Matter PKI Compliance Guide

AWS Private Certificate Authority

First published December 20, 2022

Last updated February 16, 2024

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers, or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

Amazon is a founding member and a key contributor to the Matter initiative, an effort managed by the Connectivity Standards Alliance to develop an open standard for device interoperability across smart home systems with security and privacy as key design tenets. The purpose of this document is to provide guidance on how you can use AWS Private Certificate Authority to properly set up and manage a certificate authority that is aligned to the Alliance Matter PKI certificate policy.

Key terms

Acronym	Term
ACL	Access control list
API	Application programming interface
CA	Certificate authority
CAAF	Certificate authority auditing framework
CDK	AWS Cloud Development Kit
CLI	Command line interface
CP	Certificate policy
CPS	Certification Practice Statement
CRL	Certificate revocation list
DAC	Device attestation certificate
DCL	Distributed compliance ledger
DSP	Delegated service provider
HSM	Hardware security module
IAM	AWS Identity and Access Management
ISO	International Organization for Standardization
MFA	Multi-factor authentication
OCSP	Online Certificate Status Protocol
PAA	Product Attestation Authority
PAI	Product Attestation Intermediate
PID	Product ID
PKI	Public key infrastructure
RA	Registration authority
RAD	Requestor agreement document
SOC	System and Organization Controls
SoD	Separation of duties
VID	Vendor ID

Introduction

Matter is a new protocol created by the Connectivity Standards Alliance (Alliance) that allows smart home devices from different vendors to work together. Matter relies on digital certificates called device attestation certificates (DACs) to verify that the devices on the smart home network are Matter certified. The Alliance has specific requirements for anyone creating a Matter certificate authority (CA) to issue DACs.

The Alliance allows the use of delegated service providers (DSPs) to provide you with public key infrastructure (PKI) services to create your Matter CA. You can use AWS Private Certificate Authority as a DSP to create a Matter CA to issue DACs. When you use AWS Private CA to create a Matter CA, you are considered the CA in the Alliance Matter PKI hierarchy. The objective of this guide is to provide you with information to help you plan for and document the Alliance Matter PKI certificate policy (CP) compliance of your Matter CA. This includes details regarding the responsibility of controls to help you achieve Matter PKI CP compliance, planning of evidence gathering to meet Matter PKI assessment testing procedures, and explaining your control implementation to the Alliance.

You should carefully plan to implement and demonstrate compliance with the Alliance Matter PKI CP requirements when you issue Matter certificates using the CA infrastructure services provided by AWS Private CA. Matter PKI CP is not just a technical standard; it also covers people, processes, and technology.

Using AWS Private CA to help meet Matter PKI CP requirements

AWS Private CA is a DSP that provides CA infrastructure services for you to create a Matter CA. AWS Private CA is International Organization for Standardization (ISO) 27001 certified and System and Organization Controls 2 (SOC 2) Type 2 attested as required by the Alliance. You can use AWS Private CA to help you build Matter PKI CP compliant CAs and issue DACs with appropriate configuration. AWS Private CA as a DSP is responsible for a subset of the requirements specified in the Alliance Matter PKI CP. This does not mean that your use of AWS Private CA is automatically compliant. You are responsible for ensuring your own compliance with the Matter PKI CP, including the implementation of controls specific to your use of the services that might be necessary or applicable.

You can further use AWS security, identity, and compliance services to help you meet the Matter PKI CP compliance for your Matter CA. Examples of these services include AWS Identity and Access Management (IAM), Amazon CloudWatch, AWS CloudTrail, and Amazon Time Sync Service. Additionally, AWS Private CA has sample AWS Cloud Development Kit (CDK) scripts and AWS CloudFormation stack templates available to help you meet the requirements of the Matter PKI CP approved on December 19, 2022.

AWS Shared Responsibility Model

Alliance Matter PKI security is a shared responsibility between you and AWS Private CA. This shared model can help relieve your operational burden because AWS operates, manages, and controls the components from the AWS Private CA service down to the physical security of the facilities in which the service operates. You assume responsibility and management of your use of AWS Private CA, such as logical access and other technical settings (for example, encryption, logging, and backups of logging data). For more information, see the Shared Responsibility Model.

The shared responsibility model also extends to information technology (IT) controls. Just as the responsibility to operate the IT environment is shared between you and AWS Private CA, so is the management, operation, and verification of IT controls shared. AWS Private CA can help relieve your burden of operating controls by managing the controls associated with the physical infrastructure deployed in the AWS environment that you might have previously managed. You can then use the AWS control and compliance documentation, such as the AWS SOC 2 Type 2 report, to perform your control evaluation and verification procedures as required. For more information about the shared responsibility between you and AWS Private CA related to Matter PKI CP compliance, see Appendix A.

