TID翻转计划清单和时间表

STS协会

版本1.0,

2015年9月

目录

1. 背景介绍

Token标识符（TID）是STS Token中一个长为24比特的数据域。它表达了Token生成时的日期和时间。预付费表通过判断TID确定该Token是否已被使用过。TID值代表的是从1993年1月1日到Token生成的那一刻这期间累计的分钟数。随着TID值递增， 24比特域意味着TID值会在某一时刻重新翻转并从0开始计数。

所有STS预付费表将受到2024年11月24日TID翻转影响。 在此日期之后产生的使用24比特位TID的token将被表计认为是旧的token而拒绝，因为token中TID值将重置回0。

为了解决这个问题，所有的表计都需要使用翻转标志位（RO）置1的密钥转换token。 除此之外，基准日期1993年1月1日需更改为下一个基准日期。 该过程将强制表计将TID堆栈清零。为了避免以前Token由于TID重置而被表计接受，必须给表计赋予一个新密钥。

因此，需要一个管理密钥转换流程尽量减小对公用事业和设备供应商所带来的影响。

2. TID翻转的益处

过去二十年来STS系统稳定且成功，但其技术还在持续发展。 现在，STS系统已经到了需要积极变化来确保系统继续运行的时候。

TID翻转的益处有：

1. 使用了更加强大的算法生成和保护贩售密钥——新系统使用高达192比特的先进加密算法。

2. 密钥过期——新系统增加了贩售密钥的过期时间（由SGC所有者选择）。即使贩售密钥被盗，在某个时间之后贩售密钥也将失效。因此如果售电系统或者加密盒被盗取，此功能也大大减少了风险。

3. 保证STS系统的可持续性。

4. 用户不允许再从之前非法的贩售商购买Token给表计使用。

3. 项目综述

为保证项目顺利成功地进行，请根据以下罗列的章节要求执行表计的TID翻转计划。

3.1 升级（开发）加密盒

更新贩售和生产加密盒，满足在新基准日期情况下翻转标志位（RO）置1的密钥转换需求。在新密钥管理中心成功部署之后，才开始着手进行新加密盒的部署。

3.2 升级密钥管理中心

升级密钥管理中心，新密钥管理中心基于基准日期生成贩售密钥。新密钥管理中心将允许对新升级的加密盒进行编码。同时新密钥管理中心引入更强的算法保护贩售密钥的安全。升级密钥管理中心是整个TID翻转计划项目的第一步。

3.3 升级表计

选择基准日期为2014年的贩售密钥已经生产的预付费表无需进一步更改。为了满足在整个密钥转换的时期中使用多个不同基准日期，需升级生产加密盒，升级生产流程。

3.4 升级贩售系统

升级贩售系统以满足加密盒中多个不同基准日期功能，包括对STS600-4-2标准中新密钥下装文件（KLF）的格式处理。

3.5 STS 协会测试中心认证所有新贩售系统和加密盒

测试中心认证所有升级的贩售系统和加密盒。STS协会发布相关证书。

3.6 表计密钥转换计划

表计密钥转换计划是用于更新现场所有表计密钥。公共事业单位和子供销商以其整个供应群体（如SGC）为单位，或者有必要的话以供应群体里内的小范围表计群为单位共同联合开展计划。

4. 行动方案

4.1. STS协会

在这个项目中STS协会直接或间接联系会员和公共事业单位，确保所有STS用户知晓TID翻转项目。

STS协会还负责对整个项目的计划时间进行管理，但不包括项目的实施。

STS协会将进一步管理新密钥管理中心和新升级的加密盒的推出。

4.1.1 所需行动清单

- 开发本文档。
- 通知所有会员有关TID翻转计划。
- 为TID翻转项目所遇到的问题提供协助。

- 为新的加密盒和密钥管理中心开发认证测试规范（CTS）。
- 管理新密钥管理中心项目
- 可能有必要更新IEC 62055-41标准以满足密钥转换操作以及正常生成贩售Token时加密盒中需同时存在两个不同贩售密钥的要求。这样隶属于一个供应群（SGC）下的表计可以分批次进行密钥转换而无需整个供应群中的表计同时执行密钥转换操作。

4.2 加密盒供应商

加密盒供应商升级加密盒，支持TID翻转标志位（RO）和处理多个不同基准日期功能。加密盒供应商应与其客户联系沟通，通知有关升级加密盒的事宜。

4.2.1 所需行动清单

- 升级加密盒以处理TID翻转标志位（RO）和多个不同基准日期功能
- 测试加密盒——符合STS600-4-2标准要求的初始化、密钥下装以其他新固件功能。
- 加密盒进行认证测试，符合认证测试规范（CTS）和STS600-4-2（STS531-8-2）标准
- 现场测试加密盒——在新密钥管理中心进行编码，用现场使用的密钥进行Token测试。
- 一旦新密钥管理中心部署完成，贩售系统也完成升级，加密盒就进行现场部署。

