ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0140—2024

支付系统个人可信确认密码应用技术规范

Cryptography application technical specification for personal trusted confirmation in payment system

2024-12-27 发布　　2025-07-01 实施

国家密码管理局　　发布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
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　个人可信确认系统组成 …… 2
6　个人可信确认业务流程 …… 3
7　个人可信确认密码应用需求 …… 4
8　个人可信确认密码应用技术要求 …… 4
8.1　密码应用总体要求 …… 4
8.2　密钥管理安全要求 …… 5
8.2.1　密钥种类 …… 5
8.2.2　密钥存储要求 …… 5
8.3　个人可信确认服务系统与个人可信确认设备通信安全要求 …… 6
8.3.1　通信协议流程 …… 6
8.3.2　报文协议内容 …… 7
8.4　个人可信确认服务系统与支付系统通信安全要求 …… 8
8.4.1　通信协议流程 …… 8
8.4.2　报文协议内容 …… 9
8.5　个人可信确认服务系统与证书认证系统通信安全要求 …… 9

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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

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：西安电子科技大学、睿丰宝科技有限公司、国家新闻出版广电总局广播电视规划院、支付宝（中国）网络技术有限公司、中国科学院信息工程研究所、暨南大学、中电科网络安全科技股份有限公司、北京创原天地科技有限公司、西安电子科技大学广州研究院、密码与网络安全（黄埔）研究院、北京大学、中国金融电子化公司、兴唐通信科技有限公司。

本文件主要起草人：樊凯、白宇晗、刘婷婷、韩小军、王晨、王晓英、秦勇、李东风、高能、谭武征、苏锐丹、李晖、宋峥、周君平、王鑫、杨凤春、韩竺吾、刘辛越、王妮娜。

引　言

本文件的目标是给出一种个人用户直接参与支付流程并进行可信确认的机制，为需要可信确认的业务系统搭载一种逻辑上不同于现有支付系统传输的另一种独立传输通道，从而全方位控制支付的安全性和可靠性。

本文件针对不同业务抽象其密码技术需求，从解决个人可信确认安全需求的角度进行阐述，重点阐述如何在支付系统个人可信确认中使用密码技术，能够为支付系统个人可信确认的系统研发、建设过程提供合规性指导，规范密码技术在辅助支付系统进行可信确认过程中的应用。

支付系统个人可信确认密码应用技术规范

1 范围

本文件规定了支付系统个人可信确认的密码应用、通信协议等技术要求，描述了相应的密码协议。

本文件适用于支付系统个人可信确认相关系统的构建、使用和管理。

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 15843.3 信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制

GB/T 15852(所有部分) 信息技术 安全技术 消息鉴别码

GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 25069 信息安全技术 术语

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 32918.4 信息安全技术 SM2椭圆曲线公钥密码算法 第4部分：公钥加密算法

