ICS 03.060；35.240.40
CCS A11

团　体　标　准

T/CBA 211—2021

银行函证服务平台 加密体系

Banking confirmation service platform — Encryption system

2021－11－10 发布　　2021－11－10 实施

中国银行业协会　发布

目　　次

前　言

中国银行业协会(China Banking Association，CBA)成立于2000年5月，是经中国人民银行和民政部批准成立，并在民政部登记注册的全国性非营利社会团体，是中国银行业自律组织。2003年中国银监会成立后，中国银行业协会主管单位由中国人民银行变更为中国银监会。2018年3月，中国银行保险监督管理委员会成立后，中国银行业协会主管单位由中国银监会变更为中国银行保险监督管理委员会。凡经业务主管单位批准设立的、具有独立法人资格的银行业金融机构(含在华外资银行业金融机构)和经相关监管机构批准、具有独立法人资格、在民政部门登记注册的各省(自治区、直辖市、计划单列市)银行业协会以及相关监管机构批准设立，具有独立法人资格的依法与银行业金融机构开展相关业务合作的其他类型金融机构，以及银行业专业服务机构均能申请加入中国银行业协会成为会员单位。

中国银行业协会日常办事机构为秘书处。秘书处设秘书长1名，副秘书长若干名。根据工作需要，中国银行业协会设立32个专业委员会，其中银行业产品和服务标准化专业委员会旨在开展银行业产品和服务标准化工作，包括制定和发布银行业的产品和服务标准，积极参与制定国家标准、行业规划，参与制定有关政策和法律法规，不断提高银行业产品和服务质量。

本文件按照T/CBA 1—2021《中国银行业协会团体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。

T/CBA 211—2021《银行函证服务平台 加密体系》是按照财政部和银保监会的要求构建的银行函证服务平台的工作技术依据系列文件之一，本系列文件结构如下：

——T/CBA 210—2021《银行函证服务平台 接入要求》；

——T/CBA 211—2021《银行函证服务平台 加密体系》；

——T/CBA 212《银行函证服务平台 基础数据元》；

——TR/CBA 213《银行函证服务平台 服务接口》；

——TR/CBA 214《银行函证服务平台 差错处理》。

本文件由中国银行业协会银行函证平台服务中心提出。

本文件由中国银行业协会银行业产品和服务标准化专业委员会归口。

本文件起草单位：中国银行业协会、工银科技股份有限公司、中国工商银行股份有限公司、中国农业银行股份有限公司、兴业银行股份有限公司、湖南三湘银行股份有限公司、沧州银行股份有限公司、河南省农村信用社联合社。

本文件主要起草人：潘光伟、刘峰、张亮、艾亚萍、高峰、李宽、李朋乐、仲峻锋、张贺、王恩雷、张俊凯、赵成刚、林松、唐新、阮仪容、吴春晖、徐金玉、严彪、谢经纬、张福胜、丁明皓、胡文华。

地 址：北京市西城区金融街 20 号交通银行大厦 B 座
电 话：010-66553368 010-66291132
邮 编：100033
邮 箱：cba.china@china-cba.net
传 真：010-66553356

引　言

银行函证系统是实现银行函证业务数字化转型的重要技术支撑，其中，加密体系则是提供安全可控服务的底层技术保障，设计良好的加密体系，可以确保在函证业务中，不会出现未经授权的变更，也不会出现未经授权的查看，且具有良好的抗抵赖和核查能力。

本文件描述了为了实现函证业务端到端安全传输，且在传输过程中确保不会出现未经授权的变更和未经授权的查看所须安全机制中的加密体系。

通过实施本文件，配套以相关的安全管理和技术措施，能达到确保银行函证仅有发起方和接收方可见的业务目的。

银行函证服务平台 加密体系

1 范围

本文件给出了银行函证系统的加密体系。

本文件适用于构成银行函证系统的银行函证服务平台、银行业金融机构、会计师事务所和相关机构。

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 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—2017 信息安全技术 SM2密码算法使用规范

