08-22-2022)
Compromise and Disaster Recovery

(1) In the event an OLT PKI CA is suspected of being compromised or otherwise unable to operate, the OLT MA shall declare the CA revoked and immediately reestablish the CA and subordinate CAs if applicable. Subscribers will be required to obtain new certificates. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.7.8
(08-22-2022)
CA and RA Termination

(1) If an OLT CA is terminated for convenience prior to the expiration of its signing certificate, the CA shall be considered compromised and, if required, replaced as specified in Section 10.8.52.7.7 of this IRM. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.8
(08-22-2022)
Technical Security Controls

(1) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.8.1
(08-22-2022)
Key Pair Generation and Installation

(1) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.8.1.1
(08-22-2022)
Key Pair Generation

(1) An OLT CA shall generate cryptographic keying material used to sign certificates, CRLs or status information in FIPS 140 validated cryptographic modules. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.8.2
(08-22-2022)
Private Key Protection and Cryptographic Module Engineering Controls

(1) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.8.2.1
(08-22-2022)
Cryptographic Module Standards and Controls

(1) The minimum level of FIPS validation for an OLT CA is Level 1 (Hardware or Software). At some time in the future, there may be a requirement to move to Level 2 (Hardware) and OLT CAs are encouraged to use a Level 2 or higher module if possible. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance..

10.8.52.8.2.2
(08-22-2022)
Private Key Multi-Person Control

(1) No multiparty control is required. (Treasury OLT PKI Policy)

10.8.52.8.3
(08-22-2022)
Other Aspects of Key Management

(1) No further stipulations beyond the Treasury Basic policy. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.8.4
(08-22-2022)
Activation Data

(1) No further stipulations beyond the Treasury Basic Policy. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.8.5
(08-22-2022)
Computer Security Controls

(1) Computer security controls for OLT PKI CA equipment shall be consistent with the security provided to the servers that provide network security and administration support (e.g., Microsoft Domain Controllers) to the local environment. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.9
(08-22-2022)
Certificate, CARL/CRL, and OCSP Profiles Format

(1) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.9.1
(08-22-2022)
Certificate Profile

(1) OLT PKI certificate should conform to [FPKI-Prof] but may deviate as necessary to meet operational requirements. The OLT MA shall provide a copy of certificate profiles that deviate from [FPKI-Prof] to the Treasury PMA prior to implementing the profile in operational certificates. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.10
(08-22-2022)
Compliance Audits and Other Assessments

(1) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.10.1
(08-22-2022)
Frequency of Audits or Assessments

(1) OLT PKI CAs shall undergo a compliance audit by a PMA approved auditor at least every three (3) years. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.10.2
(08-22-2022)
Identity & Qualifications of Assessor

(1) No further stipulations beyond the Treasury Basic policy. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.10.3
(08-22-2022)
Assessor's Relationship to Assessed Entity

(1) No further stipulations beyond the Treasury Basic policy. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.10.4
(08-22-2022)
Topics Covered by Assessment

(1) The OLT PKI compliance audit shall cover those aspects of PKI operations of the OLT CA not covered by the security review. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

10.8.52.11
(08-22-2022)
Other Business and Legal Matters

(1) No further stipulations beyond the Treasury Basic policy. (Treasury OLT PKI Policy)

(2) Refer to Department of the Treasury Public Key Infrastructure (PKI) X.509 Certificate Policy for additional guidance.

This Page Intentionally Left Blank

Exhibit 10.8.52-1 (08-22-2022)
Summary of Available Policies (Certificate types)

(1) This policy addendum specifies a single level of assurance, defined in subsequent sections as “OLT.” This level of assurance has an OID that will be asserted in certificates issued by CAs who comply with the policy stipulations herein. The OID will be registered under the id-infosec arc as; (Treasury OLT PKI Policy)

- {joint-iso-ccitt (2) country (16) us (840) organization (1) gov (101) csor (3) pki (2) cert-policy (1) treasury-policies (5) id-treacertpcy-internalnpe (9)}, or

- {joint-iso-ccitt (2) country (16) us (840) organization (1) gov (101) csor (3) pki (2) cert-policy (1) treasury-policies (5) treasury-certpcy-internalperson (14)}

(2) The Internal NPE policy identifier shall never be cross certified with any entity outside of the Treasury. Initially, OLT PKIs will only be established within Treasury Bureaus. If it is determined that there is a need to establish an OLT PKI that is trusted across the entire Department, Bureau OLT PKIs may be aggregated into a single PKI under a Treasury operated Root. To preclude unintentional trust of an OLT certificate, if there is a need for a Treasury-wide trust of an OLT PKI, it shall be operated under a separate trust anchor from TRCA. (Treasury OLT PKI Policy)