GB/T 37092 信息安全技术 密码模块安全要求

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GM/Z 4001 密码术语

3 术语和定义

GB/T 25069、GB/T 37092和GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

支付系统 payment system

由客户、商家、认证中心、支付网关、客户银行、商业银行、金融专网七个要素组成，用以提供支付结算服务以及专业技术手段，实现债权债务清偿及资金转移的一种金融安排。

3.2

个人可信确认系统 personal trusted confirmation system；PTCS

由支付机构建立，允许个人用户针对个人信息、支付信息或资产信息等信息在各支付环节进行可信确认的系统。

3.3

个人可信确认服务系统 service system of PTCS

用于对个人相关业务进行可信确认处理的个人可信确认系统的服务器端或服务端系统。

注：也称或简称服务系统。

3.4

个人可信确认设备 user device of PTCS

用于用户进行个人策略设置、支付确认等业务处理的个人可信确认系统的终端设备。

3.5

密码模块　cryptographic module

实现密码运算功能的、相对独立的软件、硬件、固件或其组合。

3.6

密码协议　cryptographic protocol

两个或两个以上参与者使用密码算法，为达到某种特定目的，采取的一系列步骤而形成的约定规则。

4　缩略语

下列缩略语适用于本文件。

MAC：消息认证码（Message Authentication Code）

PTCS：个人可信确认系统（Personal Trusted Confirmation System）

SSPTCS：个人可信确认服务系统（Service System of PTCS）

UDPTCS：个人可信确认设备（User Device of PTCS）

5　个人可信确认系统组成

个人可信确认系统是个人用户的一种支付风险控制解决方案，由个人可信确认服务系统和个人可信确认设备构成，个人可信确认系统模型的示意图见图 1。

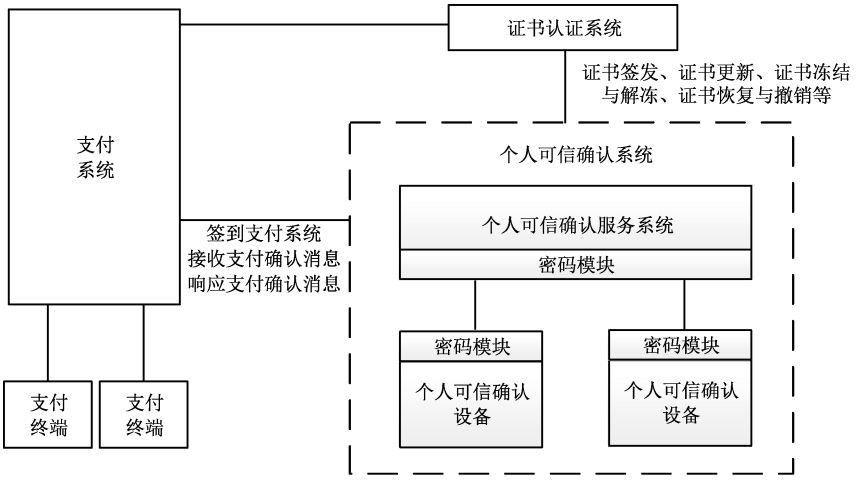

图 1　个人可信确认系统模型

个人可信确认系统主要包括：

a）　个人可信确认服务系统：用于对个人相关业务进行可信确认处理的 PTCS 的服务器端或服务端系统；

b）　个人可信确认设备：用于用户进行个人策略设置、支付确认等业务处理的 PTCS 的终端设备。

其中，证书认证系统为个人可信确认系统和支付系统提供生命周期内的数字证书管理，包括证书签发、证书更新、证书冻结与解冻、证书恢复与撤销等功能。支付系统根据个人可信确认策略设置与 PTCS 进行交互，包括签到支付系统、接收支付确认消息和响应支付确认消息。支付终端向支付系统发起的支付业务需要个人可信确认设备最终确认，通过个人可信确认服务系统与支付系统交互实现可信确认信息传递。

支付系统、支付终端、证书认证系统是支付业务的构成元素，是个人可信确认系统的相关外部系统。外部系统的密码应用与密钥管理不在本文件内定义，但本文件规定个人可信确认系统与外部系统的交互报文格式。