GB/T 32907—2016 信息安全技术 SM4分组密码算法

T/CBA 210—2021 银行函证服务平台 接入要求

3 术语、定义和缩略语

下列术语和定义适用于本文件。

3.1

银行函证业务 banking confirmation business

会计师事务所等在获取被审计单位授权后，直接向银行业金融机构发出询证函，银行业金融机构针对所收到的询证函，查询、核对相关信息并直接提供回函的过程。

术语条目注 1：询证函可能是能够进行数据元解析的，也可能仅是一个图像或不可更改格式的文件。

术语条目注 2：《关于进一步规范银行函证及回函工作的通知》（财会〔2020〕12 号）中，界定的相关概念为“银行函证及回函，是注册会计师在获取被审计单位授权后，直接向银行业金融机构发出询证函，银行业金融机构针对所收到的询证函，查询、核对相关信息并直接提供书面回函的过程”。因本文件面向的实施对象不是注册会计师个人，而是会计师事务所，故对定义进行了调整。

[来源：T/CBA 210—2021，3.1，有修改——增加了术语条目注2]

3.2

银行函证系统 banking confirmation business system

处理银行函证业务的应用系统。

术语条目注 1：银行函证系统由银行函证服务平台、银行业金融机构、会计师事务所和相关机构构成，其框架和基本工作过程见 T/CBA 210—2021。

3.3

密钥 key

一种用户控制密码变换操作（例如加密、解密、密码校验函数计算、签名生成或签名验证）的符号序列。

[来源：GB/T 17901.1—2020，3.8]

3.4

非对称密钥对 asymmetric key pair

一对相关的密钥（3.3），其中私钥（3.5）规定私有变换，公钥（3.6）规定公开变换。

术语条目注 1：GB/T 17901.1—2020 中 3.2 的原文为“一对相关的密钥，其中私有密钥规定私有变换，公开密钥规定公开变换”，鉴于本文件后继定义了私钥和公钥的概念，为了使得术语引用合理，故做了上述改动。

术语条目注 2：GB/T 17901.1—2020 中 3.2 的来源标注为[ISO/IEC 11770-3：2008，定义 3.3]。

[来源：GB/T 17901.1—2020，3.2，有修改——增加了术语条目注1和术语条目注2]

3.5

私钥 private key

在某一实体的非对称密钥对（3.4）中，只由该实体使用的密钥（3.3）。

术语条目注 1：在银行函证系统（3.2）中，实体可能是银行函证服务平台、银行业金融机构、会计师事务所和相关机构。

[来源：GB/T 17901.1—2020，3.3，有修改——增加了术语条目注1]

3.6

公钥 public key

在某一实体的非对称密钥对（3.4）中，能够公开的密钥（3.3）。

术语条目注 1：在银行函证系统（3.2）中，实体可能是银行函证服务平台、银行业金融机构、会计师事务所和相关机构。

[来源：GB/T 17901.1—2020，3.4，有修改——增加了术语条目注1]

3.7

密钥协商 key agreement

在实体之间建立一个共享的秘密密钥的过程，其中任何实体都不能预先确定该密钥的值。

术语条目注 1：在银行函证系统（3.2）中，实体可能是银行函证服务平台、银行业金融机构、会计师事务所和相关机构。

[来源：GB/T 17901.1—2020，3.9，有修改——增加了术语条目注1]

3.8

密钥建立 key establishment

为一个或多个实体生成一个可用的、共享的秘密密钥的过程，包括密钥协商（3.7）、密钥传送等。

术语条目注 1：GB/T 17901.1—2020 中 3.11 的来源标注为[ISO/IEC 11770-3：2008，定义 3.22]。

术语条目注 2：在银行函证系统（3.2）中，实体可能是银行函证服务平台、银行业金融机构、会计师事务所和相关机构。

[来源：GB/T 17901.1—2020，3.11，有修改——增加了术语条目注1和术语条目注2]

