大规模吊销事件准备与测试计划（MRIP&TP）

版本历史

生效日期	变更描述	版本
2025.8.31	初次发布	1.0
2025.9.12	措辞调整	1.1
2025.11.20	增加特别声明 增加对于合作伙伴的演练要求 响应团队角色	1.2
2026.11.11	售后渠道标准转办路径 证书影响范围的评估 客户信息更新维护 事件结束后复盘报告的编写	1.3

CA 运营商联系信息

上海市数字证书认证中心有限公司有限公司

地址：中国上海市四川北路 1717 号嘉杰国际广场 18 层

邮政编码：200080

电话：86-21-36393197

电子邮件：report@sheca.com

1. 引言

上海市数字证书认证中心有限公司**（以下简称“SHECA”）**管理层认为，关键 CA 服务的连续性依赖于有效的证书吊销及替换流程。这些流程依赖于稳健的 IT 基础设施、有效的客户沟通及快速响应能力。

为降低可能导致客户中断、财务损失及信任受损的大规模吊销事件（MRE）相关风险，管理层已授权制定、实施及维护本大规模吊销事件准备与测试计划（MRIP&TP）。

大规模吊销事件准备与测试计划（MRIP&TP）符合 SHECA 的政策、合规义务及行业最佳实践。该计划为大规模吊销事件响应、客户沟通、证书更换、吊销及计划测试提供了框架。

本计划旨在确保符合行业及根证书库要求，如 CA/Browser 论坛 TLS 基线要求和 Mozilla 根证书库政策。

特别声明

公共可信 TLS 证书的吊销严格遵循 TLS Baseline Requirements 的强制性要求，无论证书应用于何种场景(包括**关键基础设施**相关服务),SHECA 均**不**接受任何形式的**延迟吊销**申请，这是保障证书信任体系有效性的核心原则。

一旦触发 TLS Baseline Requirements（或 SHECA TLS CP/CPS，UniTrust Global 订户协议）规定的吊销条件，SHECA 将立即启动本吊销计划，并同步提供替换证书签发服务。请客户在规定时限内完成证书切换。为满足最低合规要求，时限届满 SHECA 有权执行**强制吊销**。客户未及时替换证书导致业务中断或安全事件所造成的损失，SHECA 不承担责任。

2. 使命与目标

本计划的使命是**确保对大规模吊销事件的协调有序、快速且有效的响应**，同时保持合规并最大限度减少中断。

计划目标包括：

- 明确负责处理大规模吊销事件的团队角色与职责。
- 识别大规模吊销准备中的关键流程和时间点里程碑。
- 向客户及其他利益相关方提供及时、清晰的沟通机制，以最大限度减少业务中断。
- 制定并记录证书吊销策略和程序，确保证书更换符合吊销时限要求。
- 向 Bugzilla 报告任何延迟的吊销。
- 通过有效的培训、测试及持续改进大规模吊销程序，提高准备度。

3. 范围

本计划适用于上海市数字证书认证中心有限公司（SHECA）大规模吊销流程的范围界定、实施、执行、审查、培训、测试及改进，支持遵守 Mozilla 根证书库政策第 6.1.3 节，涵盖以下要点：

- 维护一份文档完善且可操作的大规模吊销计划。
- 与客户及受影响第三方的快速沟通。
- 证书更换策略。
- 吊销执行及证书状态发布。
- 运营协调与团队职责。
- 遵守 CA/Browser Forum 要求。
- 通过年度测试（模拟、桌面演练或受控测试环境）展示实施的可行性。

- 通过吸取经验教训，持续改进计划。
- 第三方评估及外部合规性审核。

4. 分类

4.1 大规模吊销事件的定义与声明

4.1.1 大规模吊销事件（MRE）定义

因共同原因、合规要求或安全事件，在较短时间内吊销大量 TLS 服务器证书。阈值基于 CA 的总签发量及运营规模。

4.1.2 触发条件与启动依据

触发阈值：当撤销的 TLS 证书数量达到或超过 100 个，或撤销的证书数量达到或超过 CA 有效 TLS 证书总数的 1% 时触发。

具体触发场景：

CA 私钥泄露或疑似泄露：若私钥泄露导致需撤销的证书数量达到上述阈值，触发大规模吊销事件。

影响 TLS 服务器证书的合规失败：如证书签发不符合 CA/Browser Forum 或 Mozilla 根证书库要求，且受影响证书数量超阈值，触发事件。

发现影响服务器私钥的重大漏洞：如 HeartBleed 类漏洞，若受影响证书数量达阈值，触发事件。

其他：其他导致需吊销证书数量超阈值的情况。

SHECA 会根据实际情况判断是否触发大规模撤销事件并进行通知。

4.1.3 执行要求

启动大规模吊销事件后，需在 TLS 基线要求第 4.9.1.1 节规定的时间框架内完成所有吊销操作，确保证书状态及时更新。

事件响应中需应对客户通知、运营调整、合规报告等工作，需协调各部门资源，保障在规定时间内完成操作并维持正常业务运转。

4.2 客户联系信息

上海市数字证书认证中心有限公司已建立完善的客户信息管理系统，用于存储和管理客户的联系信息，包括但不限于客户名称、联系人姓名、职位、手机号码、电子邮件地址及公司地址等。