6 个人可信确认业务流程

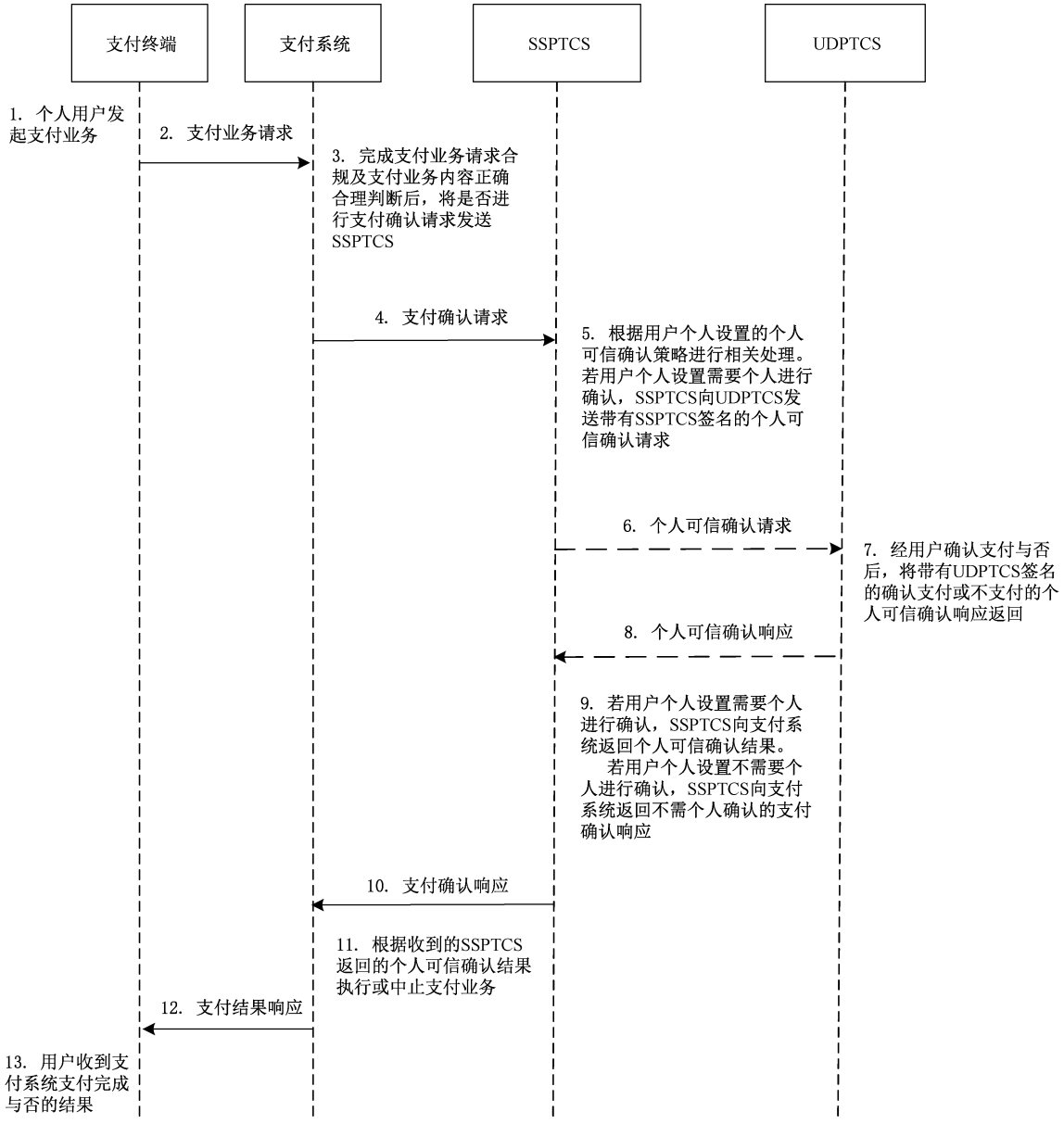

图 2 个人可信确认流程

个人可信确认流程的示意图见图 2，个人可信确认基本过程具体如下。

a) 个人用户在支付终端发起支付业务后，支付系统进行支付业务识别及其请求合规及支付业务内容正确合理性判断。

b) 支付系统完成相关判断后，将是否进行支付确认请求发送 SSPTCS。

c) PTCS 的服务系统 SSPTCS 根据用户个人设置的个人可信确认策略进行相关处理，包括：

1) 若用户个人设置需要由个人进行最终确认，SSPTCS 向 UDPTCS 发送带有 SSPTCS 签名

的支付确认请求；UDPTCS 接收相关请求后，经用户确认支付与否，将带有 UDPTCS 签名的确认支付或不支付的个人可信确认响应返回；SSPTCS 向支付系统返回个人可信确认结果；

2） 若用户个人设置不需要由个人进行最终确认，SSPTCS 向支付系统发出该项支付不需用户确认支付的信息。

d） 支付系统收到 SSPTCS 返回的信息后，执行或中止该项支付。结果返回个人用户支付终端。

7 个人可信确认密码应用需求

SSPTCS 与 UDPTCS 之间传输数据时，PTCS 应通过密码模块保障数据机密性、完整性、真实性和不可否认性。PTCS 功能说明如下。

a） 密钥管理

在支付系统个人可信确认过程中，确保密钥在整个生命周期的安全管理，包括密钥的生成、分发、存储、备份、使用、更新、销毁等，涉及对 PTCS 的安全功能要求，对 PTCS、支付系统和证书认证系统等机构实体的管理职责要求，以及贯穿整体过程的流程控制要求。

