



中华人民共和国密码行业标准

GM/T 0113—2021

在线快捷身份鉴别协议

Fast online identity authentication protocol

2021-10-18 发布

2022-05-01 实施

国家密码管理局 发 布

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 通用在线快捷身份鉴别协议 2

 5.1 协议架构 2

 5.2 协议消息相关数据结构 5

 5.3 协议流程和要求 9

6 双因素在线快捷身份鉴别协议..... 15

 6.1 协议架构 15

 6.2 协议消息框架 17

 6.3 协议流程和要求 19

附录 A（资料性） 安全风险及措施建议 28

附录 B（资料性） 可信环境实现方式 31

附录 C（资料性） 协议接口 32

参考文献 36

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：中国科学院数据与通信保护研究教育中心、联想（北京）有限公司、中国科学院大学、国民认证科技（北京）有限公司、北京数字认证股份有限公司、浙江蚂蚁小微金融服务集团有限公司、北京天融信网络安全技术有限公司、中国科学院信息工程研究所、飞天诚信科技股份有限公司、成都卫士通信息产业股份有限公司、中国金融认证中心、吉大正元信息技术股份有限公司、中孚信息股份有限公司、杭州天谷信息科技有限公司、神州融安科技（北京）有限公司、北京握奇智能科技有限公司、郑州信大捷安信息技术股份有限公司、北京眼神智能科技有限公司。

本文件主要起草人：钱文飞、赵欣怡、贾世杰、刘丽敏、柴海新、荆继武、李俊、张永强、宋铮、景鸿理、王平建、牛莹姣、高彪、吕娜、陈天宇、张咪、朱鹏飞、罗俊、孙国栋、赵丽丽、苗功勋、程亮、李登峰、张渊、刘熙胖、杨春林。

在线快捷身份鉴别协议

1 范围

本文件规定了在线快捷身份鉴别协议,包括通用在线快捷身份鉴别协议、双因素在线快捷身份鉴别协议等内容。

本文件适用于在线快捷身份鉴别服务的开发、测试和评估。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 16262(所有部分) 抽象语法记法(ASN.1)
GB/T 16649.4 识别卡 集成电路卡 第4部分:用于交换的结构、安全和命令
GB/T 25069 信息安全技术 术语
GB/T 32905 信息安全技术 SM3 密码杂凑算法
GB/T 32918(所有部分) 信息安全技术 SM2 椭圆曲线公钥密码算法
GB/T 35276 信息安全技术 SM2 密码算法使用规范
GB/T 36651 信息安全技术 基于可信环境的生物特征识别身份鉴别协议框架
GB/T 37092 信息安全技术 密码模块安全要求
GB/T 38636 信息安全技术 传输层密码协议(TLCP)
GM/Z 4001 密码术语

3 术语和定义

GB/T 25069、GB/T 36651、GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

鉴别客户端 authentication client

在用户代理中处理双因素身份鉴别协议消息的软件组件,用于双因素身份鉴别协议中用户代理与鉴别器之间的通信。

3.2

鉴别客户端接口 authentication client interface

由鉴别客户端提供的协议接口,用于双因素身份鉴别协议中用户代理与鉴别客户端之间的通信。

3.3

生物特征识别密钥管理器标识符 biometric authentication protocol key manager identifier

分配给同一型号生物特征识别密钥管理器的唯一标识符,依赖方可通过该标识符唯一确定厂商公钥。

3.4

用户代理 user agent

安装在用户设备上的浏览器或者其他应用程序。

4 缩略语

下列缩略语适用于本文件。

APDU:应用协议数据单元(Application Protocol Data Unit)

AppID:应用程序标识符(Application Identifier)

ASN.1:抽象语法标记(Abstract Syntax Notation One)

BAP:生物特征识别身份鉴别协议(Biometric Authentication Protocol)

BAPV:生物特征识别身份鉴别协议版本(Biometric Authentication Protocol Version)

bkmID:生物特征识别密钥管理器标识符(BAP Key Manager Identifier)

KeyID:密钥标识符(Key Identifier)

KRD:密钥注册数据(Key Registration Data)

PII:个人识别信息(Personal Identifiable Information)

PIN:个人识别码(Personal Identification Number)

TAP:双因素在线快捷身份鉴别协议(Two-factor Authentication Protocol)

TEE:可信执行环境(Trusted Execution Environment)

TLCP:传输层密码协议(Transport Layer Cryptography Protocol)

TPM:可信平台模块(Trusted Platform Module)

VPN:虚拟专用网络(Virtual Private Network)

5 通用在线快捷身份鉴别协议

5.1 协议架构

5.1.1 概述

通用在线快捷身份鉴别协议借助智能设备,结合生物特征识别技术,提供了无口令、安全性能高、使用方便的身份鉴别方案,该协议在 GB/T 36651 规定的基于可信环境的生物特征识别身份鉴别协议框架基础上,针对协议架构、协议流程和要求等进行了细化,并在协议流程和要求中规定了协议的相关消息数据格式。其中,安全风险及措施建议见附录 A,关于可信环境实现方式见附录 B,关于协议接口见附录 C。在实际部署过程中使用的商用密码产品,应当由具备资格的商用密码检测、认证机构检测认证合格后,方可部署到实际系统中。

在执行通用在线快捷身份鉴别协议之前,身份鉴别服务器通过用户代理调用生物特征识别密钥管理器接口的发现方法,检查用户设备是否支持通用在线快捷身份鉴别协议。本文件不规定身份鉴别服务器获取生物特征识别密钥管理器相关信息以及厂商公钥信息的方式,身份鉴别服务器可利用生物特征识别密钥管理器接口的发现方法中返回的结果,通过生物特征识别密钥管理器相关提供方的服务来获取这些信息。

通用在线快捷身份鉴别协议的交互图如图 1 所示。其中,图中实线表示消息流由图例中的左侧实体到右侧实体,虚线部分表示消息流由图例中的右侧实体到左侧实体或者是重定向消息流,双向箭头表示两个实体进行交互以完成某操作,跨越实体的虚线表示其他实体通过该实体进行通信,后续交互图中均以此说明为准。图中采用 HTTP 重定向方式对协议交互情况进行说明。