It is critical that you understand the Alliance Matter PKI CP requirements for operating your CA. It is your responsibility to maintain your Matter CA environment and scope on AWS Private CA, and to be able to demonstrate compliance with requirements, including for your CA systems that are not hosted on AWS, such as your workstations used to remotely connect to AWS Private CA. You should prepare a complete and accurate description of your CAs and their relationships and the reasoning for your decisions about CA structure to help you plan and demonstrate Matter PKI CP compliance. For example, the Matter PKI CP compliance assessment requirements vary based on whether your CA is a vendor ID (VID)-Scoped Product Attestation Authority (PAA) or a non-VID-scoped PAA. For details, see Requirement 8: Compliance audit and other assessments. Figure 1 shows how you can use AWS

Private CA, along with your own controls, to help you meet the Matter PKI CP requirements.

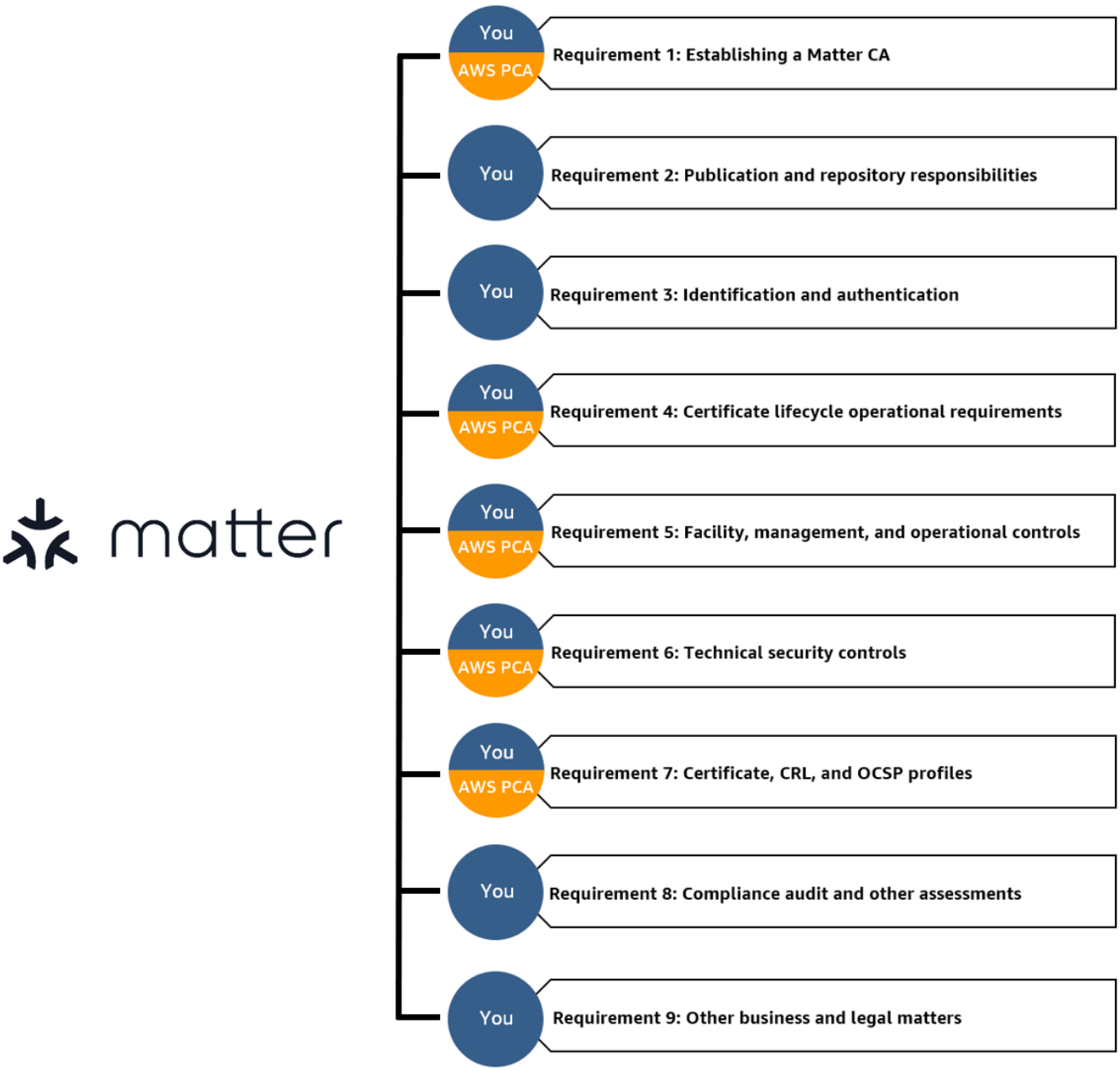

Figure 1: Shared responsibility for Matter PKI CP requirements

Using AWS Private CA to help establish a Matter CA

The following list is provided for guidance purposes only; you should make your own determination of control implementation based on your specific environment. Although the list is intended to be comprehensive, it is your responsibility to maintain Alliance Matter PKI CP compliance and to know your obligations under the Alliance Matter PKI CP**.** The guidance is based on the Alliance Matter PKI CP version from December 19, 2022. You should implement procedures to monitor for updates to the Alliance Matter PKI CP. AWS Private CA offers no warranties that following this guidance will guarantee Matter PKI CP compliance.