b） 身份鉴别

在个人可信确认过程中，为了防止个人用户可能存在欺骗行为应对个人身份进行鉴别，应采用确认数据结构、数字证书、加密和签名等技术方法。

c） 信源鉴别

SSPTCS 与 UDPTCS 之间传输用户鉴别数据、用户个人敏感数据、业务数据时，应采用数字签名算法计算和校验数据真实性。

d） 数据加密

为确保数据保密，应对资金账号、用户口令、支付金额、支付期限等网络支付隐私信息的资金流数据进行加密操作，如需要对用户登录过程进行签名验签，交易确认信息的加密传输，正常和异常支付报告的加密传输等。传输用户或系统鉴别数据时，应以非明文（密文或杂凑值）形式传输，应采用密码杂凑算法、对称密码算法或非对称密码算法。传输用户个人敏感数据时，应以密文形式传输，应采用对称密码算法或非对称密码算法。传输业务数据时，应以密文形式传输，应采用对称密码算法或非对称密码算法。

e） 数据审计

考虑数据的伪造、篡改问题，如各关联方数据收到未经许可的修改和伪造，应保护数据的完整性。为保证数据的完整性，需要对数据（亦称报文）进行验证。在 SSPTCS 与 SSPTCS 进行传输用户鉴别数据、用户个人敏感数据、业务数据时，应计算和校验数据的完整性，应采用密码杂凑算法。

f） 数据查验

为保证数据的不可否认性，防止各关联方对数据否认和抵赖，应对数据进行数字签名和签名验证，借助私钥的机密性确保该数据传输过程具有抗抵赖效力。应记录和保存事后可查验的日志记录，提供追溯、仲裁和责任认定的依据。

8 个人可信确认密码应用技术要求

8.1 密码应用总体要求

PTCS 中的 SSPTCS、UDPTCS 需要分别部署密码模块，提供密钥生成、存储、分发、导入与导出、使用、备份与恢复、归档、销毁等环节的密钥安全管理和密码运算服务。SSPTCS 和 UDPTCS 应分别采用支持 SM2、SM3、SM4 密码算法的密码模块。采用证书认证系统作为各密码模块的证书管理中心。

8.2 密钥管理安全要求

8.2.1 密钥种类

系统使用的密钥分为签名密钥、加密密钥、会话密钥三种类型。签名密钥(私钥)用于对通信发起方原文进行签名,保证数据来源真实性、完整性、不可否认性;加密密钥用于对会话密钥进行加密处理,保证会话密钥的安全性;会话密钥由通信双方协商产生,用于对原文进行加密处理,保证数据的机密性。

证书认证系统为 PTCS 提供证书签发和签名服务。

SSPTCS 使用的密钥包括:服务端签名公私钥、服务端加密公私钥和服务端会话密钥。UDPTCS 使用的密钥包括:用户端签名公私钥、用户端加密公私钥和用户端会话密钥。其密钥使用具体如下。

a) 服务端签名公私钥:
   1) 由 SSPTCS 部署的密码模块采用 SM2 密码算法生成;
   2) 服务端签名私钥用于 SSPTCS 对外通信时对数据进行签名;
   3) 服务端签名公钥提交至证书认证系统,用于申请服务端签名证书、对协商会话密钥数据进行签名验签;
   4) 服务端签名公钥导入 UDPTCS 密码模块。
b) 服务端加密公私钥:
   1) 由 SSPTCS 的密码模块采用 SM2 密码算法生成;
   2) 服务端加密公钥导入 UDPTCS,用于 UDPTCS 对 SSPTCS 发送会话密钥数据时进行加密;
   3) 服务端加密私钥用于接收协商会话密钥时进行解密。
c) 服务端会话密钥:
   由服务端和用户端的密码模块采用 SM4 算法产生,用于 SSPTCS 和 UDPTCS 之间的通信加密。
d) 用户端签名公私钥:
   1) 由 UDPTCS 部署的密码模块采用 SM2 密码算法生成;
   2) 用户端签名私钥用于 UDPTCS 对外通信时对数据进行签名;
   3) 用户端签名公钥提交至证书认证系统,用于申请用户模块证书,对协商会话密钥数据进行签名验签;
   4) 用户端签名公钥导入 SSPTCS 密码模块。
e) 用户端加密公私钥:
   1) 由 UDPTCS 的密码模块采用 SM2 密码算法生成;
   2) 用户端加解密公钥导入 SSPTCS,用于 SSPTCS 对 UDPTCS 发送会话密钥数据时进行加密;
   3) 用户端加密私钥用于接收 SSPTCS 会话密钥时进行解密。
f) 用户端会话密钥:
   由服务端和用户端的密码模块采用 SM4 算法产生,用于 UDPTCS 和 SSPTCS 之间的通信加密。

