U版国密加密算法

改造方案

|  |  |  |  |
| --- | --- | --- | --- |
| **文档状态** | [√] 初稿  [ ] 评审通过  [ ] 修改  [ ] 发布  [ ] 作废 | **文档标识** | 金证国密加密算法改造方案 |
| **当前版本** | V1.0 |
| **作者** |  |
| **部门** |  |
| **完成日期** |  |

**修改说明**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本号** | **作者** | **操作** | **日期** | **说明** |
| V1.0 |  | 创建 | 2018-04-16 |  |
|  |  |  |  |  |
|  |  |  |  |  |

[一·引言 1](#_Toc511846939)

[1.1 编写目的 1](#_Toc511846940)

[1.2 背景 1](#_Toc511846941)

[二·需求分析 1](#_Toc511846942)

[2.1 总体需求概述 1](#_Toc511846943)

[三·总体设计 2](#_Toc511846944)

[3.1 加密算法选择 2](#_Toc511846945)

[3.3 加密控件说明 3](#_Toc511846946)

[四·设计方案 3](#_Toc511846947)

[4.1 柜台加密控件改造 3](#_Toc511846948)

[4.2 密码检查函数改造 3](#_Toc511846949)

[4.3 外部系统接口调用 4](#_Toc511846950)

[4.4 国密批量转换菜单 4](#_Toc511846951)

# 一·引言

## 1.1 编写目的

本文档用于描述U版柜台系统如何设计实现：集中交易底层加密算法库，迁移到金证国密加密算法的改造方案。

## 1.2 背景

随着金融产业的发展，站在国家安全及长远战略的角度考虑，提出了推动国密算法应用实施、加强行业安全可控的要求。

为配合国家对金融安全领域的升级，我司提出了对自身系统的改造计划，推出了金证国密算法库，U版交易系统通过切换新的算法库，将现有的加密体系切换到新的国密加密体系，完成对加密算法的升级。

# 二·需求分析

## 2.1 总体需求概述

本次改造总的设计原则是与集中交易对接的周边系统，仅通过更新底层加密算法库encrypt.o完成升级，业务接口不做任何改动。

集中交易本身要实现升级前后的兼容处理，一方面在检查外部系统传入的密码时，要能正确识别其加密算法，并适配后台存量密码的加密算法进行正确转换，另一方面，对存量的客户数据，要能做到分阶段、分批次，增量切换到国密算法。

# 三·总体设计

本次改造的影响范围包括：

* 集中交易柜台
* 报盘机
* 账户系统
* 外围系统
* 其他与集中交易对接的系统

在升级过程中，除了集中交易本身需要进行改造之外，其他外部系统均需要配合进行调整。

## 加密算法选择

|  |  |
| --- | --- |
| 算法 | 说明 |
| SM1 | 为硬件层的加密算法，本次改造不涉及，不做考虑 |
| SM2 | 非对称算法，公钥、私钥分开管理，生成的加密数据比原文多出90多个字符 |
| SM3 | 摘要算法，一般用于文件签名，加密不可逆，本次改造不涉及 |
| SM4 | 对称加密算法，加解密使用相同的密钥，生成的密文与原文长度一致 |

国密加密体系提供了4套加密算法，分别为SM1、SM2、SM3、SM4，其中，SM1、SM3不适合柜台的业务场景，因此，不做考虑。

SM2算法加密出来的密文比原文多出90多个字符，如果使用此算法，现有的密码字段需要扩位，同时，此算法本身有一套密钥管理机制，与柜台现有的以客户代码或操作员代码作为Key值进行加解密的方式不相同，使用此算法后，现有的Key值将失去意义。

SM4算法与柜台现有的算法比较接近，基本可以做到无缝对接，但由于算法公开，且不区分公钥、私钥，因此，密码的安全强度不高。

**后文假设将SM4算法作为本次改造使用的算法进行相关设计。**

## 加密控件说明

|  |  |  |  |
| --- | --- | --- | --- |
| 控件名称 | 关联文件 | 调用程序/接口 | 说明 |
| CITICS\_CE.dll | 无 | Xone.exe | 柜台客户端用对于前端客户密码加密 |

# 四·设计方案

## 柜台加密控件改造

提供新版本的CITICS\_CE.dll，实现对国密加密算法的包装，柜台程序业务处理部分代码不做调整，通过替换CliEncrypt.dll实现对国密算法的升级。

## 密码检查函数改造

现有的密码检查处理逻辑，是拿外部传入的加密后的密码，与柜台数据库中记录的密码，直接进行比较，两者相同则检查通过，否则，校验失败，检查过程不涉及密码加解密的处理。

本次改造，引入新的密码检查函数，其作用是做密码兼容处理，在检查通过后，更新后台数据库的数据。

在正式切换到国密算法后，后台数据库中存储的密码需要逐步切换到新的加密算法，切换条件如下：

* 如果数据库中的密码为老算法加密，传入密码为新算法加密，则用新密码更新后台数据库，并记录操作流水，此步骤是在后台自动进行，通过函数QueryType获取送入客户密码类型。
* 如果数据库中的密码为老算法加密，传入密码为老算法加密，则不修改后台数据
* 如果数据库中的密码为新算法加密，不管传入的密码是用的何种加密算法，均不修改后台数据

所有后台涉及到的UF\_Encrypt函数、UF\_CommDecrypt函数调用都涉及到修改。首先调QueryType函数，判断此密码是新密码类型，还是旧密码类型。

再查询数据库密码，通过QueryType函数校验密码类型。如果是旧密码类型，则转换为新密码进行业务操作。并且更新密码表为新密码。如果是新密码类型，则直接按照新密码类型转化后，进行业务比较。

涉及到功能点L0102015、L0102016、L0102017、L0102018、L0203015、L0206112、L0206021、L0204002。有AUTO\_INFO入参的都涉及到改动。另外注意统一认证也涉及到相关的改造。

## 外部系统接口调用

涉及外部系统的功能号调用，入参中的密码需做兼容处理数据库增加加密类型字段

针对数据库中所有包含密码字段的表，均需增加“加密类型”字段，初始值为6，表示对应的密码字段为老算法加密，密码字段本身的值不做调整。

有密码字段的表清单如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 状态 | 表名 | 描述 | 字段名 | 中文名 | 加密因子 |
| 使用中 | AUTHENTICATION | 用户认证信息表 | AUTH\_INFO | 用户密码 | USER\_CODE |

## 国密批量转换菜单

增加专门的菜单，用于将后台数据库中存放的密码，批量转换为国密加密方式。