Mass Revocation Incident Preparation and Testing Plan (MRIP&TP)

Shanghai Electronic Certification Authority (SHECA)

Version History

Date	Description of Changes	Version
2025.8.29	Original	1.0
2025.9.12	Supplementary Enhancements	1.1

CA Operator Contact Information

Shanghai Electronic Certification Authority Co., Ltd.

Address: 18/F, JiaJie International Plaza, No.1717, North Sichuan Road, Shanghai, China

Postal Code: 200080

Tel: 86-21-36393197

E-mail: report@sheca.com

1. Introduction

The management of **Shanghai Electronic Certification Authority** (hereinafter referred to as "**SHECA**") recognizes that the continuity of essential CA services depends on **effective certificate revocation and replacement processes**. These processes rely on robust IT infrastructure, effective customer communication, and rapid response capabilities.

To mitigate risks associated with a **Mass Revocation Event (MRE)**, which could cause disruption to customers, financial losses, and damage to trust, management has authorized the development, implementation, and maintenance of this **Mass Revocation Incident Preparation and Testing Plan (MRIP&TP)**.

The MRIP&TP is aligned with SHECA policies, compliance obligations, and industry best practices. It provides a framework for MRE response, customer communication, certificate replacement, revocation, and plan testing. This plan also aims to **ensure compliance** with industry and root store requirements, such as the CA/Browser Forum TLS Baseline Requirements and Mozilla Root Store Policy.

2. Mission and Objectives

The mission of this plan is to **ensure a well-coordinated, rapid, and effective response to a Mass Revocation Event** while maintaining compliance and minimizing disruptions.

Plan objectives are to:

- **Define clear roles and responsibilities** for the teams assigned with handling MREs.
- **Identify critical processes and time-sensitive milestones** for mass revocation preparedness.

- **Provide timely, clear communication** to customers and other stakeholders to **minimize disruptions**.
- **Develop and document certificate revocation** strategies and procedures to ensure **swift certificate replacement** and compliance with revocation deadlines.
- **Report any delayed revocations** to Bugzilla.
- **Improve readiness** through effective training, testing, and continuous improvement of mass revocation procedures.

3. Scope

This plan applies to the **scoping, implementation, execution, review, training, testing, and improvement** of **mass revocation processes** at SHECA. It supports compliance with Mozilla Root Store Policy Section 6.1.3 and covers:

- Maintenance of a well-documented and actionable mass revocation plan.
- Rapid communication with customers and affected third parties.
- Certificate replacement strategies.
- Revocation execution and publication of certificate status.
- Operational coordination and team responsibilities.
- Compliance with CA/Browser Forum requirements.
- Demonstrating implementation and feasibility through annual testing (simulations, tabletop exercises, or controlled test environments).
- Incorporating lessons learned by making plan improvements.
- Third-party assessment and external compliance evaluation.

4. Classification

4.1 Definition and Declaration of an MRE

4.1.1 Definition of an MRE

A Mass Revocation Event (MRE) is defined as:

The revocation of a substantial number of TLS server certificates within a relatively short timeframe due to a common cause, compliance requirement, or security incident. The impact threshold is based on the CA's total issuance volume and operational scale.

4.1.2 Trigger Conditions and Activation Criteria of an MRE

- Trigger threshold: A Mass Revocation Event is triggered when the number of affected TLS certificates **≥ 100** TLS certificates, or **≥ 1%** of the CA's active TLS certificates.
- Specific triggering scenarios:

Compromise or suspected compromise of a CA private key: A Mass Revocation Event is triggered if the number of certificates requiring revocation due to private key compromise meets or exceeds the aforementioned threshold.

Compliance failures affecting TLS server certificates: A Mass Revocation Event is triggered by certificate issuance not conforming to the CA/Browser Forum or Mozilla Root Certificate Store policies, where the number of affected certificates exceeds the threshold.

Discovery of major vulnerabilities impacting server private keys: A Mass Revocation Event is triggered by HeartBleed-class vulnerabilities when the number of affected certificates reaches the threshold.

Other circumstances: Other circumstances causing the number of certificates to be revoked to exceed the threshold.

Note: The management team will evaluate and decide whether to initiate a mass revocation event based on these criteria.

