|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 部门名称 | 文档编号 |  | 版本 |  | 密级 |  |
| 项目名称 |  | | | | |
| 项目来源 |  | | | | |

**可监管idmixer算法实现说明书**

编 写： \_\_\_\_ 日 期：

检 查： \_\_\_\_ 日 期：

审 核： \_\_\_\_ 日 期：

批 准： \_\_\_\_ 日 期：

文档变更记录

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 变更(+/-)说明 | 作者 | 版本 | 日期 | 批准 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |

目录

[1. 引言 2](#_Toc526004142)

[1.1 背景 2](#_Toc526004143)

[1.2 术语和缩略语 2](#_Toc526004144)

[1.3 参考资料 2](#_Toc526004145)

[2. 总体设计 2](#_Toc526004146)

[2.1 需求 2](#_Toc526004147)

[2.2 架构设计目标和约束 2](#_Toc526004148)

[2.2.1 运行环境 2](#_Toc526004149)

[2.2.2 开发环境 2](#_Toc526004150)

[2.3 设计思想 3](#_Toc526004151)

[2.4 软件架构 3](#_Toc526004152)

[2.5 重要业务流程 3](#_Toc526004153)

[2.5.1 流程1 3](#_Toc526004154)

[2.5.2 流程2 3](#_Toc526004155)

[2.6 模块划分 3](#_Toc526004156)

[3. 接口设计 3](#_Toc526004157)

[3.1 外部接口 3](#_Toc526004158)

1. 引言
   1. 背景

可监管idmixer方案在原idmixer方案的基础上结合群签名方案实现了用户身份监管的功能，通过CA对用户的身份进行强制性监管。

方案可应用于联盟链中的匿名资产中，可以允许交易方在满足资产管理规定的条件下转移匿名资产。例如，在交易过程中，交易方按照规定利用证书显示交易需要公开的内容，如资产来源银行代号，资产到账银行代号等，其他个人信息则可以进行隐藏，同时资产的可监管性满足了审计业务的需求，审计人员可随时恢复出资产内容和交易方身份信息。

* 1. 术语和缩略语

p:阶数。

:阶数为的整数群。

G1:椭圆曲线上的阶数为p的加法循环群。

G2:椭圆曲线上的阶数为p的加法循环群。

GT:椭圆曲线上的阶数为p的乘法循环群。

g1:G1的生成元。

g2:G2的生成元。

（双线性对运算）

* 1. 参考资料

https://www.zurich.ibm.com/identity\_mixer/,

<https://github.com/hyperledger/fabric/tree/release-1.3/idemix>.

https://link.springer.com/content/pdf/10.1007%2F978-3-540-28628-8\_3.pdf.

1. 总体设计
   1. 需求
   2. 架构设计目标和约束
      1. 运行环境

Go 1.9.2

* + 1. 开发环境

Go 1.9.2

* 1. 设计思想

可监管idmixer方案在原idmixer方案的基础上结合群签名方案实现了用户身份监管的功能，通过CA对用户的身份进行强制性监管。方案参与方包括CA，用户和验证者，系统建立后，CA产生发行密钥对，追踪密钥以及群公钥。然后用户进行注册，CA为其分配一对私钥，同时CA根据用户提交的属性信息为用户颁发相关的证书。在用户出示证书时，验证者可指定用户证书上需要出示的属性，用户对证书进行签名，同时隐藏无需出示的属性值。验证者可对签名进行验证，若签名通过验证，则用户出示的证书有效，否则，用户出示的证书无效。

* 1. 软件架构
  2. 重要业务流程
     1. 流程1
     2. 流程2
  3. 模块划分
     1. 模块1
     2. 模块2

1. 接口设计
   1. 外部接口

本算法对外有哪些接口，逐一详细说明参数、返回值、调用约束（如能否并发调用）等.