8.2.2 密钥存储要求

PTCS 中会话密钥为临时密钥,由用户端和服务端共同保存的对称根密钥计算生成,使用完应立即销毁,不需要长期存储。

其余相关密钥存储要求具体如下。

a） SSPTCS：
   1） 服务端签名私钥存储在 SSPTCS 密码模块(密码服务设备)；
   2） 服务端签名公钥(证书)存储在 UDPTCS 密码模块；
   3） 服务端加密私钥存储在 SSPTCS 密码模块(密码服务设备)；
   4） 服务端加密公钥(证书)存储在 UDPTCS 密码模块。
b） UDPTCS：
   1） 用户端签名私钥存储在 UDPTCS 密码模块；
   2） 用户端签名公钥(证书)存储在 SSPTCS；
   3） 用户端加密私钥存储在 UDPTCS 密码模块；
   4） 用户端加密公钥(证书)存储在 SSPTCS。

8.3 个人可信确认服务系统与个人可信确认设备通信安全要求

8.3.1 通信协议流程

SSPTCS 和 UDPTCS 之间应采用 SM3 算法和 SM2 算法实现双向认证及会话密钥协商，应采用 SM4 算法用产生的会话密钥对数据进行对称加密并通信。其中，非对称加密算法应采用 SM2 算法，应满足 GB/T 32918.4 的要求；密码杂凑算法应采用 SM3 算法，应满足 GB/T 15852(所有部分)的要求；对称加密算法应采用 SM4 算法，应满足 GB/T 32907 的要求。

SSPTCS 和 UDPTCS 之间的通信协议包括服务端发起和用户端发起两种方式。其中，服务端的系统实现应满足 GB/T 39786 的要求，用户端的系统实现应满足 GB/T 37092 的要求。个人可信确认应采用用户端发起方式，包含会话协商和数据传输两个过程。其中，数据传输过程的示意图见图 3。

