

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

Shanghai Electronic Certification Authority (SHECA)

Version History

Date	Description of Changes	Version

CA Operator Contact Information

1. Introduction

Shanghai Electronic Certification Authority SHECA
effective certificate revocation and replacement
processes

Mass Revocation Event (MRE)
Mass Revocation Incident Preparation and Testing Plan (MRIP&TP)
ensure compliance

2. Mission and Objectives

ensure a well-coordinated, rapid, and effective response to a Mass Revocation
Event

- Define clear roles and responsibilities
- Identify critical processes and time-sensitive milestones
- Provide timely, clear communication minimize disruptions

- Develop and document certificate revocation replacement swift certificate
- Report any delayed revocations
- Improve readiness

3. Scope

scoping, implementation, execution, review, training, testing, and improvement mass revocation processes

-
-
-
-
-
-
-
-
-

4. Classification

4.1 Definition and Declaration of an MRE

Mass Revocation Event (MRE)

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.

- Absolute Volume Impact
- Relative Issuance Impact
- Timeframe Impact
- Operational Burden
- Compromise or suspected compromise

- Compliance failures
- Discovery of a major vulnerability

Management Team

4.2 Customer Contact Information

-
- 30 days
- 3 working days
-

4.3 Identification of Manual and Automated Processes

Automated Processes

- Batch generation of certificate revocation instructions:
- Batch upload of revocation information to the CRL (Certificate Revocation List) system:
- Sending initial revocation notification emails to customers:

Manual Processes

- Evaluation and confirmation of MRE:
- Personalized communication with special customers:

- Handling of complex certificate replacement cases:
- Handling of abnormal situations during revocation:
- Communication and coordination with third-party organizations:

5. Decision Points and Strategies

5.1 Initial Assessment and Activation

Management Team

-
-
-
-
-
-

5.2 Response Phases

four structured phases

Phase 1 – Customer Communication

- 24 hours

-
-
-
-

Phase 2 – Certificate Replacement

-

24 hours

- 24 hours

-

-

Phase 3 – Certificate Revocation

-

- 24 hours

-

24 hours

-

Phase 4 – Post-Mortem and Improvement

-

-

-

-

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]		
Customer Relations Team - [Alvin.Wang]		
Certificate Replacement Team -		

[Jasmin.Tang]		
Certificate Revocation Team - [Damon.Zhang]		
External Communications - [Yihang Shao]		
Compliance and Legal Teams - [Ning Zheng]		

7. Plan Training, Testing, and Continuous Improvement

7.1 Training and Awareness

7.2 Plan Testing and Simulation

-
-
-
-

7.3 Continuous Improvement

8. Third-Party Assessment

-
-
-
-
-
-
-

9. Conclusion

Mass Revocation Incident Preparation and Testing Plan