4.1.3 Execution Requirements

Upon initiation of a Mass Revocation Event, all revocation operations must be completed within the timeframe specified in Section 4.9.1.1 of the TLS Baseline Requirements to ensure timely updates of certificate status.

Incident response requires managing customer notification, operational adjustments, compliance reporting, and other tasks, demanding coordination across departments to ensure completion within the prescribed timeframe while maintaining normal business operations.

4.2 Customer Contact Information

SHECA has established a comprehensive customer information management system, specifically used for storing and managing customer contact information, including but not limited to customer name, contact person's name, position, mobile phone number, email address, company address, etc.

To ensure the accuracy and timeliness of customer contact information, the following measures are taken:

- When applying for a certificate, customers are required to accurately fill in and submit contact information, and SHECA staff conduct preliminary verification of the information.
- Establish a regular update mechanism, sending a contact information confirmation notice to customers at least once a year, and customers are required to feedback the update status within **30 days** after receiving the notice.
- When a customer has a change in company name, contact person, etc., they should actively submit a change application to SHECA in a timely manner, and SHECA will complete the information update within **3 working days** after receiving the application.
- Arrange special personnel to be responsible for the maintenance and monitoring of the customer information management system, regularly check the integrity and validity of the information, and mark and follow up on invalid or expired information.

4.3 Identification of Manual and Automated Processes

4.3.1 Automated Processes

- **Automated Script:** Execute automated scripts for detection and reissuance of all affected certificates.

- **Customer Notification:** The system notifies Customers of the impending revocation time of the original certificate through multiple channels (such as Email, SMS, and the official WeChat public account) and reminds them that the certificate has been reissued.
- **Automated Certificate Reissuance:** After notifying Customers, the system automatically triggers the certificate update script to reissue subscriber certificates using the automated service.
- **Automated Certificate Revocation:** Prior to the established revocation timeframe, the system automatically executes the revocation script to revoke all affected certificates.
- **CRL and OCSP Publication:** SHECA's Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) are automatically published and updated by the system to ensure timely synchronization of revocation information.
- **Certificate monitoring:** During the execution of Mass Revocation, the system continuously monitors all affected sites to ensure comprehensive detection and updating of all relevant certificates.

4.3.2 Manual process

- **After-sales assistance:** For key customers or those with special requirements, in addition to the automatically sent Email, the Customer relations team shall proactively conduct manual communication to provide a detailed explanation of the situation.
- **Handling of complex certificate replacement cases:** For complex scenarios where certificate replacement is challenging due to technical causes or unique customer configurations, the Certificate Replacement Team shall provide manual technical support and solutions.
- **Handling abnormal revocation situations:** In instances where revocation commands fail to execute properly due to system failures, the relevant teams shall undertake manual intervention.
- **Communication and Coordination with Third-Party Entities:** Communication with third-party entities such as root stores and regulatory authorities shall be conducted manually to transmit and coordinate information.

5. Decision Points and Strategies

5.1 Initial Assessment and Activation

Upon identification of a potential MRE, the **Management Team** will:

- Assess the incident's scope and severity against the defined MRE criteria.
- Issue an internal alert to notify team members of possible activation.
- Determine affected certificate population and impacted customers.
- Estimate timelines required to perform notification, replacement, and revocation.
- Initiate a conference call to validate findings and coordinate response.
- Mobilize internal teams and notify external stakeholders as needed.

5.2 Response Phases

An MRE will be managed in **four structured phases**:

Phase 1 – Customer Communication

- Within **24 hours** after confirming the mass revocation event, send an initial revocation notification email to the affected customers, stating the basic situation of the event, the expected impact, and the subsequent processing procedures in the email.
- Publish an MRE notification on SHECA's website to provide certificate replacement timelines and procedures.
- Arrange special personnel to answer customer calls or emails, respond to customer inquiries and feedback in a timely manner.
- Engage technical support teams for high-priority customers, to ensure they have been aware of the event and their technical problems are properly addressed.
- Target: Affected customers are notified in effective communication channels, and necessary guidance is in place.