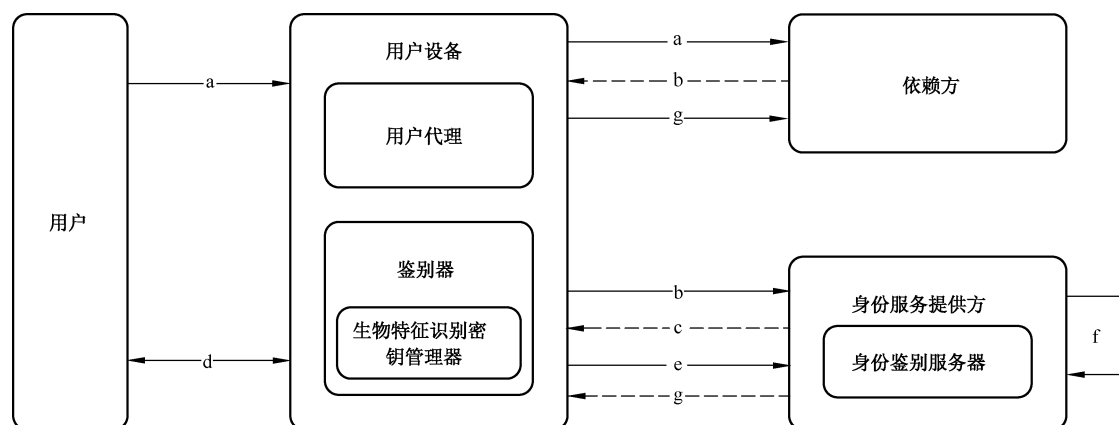


图 1 协议交互图

用户身份鉴别流程主要分为 8 个步骤：

- 用户使用用户设备中的用户代理访问依赖方；
- 依赖方将用户代理重定向至身份服务提供方；
- 身份服务提供方对用户代理发送鉴别请求；
- 用户使用用户设备的鉴别器进行身份验证；
- 用户身份验证通过后，鉴别器将鉴别响应通过用户代理传递给身份服务提供方；
- 身份服务提供方对鉴别响应进行验证；
- 身份服务提供方通过用户代理将身份鉴别结果重定向至依赖方。

5.1.2 注册

在用户向身份鉴别服务器进行注册的流程中，用户使用生物特征识别密钥管理器创建一对新的鉴别公私钥并且将鉴别私钥保存在生物特征识别密钥管理器中，将鉴别公钥注册在身份鉴别服务器中。注册流程如图 2 所示，图中采用 HTTP 重定向方式对协议流程进行说明，详细流程和消息见 5.3.1。

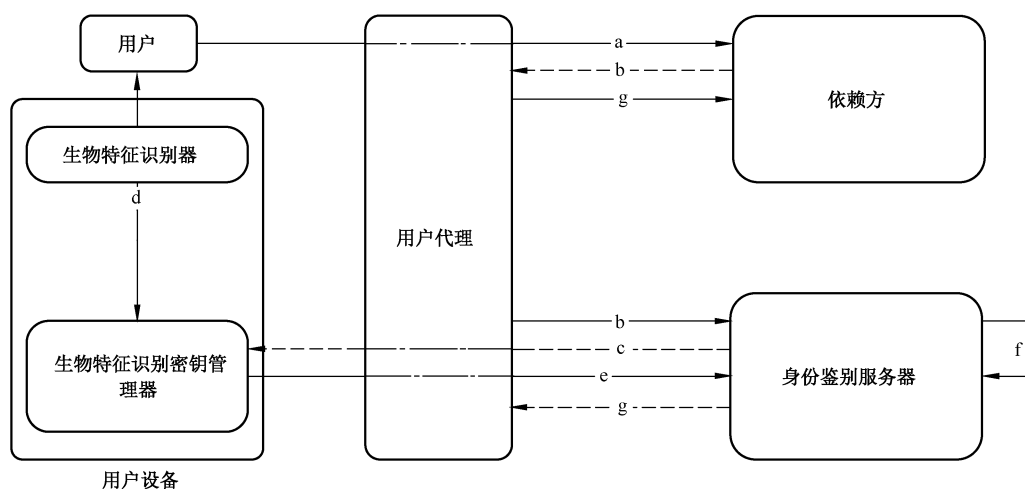


图 2 注册/鉴别流程

- a) 用户使用用户设备中的用户代理访问依赖方。
- b) 当用户需要进行生物特征识别身份鉴别注册时,依赖方将用户定向到身份鉴别服务器。可使用 HTTP 重定向方式将用户设备重定向到身份鉴别服务器,或者使用消息转发方式。
- c) 身份鉴别服务器向用户设备中的生物特征识别密钥管理器发送注册请求消息;用户设备的生物特征识别密钥管理器在收到身份鉴别服务器的注册请求消息时,验证身份鉴别服务器的真实性,验证通过则提示用户选择本地可用的生物特征识别器,否则拒绝该消息。本文件中涉及生物特征识别密钥管理器验证身份鉴别服务器真实性的方法,宜采用证书方式或者其他可验证身份鉴别服务器真实性的方法。
- d) 用户选择本地合适的生物特征识别器,使用生物特征识别信息解锁生物特征识别密钥管理器,完成用户生物特征识别验证。如果用户之前未将生物特征识别信息登记到该生物特征识别器,则进行登记;如果用户已进行登记,则使用已登记的生物特征识别信息完成解锁过程。用户生物特征识别验证成功后,生物特征识别密钥管理器创建一对与生物特征识别密钥管理器、身份鉴别服务器相关联的唯一的鉴别公私钥,鉴别私钥保存在本地的生物特征识别密钥管理器,并且不允许从生物特征识别密钥管理器导出。如果生物特征识别密钥管理器没有能力保存鉴别私钥,则该生物特征识别密钥管理器将鉴别私钥进行加密,然后将加密后的鉴别私钥保存在用户设备中,用于加密用户私钥的密钥则保存在生物特征识别密钥管理器中并且不允许从生物特征识别密钥管理器导出;本协议中有关密钥等关键安全参数的全生命周期管理或安全管理的要求应符合 GB/T 37092 的规定。
- e) 生物特征识别密钥管理器生成密钥注册数据,然后生成注册响应消息,将注册响应消息发送到身份鉴别服务器。其中,密钥注册数据中包含上一步生成的鉴别公钥,注册响应消息中包含密钥注册数据,以及使用厂商私钥对密钥注册数据进行签名的签名值。厂商公私钥为用户设备制造厂商在生物特征识别密钥管理器中预先植入的用于证明生物特征识别密钥管理器身份的密钥对。
- f) 身份鉴别服务器通过 5.2.7 的生物特征识别密钥管理器信息获取厂商公钥,利用厂商公钥验证注册响应消息中的签名,签名正确则提取出鉴别公钥并保存该鉴别公钥,同时应保存该鉴别公钥与用户之间的对应关系。
- g) 身份鉴别服务器将注册结果返回给依赖方。