Requirement 1: Establishing a Matter CA

You are responsible for the following:

- Requesting membership and maintaining a good standing with the Alliance, including payment of membership fees;
- Following the applicable processes determined by the Alliance when submitting your PAA in the distributed compliance ledger (DCL), including the Matter PAA approval process;
- Reviewing and complying with the requirements defined in the Alliance Matter PKI CP, DCL Policies Procedures and Governance, and the Matter Specification;
- Creating a CPS that aligns with the requirements described in the Alliance Matter PKI CP (for guidance on using AWS Private CA when creating your CPS, see Appendix B);
- Negotiating and documenting a requestor agreement document (RAD) for each requestor that aligns with the requirements in the Alliance Matter PKI CP;
- Completing the Certificate Policy Self-Attestation Compliance Form and submitting the applicable information for inclusion of your PAA certificate in the DCL for issuance (VID-scoped PAA);
- Performing a periodic independent certificate authority auditing (CAAF) audit (non-VID-scoped PAA);
- Attesting and reporting on adherence to the Alliance Matter PKI CP;
- Documenting policies, procedures, and controls that align with the Alliance Matter PKI CP;
- Periodically assessing your control environment to verify that controls are operating as required by the Alliance Matter PKI CP;
- Assigning a unique Product ID (PID) for each generic module/chip customer (if you are a generic module/chip builder).

AWS Private CA provides the following to help you establish your Matter CA:

- Using a FIPS 140-2 Level 3 validated hardware security module (HSM) to protect and operate CA private keys (when you select the appropriate Region from Appendix C); and
- Managing the underlying infrastructure that issues Matter certificates.

Requirement 2: Publication and repository responsibilities

You are responsible for making the publication of certificate information available within the timeframe required by the Alliance Matter PKI CP. You are also responsible for implementing access controls to the DCL repository.

Requirement 3: Identification and authentication

You are responsible for verifying that certificate naming and identity validation requirements are met as required by the Alliance Matter PKI CP.

Requirement 4: Certificate lifecycle operational requirements

You are responsible for the following:

- Creating and maintaining processes and procedures related to certificate issuance such as:
    - Certificate application
    - Certification application processing
    - Certificate issuance
    - Certificate acceptance
    - Key pair and certificate usage
    - Certificate revocation and suspension
- Configuring your Matter CA to generate Certificate Revocation Lists (CRLs); and
- Publishing revocation information in the DCL within the timeframes defined by Alliance Matter PKI CP.

AWS Private CA provides the following:

- FIPS 140-2 Level 3 (see note below) validated HSMs to help safeguard private keys that are used to issue certificates. AWS customers can download CA certificates from the AWS Management Console, AWS Private CA API, or AWS Command Line Interface (AWS CLI).

> You are required to select AWS Regions listed in Appendix C.

- Supporting Matter revocation and CRL generation.

> You are required to maintain the CAs for the lifetime of the certificates/devices and configure your Matter CA to generate CRLs. The Alliance CP recommends you implement revocation beginning May 1, 2024 and requires you to implement revocation beginning September 1, 2024. To help you conform to these revocation requirements, refer to the Implementing Matter User guide.

Requirement 5: Facility, management, and operational controls

You are responsible for the following:

- Protecting your AWS Identity and Access Management (IAM) account credentials;
- Creating individual user accounts and provisioning the least privilege permissions necessary to fulfill job duties with IAM (for details, see IAM for AWS Private CA);
- Reviewing and approving AWS account access to AWS Private CA;
- Enforcing multi-factor authentication (MFA) with each AWS account;
- Using AWS encryption solutions, along with default security controls within AWS services;
- Configuring CloudWatch to collect and track metrics, set alarms, and automatically react to changes in your AWS resources;
- Configuring CloudTrail to record API calls that are made by AWS Private CA;
- Periodically generating audit reports that list the certificates that your private CA has issued or revoked;
- Creating snapshots (which are backups or archives) of logging and audit data with retention policies commensurate with the Alliance Matter PKI CP requirements;
- Restricting access to Amazon S3 and CloudTrail by using fine-grained IAM policies to allow only specific information security personnel to have access to audit trails;
- Configuring log file integrity validation in CloudTrail;
- Securing registration authority (RA) equipment from unauthorized access; and

- Documenting and maintaining the following operating policies and procedures as defined by the Alliance Matter PKI CP:
    - Trusted roles and separation of duties
    - Background screening
    - Trusted roles training
    - Incident and compromise handling
    - Disaster recovery and business continuity

AWS Private CA provides the following control coverage:

- Physical security and environmental protections that are assessed as part of a SOC 2 Type 2 report.

> You are responsible for the physical security and data classification of CA data exported or transferred out of the AWS environment under Matter PKI CP Requirement 5 but not for the physical security of CA data stored on AWS.

- Availability and redundancy mechanisms that are assessed as part of a SOC 2 Type 2 report to verify log and key availability.

> Your data to support the CA hierarchy stored in S3 buckets, such as logs and audit data, require you to configure and store backup retention policies commensurate with the requirements in the Alliance Matter PKI CP.