Exhibit 10.8.52-2 (11-03-2023)
Terms and Acronyms

Term	Definition or description
Access Control	Process of granting access to system resources only to authorized users, programs, processes, or other systems.
ACM	Automated Certificate Issuance and Life-Cycle Management
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
AO	Authorizing Official
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's identity.
Certificate	A digital representation of information, which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG] As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.
Certificate Authority (CA)	A trusted entity in a public key infrastructure (PKI) that issues and revokes certificates exacting compliance to a PKI policy. A certificate issued by a CA contains the subscriber's name, the name of the CA, the subscriber's public key, and it is signed by the CA.
CA Certificate	The certificate of the Certification Authority (CA). This certificate is used to verify signature on certificates issued by the CA.
CIMC	Certificate Issuing and Management Components
CIO	Chief Information Officer
Certificate Management Authority (CMA)	Either a Certification Authority or a Registration Authority.
Certificate Policy (CP)	A specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a Certificate Policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	The statement of the practices which a Certification Authority employs in issuing certificates to a subscriber. This includes certificate application, use and revocation or suspension of certificates.

Exhibit 10.8.52-2 (Cont. 1) (11-03-2023)
Terms and Acronyms

Term	Definition or description
Certificate Revocation List (CRL)	A list of revoked public key certificates created and digitally signed by a Certification Authority.
Certificate Status Authority	A trusted Entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Confidentiality	Preserving authorized restrictions on information access and disclosure, (including means for protecting personal privacy and proprietary information) from unauthorized individuals, entities, or processes.
Contingency Plan	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.
Credentials	An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber.
Cross Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptography	The discipline that embodies principles, means, and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity.
Cryptographic module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
CSA	Certificate Status Authority
CSS	Certificate Status Server
DC	Domain Component
DNS	Domain Name System
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Disaster Recovery Plan	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.
DN	Distinguished Name
DSS	Digital Signature Standard

Exhibit 10.8.52-2 (Cont. 2) (11-03-2023)
Terms and Acronyms

Term	Definition or description
EA	Enterprise Architecture
End Entity Certificate (EEC)	A certificate belonging to a non-CA entity, e.g. you, me or the computer, firewall.
EOps	Enterprise Operations
Encypherment	Convert (a message or piece of text) into a coded form
ESP	Enterprise Standards Profile
FBCA Operational Authority (FBCA OA)	The Federal Public Key Infrastructure Operational Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.
Federal Public Key Infrastructure Policy Authority (FPKIPA)	The FPKIPA is a federal government body responsible for setting, implementing, and administering policy decisions regarding inter-Entity PKI interoperability that uses the FBCA.
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GAO	Government Accountability Office
HSPD-12	Homeland Security Presidential Directive 12
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
Identification	The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in a system.
Integrity	The prevention of the unauthorized/improper modification or destruction of information; includes ensuring information non-repudiation and authenticity.
IP	Internet Protocol
IP Sec	Internet Protocol Security
IT	Information Technology
Key Escrow	The retention of the private component of the key pair associated with a Subscriber's encryption certificate to support key recovery.
Lightweight Directory Access Protocol (LDAP)	The Lightweight Directory Access Protocol is an application protocol for reading and editing directories over an IP network. A directory in this sense is an organized set of records: for example, a telephone directory is an alphabetical list of persons and organizations with an address and phone number in each ″record″.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community

Exhibit 10.8.52-2 (Cont. 3) (11-03-2023)
Terms and Acronyms

Term	Definition or description
MA	Management Authority
Naming Authority	An organizational Entity responsible for assigning Distinguished Names (DNs) and for assuring that each DN is meaningful and unique within its domain.
NARA	National Archives and Records Administration
NDES	Network Device Enrollment Services
NIST	National Institute of Standards and Technology
NPE	Non Person Entities
Non-repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. • Technical non-repudiation refers to the assurance a user has, that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. • Legal non-repudiation refers to how well possession or control of the private signature key can be established.
OA	Operational Authority
OCIO	Office of Chief Information Officer
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI, they are used to identify uniquely each of the policies and cryptographic algorithms supported.
OLT	Only Locally Trusted
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
PIT	Part-time/Intermittent/Temporary
PIV	Personal Identity Verification
PKI Sponsor	Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.

