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

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

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.*

A Mass Revocation Event would be triggered, and this plan activated, based on:

- **Absolute Volume Impact** – Affects ≥ 100 TLS certificates.
- **Relative Issuance Impact** – Affects ≥ 1% of the CA's active TLS certificates.
- **Timeframe Impact** – Requires revocation within timeframes set forth in section 4.9.1.1 of the TLS Baseline Requirements.
- **Operational Burden** – Requires major customer outreach, urgent operational changes, or compliance reporting.

Or in response to any of the following:

- **Compromise or suspected compromise** of a CA private key.

- **Compliance failures** affecting TLS server certificates.
- **Discovery of a major vulnerability** impacting server private keys (e.g., HeartBleed).

The **Management Team** will assess and declare a Mass Revocation Event based on these criteria.

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

Automated Processes

- **Batch generation of certificate revocation instructions:** Through the system's built-in rule engine, according to the conditions triggering the mass revocation event, automatically generate revocation instructions for the affected certificates.
- **Batch upload of revocation information to the CRL (Certificate Revocation List) system:** After generating revocation instructions, the system automatically uploads relevant information to the CRL system to ensure the timely update of CRL.
- **Sending initial revocation notification emails to customers:** Using the email automated sending system, according to the email addresses in the customer information management system, automatically send initial revocation notification emails to affected customers.

Manual Processes

- **Evaluation and confirmation of MRE:** After receiving information about potential mass revocation events, the management team should conduct manual investigation and evaluation, and confirm whether it constitutes a mass revocation event.
- **Personalized communication with special customers:** For important customers or customers with special needs, in addition to automatically sent emails, the customer relations team is encouraged to conduct manual communication to explain the situation in detail.

- **Handling of complex certificate replacement cases:** For complex cases where certificate replacement is difficult due to technical reasons or special customer configurations, the certificate replacement team should provide manual technical support and solutions.
- **Handling of abnormal situations during revocation:** For system failures causing revocation instructions failed to be executed normally, relevant teams should manually intervene.
- **Communication and coordination with third-party organizations:** Communication with third-party organizations such as root stores and regulatory authorities requires manual transmission and coordination of 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 a 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.

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 -	Validation and	Assists customers with certificate

[Jasmin.Tang]	Technical Support	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 receive initial training on mass revocation response procedures during onboarding and participate in annual update training. The training content includes the details of this MRIP&TP, the responsibilities of each team, response processes, communication skills, etc. Training is conducted through various methods such as online courses, on-site lectures, and case studies to ensure that team members fully understand and master relevant knowledge and skills.

Regularly send information and reminders related to mass revocation events to team members to improve their vigilance and response awareness to mass revocation events. Team members are required to pass an assessment after training, and those who fail the assessment should retake the training until they pass.

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.

It is strongly recommended that assessment results be included as part of the CA operator'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 is expected to 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.