- Monitoring and incident response mechanisms that are assessed as part of a SOC 2 Type 2 report to provide a high level of service performance and availability.

> You are required to implement monitoring and incident response procedures as a result of configuring logs specific to AWS Private CA.

- Employee user access controls that are assessed as part of a SOC 2 Type 2 report to verify appropriate background screening, account provisioning, access management, periodic access reviews, and access removal.

> You are required to implement user access controls to AWS Private CA commensurate with the requirements in the Alliance Matter PKI CP.

- Employee user training programs and annual evaluations that are assessed as part of a SOC 2 Type 2 report to verify employees understand their individual roles and responsibilities and align employee qualifications as required.

> You are required to implement employee training and evaluation procedures for your internal employees commensurate with the requirements in the Alliance Matter PKI CP.

Requirement 6: Technical security controls

You are responsible for the following:

- Implementing multi-person logical access controls anytime that the cryptographic module is accessed, such as key generation ceremonies and creation and renewals for PAA and PAI certificates;

> You can meet multi-person logical access requirements through documented change management procedures that require more than one person to be present virtually over encrypted video and desktop sessions when generating and activating PAA and PAI certificates. AWS Private CA recommends that you document the date, individuals present, a description of the steps to be performed during access to the cryptographic module, and approvals prior to key generation. In addition, AWS Private CA recommends that you record and retain video sessions (PAA and PAI key generation) and change management documentation to support audit requirements.
>
> Alternatively, you can use Change Manager, a capability of AWS Systems Manager, to help you meet the multi-person approval requirement. Automation documents for PAA and PAI creation are available in the GitHub repository, or you can create your own automation documents for multi-person approvals.

- Provisioning a logically isolated section of the AWS Cloud through Amazon Virtual Private Cloud (Amazon VPC), where AWS resources can be launched in a virtual network that you define (where applicable);
- Defining network access control lists (ACLs) as an optional layer of security for VPCs that acts as a stateless router for controlling traffic in and out of one or more subnets (where applicable);

- Setting up security groups to act as stateful firewalls for resources in a VPC, controlling both inbound and outbound traffic at the virtual network interface (where applicable);

> You can use security groups to restrict traffic by IP address, port, and protocol, and satisfy elements of the Matter PKI CP requirements. By default, security groups allow outbound connections; you are responsible for configuring specific outbound connection rules for Matter PKI CP compliance.

- Using IAM to evaluate and deny traffic to AWS Private CA endpoints based on the connection source, whether in standard CIDR IPv4 or IPv6 format (where applicable);
- Configuring the IAM password policy to enforce a minimum password length, combination of alphanumeric and special characters, and password rotation;
- Establishing a process to perform routine self-assessments of security controls for vulnerabilities.

AWS Private CA provides the following control coverage:

- FIPS 140-2 Level 3 validated HSMs to safeguard private keys that are used to issue PAA and PAI certificates.

> You are required to select AWS Regions listed in Appendix C.

- NIST P-256 key sizes for Matter PKI Certificates as required in the Matter Specification.
- Internal AWS network security controls that are assessed as part of the SOC 2 Type 2 report to verify protection against traditional network security threats.
- Password policy controls that are assessed as part of the SOC 2 Type 2 report to verify required configurations and expiration intervals.

> You are responsible for verifying that your IAM password policy is configured to enforce a minimum password length, combination of alphanumeric and special characters, and expiration intervals.

- Remote access controls that are assessed as part of the SOC 2 Type 2 report to verify secure connections to AWS Private CA.

> You are responsible for verifying secure remote access controls are implemented for your connections to AWS Private CA.

- Software development practices related to AWS Private CA that are assessed as part of the SOC 2 Type 2 report to verify that proper testing, validation, and approval occurs, whether manual or automated, at each stage of the software development lifecycle.
- Infrastructure configuration management practices related to AWS Private CA that are assessed as part of the SOC 2 Type 2 report to verify that a consistent updated baseline is automatically applied.

Requirement 7: Certificate, CRL, and OCSP profiles

You are responsible for creating your Matter certificates according to the Matter specification. AWS Private CA provides Matter certificate templates for use when creating the PAA and PAI CA and issuing Matter DAC certificates.

CRL and OCSP profile requirements are not defined in Version 1 of the Alliance Matter Specification released on October 4, 2022. CRL and OCSP profile requirements are expected to be defined in a later version of the Alliance Matter Specification.

Requirement 8: Compliance audit and other assessments

You are responsible for verifying that your compliance audit and other assessment requirements are met as required by the Alliance Matter PKI CP. You are responsible for determining the scope of your compliance requirements based on the following:

- A VID-scoped PAA is scoped to a single VID and therefore can only sign PAIs for the applicable Vendor ID. VID-scoped PAAs only attest that internal audits are periodically performed and that the results are shared with the Alliance.
- A non-VID-Scoped PAA is not scoped to a VID and therefore can sign PAIs for applicable Vendor IDs. Non-VID-scoped PAAs undergo a periodic independent certificate authority auditing framework (CAAF) audit.