5.1.3 鉴别

在鉴别流程中,用户通过生物特征识别密钥管理器使用鉴别私钥对服务器挑战签名,向身份鉴别服务器证明其拥有该私钥,完成身份鉴别过程。鉴别流程如图 2 所示,图中采用 HTTP 重定向方式对协议流程进行说明,协议详细流程和消息见 5.3.2。

- a) 用户使用用户设备中的用户代理访问依赖方。
- b) 当用户需要进行生物特征识别身份鉴别时,依赖方将用户定向到身份鉴别服务器,可使用 HTTP 重定向方式将用户设备重定向到身份鉴别服务器,或者使用消息转发方式。
- c) 身份鉴别服务器向用户设备中的生物特征识别密钥管理器发送鉴别请求消息;用户设备的生物特征识别密钥管理器在收到身份鉴别服务器的鉴别请求消息时,验证身份鉴别服务器的真实性,验证通过则提示用户选择可用的生物特征识别器,否则拒绝该消息。本文件中涉及生物特征识别密钥管理器验证身份鉴别服务器真实性的方法,宜采用证书方式或者其他可验证身份鉴别服务器真实性的方法。
- d) 用户选择本地合适的生物特征识别器,使用生物特征识别信息解锁存储在生物特征识别密钥管理器中的用户鉴别私钥,完成用户生物特征识别验证。用户生物特征识别验证成功后,生物

特征识别密钥管理器选择相应的鉴别私钥对待签名数据签名。

- e) 生物特征识别密钥管理器将包含签名结果的鉴别响应消息发送到身份鉴别服务器。
- f) 身份鉴别服务器使用相应的鉴别公钥对签名进行验证,验证成功后,用户身份鉴别成功,否则用户身份鉴别失败。
- g) 身份鉴别服务器将鉴别结果返回给依赖方。

5.1.4 注销

当用户删除在依赖方注册的账户,或丢失用户设备,或依赖方在需要删除用户绑定的公私钥等情形下,身份鉴别服务器应发起注销流程。其中,身份鉴别服务器在执行注销流程前应鉴别用户的身份,应使用 5.1.3 中规定的鉴别流程,若无法使用上述鉴别流程,则使用其他身份鉴别方式,例如线下身份鉴别方式。具体注销流程如图 3 所示,图中采用 HTTP 重定向方式对协议流程进行说明,图中为完整的注销流程,若丢失用户设备,则不需要向生物特征识别密钥管理器发送注销请求消息。

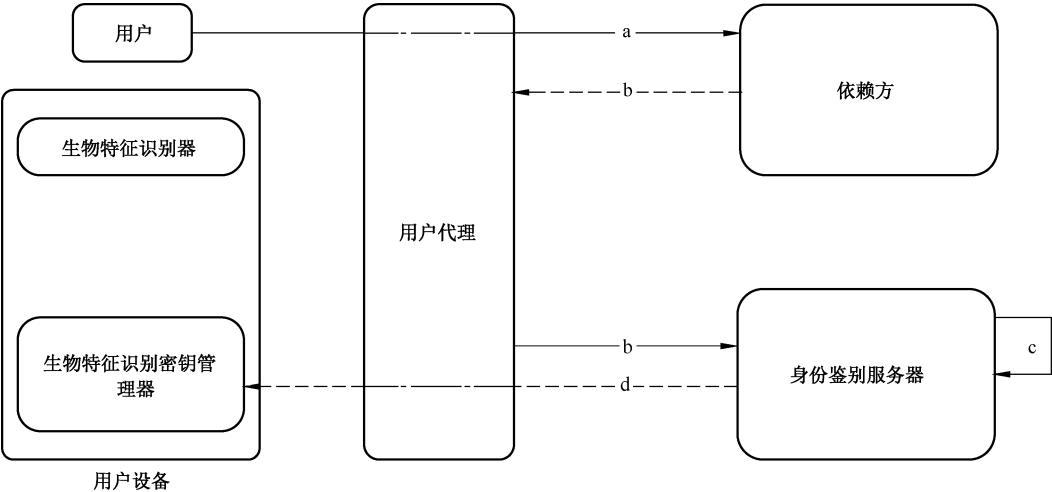


图 3 注销流程

- a) 用户使用用户设备中的用户代理向依赖方发起注销流程。
- b) 依赖方将用户定向到身份鉴别服务器,可使用 HTTP 重定向方式将用户设备重定向到身份鉴别服务器,或者使用消息转发方式。首先进行用户的身份鉴别,鉴别通过后执行后续注销流程,否则拒绝执行注销流程。
- c) 身份鉴别服务器删除相应的鉴别公钥,并向生物特征识别密钥管理器发送注销请求消息。
- d) 用户设备的生物特征识别密钥管理器在收到身份鉴别服务器的注销请求消息时,验证身份鉴别服务器的真实性,验证通过则删除相应的鉴别私钥,否则拒绝该消息。