Phase 2 – Certificate Replacement

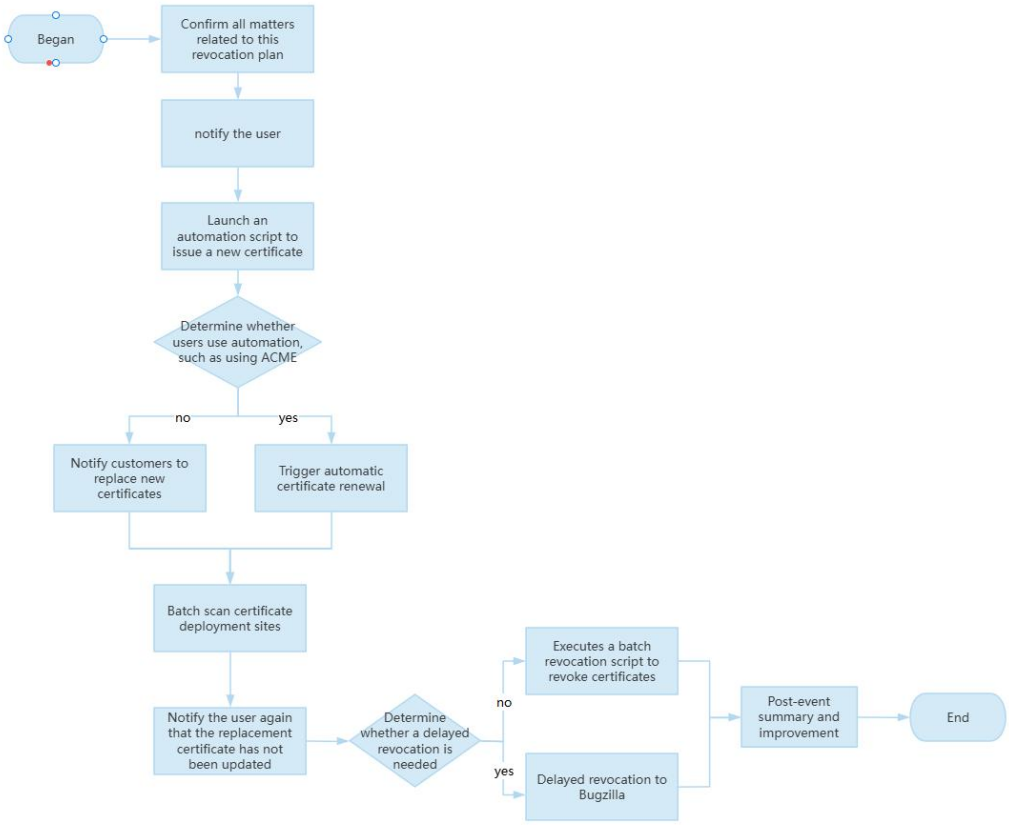
- For automated renewal or reissuance, the certificate replacement will be completed through the automated system within **24 hours** after confirming the mass revocation event.
- For complex cases, the certificate replacement team will contact the customer within **24 hours** after confirming the mass revocation event, and continually offer manual assistance until the certificate replacement is completed.
- Establish a certificate replacement progress tracking mechanism, update the progress of customer certificate replacement daily, and focus on following up on customers who have not completed replacement.
- Target: Complete customers' certificate replacement in a timely manner.

Phase 3 – Certificate Revocation

- Execute mass revocation operation in compliance with the revocation timelines specified in the latest CA/B Forum TLS baseline requirements.
- Update the CRL and ensure the accuracy and timeliness of OCSP responses within **24 hours** after the revocation operation is completed.
- In case of failure to complete revocation on time, immediately analyze the reasons and report the delay and handling measures to Bugzilla within **24 hours**.
- Target: Complete the revocation of all certificates that should be revoked in accordance with the specified time frame.

Phase 4 – Post-Mortem and Improvement

- Conduct an internal review after the handling of the mass revocation event is completed to review and analyze the effectiveness of event response.
- Sort out and form a written report on lessons learned, clarifying existing problems and improvement directions.
- Update the MRIP&TP based on findings, and release new versions on SHECA's official website.
- Target: Comprehensively summarize the experience of event handling, effectively improve plans and processes, and enhance the ability to respond to similar events.



Picture1. Diagram of the response phases

6. Response Team Organization and Responsibilities

6.1 Organizational Chart

Response Team Roles

Team and Team Leader	Role	Responsibilities
Management Team - [SHECA Security Certification Committee]	Senior Leadership	Approves, monitors, and authorizes mass revocation responses.
Customer Relations Team - [Alvin.Wang]	Public Relations and Support	Communicates with customers and handles inquiries.
Certificate Replacement Team - [Jasmin.Tang]	Validation and Technical Support	Assists customers with certificate replacement.
Certificate Revocation Team - [Damon.Zhang]	Compliance and Operations	Executes revocation and publishes status updates.