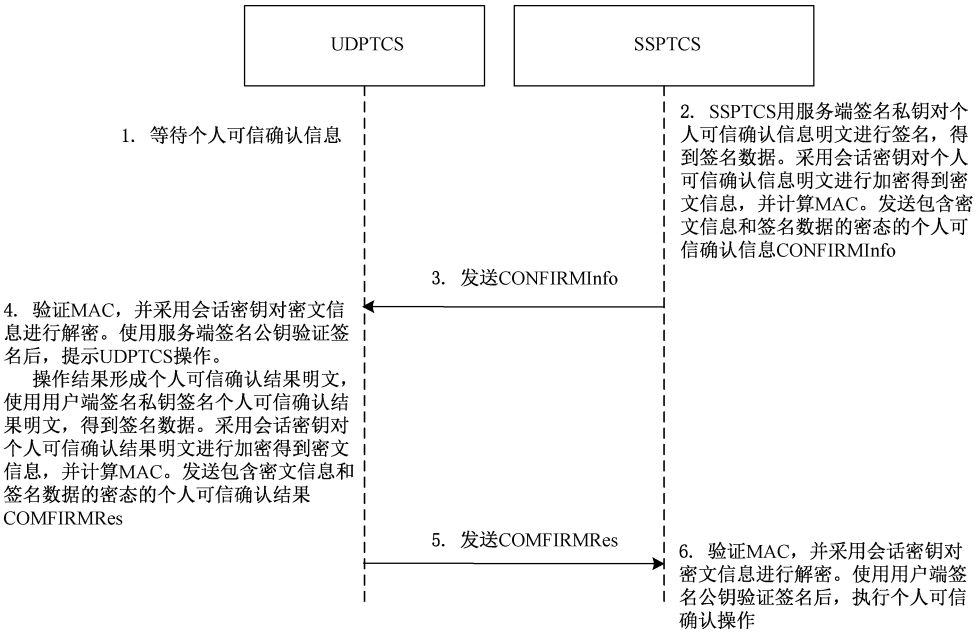

图 3 数据传输过程

密码应用流程具体如下。

a） 会话协商过程是 SSPTCS 和 UDPTCS 之间进行双向认证及协商会话密钥的过程。其中，双向认证过程使用用户端签名密钥和服务端签名密钥实现，协商会话密钥过程使用用户端加密密钥和服务端加密密钥实现，应满足 GB/T 15843.3 的要求。

b） 数据传输过程是 SSPTCS 和 UDPTCS 之间进行数据传输的过程，应采用先签名后加密形式。

SSPTCS 与 UDPTCS 之间的密码应用协议，主要包含发送个人可信确认信息和接收个人可信确认结果。

8.3.2 报文协议内容

8.3.2.1 个人可信确认信息

SSPTCS 发送给 UDPTCS 的个人可信确认信息的逻辑结构，应与图 4 相符合。

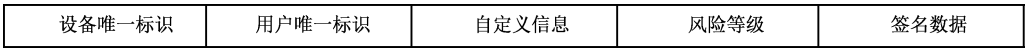

图 4 个人可信确认信息的逻辑结构

SSPTCS 需将设备唯一标识、用户唯一标识、自定义信息、风险等级按顺序串联得到个人可信确认信息明文。SSPTCS 发送 UDPTCS 的个人可信确认信息的 ASN.1 定义为：

```
CONFIRMInfo :: = SEQUENCE{
    deviceID        UTF8String,                          --设备唯一标识
    userID          UTF8String,                          --用户唯一标识
    extDatas        EXPLICIT ExtensionDatas OPTIONAL,    --自定义信息
    riskRating      OCTET STRING                         --风险等级
    signInfo        SES_SignInfo                         --签名数据
}
```

其中：

a) 自定义信息

extDatas：用于服务器使用的自定义信息。

```
ExtensionDatas :: = SEQUENCE SIZE (0..MAX) OF ExtData
ExtData :: = SEQUENCE{
extnID          OBJECT IDENTIFIER,          --自定义扩展字段标识
critical        BOOLEAN DEFAULT FALSE,      --自定义扩展字段是否关键
extnValue       OCTET STRING                --自定义扩展字段数据值
}
```

自定义信息内容与业务相关，不在本文件内定义。

b) 签名数据

签名数据是对设备唯一标识、用户唯一标识、自定义信息和风险等级的明文信息的签名。签名数据的结构，应与图 5 相符合。

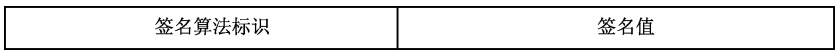

图 5 签名数据的结构图

签名数据的 ASN.1 定义为：

```
SES_SignInfo :: = SEQUENCE{
signatureAlgorithm      OBJECT IDENTIFIER,      --签名算法标识
signData                INTEGER                 --签名值
}
```

8.3.2.2 个人可信确认结果

UDPTCS需将设备唯一标识、用户唯一标识、确认结果信息、风险等级按顺序串联得到个人可信确认结果明文。SSPTCS接收UDPTCS的个人可信确认结果的报文定义为：

```
CONFIRMRes ::= SEQUENCE{
    deviceID            UTF8String,         --设备唯一标识
    userID              UTF8String,         --用户唯一标识
    confirmResInfo      OCTET STRING,       --确认结果信息
    riskRating          OCTET STRING        --风险等级
    signInfo            SES_SignInfo        --签名数据
}
```

其中：

a) 确认响应签名值

confirmResInfo：如果对当次支付不确认，则confirmResInfo=0；如果确认，则计算签名，原文为extDatas全部报文。

b) 签名数据

签名数据是对设备唯一标识、用户唯一标识、确认结果信息和风险等级的明文信息的签名。签名数据的报文定义为：

```
SES_SignInfo ::= SEQUENCE{
    signatureAlgorithm      OBJECT IDENTIFIER,      --签名算法标识
    signData                INTEGER                 --签名值
}
```