5.2 协议消息相关数据结构

5.2.1 概述

通用在线快捷身份鉴别协议所有数据格式采用 GB/T 16262 描述。

5.2.2 版本

Version ::= SEQUENCE(
 major INTEGER,

```

        minor    INTEGER
    }

```

major: 主要版本。

minor: 次要版本。

本文件的协议主要版本为 1, 次要版本为 0。

5.2.3 操作类型

```
Operation ::= PrintableString
```

本文件有以下三种操作类型:

Reg: 注册, Operation 值为“Reg”。

Auth: 鉴别, Operation 值为“Auth”。

Dereg: 注销, Operation 值为“Dereg”。

5.2.4 扩展

```

Extension ::= SEQUENCE{
    id          PrintableString,
    data        PrintableString,
    fail_if_unknown  BOOLEAN
}

```

该结构描述的是在各种操作中使用的通用扩展。

id: 扩展的标识符。

data: 该值可包含任意字符串, 身份鉴别服务器和生物特征识别密钥管理器应对该值的语义协商一致。该值可为空。

fail_if_unknown: 当 fail_if_unknown 是 false 时表示未知扩展应被忽略, 当 fail_if_unknown 是 true 时表示未知扩展应导致错误。

5.2.5 操作头

```

OperationHeader ::= SEQUENCE{
    bapv          Version,
    op            Operation,
    appID         PrintableString,
    serverData    PrintableString OPTIONAL,
    exts          SEQUENCE OF Extension OPTIONAL
}

```

bapv: 在线快捷身份鉴别协议版本, 抽象语法标记(ASN.1)描述见 5.2.2。

op: 值应为“Reg”, “Auth”或者“Dereg”, 在线快捷身份鉴别协议操作的类型, ASN.1 描述见 5.2.3。

appID: 依赖方应用程序标识符。

serverData: 依赖方创建的会话标识符。

exts: 扩展列表, ASN.1 描述见 5.2.4。

5.2.6 最终挑战参数

```

FinalChallengeParams ::= SEQUENCE{
    appID          PrintableString,

```

```

        challenge      PrintableString
    }

```

appID:该参数值设置为操作头的 appID 参数值。

challenge:该参数值设置为注册请求或鉴别请求中的服务器挑战参数值,服务器挑战是服务器提供的随机参数值。

5.2.7 生物特征识别密钥管理器信息

身份鉴别服务器可获取生物特征识别密钥管理器相关信息,例如生物特征识别密钥管理器厂商在生成厂商密钥时所使用的相关算法和信息,以及生物特征识别密钥管理器生成鉴别公私钥时所使用的算法和信息。身份鉴别服务器可使用生物特征识别密钥管理器相关提供方的服务来获取这些信息。

5.2.8 断言描述信息

```

AssertionInfo ::= SEQUENCE {
    version                Version,
    mode                   AuthenticationMode,
    signatureAlgAndEncoding INTEGER,
    publicKeyAlgAndEncoding INTEGER OPTIONAL
}

```

version:断言的版本,ASN.1 描述见 5.2.2。

mode:断言模式。

AuthenticationMode:用户验证方式,ASN.1 描述如下:

AuthenticationMode ::= INTEGER {explicitly(0x01)}

explicitly:应进行显式的用户验证,例如指纹输入、虹膜扫描等。

signatureAlgAndEncoding:该值代表签名算法相关信息,身份鉴别服务器和生物特征识别密钥管理器应对该值的语义协商一致,即能够通过该值在身份鉴别过程中使用一致的签名算法和相关参数。在通用在线快捷身份鉴别协议中,宜采用 SM2 算法,SM2 算法的实现应符合 GB/T 32918 的规定,该值为 0x0007。

publicKeyAlgAndEncoding:该值代表公钥算法相关信息,身份鉴别服务器和生物特征识别密钥管理器应对该值的语义协商一致,即能够通过该值在身份鉴别过程中使用一致的公钥算法和相关参数。在通用在线快捷身份鉴别协议中,宜采用 SM2 算法,SM2 算法的实现应符合 GB/T 32918 的规定,该值为 0x0007。

5.2.9 生物特征识别密钥管理器计数器值

```

Counters ::= SEQUENCE {
    SignCounter           INTEGER,
    RegCounter            INTEGER
}

```

SignCounter:签名计数器的值。

RegCounter:注册计数器的值。

5.2.10 发现数据

```

DiscoveryData ::= SEQUENCE {

```

```

supportedBAPVersions    SEQUENCE OF Version,
clientVendor            PrintableString,
clientVersion           Version,
availableBAPKeyManagers SEQUENCE OF PrintableString
}

```

描述：

supportedBAPVersions:支持的在线快捷身份鉴别协议版本,ASN.1 描述见 5.2.2。

clientVendor:生物特征识别密钥管理器厂商。

clientVersion:生物特征识别密钥管理器版本。

availableBAPKeyManagers:可使用的生物特征识别密钥管理器标识符。

5.2.11 错误码

```

ErrorCode ::= INTEGER{
    NO_ERROR(0x0),
    WAIT_USER_ACTION(0x1),
    INSECURE_TRANSPORT(0x2),
    USER_CANCELLED(0x3),
    UNSUPPORTED_VERSION(0x4),
    NO_SUITABLE_BAPKEYMANAGER(0x5),
    PROTOCOL_ERROR(0x6),
    UNTRUSTED_FACET_ID(0x7),
    KEY_DISAPPEARED_PERMANENTLY(0x09),
    BAPKEYMANAGER_ACCESS_DENIED(0x0c),
    USER_NOT_RESPONSIVE(0x0e),
    INSUFFICIENT_BAPKEYMANAGER_RESOURCES(0x0f),
    USER_LOCKOUT(0x10),
    USER_NOT_ENROLLED(0x11),
    UNKNOWN(0xff)
}