External Communications - [Yihang Shao]	Legal and Policy	Notifies root stores, regulators, and stakeholders.
Compliance and Legal Teams - [Ning Zheng]	Risk and Governance	Ensures adherence to legal and compliance obligations.

7. Plan Training, Testing, and Continuous Improvement

7.1 Training and Awareness

All team members must undergo initial training on the Mass Revocation response procedures upon onboarding and participate in annual refresher training. The training shall include, but is not limited to, the following:

- A detailed introduction to this Mass Revocation Incident Preparation and Testing Plan (MRIP&TP).
- Duties and responsibilities of each team.
- Various response procedures and their execution standards.
- Effective communication skills and crisis management.

Training methods encompass various formats, including online courses, in-person lectures, and case studies, to ensure each team member fully comprehends and masters the relevant knowledge and skills.

Furthermore, information, case studies, and reminders related to Mass Revocation events are regularly disseminated to team members to enhance their vigilance and responsiveness. All training sessions incorporate assessments; individuals who do not pass are required to retake the training until successfully qualified.

7.2 Plan Testing and Simulation

This plan will be tested at least once a year. The test will be conducted through simulated revocation scenarios to evaluate the following aspects:

- **Effectiveness of customer communication:** Including the timeliness, accuracy, clarity of notifications, and the efficiency of handling customer feedback.
- **Speed and accuracy of certificate replacement:** Test the proportion of certificate replacements completed within the specified time and the validity of the replaced certificates.
- **Efficiency of revocation execution:** Evaluate the timeliness of revocation operations and the update speed and accuracy of CRL and OCSP responses.
- Test forms include tabletop exercises, simulated actual combat exercises, etc. During the test, record the completion of various indicators and identify existing problems and gaps.

7.3 Continuous Improvement

After each test and the handling of actual mass revocation events, a detailed post-test analysis will be conducted. A special analysis team will be established to collect and analyze data during the test or event handling process, and summarize successful experiences and existing problems.

Based on the analysis results, formulate improvement measures and action plans, clarify responsible persons and completion times. Conduct a comprehensive review of this MRIP&TP at least every year, and update and improve the plan according to the actual situation, changes in industry standards, and lessons learned. Ensure that the plan always remains applicable and effective and can respond to changing situations and needs.

For the latest version of the plan, please visit our website https://www.sheca.com/repository.

8. Third-Party Assessment

Engage a third-party assessment agency for evaluation annually, starting from the next audit cycle of CA occurring on or after June 1, 2025.

Provide documentation demonstrating that:

- This MRIP&TP is well-documented and actionable.
- Testing exercises have been conducted and documented, including test processes, timelines, results, and any remediation steps taken.

The assessment results will be included as part of the SHECA's regular audit, using its audit reporting cadence, under the ETSI/ACAB'c or WebTrust audit framework. Reporting must include:

- Confirmation that the assessment or review was conducted
- A summary of the scope and methodology used
- Key findings, including whether the plan is documented, feasible, and regularly tested
- Recommendations or remediation items, if applicable
- A statement of overall plan sufficiency, testing, and plan improvement
- Any other information necessary to provide Mozilla with clear insight into the CA operator's mass-revocation readiness

A report summarizing this information will be submitted on an annual basis, until Mozilla indicates otherwise.

The third-party assessment agency should have relevant professional knowledge and experience, including aspects such as CA operations, policy compliance, disaster recovery, business continuity, certificate revocation, and certificate replacement. Ideally, the assessors should be familiar with ETSI or WebTrust frameworks. To ensure objectivity, the assessors must be sufficiently independent from the operations of the CA organizationally and capable of providing a comprehensive and impartial assessment.

9. Conclusion

This **Mass Revocation Incident Preparation and Testing Plan** is a critical component of SHECA's commitment to operational resilience and compliance.

By strictly implementing this plan, SHECA will be able to respond quickly and effectively in the face of mass revocation events, minimize the impact on customers and its own business, and maintain industry trust and reputation. SHECA will continuously improve this plan to ensure that it always meets the latest industry standards and requirements and provides reliable CA services to customers.