Exhibit 10.8.52-2 (Cont. 4) (11-03-2023)
Terms and Acronyms

Term	Definition or description
Plan of Action and Milestones (POA&M)	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks and scheduled completion dates for the milestones.
PM	Program Manager
PMO	Program Management
Policy Management Authority (PMA)	Entity established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the FBCA, the PMA is the FPKIPA.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt information. This key is accessible only to the owner.
Public key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	Entity responsible for identification and authentication of certificate subjects that has automated equipment for the communication of applicant data to Certification Authorities and does not sign or directly revoke certificates.
RBD	Risk Base Decision
Relying Party	A relying party is the entity that relies on the validity of the binding of the subscriber's name to a public key. The relying party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. A relying party may use information in the certificate (such as CP identifiers) to determine the suitability of the certificate for a particular use.
Repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

Exhibit 10.8.52-2 (Cont. 5) (11-03-2023)
Terms and Acronyms

Term	Definition or description
Rekey (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application.
SBU	Sensitive but Unclassified
SOP	Standard Operating Procedure
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate.
Subordinate CA	When there are multiple CAs in a PKI, the CAs are structured in a hierarchy or chain. The CA above another CA in a chain is called an root CA; a CA below another CA in the chain is called a subordinate CA. A CA can also be subordinate to a root outside of the Certificate System deployment; for example, a CA which functions as a root CA within the Certificate System deployment can be subordinate to a third-party CA.
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
TD	Treasury Division
Technical non-repudiation	The contribution public key mechanisms make to the provision of technical evidence supporting a non-repudiation security service.
TIGTA	Treasury Inspector General Tax Administration
TPKI	Treasury Public Key Infrastructure
TRCA	Treasury Root Certificate Authority.
Trust List	Collection of Trusted Certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Entity in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a ″trust anchor.”
WWW	World Wide Web
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.

Exhibit 10.8.52-3 (11-03-2023)
Related Resources

IRS Publications

- IRM 1.15 Series, *Records and Information Management*
- IRM 10.5.1 - *Privacy and Information Protection, Privacy Policy*
- IRM 10.8.1 - *Information Technology (IT) Security, Policy and Guidance*
- IRM 10.8.2 - *Information Technology (IT) Security, Roles and Responsibilities*
- IRM 10.8.15 - *Information Technology (IT) Security, General Platform Operating System Security Policy*
- IRM 10.8.22 - *Information Technology (IT) Security, Web Server Security Policy*
- IRM 10.8.33 - *Information Technology (IT) Security, Mainframe System Security Policy*
- IRM 10.8.60 - *Information Technology (IT) Security, Service Continuity Management (ITSCM) Policy and Guidance*
- IRM 10.8.62 -*Information Technology (IT) Security, Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Testing, Training, and Exercise (TT&E) Process*

Department of the Treasury Publications

- Treasury Only Locally Trusted (OLT) Public Key Infrastructure (PKI) X.509 Certificate Policy, Version 1.0, December 22, 2021
- *Treasury Public Key Infrastructure(PKI) X.509 Certificate Policy, Version 3.5 December 7, 2021*
- TD P 85-01, Version 3.1.3, *Treasury Information Technology (IT) Security Program*, *February 28,2022*
- TD P 80-08, *Controlled Unclassified Information (CUI) Guide*, September 4, 2018

National Institute of Standards and Technology (NIST) Publications

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February, 2004
- FIPS 140-3, *Security Requirements for Cryptographic Modules*, March 22, 2019 .
- FIPS 186-4, *Digital Signature Standard*, July 2013
- FIPS 200: *Minimum Security Requirements for Federal Information and Information Systems*
- FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013
- NIST SP 800-37 Rev 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, September 20, 2018
- NIST SP 800-53 Rev 5, *Security and Privacy Controls for Federal Information Systems and Organizations*,September 2020 (includes updates as of Dec 10, 2020)
- NIST SP 800-53A Rev 5, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, January 25 2022
- NIST SP 800-57, Part 3, Rev. 1 *Recommendation for key Management, Part 3 Application-Specific Key Management Guidance*, January 2015
- NIST SP 800-73-4, *Interfaces for Personal Identity Verification*, May 2015 (Update February 08, 2016)
- NIST SP 800-76-2, *Biometric Data Specification for Personal Identity Verification*, July 11, 2013
- NIST 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV)*, May 29, 2015

Other Publications

- *X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework*, Version 2.2, December 1, 2021