```

描述：

NO_ERROR:操作完成,没有错误发生。

WAIT_USER_ACTION:等待用户操作。

INSECURE_TRANSPORT:不安全的传输,例如没有使用 HTTPS。

USER_CANCELLED:用户取消当前操作。

UNSUPPORTED_VERSION:生物特征识别密钥管理器不支持该版本的协议消息。

NO_SUITABLE_BAPKEYMANAGER:没有与身份鉴别服务器策略相匹配的生物特征识别密钥管理器。

PROTOCOL_ERROR:发生协议错误。

UNTRUSTED_FACET_ID:不受信任的依赖方应用程序。

KEY_DISAPPEARED_PERMANENTLY:鉴别私钥丢失并且无法恢复。

BAPKEYMANAGER_ACCESS_DENIED:生物特征识别密钥管理器拒绝访问。

USER_NOT_RESPONSIVE:用户长时间无响应。

INSUFFICIENT_BAPKEYMANAGER_RESOURCES:生物特征识别密钥管理器没有足够的资

源执行操作。

USER_LOCKOUT:由于用户锁定,操作无法执行。

USER_NOT_ENROLLED:用户没有登记。

UNKNOWN:以上没有列出的其他错误。

5.2.12 协议消息

协议消息是通用在线快捷身份鉴别协议的各个参与方交互时传递的消息,ASN.1 描述如下:

```
BAPMessage ::= SEQUENCE {
    bapProtocolMessage OCTET STRING,
    additionalData      OCTET STRING
}
```

bapProtocolMessage:协议消息,例如注册请求消息、注册响应消息、鉴别请求消息、鉴别响应消息、注销请求消息等。

additionalData:附加参数。

5.3 协议流程和要求

5.3.1 注册流程

5.3.1.1 概述

图 4 描述用户注册流程,本流程中用户访问依赖方进行用户名和口令验证的过程作为注册流程的前提条件,不在本流程中进行说明。

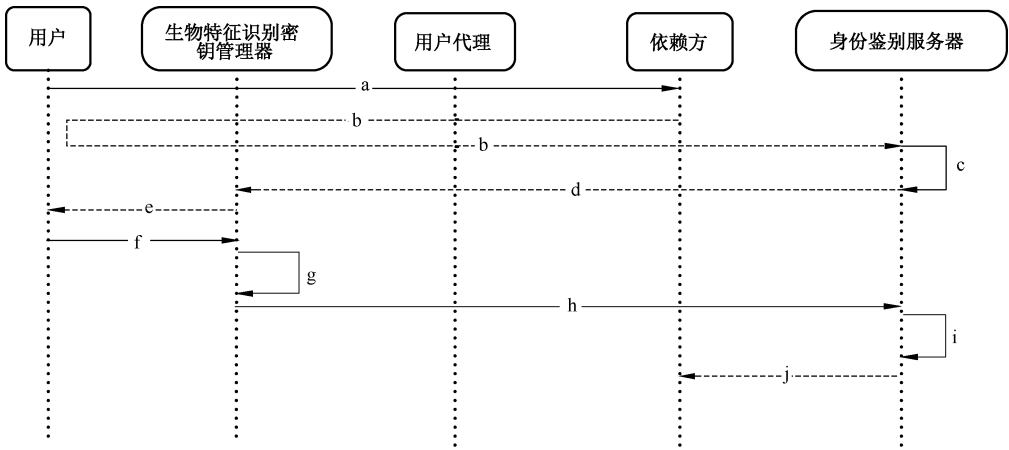


图 4 注册/鉴别详细流程

- a) 用户通过用户代理访问依赖方,发起注册流程。
- b) 依赖方将用户重定向到身份鉴别服务器。
- c) 身份鉴别服务器生成注册请求消息,见 5.3.1.2.1 a) 步骤。
- d) 身份鉴别服务器通过用户代理将注册请求消息发送至生物特征识别密钥管理器,见 5.3.1.2.1 a) 步骤。
- e) 生物特征识别密钥管理器首先验证身份鉴别服务器的真实性,然后生物特征识别密钥管理器发起本地用户校验,提示用户使用生物特征识别信息进行身份验证,见 5.3.1.2.2 a)、b) 步骤。
- f) 用户提交生物识别信息,例如指纹、虹膜等信息。
- g) 生物特征识别密钥管理器验证用户提交的生物识别信息,验证通过后,生成一对新的鉴别公

私钥,然后生成注册响应消息,注册响应消息中包含使用厂商私钥对鉴别公钥等信息的签名,见 5.3.1.2.2 c)、d)步骤。

- h) 生物特征识别密钥管理器通过用户代理将注册响应消息返回给身份鉴别服务器,见 5.3.1.2.2 e)步骤。
- i) 身份鉴别服务器使用厂商公钥验证注册响应消息,验证成功后存储相关信息,否则返回错误信息,见 5.3.1.2.3 a)~c)步骤。
- j) 身份鉴别服务器将结果返回给依赖方。

5.3.1.2 注册流程处理规则

5.3.1.2.1 身份鉴别服务器生成注册请求规则

身份鉴别服务器应遵循以下步骤:

- a) 创建注册请求消息,并初始化注册请求消息的各个参数。注册请求消息格式如下:

```
RegistrationRequest ::= SEQUENCE {
    header          OperationHeader,
    challenge        PrintableString,
    username        PrintableString
}
```

header:操作头,header.op 的值应为“Reg”,ASN.1 描述见 5.2.5。

challenge:身份鉴别服务器提供的挑战值。

username:用户在某依赖方的账号名称;

- b) 将注册请求消息发送给生物特征识别密钥管理器。

5.3.1.2.2 生物特征识别密钥管理器处理注册请求规则

生物特征识别密钥管理器应遵循以下步骤:

- a) 验证身份鉴别服务器的真实性,验证成功则执行以下步骤,否则拒绝该消息;
- b) 解析注册请求消息,判断注册请求消息是否包含必要的参数以及每个参数是否符合要求,若符合要求则执行以下步骤,否则拒绝该消息;
- c) 提示用户选择本地生物特征识别器,用户选择后,使用用户选择的本地生物特征识别器验证用户,验证通过后执行以下操作,否则返回错误;
- d) 创建注册响应消息,并根据注册请求消息的参数初始化注册响应消息的参数。注册响应消息格式如下:

```
RegistrationResponse ::= SEQUENCE {
    header          OperationHeader,
    fcParams        FinalChallengeParams,
    assertion       RegistrationAssertion
}
```

header:操作头,header.op 应为“Reg”,ASN.1 描述见 5.2.5。

fcParams:最终挑战参数 FinalChallengeParams,ASN.1 描述见 5.2.6。该参数使用 UTF8 编码,然后使用[RFC 4627]定义的序列化方法序列化后,再使用 base64url[RFC 4648]对其进行编码后的值。

assertions:注册请求断言,生物特征识别密钥管理器的响应数据,ASN.1 描述如下:

```
RegistrationAssertion ::= SEQUENCE {
```

```

    assertionScheme      PrintableString,
    assertion             RegAssertion,
    exts                  SEQUENCE OF Extension OPTIONAL
}

```

assertionScheme:用来编码断言的断言模式名称。例如,该值可为“BAPV1TLV”。

exts:生物特征识别密钥管理器支持的扩展,ASN.1 描述见 5.2.4。

assertion:注册断言,ASN.1 描述如下:

```

RegAssertion ::= {
    krd          KRD,
    sig          BIT STRING
}

```

krd:密钥注册数据,数据格式如下所示:

```

KRD ::= SEQUENCE {
    bkmID          PrintableString,
    assertionInfo  AssertionInfo,
    challengeHash  BIT STRING,
    keyID          PrintableString,
    counters       Counters,
    uauthPubKey    OCTET STRING
}

```

bkmID:生物特征识别密钥管理器标识符。

assertionInfo:断言描述信息,ASN.1 描述见 5.2.8。

challengeHash:服务器挑战的 SM3 杂凑值,SM3 算法应符合 GB/T 32905 的规定。

keyID:鉴别私钥标识符。

counters:生物特征识别密钥管理器计数器值,ASN.1 描述见 5.2.9。

uauthPubKey:生成的鉴别公钥,是符合 GB/T 32918 规定的公钥。

sig:使用厂商私钥,利用 SM2 算法对 krd 进行签名后的签名值,格式应符合 GB/T 35276 的规定,使用的 SM2 算法应当符合密码国家标准、行业标准的相关要求;

e) 将注册响应消息发送给身份鉴别服务器。

5.3.1.2.3 身份鉴别服务器处理注册响应规则

身份鉴别服务器应遵循以下步骤:

- 解析注册响应消息,判断注册响应消息是否包含必要的参数以及每个参数是否符合要求,若符合要求则执行以下步骤,否则拒绝该消息;
- 使用厂商公钥验证注册响应消息中签名的正确性;
- 如果注册响应消息通过验证,将用户鉴别公钥等相关信息保存在身份鉴别服务器,完成注册,返回注册成功;否则返回注册失败。

5.3.2 鉴别流程

5.3.2.1 概述

鉴别流程如图 4 所示,具体流程如下:

- 用户通过用户代理访问依赖方,发起鉴别流程;

- b) 依赖方将用户重定向到身份鉴别服务器；
- c) 身份鉴别服务器生成鉴别请求消息,见 5.3.2.2.1 a)步骤；
- d) 身份鉴别服务器通过用户代理将鉴别请求消息发送至生物特征识别密钥管理器,见 5.3.2.2.1 b)步骤；
- e) 生物特征识别密钥管理器首先验证身份鉴别服务器的真实性,然后生物特征识别密钥管理器发起本地用户校验,提示用户使用生物特征识别信息进行身份验证,见 5.3.2.2.2 a)、b)步骤；
- f) 用户提交生物识别信息,例如指纹、虹膜等信息；
- g) 生物特征识别密钥管理器验证用户提交的生物识别信息,验证通过后,生成鉴别响应消息,见 5.3.2.2.2 c)、d)步骤；
- h) 生物特征识别密钥管理器通过用户代理将鉴别响应消息返回给身份鉴别服务器,见 5.3.2.2.2 e)步骤；
- i) 身份鉴别服务器验证鉴别响应消息,见 5.3.2.2.3 a)~c)步骤；
- j) 身份鉴别服务器将结果返回给依赖方。

5.3.2.2 鉴别流程处理规则

5.3.2.2.1 身份鉴别服务器生成鉴别请求规则

身份鉴别服务器应遵循以下步骤：

- a) 创建鉴别请求消息,并初始化鉴别请求消息的各个参数。鉴别请求消息格式如下：

```
AuthenticationRequest ::= SEQUENCE {
    header          OperationHeader,
    challenge       PrintableString
}
```

header:操作头,header.op 的值应为“Auth”,ASN.1 描述见 5.2.5。

challenge:服务器提供的挑战值；

- b) 将鉴别请求消息发送给生物特征识别密钥管理器。

5.3.2.2.2 生物特征识别密钥管理器处理鉴别请求规则

生物特征识别密钥管理器应遵循以下步骤：

- a) 验证身份鉴别服务器的真实性,验证成功则执行以下步骤,否则拒绝该消息；
- b) 解析鉴别请求消息,判断鉴别请求消息是否包含必要的参数以及每个参数是否符合要求,若符合要求则执行以下步骤,否则拒绝该消息；
- c) 提示用户选择本地生物特征识别器,用户选择后,使用用户选择的生物特征识别器验证用户,验证通过后执行以下操作,否则返回错误；
- d) 创建鉴别响应消息,并根据鉴别请求消息的参数初始化鉴别响应消息的各个参数。鉴别响应消息如下：

```
AuthenticationResponse ::= SEQUENCE {
    header          OperationHeader,
    fcParams        FinalChallengeParams,
    assertions      AuthAssertion
}
```

header:操作头,header.op 应为“Auth”,ASN.1 描述见 5.2.5。

fcParams:最终挑战参数 FinalChallengeParams,ASN.1 描述见 5.2.6。该参数使用 UTF8 编码,然后使用[RFC 4627]定义的序列化方法序列化后,再使用 base64url[RFC 4648]对其进行编码后的值。