为确保客户联系信息的准确性和及时性，采取以下措施：

- 信息提交与核实：客户在申请证书时，必须准确填写并提交联系信息。上海市数字证书认证中心有限公司将对提交的联系信息进行初步核实，确保信息的完整性和准确性。
- 定期更新机制：每年至少一次，向客户发送联系信息确认通知，客户应在收到通知后 30 天内完成信息确认或更新。如有变更，客户需在规定时间内反馈更新情况。
- 主动变更通知：若客户公司名称、联系人或其他关键信息发生变更，客户应主动向上海市数字证书认证中心有限公司提交变更申请。公司将在收到申请后 3 个工作日内完成信息更新。
- 信息维护与监控：SHECA 在万维信订单系统制定并维护客户联系信息清单，以确保客户联系信息的准确性和及时性。客户联系信息清单包含客户名称、联系人姓名、职位、手机号码、电子邮件地址及公司地址等信息；万维信订单系统会自动向 90 天内未更新信息的订户发送提示，提醒其核查并更新订单系统中留存的联系信息及其他关键数据，以确保订户信息的持续准确与有效。专人负责客户信息管理系统的日常维护与监控，定期检查信息的完整性和有效性，对无效或过期的信息进行标记，并及时跟进处理，确保信息始终保持最新状态。

4.3 手动与自动流程的识别

4.3.1 自动化流程

- 自动化脚本重签证书：调用自动化脚本批量重签涉及的所有证书，确保证书快速且准确地更新。
- 系统通知：系统通过多种方式（如电子邮件、短信和微信公众号）通知客户原证书即将吊销的时间，并提醒证书已经重新签发。
- 自动化更新证书：在通知客户后，系统自动触发证书更新脚本，更新使用自动化服务的订户证书。
- 自动化吊销证书：在设定的截止时间，系统自动执行吊销脚本，吊销所有受影响的证书。
- CRL 和 OCSP 发布：SHECA 的证书吊销列表（CRL）和在线证书状态协议（OCSP）由系统自动发布和更新，确保吊销信息及时同步。
- 证书扫描：在大规模吊销执行期间，系统会持续扫描所有受影响站点，确保相关证书得到全面检测和更新。

4.3.2 手动流程

- **售后协助**：对于重要客户或有特殊需求的客户，除自动发送的电子邮件外，客户关系团队应主动进行人工沟通，详细说明情况。
- **复杂证书更换案例的处理**：对于因技术原因或客户特殊配置导致证书更换困难的复杂案例，证书更换团队应提供人工技术支持和解决方案。
- **吊销异常情况的处理**：对于因系统故障导致吊销指令未能正常执行的情况，相关团队应进行人工干预。
- **与第三方机构的沟通协调**：与根存储库及监管机构等第三方机构的沟通需通过人工方式传递和协调信息。

5. 决策点与策略

5.1 初步评估与启动

在识别潜在的大规模吊销事件（MRE）后，管理团队将按照以下步骤进行初步评估与启动：

- 评估适用规则：内控合规部判断所违反的 BR 条款及适用的 BR 吊销时间限制（部门负责人审核）。
- 评估事件范围与严重性：万维信事业部根据适用规则，准确计算受影响的证书数量（部门负责人审核），确定是否符合触发大规模吊销的条件。
- 暂停签发和吊销服务：一旦确认触发大规模吊销条件，立即暂停所有 TLS 证书的签发和吊销服务，直至完成大规模吊销。
- 发布内部警报：及时发布内部警报，通知相关团队成员事件的潜在发生，并启动预警机制，为可能的事件响应做好准备。
- 识别受影响的证书群体与客户：明确受影响的证书群体和客户，确保能够迅速定位需要吊销的证书以及可能需要特别关注的客户。
- 时间估算与资源规划：根据事件的严重性，估算吊销、证书更换和客户通知所需的时间，并合理安排资源，确保各项任务按时完成。
- 召开协调会议：召集相关团队召开紧急电话会议，确认事件调查结果，讨论并协调响应措施，包括后续的行动计划、责任分配以及可能的外部沟通需求。
- 动员内部团队与通知外部方：动员内部各部门迅速行动，确保协调一致。同时，根据事件的影响范围和合规要求，及时通知外部相关方，如监管机构、根证书存储库等，以便共同应对事件。