AWS Private CA is ISO 27001 certified and SOC 2 Type 2 attested as required by the Alliance.

Requirement 9: Other business and legal matters

You are responsible for verifying other business and legal matters are met as required by the Alliance Matter PKI CP.

Conclusion

You can use AWS Private CA to help you achieve Alliance Matter PKI CP compliance. With careful planning and by maintaining compliance awareness throughout the lifecycle of your CA hierarchy, you can take the stress out of demonstrating Alliance Matter PKI CP compliance.

Contributors

Contributors to this document include:

- Lorey Spade, Sr. Industry Specialist, Amazon Trust Services
- Alexander Truskovsky, Sr. Product Manager, AWS Private Certificate Authority

Further reading

For more information, see the following resources.

- Matter Resource Kit
- Alliance Matter PKI CP
- AWS Matter PKI CDK project
- AWS Private CA Implementing Matter User Guide
- AWS Private CA SOC 2 Type 2 Report (available through AWS Artifact)
- AWS Private CA ISO 27001:2013 Certification (available through AWS Artifact)

Document revisions

Date	Description
February 2024	Addition of Requirement 4.9: Revocation and Suspension
September 2023	Addition of Appendix C; removal of Requirement 5.1.2.1 from Appendix A and Appendix B

Date	Description
March 2023	Addition of Matter CP Requirement 1.4.2 and 6.2.5 in Appendix A; addition of Appendix B
December 2022	First publication

Appendix A

AWS Private CA Matter PKI CP compliance responsibility summary

Matter CP requirement	Matter CP description	Responsibility	Customer specific
1.4.2	Certificate authorities (CAs)	Shared	CPS creation, issuing compliant certificates
4.3.2	Security for certificate issuance	PCA	N/A
4.3.3	Notification to requestor by the CA of issuance of certificates	Shared	Notification to requestors
4.9.6	Revocation Checking Requirement for Relying Parties	Shared	Configure CRL generation
5.1.1	Site location and construction	PCA – SOC2	N/A
5.1.2	Physical access	PCA – SOC2	N/A
5.1.3	Power and air conditioning	PCA – SOC2	N/A
5.1.4	Water exposures	PCA – SOC2	N/A
5.1.5	Fire prevention and protection	PCA – SOC2	N/A
5.1.6	Media storage	PCA – SOC2	N/A
5.1.7	Waste disposal	PCA – SOC2	N/A
5.1.8	Off-site backup	Shared – SOC2	Configure replication of audit logs
5.2.1	Trusted roles	Shared	Define trusted roles for CA
5.2.2	Number of persons required per task	Shared – SOC2	Multi-person logical access controls
5.2.3	Identification and authentication for each role	Shared – SOC2	Identity checks for trusted persons
5.2.4	Roles requiring separation of duties (SoD)	Shared	Assign roles for appropriate SoDs
5.3.1	Qualifications, experience, and clearance requirements	Shared – SOC2	Employee background checks
5.3.2	Background check procedures	Shared – SOC2	Employee background checks
5.3.3	Training requirements	Shared – SOC2	Employee training requirements
5.3.4	Retraining frequency and requirements	Shared – SOC2	Employee training requirements
5.3.6	Sanctions for unauthorized actions	Shared – SOC2	Policies for unauthorized actions
5.3.8	Documentation supplied to personnel	Shared – SOC2	Employee training documentation
5.4	Audit logging procedures	Shared – SOC2	Configure event logging
5.4.1	Types of events recorded	Shared – SOC2	Configure event logging
5.4.2	Frequency of processing logs	Shared – SOC2	Procedures for reviewing logs
5.4.3	Retention period for audit log	Shared – SOC2	Configure retention

			policies
5.4.4	Protection of audit log	Shared – SOC2	Configure appropriate IAM access
5.4.5	Audit log backup procedures	Shared – SOC2	Configure replication of backups
5.4.6	Audit collection system (internal versus external)	Shared – SOC2	Configure event logging
5.4.8	Vulnerability assessments	Shared – SOC2	Perform vulnerability assessments
5.5.1	Types of events archived	Shared – SOC2	Configure audit log archival
5.5.2	Retention period for archive	Shared – SOC2	Configure retention for archival
5.5.3	Protection of archive	Shared – SOC2	Configure appropriate IAM access
5.5.4	Archive backup procedures	Shared – SOC2	Configure replication of backups
5.5.5	Requirements for time-stamping of records	PCA	N/A
5.5.7	Procedures to obtain and verify archive information	Shared – SOC2	Configure audit log archival
5.7.1	Incident and compromise handling procedures	Shared – SOC2	Procedure for CA incident response
5.7.2	Computing resources, software, or data are corrupted	Shared – SOC2	Procedure for CA incident response
5.7.3	Entity (CA) private key compromise procedures	Shared – SOC2	Procedure for CA incident response
5.7.4	Business continuity capabilities after a disaster	PCA – SOC2	N/A
5.8	CA and RA termination	Shared – SOC2	Procedure for CA and RA termination
6.1.1.1	CA key pair generation	Shared	Create keys in appropriate Regions
6.1.5	Key sizes	Shared	Configure Matter certificates
6.2.1	Cryptographic module standards and controls	PCA	Configure HSMs in appropriate Regions
6.2.2	Private key (n out of m) multi-person control	Shared	Multi-person logical access controls
6.2.4	Private key backup	PCA – SOC2	N/A
6.2.5	Private key archival	Shared	Do not archive requestor private keys
6.2.6	Private key transfer into or from a cryptographic module	PCA	N/A
6.2.7	Private key storage on cryptographic module	PCA	Configure HSMs in appropriate Regions
6.2.9	Method of deactivating private keys	PCA	N/A
6.5.1	Specific computer security technical requirements	Shared – SOC2	Configure appropriate IAM access, password