8.4 个人可信确认服务系统与支付系统通信安全要求

8.4.1 通信协议流程

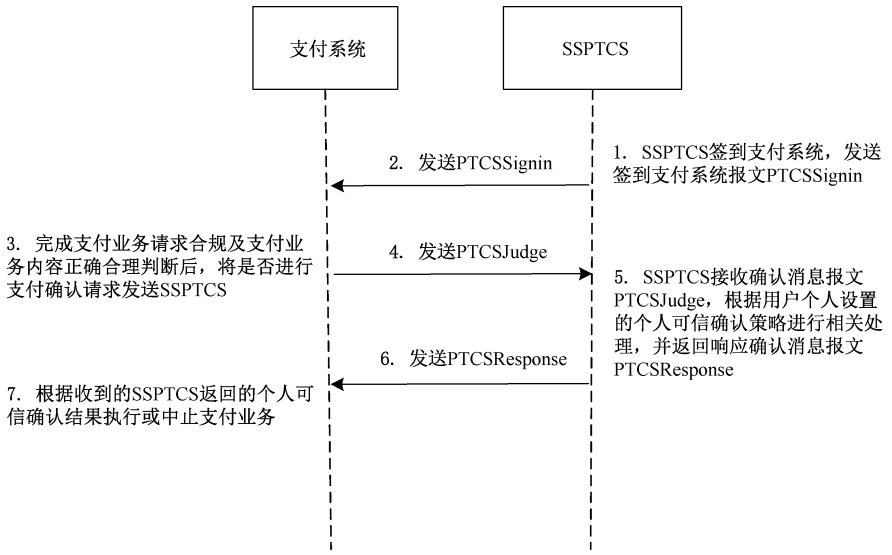

图6 SSPTCS与支付系统之间的密码应用协议

SSPTCS与支付系统之间的密码应用协议的示意图见图6，主要包含签到支付系统、接收支付确认消息以及响应支付确认消息。

8.4.2 报文协议内容

8.4.2.1 签到支付系统

SSPTCS 签到支付系统报文定义为：

```
PTCSSignin:: =SEQUENCE{
PTCSSn        OCTET STRING        --个人可信确认服务机构编码
signature      OCTET STRING       --预留的机构自定义信息
}
```

8.4.2.2 接收确认消息

SSPTCS 接收确认消息报文定义为：

```
PTCSJudge:: =SEQUENCE{
PTCSPayNo          OCTET STRING      --支付系统当次业务流水号
PTCSAccount        INTEGER           --支付系统当次交易账号
PTCSPayment        INTEGER           --支付系统当次交易额
PTCSPayTime        OCTET STRING      --支付系统当次交易时间
PTCSPaySignature    OCTET STRING     --支付系统当次交易终端签名
PTCSPayMac         INTEGER           --支付系统当次交易报文 MAC
}
```

8.4.2.3 响应确认消息

SSPTCS 响应确认消息报文定义为：

```
PTCSResponse:: = SEQUENCE{
PTCSResNo          OCTET STRING          --支付确认响应流水号
PTCSResSignature   OCTET STRING          --支付确认响应签名值
}
```

其中：

a) PTCSResNo：PTCSResNo=PTCSPayNo；

b) PTCSResSignature：如果对当次支付不确认，则 PTCSResSignature=0；如果确认，则计算签名，原文为 PTCSJudge 全部报文。

8.5 个人可信确认服务系统与证书认证系统通信安全要求

SSPTCS 与证书认证系统之间的密码应用协议，主要提供证书签发、证书更新、证书冻结与解冻、证书恢复与撤销等功能，应满足 GB/T 25056 的要求。

中华人民共和国密码
行业标准
支付系统个人可信确认密码应用技术规范
GM/T 0140—2024
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
网址 www.spc.net.cn
总编室:(010)68533533　发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1　字数 23 千字
2025年6月第1版　2025年6月第1次印刷
*
书号:155066·2-39032　定价 31.00 元

GM/T 0140-2024