5.2 响应阶段

大规模吊销事件将分为四个结构化阶段进行管理：

阶段 1 – 客户沟通

在确认大规模吊销事件后的 24 小时内，向受影响客户发送初步吊销通知邮件，说明事件基本情况、预期影响及后续处理流程。

在上海市数字证书认证中心有限公司（SHECA）网站发布大规模吊销事件通知，提供证书更换的时间安排和流程。

安排专门人员接听客户电话或回复邮件，及时响应客户咨询与反馈。

对于客户反馈的证书问题，进行书面记录，其中合规性问题应通过统一渠道报告内控合规部（report@sheca.com）。

动员技术支持团队为高优先级客户提供服务，确保其知晓事件并妥善解决技术问题。

目标：通过有效沟通渠道通知受影响客户，并提供必要指导。

第二阶段 – 证书更换

对于具备自动续期或重新签发条件的客户，通过自动化系统在 24 小时内完成证书更换。

对于需要人工协助的客户，证书更换团队将在收到客户请求后 24 小时内联系客户，了解具体情况并提供技术支持。

建立证书更换进度跟踪机制，每日更新客户证书更换进度，重点跟进尚未完成更换的客户。

目标：及时完成所有客户的证书更换。

备注：未避免业务中断，客户应及时更换证书。SHECA 不接受任何延迟吊销请求。

第三阶段 – 证书吊销

按照最新 CA/B 论坛 TLS 基线要求中规定的吊销时间表执行大规模吊销操作。

检查吊销清单完整性，确保所有受影响的正式订户证书和预证书均已吊销。

更新 CRL，确保吊销操作完成后 24 小时内 OCSP 响应的准确性与及时性。

如未能按时完成吊销，须立即分析原因，并在 24 小时内向 Bugzilla 报告延迟情况及处理措施。

目标：在规定时间内完成所有应吊销证书的吊销工作。

第四阶段——事后总结与改进

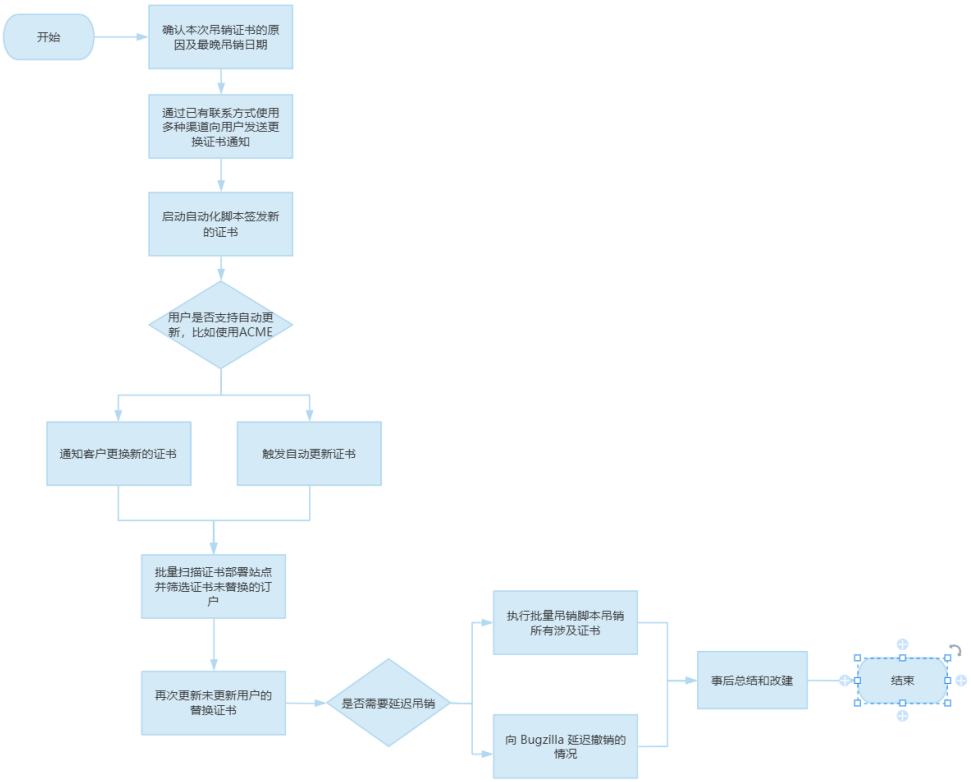
大规模吊销事件处理完成后，开展内部复盘，审查并分析事件响应的有效性。

整理并形成书面报告，总结经验教训，明确存在的问题及改进方向。

根据复盘结果更新大规模吊销事件准备与测试计划（MRIP&TP），并在上海市数字证书认证中心有限公司官方网站发布新版。

目标：全面总结事件处理经验，有效完善计划与流程，提升应对类似事件的能力。

总体流程如下：



6. 响应团队组织与职责

6.1 组织结构图

响应团队角色

团队及团队负责人	角色	职责
管理团队 - [SHECA 安全认证委员会]	高级领导	批准、监督并授权大规模吊销响应工作。
客户关系团队 - [王家泰]	公共关系与支持	负责与客户沟通及处理咨询。
证书更换团队 - [石慧]	验证与技术支持	协助客户完成证书更换重签及组织验证工作。
证书吊销团队 - [张晓]	合规与运营	执行订户证书批量吊销操作及吊销清单核对工作。

证书吊销团队-【赵鹰侠】	开发与技术支持	协助完成已吊销证书的统计核对，以及 CRL 的发布的工作。
证书吊销团队-【东樑】	运维与技术支持	负责数据库数据导出工作。