1. 生成发行方密钥对：func NewIssuerKey(AttributeNames []string, rng \*amcl.RAND) (\*IssuerKey, error)
2. 传入参数：
3. AttributeNames:属性名。
4. Rng：随机数。
5. 传出参数：
   1. IssuerKey:发行方密钥对，包括私钥ISK和公钥IPK。
   2. error:错误类型。
6. 发行方密钥对验证：func (IPk \*IssuerPublicKey) Check() error
7. 传入参数：
8. IPK:发行方公钥。
9. 传出参数：
   1. error:错误类型。
10. 生成群公钥和追踪密钥：func NewGroupKey(rng \*amcl.RAND) (\*GroupKey,error)
11. 传入参数：
12. rng:随机数。
13. 传出参数：
    1. GroupKey:群公钥，其中群密钥包括追踪密钥TK和群公钥GPK。
    2. error:错误类型。
14. 生成用户私钥：func Registration(key \*IssuerKey, rng \*amcl.RAND) (\*UserKey, error)
15. 传入参数：
16. key:发行方密钥对。
17. rng:随机数。
18. 传出参数：
19. UserKey:用户密钥对
20. Error:错误类型
21. 生成证书请求：func NewCredRequest(sk \*FP256BN.BIG, credS1 \*FP256BN.BIG, IssuerNonce \*FP256BN.BIG, ipk \*IssuerPublicKey, rng \*amcl.RAND) \*CredRequest
22. 传入参数：
    1. sk:用户私钥。
    2. credS1:用户选择的随机数。
    3. IssuerNonce:发行方选择的随机数。
    4. Ipk:发行方公钥。
    5. Rng:随机数
23. 传出参数：
24. CredRequest:证书请求
25. 验证证书请求：func (m \*CredRequest) Check(ipk \*IssuerPublicKey) error
26. 传入参数：
    1. m:证书请求。
    2. ipk:发行方公钥。
27. 传出参数：
28. Error:错误类型
29. 生成证书：func NewCredential(key \*IssuerKey, m \*CredRequest, attrs []\*FP256BN.BIG, rng \*amcl.RAND) (\*Credential, error)
30. 传入参数：
    1. Key:发行方密钥对。
    2. m:证书请求。
    3. attrs:用户属性值。
31. 传出参数：
32. Credential:证书
33. Error:错误类型
34. 证书验证：func (cred \*Credential) Ver(sk \*FP256BN.BIG, ipk \*IssuerPublicKey) error
35. 传入参数：
    1. cred:证书。
    2. sk:用户私钥。
    3. ipk:发行方公钥。
36. 传出参数：
37. Error:错误类型
38. 出示证书：func NewSignature(cred \*Credential, sk \*FP256BN.BIG, Nym \*FP256BN.ECP, RNym \*FP256BN.BIG, ipk \*IssuerPublicKey, gpk \*GroupPublicKey, uk \*UserKey, Disclosure []byte, msg []byte, rng \*amcl.RAND) (\*Signature, error)
39. 传入参数：
    1. cred:证书。
    2. sk:用户私钥。
    3. Nym:假名。
    4. RNym:随机数。
    5. ipk:发行方公钥。
    6. gpk:群公钥。
    7. uk:用户私钥。
    8. Disclosure：出示属性值的下标。
    9. Msg:待签名消息。
    10. rng:随机数。
40. 传出参数：
41. Signature:出示的证书
42. Error:错误类型
43. 验证出示的证书 func (sig \*Signature) Ver(Disclosure []byte, ipk \*IssuerPublicKey, gpk \*GroupPublicKey, msg []byte, attributeValues []\*FP256BN.BIG) error
44. 传入参数：
    1. Sig:出示的证书。
    2. Disclosure:出示属性值的下标。
    3. Ipk:发行方公钥。
    4. Gpk:群公钥。
    5. Msg:签名消息。
    6. attributeValues:属性值。
45. 传出参数：
46. K:用户私钥
47. Error:错误类型
48. 追踪签名者身份：func Tracing(sig \*Signature, tk \*TracingKey) (\*K,error)
49. 传入参数：
    1. Sig:出示的证书。
    2. tk:追踪密钥TK。
50. 传出参数：
51. K:用户私钥。
52. Error:错误类型