# Implementation Procedure for CSP and CSC Audits under ADEC Cryptographic Erasure System Certification for Cloud

Ver. 1.0

December 17, 2024

## Introduction

This standard defines the criteria for issuing erasure certificates for encrypted erasure of cloud storage in order to satisfy Compliance Requirement 4.2.2(5), “Measures at the time of renewal or disposal of information systems using cloud services,” as stipulated in the Guidelines for Establishing Standards for Measures by Government Agencies and Related Organizations (FY2023 edition), with respect to data erasure when using cloud storage.

The target organizations are Cloud Service Providers (CSPs), which provide cloud services, and Cloud Service Customers (CSCs), which use cloud services.

Encrypted erasure of cloud services is part of the information security management system. As a prerequisite for the audit implementation criteria, the target organization is assumed to be operating systems for the management of its own activities and services in accordance with the organization’s policies and the requirements of each management system standard.

This standard specifies the audit procedures and requirements (checklists) for target organizations, namely CSPs and CSCs.

Audit activities comprise the individual activities that make up the overall process from review of the application documents through completion of the audit.

## 1 Scope

This standard specifies the implementation procedure for audits of CSPs and CSCs. This audit shall be conducted by auditors appointed by ADEC (Association for Data Erase Certification).

## 2 Referenced Standards

The standards listed below constitute part of the provisions of this standard by being referenced herein. The latest editions of these referenced standards, including amendments, shall apply.

2.1 Security Assessment System for Government Information Systems (ISMAP)
(Information system Security Management and Assessment Program)

2.2 Standards referenced by the ISMAP Management Standards

| | |
|---|---|
| JIS Q 27001 | Management standards |
| JIS Q 27002 | Security controls |
| JIS Q 27017 | Controls related to cloud services |
| JIS Q 27014 | Governance standards (objectives and processes) |
| Unified Standards | A set of unified standards for cybersecurity measures for government agencies and related organizations |
| NIST SP 800-53 | A standard that specifies security and privacy controls for information systems and organizations of the United States federal government |

## 3 Terms and Definitions

3.1 CSC (Cloud Service Customer) An organization that uses cloud services and undergoes an audit for the purpose of using cloud encrypted erasure certificates.

3.2 CSP (Cloud Service Provider) An organization that provides cloud services and undergoes an audit for the purpose of issuing cloud encrypted erasure certificates.

3.3 ADEC (Association Data Erase Certification) Association for Data Erase Certification.

3.4 Client A person who requests an audit.

3.5 Auditor A person appointed by ADEC to conduct an audit.

3.6 Specification hearing A hearing meeting in which the auditor confirms service specifications with the CSP face-to-face or by other means.

3.7 Preliminary determination A determination by the auditor on service certification based on the specification hearing, checklist, log data, and other information.

3.8 Final approval meeting A meeting at ADEC to grant final approval based on the auditor's preliminary determination results.

3.9 Data storage system A service that enables data and files to be stored and managed via the Internet.

3.10 Encryption system Technology that encrypts data stored in the cloud and protects it from unauthorized access and misuse.

3.11 Key management system A system that centrally manages encryption keys in the cloud from generation through erasure.

3.12 Log data Data in which histories and information, such as usage status and data communications of the above systems, are recorded.

3.13 Nonconformity Failure to satisfy a requirement.

3.14 Major nonconformity A nonconformity that affects the system's ability to achieve intended results.

3.15 Minor nonconformity A nonconformity that does not affect the system's ability to achieve intended results.

## 4 Procedure for CSP Service Certification

### 4.1 Overall Flow

At the request of the CSP, ADEC audits whether the CSP's service satisfies the requirements for issuing erasure certificates for encrypted erasure of cloud storage. If nonconformities are found as a result of the audit, ADEC requests the CSP to implement corrective actions within a specified period. If the audit result is conforming, ADEC certifies the CSP's service as a certified service.