assertions:AuthAssertion 对象,生物特征识别密钥管理器针对鉴别请求生成的签名断言,ASN.1 描述如下:

```
AuthAssertion ::= SEQUENCE {
    assertionScheme    PrintableString,
    assertion          SignAssertion,
    exts               SEQUENCE OF Extension OPTIONAL
}
```

assertionScheme:用来编码断言的断言模式名称。例如,该值可为“BAPV1TLV”。

exts:生物特征识别密钥管理器支持的扩展,ASN.1 描述见 5.2.4。

assertion:生物特征识别密钥管理器针对鉴别请求数据生成的签名断言,ASN.1 描述如下:

```
SignAssertion ::= {
    signData          SignData,
    sig               BIT STRING
}
```

signData:待签名数据,数据格式如下所示:

```
SignData ::= SEQUENCE {
    bkmID             PrintableString,
    assertionInfo     AssertionInfo,
    nonce             OCTET STRING,
    challengeHash     OCTET STRING,
    keyID             PrintableString,
    counters          Counters
}
```

bkmID:生物特征识别密钥管理器标识符。

assertionInfo:断言描述信息,ASN.1 描述见 5.2.8。

nonce:生物特征识别密钥管理器生成的随机临时参数值。

challengeHash:服务器挑战的 SM3 杂凑值,SM3 算法应符合 GB/T 32905 的规定。

keyID:鉴别私钥标识符。

counters:生物特征识别密钥管理器计数器值,ASN.1 描述见 5.2.9。

sig:使用鉴别私钥,利用 SM2 算法对 signData 进行签名后的签名值,格式应符合 GB/T 35276 的规定,使用的 SM2 算法应当符合密码国家标准、行业标准的相关要求;

e) 将鉴别响应消息发送给身份鉴别服务器。

5.3.2.2.3 身份鉴别服务器处理鉴别响应规则

身份鉴别服务器应遵循以下步骤:

- 解析鉴别响应消息,判断鉴别响应消息是否包含必要的参数以及每个参数是否符合要求,若符合要求则执行以下步骤,否则拒绝该消息;
- 使用鉴别公钥验证鉴别响应消息的正确性;

- c) 如果验证通过,则鉴别成功,否则失败。

5.3.3 注销流程

5.3.3.1 概述

图 5 描述注销流程:

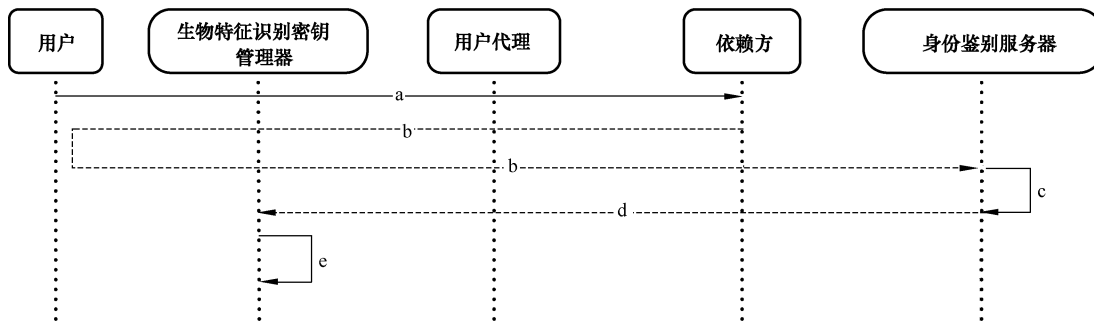


图 5 注销详细流程

- 用户通过用户代理访问依赖方,发起注销流程;
- 依赖方将用户重定向到身份鉴别服务器,身份鉴别服务器首先进行用户身份鉴别,鉴别通过后进行后续注销流程,否则拒绝执行注销流程,见 5.3.3.2.1 a) 步骤;
- 身份鉴别服务器生成注销请求消息,删除与该用户相关的数据,见 5.3.3.2.1 b) 步骤;
- 身份鉴别服务器通过用户代理将注销请求消息发送至生物特征识别密钥管理器,见 5.3.3.2.1 c) 步骤;
- 生物特征识别密钥管理器删除用户相关数据,见 5.3.3.2.2 a)、b) 步骤。

5.3.3.2 注销流程处理规则

5.3.3.2.1 身份鉴别服务器生成注销请求规则

身份鉴别服务器应遵循以下步骤:

- 创建注销请求消息,并初始化注销请求消息的各个参数。注册请求消息格式如下:

```

DeregistrationRequest ::= SEQUENCE {
    header          OperationHeader,
    bapKeyManagers SEQUENCE OF DeregisterBAPKeyManager
}

```

header:操作头,header.op 应为“Dereg”,ASN.1 描述见 5.2.5。

bapKeyManagers:要注销的生物特征识别密钥管理器(DeregisterBAPKeyManager)列表,DeregisterBAPKeyManager 的 ASN.1 描述如下:

```

DeregisterBAPKeyManager ::= SEQUENCE {
    bkmaID          PrintableString,
    keyID           PrintableString
}

```

bkmaID:要注销的生物特征识别密钥管理器标识符(bkmaID)。

keyID:与鉴别私钥相关联的唯一的密钥标识符(KeyID);

- 删除身份鉴别服务器上与该用户相关的数据;

- c) 将注销请求消息发送到生物特征识别密钥管理器。

5.3.3.2.2 生物特征识别密钥管理器处理注销请求规则

生物特征识别密钥管理器应遵循以下步骤：

- a) 解析注销请求消息，判断注销响应消息是否包含必要的参数以及每个参数是否符合要求，若符合要求则执行以下步骤，否则拒绝该消息；
- b) 删除对应 KeyID 的密钥对等相关数据，注销成功。

6 双因素在线快捷身份鉴别协议

6.1 协议架构

6.1.1 概述

针对已部署使用用户名/口令等方式鉴别用户的依赖方，双因素在线快捷身份鉴别协议将鉴别器作为用户身份鉴别的第二因素，提升用户身份鉴别的安全性。协议规定了鉴别器应完成的功能，并且规定了协议架构、协议消息框架、协议流程和要求以及协议接口，其中，安全风险及措施建议见附录 A，关于协议接口见附录 C。在实际部署过程中使用的商用密码产品，应当由具备资格的商用密码检测、认证机构检测认证合格后，方可部署到实际系统中。