			policies, and VPC segmentation (if applicable)
6.6.1	System development controls	PCA – SOC2	N/A
6.6.2	Security management controls	Shared – SOC2	Configuration management of CA
6.7	Network security controls	Shared – SOC2	Configure appropriate IAM access and VPC segmentation (if applicable)
6.8	Time-stamping	PCA	N/A
7 (All)	Certificate, CRL, and OCSP profiles	Shared	Configure Matter certificates

PCA – Controls are inherited by AWS Private CA service functionality, processes, or procedures.
PCA – SOC2 – Controls are inherited by using AWS Private CA as attested in the AWS Private CA SOC 2 Type 2 Report.
Shared – Controls are shared between you and AWS Private CA. AWS Private CA responsibility is met with internal AWS Private CA controls.
Shared – SOC2 – Controls are shared between you and AWS Private CA. AWS Private CA controls are inherited by using AWS Private CA as attested in the AWS Private CA SOC 2 Type 2 Report.
N/A – AWS Private CA is responsible for meeting the requirement; not applicable to you.

Appendix B

AWS Private CA Matter PKI CPS guidance

Appendix B is provided as guidance to assist customers in completing their Certification Practice Statement (CPS) template as required by the CSA. This guidance is based on approved Version 1.1 released November 16, 2022. See the Matter Resource Kit for the CSA CPS template.

Matter CP requirement	Responsibility	AWS Private CA CPS response
1.4.2	Shared	You are responsible for developing and maintaining your CPS, using AWS Private CA APIs to issue Matter certificates, and securing delivery of certificates to its requestors. AWS Private CA provides the infrastructure for you to protect and operate CA private keys.
4.3.2	PCA	AWS Private CA uses cryptographic modules that help you meet the requirements in this section.
4.3.3	Shared	You are responsible for notifying requestors that CA certificates have been created and the access and means for obtaining the CA certificates. AWS Private CA makes PAA and PAI certificates available from the console. AWS Private CA makes DAC certificates available through an API or CLI.
5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.1.5, 5.1.6, & 5.1.7	PCA – SOC2	You inherit physical access controls that help you meet the requirements in this section that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section D.6 Physical Security and Environmental Protection). You are responsible for the physical security and data classification of CA data exported or transferred out of the AWS environment under Matter PKI CP Requirement 5 but not for the physical security of CA data stored on AWS.
5.1.8	Shared – SOC2	You are responsible for creating backups in separate AWS Regions and configuring retention for their audit data. You inherit physical access and storage controls that help you meet the requirements in this section that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section D.6 Physical Security and Environmental Protection and D.8 Data Integrity, Availability, and Redundancy). You are responsible for the physical security and data classification of CA data exported or transferred out of the AWS environment under Matter PKI CP Requirement 5 but not for the physical security of CA data stored on AWS.
5.2.1	Shared	You are responsible for satisfying the requirements in this section specific to defining trusted roles for the operations of your PKI hierarchy. AWS Private CA maintains trusted roles specific to physical access of cryptographic modules.
5.2.2	Shared – SOC2	You are responsible for satisfying the requirements in this section specific to logical multi-person access controls. AWS Private CA implements multi-person controls for physical access

		to cryptographic modules. You inherit multi-person physical access controls for decommissioning of cryptographic modules that help you meet the requirements in this section that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section D.6 Physical Security and Environmental Protection).
5.2.3	Shared – SOC2	You are responsible for satisfying the requirements in this section specific to identification and authentication controls for your trusted roles. You inherit controls related to identification and authentication of AWS employees that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section D.2 Employee User Access).
5.2.4	Shared	You are responsible for satisfying the requirements in this section specific to separation of duties for your trusted roles. AWS Private CA implements separation of duties for trusted roles specific to physical access to cryptographic modules.
5.3.1	Shared – SOC2	You are responsible for satisfying the requirements in this section specific to background check procedures for your trusted persons. You inherit controls related to background checks of AWS employees that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section A.1 Control Environment, B. Communications, D.1 Security Organization and D.2 Employee User Access).
5.3.2	Shared – SOC2	You are responsible for satisfying the requirements in this section specific to background check procedures for your trusted persons. You inherit controls related to background checks of AWS employees that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section A. Policies and D.2 Employee User Access).
5.3.3, 5.3.4, & 5.3.8	Shared – SOC2	You are responsible for satisfying the requirements in this section specific to implementing training procedures for your Trusted Persons. AWS Private CA implements training requirements for trusted roles specific to physical access to cryptographic modules that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section A.1 Control Environment, B. Communications, and D.1 Security Organization).
5.3.6	Shared – SOC2	You are responsible for satisfying the requirements in this section specific to disciplinary actions for your trusted persons. You inherit controls related to disciplinary actions of AWS employees that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section A.1 Control Environment).
5.4	Shared – SOC2	You are responsible for configuring and enabling CloudTrail monitoring, CloudWatch alerting, and audit reporting capabilities that satisfy the requirements in this section. AWS Private CA helps you record and store logging events when you appropriately configure the service. You inherit controls related to availability of your logs that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section C.1 Service Commitments, D.3 Logical Security, D.6 Physical Security and