### 4.2 Certification Period

The certification shall be valid for three years.

### 4.3 Detailed Procedure for CSP Service Certification

#### 4.3.1 Completion of the Application by the CSP

The CSP downloads the application form from the ADEC website, completes it, and returns it to ADEC. CSC information, such as data owners and retention periods, is also compiled by the CSP to complete the application documents.

List of application documents

・Service Certification Application Form

Service overview; service organization relationship diagram; system configuration diagram; detailed system configuration list; log data configuration

#### 4.3.2 Review of the Application by ADEC

After receiving the application, ADEC selects the auditor for this audit. The auditor reviews the obtained application documents, prepares the audit plan, estimates the audit man-hours, extracts a checklist corresponding to the service content, and sends it to the CSP. The man-hours are calculated by adding differences identified from the application documents based on the standard audit man-hour table. The schedule for the specification confirmation hearing is decided in consultation with the CSP.

List of documents used

・Service Certification Application Form

・Checklist

・Audit Plan (including audit man-hours)

#### 4.3.3 CSP Response to the Checklist

The CSP reviews and responds to the checklist sent by ADEC and submits it to ADEC.

List of documents used

・Checklist

#### 4.3.3 Specification Confirmation Hearing

The auditor reviews the obtained application documents and checklist and, if there are any questions, confirms them with the CSP by e-mail or other means. After the preliminary confirmation, the auditor conducts a specification confirmation hearing with the CSP face-to-face or by other means using the application documents and the operational checklist. During the hearing, operation is confirmed in the production environment and logs are obtained from the production environment.

List of documents used

・Service Certification Application Form

・Checklist

・Log data from the production environment

#### 4.3.4 Preliminary Determination

The auditor reviews the results of the specification confirmation hearing, the checklist, and log data from the production environment, and conducts a preliminary audit to determine conformity for certification as to whether the requirements for a certified service are satisfied, then prepares an audit report. If a nonconformity is found, the process moves to 4.3.4.1, and preliminary audits are conducted until conformity is achieved.

List of documents used

・Audit Report

#### 4.3.4.1 If a Nonconformity Is Found

If a nonconformity is found in the auditor's preliminary determination, the auditor prepares a Finding Report and requests the CSP to implement corrective action within a specified period. After the CSP corrects the nonconformity, the auditor confirms the corrective action described in the Finding Report and conducts the preliminary audit again.

List of documents used

・Finding Report

#### 4.3.4.2 If a Nonconformity Is Not Corrected

If the CSP does not correct the nonconformity within the specified period, the auditor cannot complete the preliminary determination. The auditor escalates the matter to ADEC so that corrective action by the CSP will be taken, and ADEC continues to support the CSP's corrective action. When the corrective action is completed, the preliminary audit by the auditor is resumed.

List of documents used

・Finding Report

### 4.3.5 Final Approval

When the auditor determines that the CSP's service satisfies the requirements for a certified service, the auditor prepares an audit report and, if findings were identified, a Finding Report describing the corrective actions taken. The auditor submits these reports to the final approval meeting within ADEC, where the final decision is made. If the determination at the final approval meeting is a pass, ADEC sends the Service Certificate to the CSP. At the same time, ADEC invoices the CSP for the costs according to the audit man-hours.

List of documents used

・Service Certification Application Form

・Audit Report

・Service Certificate

## 4.4 Renewal of Certification

Three months before the end of the certification period, the CSP submits a renewal application to ADEC.

### 4.4.1 If There Are Significant Changes to the Service System

If there are significant changes to the service system, such as a major update of the service system, or if the checklist has been substantially revised, the CSP must undergo a service change certification audit for the changed parts.

### 4.4.2 If There Are No Changes or Only Minor Changes to the Service System

If there are no changes to the service system, or if there are only minor changes such as a minor version upgrade, and there are no updates to the checklist, the CSP must submit a renewal application.

----- End of File -----