证书吊销团队-【王君】	CA 运营支持	执行中级根吊销操作和 ARL 的发布工作。
外部沟通 -[蔡子宁]	法律与政策	通知根证书库、监管机构及利益相关方。
合规与法律团队 -[郑宁]	风险与治理	确保遵守法律及合规义务。

7. 计划培训、测试与持续改进

7.1 培训与意识提升

所有团队成员在入职时必须接受大规模吊销响应程序的初始培训，并每年参加一次更新培训。培训内容包括但不限于：

- 本《大规模吊销事件准备与测试计划》（MRIP&TP）的详细介绍。
- 各团队的职责与分工。
- 各类响应流程及其执行标准。
- 有效的沟通技巧与危机管理。

培训方式包括在线课程、现场讲座和案例分析等多种形式，以确保每位团队成员充分理解并掌握相关知识和技能。

此外，定期向团队成员发送与大规模吊销事件相关的信息、案例和提醒，以提高他们的警觉性和响应意识。所有培训均设有考核，未通过者需重新参加培训，直到合格为止。

7.2 计划测试与模拟

7.2.1 测试内容

本计划将至少每年进行一次全面的测试，测试通过模拟吊销场景来评估和验证以下关键方面：

客户沟通的有效性：

评估客户通知的及时性、准确性和清晰度，确保信息能够迅速且准确地传递给所有受影响客户。同时，检查客户反馈的处理效率，确保客户能在最短时间内获得所需支持。

合作伙伴的响应能力：

要求合作伙伴制定 MRIP&TP 应急计划，包括组建响应团队、自动化重签脚本、网络变更流程、关键基础设施应急计划等。

核查所有合作伙伴的吊销应急计划，确认其已制定计划、文档内容完整且自动化脚本满足 24 小时吊销时限要求。

要求每个合作伙伴每年与 SHECA 开展联合演练，确保全流程可在各方协调下执行且具备可操作性。

证书更换的速度与准确性：

测试在规定时间内完成证书更换的比例，验证证书更换的有效性，确保客户能够顺利进行证书替换，并避免业务中断。

吊销执行的效率：

评估吊销操作的及时性，确保吊销指令的快速执行。特别是检查 CRL 和 OCSP 的响应速度与准确性，确保所有证书的吊销状态能够实时更新。

7.2.2 测试形式

模拟实战演练：通过模拟实际吊销事件，全面评估各项流程的执行效率，从证书吊销到客户通知、证书更换的全过程。

7.2.3 测试记录与问题识别

在测试过程中，详细记录每个环节的指标完成情况，分析存在的问题并识别性能差距。

针对发现的问题，提出改进方案，并在后续测试中进行跟踪验证，确保持续优化。

7.3 持续改进

事后分析与计划审查：

每次测试及实际大规模吊销事件处理后，将进行详细的事后分析。

内控合规部牵头复盘流程，汇总事件时间线、响应动作日志、通知记录、用户反馈、系统日志等原始数据；邀请各职能代表参会，回顾响应流程中的关键节点（如检测、决策、通知、恢复）；识别响应中的亮点与短板；记录各方提出的改进建议。

序号	复盘阶段	关键动作	责任人
1	复盘启动	成立复盘小组，概括描述本次事件，明确复盘安排	合规
2	客户数据收集	收集吊销通知记录、客户清单、客户反馈问题台账	万维信