		Environmental Protection, D.8 Data Integrity, Availability, and Redundancy, and E.1 Monitoring Activities).
5.4.1	Shared – SOC2	You are responsible for configuring and enabling CloudTrail monitoring, CloudWatch alerting, and audit reporting capabilities that satisfy the requirements in this section. AWS Private CA provides the functionality to help you record and store logging events when the service is appropriately configured by you. You inherit controls related to availability of your logs, physical access/site security, CA/RA configuration management and AWS infrastructure logs that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section C.1 Service Commitments, D.3 Logical Security, D.6 Physical Security and Environmental Protection, D.7 Change Management, D.8 Data Integrity, Availability, and Redundancy, and E.1 Monitoring Activities).
5.4.2	Shared – SOC2	You are responsible for creating log processing procedures that satisfy the requirements in this section. You inherit controls related to physical access and site security, CA and RA configuration management, and AWS infrastructure logs that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section C.1 Service Commitments, D.3 Logical Security, D.6 Physical Security and Environmental Protection, D.7 Change Management, D.8 Data Integrity, Availability, and Redundancy, and E.1 Monitoring).
5.4.3	Shared – SOC2	You are responsible for configuring retention periods that satisfy the requirements in this section. You inherit controls related to physical access and site security logs and the availability of your logs (when configured) that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section D.6 Physical Security and Environmental Protection and D.8 Data Integrity, Availability, and Redundancy).
5.4.4	Shared – SOC2	You are responsible for configuring and enabling protections of your audit log data that satisfy the requirements in this section. You inherit controls related to physical access and site security logs that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section D.2 Employee User Access and Section D.6 Physical Security and Environmental Protection).
5.4.5	Shared – SOC2	You are responsible for configuring backup and retention periods that satisfy the requirements in this section. You inherit controls related to physical access and site security logs that are within the scope of the AWS Private CA SOC 2 Type 2 Report. You inherit controls related to availability of your logs (when you configure) that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see D.8 Data Integrity, Availability, and Redundancy).
5.4.6	Shared – SOC2	You are responsible for configuring and enabling CloudTrail monitoring, CloudWatch alerting, and audit reporting capabilities that satisfy the requirements in this section. You inherit controls related to the availability of your logs (when configured) that are within the scope of the AWS Private CA

		SOC 2 Type 2 Report (see Section D.8 Data Integrity, Availability, Redundancy and Data Retention and E.1 Monitoring Activities).
5.4.8	Shared – SOC2	You are responsible for performing periodic vulnerability assessments of your use of AWS Private CA that satisfy the requirements in this section. You inherit controls related to vulnerability assessments of infrastructure security controls that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section A.1 Control Environment and D.3 Logical Security).
5.5.1	Shared – SOC2	You are responsible for configuring record archival that satisfies the requirements in this section. You inherit controls related to availability of your archives (when configured) that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see D.8 Data Integrity, Availability, and Redundancy).
5.5.2	Shared – SOC2	You are responsible for configuring archive policies that satisfy the requirements in this section. You inherit controls related to availability of your archives (when configured) that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see D.8 Data Integrity, Availability, and Redundancy).
5.5.3	Shared – SOC2	You are responsible for configuring controls to protect archived data that satisfy the requirements in this section. You inherit physical access controls and availability of your logs (when you configure) that help you meet the requirements in this section that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section D.2 Employee User Access, D.6 Physical Security and Environmental Protection, and D.8 Data Integrity, Availability, and Redundancy).
5.5.4	Shared – SOC2	You are responsible for configuring archival backup procedures that satisfy the requirements in this section. You inherit controls related to availability of your archives (when you configure) that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see D.8 Data Integrity, Availability, and Redundancy).
5.5.5	PCA	AWS Private CA automatically timestamps Private CA logs (when you configure) as they are created.
5.5.7	Shared – SOC2	You are responsible for configuring IAM user access permissions that satisfy the requirements in this section. You inherit physical access controls that help you meet the requirements in this section that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section D.2 Employee User Access, D.6 Physical Security and Environmental Protection, and D.8 Data Integrity, Availability, and Redundancy).
5.7.1, 5.7.2, & 5.7.3	Shared – SOC2	You are responsible for implementing incident and compromise handling procedures specific to your use of AWS Private CA that satisfy the requirements in this section. You inherit incident and compromise handling procedures specific to physical site housing and infrastructure operations that help you meet the requirements in this section that are within the scope of the AWS Private CA SOC 2 Type 2 Privacy Report (see Section D.10