在双因素在线快捷身份鉴别协议中，包括五个实体：鉴别器、鉴别客户端、用户代理、依赖方、身份服务提供方。鉴别器通过用户代理与身份服务提供方通信，负责生成密钥对和签名，将公钥发送给身份服务提供方用于用户身份的绑定和身份鉴别，将私钥存储在鉴别器中并保证其安全性。身份服务提供方通过用户代理与鉴别器通信，负责鉴别用户身份，提供用户鉴别结果。鉴别客户端负责构造发送给鉴别器的请求消息，接收鉴别器发送的响应消息。用户代理需支持鉴别客户端接口。

双因素在线快捷身份鉴别协议由注册、鉴别和注销三种会话组成。

注册：用户将鉴别器生成的鉴别公钥发送给身份服务提供方，身份服务提供方将鉴别公钥与用户身份进行绑定。

鉴别：在使用用户名口令鉴别用户身份的基础之上，同时使用已注册的鉴别公私钥进行身份鉴别。

注销：用户删除与身份服务提供方关联的鉴别公私钥对。

三种会话的协议流程中，协议参与方应保护协议消息数据的机密性。用户代理与身份服务提供方的通信宜采用传输层密码协议(TLCP, GB/T 38636)。鉴别客户端与鉴别器宜通过 USB、NFC、蓝牙等传输协议进行通信。

本协议中有关密钥等关键安全参数的全生命周期管理或安全管理的要求应符合 GB/T 37092 的规定。

6.1.2 注册

在用户向依赖方进行注册时，鉴别器生成一对鉴别公私钥对，将鉴别公钥发送给依赖方。依赖方保存鉴别公钥，并与用户身份绑定，完成注册过程。会话流程(注册流程)如图 6 所示，图中采用 HTTP 重定向方式对协议交互情况进行说明。

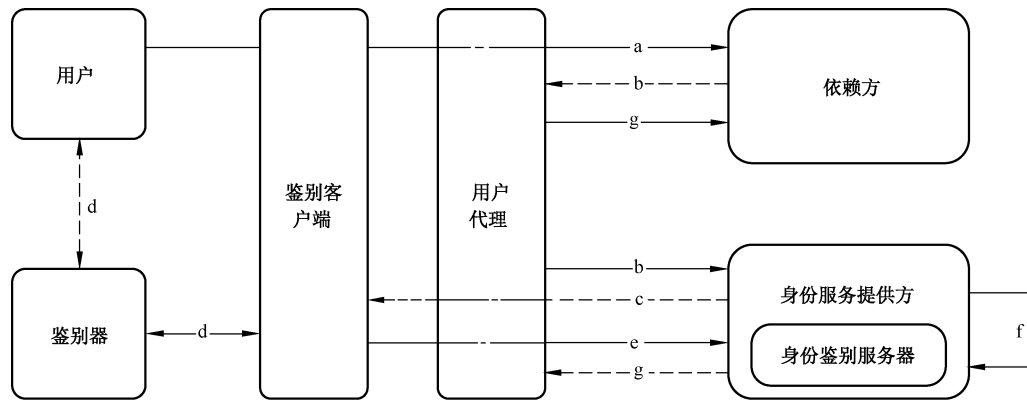


图 6 会话流程(注册流程/鉴别流程)

- a) 用户通过用户代理访问依赖方。
- b) 当用户需要进行身份鉴别注册时,依赖方将用户定向到身份鉴别服务器。可使用 HTTP 重定向方式将用户设备重定向到身份鉴别服务器,或者使用消息转发方式。
- c) 身份鉴别服务器验证用户名和口令成功后,构造注册请求参数,通过用户代理调用鉴别客户端的注册接口。
- d) 鉴别客户端验证身份鉴别服务器的身份,验证通过后构造注册请求消息,将注册请求消息发送给鉴别器。鉴别器与用户进行交互验证用户身份,其中,图中 d 虚线部分代表用户与鉴别器的交互,比如用户使用指纹或 PIN 码等。
- e) 鉴别器验证用户身份成功后,生成一对鉴别公私钥,构造包含鉴别公钥和密钥句柄等内容的注册响应消息,通过鉴别客户端和用户代理将注册响应消息发送给身份鉴别服务器。
- f) 身份鉴别服务器验证鉴别器身份并返回验证结果,若验证通过,则保存对应的鉴别公钥和密钥句柄。
- g) 身份鉴别服务器将注册结果返回给依赖方。

6.1.3 鉴别

在鉴别流程中,鉴别器使用鉴别私钥对挑战等信息进行签名,向依赖方证明其拥有该鉴别私钥,完成身份鉴别过程。会话流程(鉴别流程)如图 6 所示,图中采用 HTTP 重定向方式对协议交互情况进行说明。

- a) 用户通过用户代理访问依赖方。
- b) 当用户需要进行身份鉴别时,依赖方将用户定向到身份鉴别服务器。可使用 HTTP 重定向方式将用户设备重定向到身份鉴别服务器,或者使用消息转发方式。
- c) 身份鉴别服务器验证用户名和口令成功后,构造鉴别请求参数,通过用户代理调用鉴别客户端的签名接口。
- d) 鉴别客户端验证身份鉴别服务器的身份,验证通过后构造鉴别请求消息,将鉴别请求消息发送给鉴别器。鉴别器与用户进行交互验证用户身份,其中,图中 d 虚线部分代表用户与鉴别器的交互,比如用户使用指纹或 PIN 码等。
- e) 鉴别器验证用户身份成功后,选择对应的鉴别私钥对挑战等信息进行签名,构造鉴别响应消息,并将鉴别响应消息通过鉴别客户端和用户代理发送给身份鉴别服务器。
- f) 身份鉴别服务器使用对应的鉴别公钥对签名进行验证,验证成功则用户鉴别成功,否则用户鉴别失败。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/726132114213010201>