4.3 密钥管理中心供应商

密钥管理中心供应商需对当前密钥管理中心的升级进行管理，发布支持多个不同基准日期功能的新密钥管理中心。要求所有相关数据从旧版密钥管理中心迁移到新密钥管理中心。

4.3.1 所需行动清单

- 依照STS600-4-2标准升级密钥管理中心以处理多个不同基准日期
- 将所有数据从当前密钥管理中心迁移到新密钥管理中心
- 依据STS600-4-2标准测试加密盒初始化和密钥下载至新密钥下装文件（KLF）的功能
- 新密钥管理中心的用户友好性测试
- 新密钥管理中心现场测试
- 新密钥管理中心获取STS协会批准
- 部署新密钥管理中心

4.4 密钥管理中心

密钥管理中心负责整理一份供应群（SGC）用户通讯录方便密钥管理中心进行联系。
除此之外，密钥管理中心还需开展培训活动，对使用升级后的密钥管理中心进行充分的培训。

4.4.1 所需行动清单

- 新密钥管理中心培训
- 现场测试——对TSM250加密盒进行编码。生成TID翻转标志位（RO）置1的密钥，并在现场表上进行测试
- 生成一份包含所有供应商代码（SGC）、供应商以及对应加密盒的列表清单用于沟通联系
- 对来自厂商和公共事业单位的所有支持TID翻转（STS6）的加密盒进行编码
- 新加密盒和新密钥管理中心与目前系统不同，需对新加密盒和新密钥管理中心之间的流程进行升级

4.5 表计厂商

为了匹配新的生产加密盒，表计厂商需更新生产流程和根据整个项目的计划时间表开始生产以2014为基准日期的预付费表。

4.5.1 所需行动清单

- 更新生产加密盒
- 检验表计中TID翻转功能
- 改变生产流程以满足多个不同基准日期情况
- 基于新的基准日期生产预付费表

4.6 贩售系统厂商

贩售系统厂商需更新所有贩售系统软件，以满足新接口协议（API）、密钥下装文件（KLF）和其他规则等。贩售系统厂商必须与其用户联系，安排对现场中的贩售系统进行升级等相关事宜。此外，贩售系统厂商的联系方式需告知所有与其业务相关联的子供销商，以便通知他们有关TID翻转计划。

4.6.1 所需行动清单

- 更新系统软件以满足新密钥下装文件（KLF）规范

- 更新系统软件以处理多个不同基准日期
- 认证系统软件，符合认证测试规范
- 升级现场用户的贩售系统软件
- 获取所有使用贩售系统的子供销商的联系方式

4.7 公共事业单位

公共事业单位负责新基准日期的密钥转换计划，并根据整个TID翻转项目的时间计划表建立自己的行动计划。该行动计划是自然是整个项目中最重要而又最难的部分，因此公共事业单位在实施计划之前必须深思熟虑，考虑全面。

4.7.1 所需行动清单

- 升级所有加密盒满足STS6功能要求
- 选择某个供应群（SGC）执行密钥转换计划
- 确定密钥转换计划操作方式（人工或者自动）
- 通知计划内的所有用户和区域现场
- 考虑是否先以小范围的表计为对象设立密钥转换项目
- 开始项目计划试点
- 成功后，整个供应群（SGC）中的表计进行密钥转换
- 确保整个计划至少在2024年TID翻转之前提前一年完成。

4.8 子供销商

通过密钥管理中心、厂商列表以及通讯录等方式联系所有子供销商。因大多数的子供销商不是STS协会会员，所以未意识到TID翻转等相关事情。STS协会必须尽快开始该任务。

4.8.1 所需行动清单

- 升级加密盒满足STS6功能要求
- 给所有表计生成对应的含TID翻转的密钥转换Token
- 对所有表计执行密钥转换

4.9 更新工具和标准

4.9.1 虚拟加密盒

- 升级虚拟加密盒以处理不同的新基准日期
- 使用虚拟加密盒导入已分配好密钥的密钥下装文件（KLF）（需与Prism公司讨论确定）
- 更新虚拟加密盒以满足新密钥下装文件（KLF）规范

4.9.2 Nedysis 文件规范

虽然不是所有公共事业单位都使用Nedysis文件，但是必须更新Nedysis文件规范给需要的公共事业单位使用。更新的Nedysis文件规范中将增加基准日期字段指定表计所相配的基准日期。

4.10 STS协会测试中心

测试中心将对所有配合新加密盒而升级的贩售系统进行认证测试。新加密盒也需要认证。

4.10.1 所需行动清单

- 研究新的测试文档以批准贩售系统和加密盒
- 分配符合性测试时间

更多关于STS标准和STS协会信息请登录网站www.sts.org.za 或者咨询秘书处。

秘书处：
P.O. Box 868, Ferndale, 2160, Johannesburg, South Africa.
电话： +2711 061 5000
sts@vdw.co.za