		Privacy).
5.7.4	PCA – SOC2	You inherit business continuity and disaster recovery procedures that help you meet the requirements in this section that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see D.8 Data Integrity, Availability, and Redundancy).
5.8	Shared – SOC2	You are responsible for satisfying the requirements in this section. You inherit controls related to availability of your archives (when configured) that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see D.8 Data Integrity, Availability, and Redundancy).
6.1.1.1	Shared	AWS Private CA uses cryptographic modules that provide the cryptographic strength of the generated keys as required in this requirement. You are responsible for selecting the appropriate AWS Regions that meet the FIPS 140-2 level 3 requirement for PAA and PAI key pair generation. You are responsible for satisfying the requirements in this section specific to logical multi-person access controls.
6.1.5	Shared	You are responsible for satisfying the requirements in this section. AWS Private CA helps you create certificates according to the CSA Matter Specification when you appropriately configure the service.
6.2.1 & 6.2.7	PCA	AWS Private CA uses cryptographic modules that provide the cryptographic strength of the generated keys as required in this section. You are responsible for selecting the appropriate AWS Regions that meet the FIPS 140-2 Level 3 requirement for key pair generation and physical multi-person controls.
6.2.2	Shared	You are responsible for satisfying the requirements in this section specific to logical multi-person access controls. AWS Private CA backs up private keys entirely by automation, without human involvement or access to plaintext CA private keys. AWS Private CA implements multi-person controls for physical access to cryptographic modules. You are responsible for selecting the appropriate AWS Regions that meet the FIPS 140-2 Level 3 requirement to inherit the physical multi-person controls.
6.2.4	PCA – SOC2	AWS Private CA backs up private keys entirely by automation without human involvement. AWS Private CA does not store CA private keys in plaintext. You inherit controls related to the backups of private CA keys with physical and cryptographic protection equal to or exceeding that for cryptographic modules within the CA site that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see D.2 Employee User Access, D.6 Physical Security and Environmental Protection, and D.8 Data Integrity, Availability, and Redundancy).
6.2.5	Shared	AWS Private CA does not archive CA private signature keys. You are responsible for requestor private encryption key requirements in this section.
6.2.6	PCA	AWS Private CA prevents CA private keys from being exported.
6.2.9	PCA	AWS Private CA uses HSMs that are online and have no notion of cryptographic key activation. AWS Private CA does not store

		private keys in plaintext.
6.5.1	Shared – SOC2	You are responsible for satisfying the requirements in this section specific to logical access and computer security controls for use of AWS Private CA. AWS Private CA helps you meet this requirement when you appropriately configure the service. You inherit controls related to logical access of AWS employees, network and computer security controls of the AWS infrastructure, and password parameter controls of AWS employee accounts that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section D.2 Employee User Access, D.3 Logical Security, and D.6 Physical Security and Environmental Protection).
6.6.1	PCA – SOC2	You inherit controls related to system development controls of the AWS Private CA service that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section D.7 Change Management).
6.6.2	Shared – SOC2	You are responsible for detecting configuration drift of your AWS Private CA service. You inherit controls related to software configuration controls of the AWS Private CA software that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section D.7 Change Management).
6.7	Shared – SOC2	You are responsible for satisfying the requirements in this section specific to network security controls for use of AWS Private CA. You inherit controls related to network security controls of the AWS infrastructure that are within the scope of the AWS Private CA SOC 2 Type 2 Report (see Section C.1 Service Commitments, D.3 Logical Security, and E.1 Monitoring Activities).
6.8	PCA	AWS Private CA provides the time and date information that asserts times within three minutes for certificates issued by AWS Private CA.
7 (All)	Shared	You are responsible for satisfying the requirements in this section. AWS Private CA helps you create certificates according to the CSA Matter Specification when you appropriately configure the service.

Appendix C

AWS Private CA Regions available for Device Attestation CAs

- US East (N. Virginia) – us-east-1
- US East (Ohio) – us-east-2
- US West (N. California) – us-west-1
- US West (Oregon) – us-west-2
- Africa (Cape Town) – af-south-1
- Asia Pacific (Hong Kong) – ap-east-1
- Asia Pacific (Tokyo) – ap-northeast-1
- Asia Pacific (Seoul) – ap-northeast-2
- Asia Pacific (Mumbai) – ap-south-1
- Asia Pacific (Singapore) – ap-southeast-1
- Asia Pacific (Sydney) – ap-southeast-2
- Canada (Central) – ca-central-1
- Europe (Frankfurt) – eu-central-1
- Europe (Ireland) – eu-west-1
- Europe (London) – eu-west-2
- Europe (Paris) – eu-west-3
- Europe (Stockholm) – eu-north-1
- Europe (Milan) – eu-south-1
- Middle East (Bahrain) – me-south-1
- South America (São Paulo) – sa-east-1