序号	复盘阶段	关键动作	责任人
3	后台数据归集	收集系统日志、吊销清单、CRL/OCSP	万维信（技术中心协同）
4	客户数据收集	收集吊销通知记录、客户清单、问题台账	万维信
5	时间线还原	还原全流程关键节点时间线	各责任部门
6	合规目标完成度评估	评估是否在 BR 要求的时限内完成全部吊销，CRL/OCSP 是否及时更新，是否出现次生故障（误吊销、系统 bug 等）	合规
7	客户沟通效果评估	评估通知及时性、通知覆盖率、证书替换成功率、客户配合度、其他分工/沟通/技术问题、业务侧影响	万维信
8	根因分析	根据已有信息分析根本原因：定位系统或工具缺陷 / 操作流程问题 / 人员培训或意识问题	合规牵头（各部门协同）
9	问题与整改项	列出问题清单，制定整改项、责任人、验证标准、截止时间	合规牵头（各部门协同）
10	报告输出	编写《大规模吊销事件复盘报告》，并同步更新 Bugzilla 报告	合规牵头（各部门协同）
11	整改跟踪	督办整改，验证效果	合规
12	文档更新	修订发布 MRIP&TP 文档，更新演练计划	合规

问题报告响应小组针对本次大规模吊销事件，编制《大规模吊销事件复盘报告》。报告应包括事件概述、响应过程回顾、有效性评估、根本原因分析、存在问题清单、改进建议，明确责任人及完成时间，确保相关问题能够及时得到解决并优化流程。与合作伙伴联合演练发现的问题，双方应共同落实整改。

《大规模吊销事件复盘报告》结构参考：

- 事件基本信息（时间、影响范围、处置结果）
- 完整时间线
- 执行情况与合规性评估
- 亮点与成效
- 问题清单
- 根因分析
- 改进措施（可跟踪）
- 责任人与截止日期
- MRIP&TP 计划修订建议及下次演练重点

所有改进措施将在下次测试或实际事件中进行验证，确保问题不再发生。

年度审查与更新：

- 每年至少一次对 《大规模吊销事件准备与测试计划》（MRIP&TP） 进行全面审查，评估计划的有效性与适用性。
- 审查内容包括：根据实际情况、行业标准的变化以及事后分析总结的经验教训进行更新和完善。
- 更新后的计划将结合最新的政策要求和技术发展，确保应对不断变化的情况和需求。

有关计划的最新版本，您可以访问 SHECA 的官方网站：
https://www.sheca.com/repository 获取。

8. 第三方评估

自 2025 年 6 月 1 日 或之后的下一次 CA 审计周期起，上海市数字证书认证中心有限公司将每年聘请第三方评估机构进行大规模吊销事件准备与测试计划（MRIP&TP）的评估。评估的目的是为保证业务沟通的透明性，并提供证明文件，证明以下内容：

文档完整性与可操作性：确认 MRIP&TP 文档已完善，并具备可操作性，能够有效指导大规模吊销事件的响应。

测试与演练：确认已开展并记录相关的测试演练，包括测试流程、时间节点、结果以及采取的任何补救措施及过程中产生的所有资料，有过有可能审计人员将参与到吊销计划中作为第三方评估放方。

评估报告要求：SHECA 会将评估结果纳入 CA 运营商的常规审计流程，并结合其审计报告周期进行审查，采用 ETSI/ACAB’c 或 WebTrust 审计框架。

报告必须包括以下内容：

- 确认已完成评估或审查。
- 评估过程中所采用的范围与方法论总结。
- 关键发现，包括计划是否已记录、是否具有可行性，以及是否进行了定期测试。
- 提出的建议或整改事项。
- 关于整体计划充分性、测试与计划改进的声明。
- 任何其他必要信息，确保 Mozilla 能清晰了解 CA 运营商的大规模吊销准备情况。
- 每年将提交一份总结报告，直至 Mozilla 另行通知。

评估机构要求：

为避免大量沟通成本，SHECA 将聘请 Webtrust 团队为本吊销计划进行年度评估。

9. 结论

本大规模吊销事件准备与测试计划是上海市数字证书认证中心有限公司（SHECA）确保运营韧性和合规性的关键组成部分。通过严格执行本计划，SHECA 将能够在大规模吊销事件发生时迅速且高效地响应，最大限度地减少对客户和业务的影响，维护行业的信任和声誉。

SHECA 将持续优化本计划，确保其始终符合最新的行业标准和要求，为客户提供可靠的证书颁发服务。