3.9

秘密密钥 secret key

用于对称密码技术中的一种密钥（3.3），并仅由一组规定实体所使用。

[来源：GB/T 17901.1—2020，3.16]

3.10

数字签名 digital signature

附加在数据单元上的数据，或是对数据单元所做的密码变换。

术语条目注 1：这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人（例如接收者）伪造或抵赖。

[来源：GB/T 17901.1—2020，3.6]

3.11

平台密钥对 key pair owned by the platform

银行函证系统（3.2）中的银行函证服务平台所拥有的非对称密钥对（3.4）。

3.12

接入方密钥对 key pair owned by a participant

银行函证系统（3.2）中的银行业金融机构、会计师事务所和相关机构各自所拥有的非对称密钥对（3.4）。

术语条目注 1：从银行函证系统的视角看，各银行业金融机构、会计师事务所和相关机构均为银行函证服务平台的接入方。

3.13

文件密钥 secret key of processing document

在银行函证业务（3.1）中，加密所传送的业务文件的秘密密钥（3.9）。

4 加密体系构成原则

银行函证系统的加密体系按照如下原则构建。

a) 通过浏览器方式接入的用户应通过用户名、静态密码、图形验证码及短信验证码进行身份认证，保证数据安全。

b) 通过应用系统接入的用户应通过非对称密钥对的方式进行双向身份认证。

c) 平台密钥对和所有接入方密钥对均采用 GB/T 32918 中规定的 SM2 算法，并按照 GB/T 35276—2017 的规定使用。

注 1：按照 GB/T 35276—2017 中 5.1 的规定，SM2 的私钥长度为 256 位；公钥每个分量的长度均为 256 位。

d) 所有文件密钥均采用 GB/T 32907—2016 中规定的 SM4 算法。

注 2：按照 GB/T 32907—2016 中第 4 章的规定，密钥长度为 128 比特。

e) 所有涉及到的非对称密钥对均由银行函证服务平台和各银行函证系统接入方在本地生成，且私钥仅存储在本地。

f) 密钥建立应遵循随机或伪随机生成的原则。密钥生成工具中随机数的产生应遵循国家或国际标准中规定使用的算法，确保随机数的生成规律不能为其他方所获知。

g) 银行函证服务平台提供所需非对称密钥对和文件密钥的产生和核验的软件代码，但仅作为推荐使用；T/CBA 210—2021 的图 1 所描述的银行函证系统的各参与方，均可自行编制符合相关国家标准要求的软件代码。

h) 银行函证平台与各银行业金融机构、会计师事务所和相关机构之间的通信过程，均采用接收方密钥对加密和解密。

i) 各银行业金融机构与会计师事务所之间文件密钥的交换过程，均采用接收方密钥对加密和解密。

j) 传输的文件，均采用文件密钥加密。

k) 在函证传输的加解密过程中，发送方既可以是浏览器接入的，也可以是应用系统接入的；反之亦然。

l) 各银行业金融机构与会计师事务所必须按照《财政部 中国银保监会关于进一步规范银行函证及回函工作的通知》（财会〔2020〕12 号）的要求，使用本机构数字签名等技术对待传输文件实施有效内部控制。

5 密钥建立

5.1 平台密钥对

平台密钥对由银行函证服务平台建立，仅应用于应用系统接入方式，其建立过程如下。

a) 采用可靠方式产生随机数，确保随机数的生成规律不能为其他方所获知。
b) 按 GB/T 35276—2017 中 9.1 的要求生成平台密钥对。
c) 平台密钥对中的私钥，存储于采取了安全措施的独立介质中。
d) 平台密钥对中的公钥，通过电子邮件或其他可达方式发送给到银行函证服务平台的接入方。

5.2 接入方密钥对

所有接入银行函证服务平台的接入方密钥对均按如下要求建立。

a) 根据实际业务场景，接入方可分为发送方或接收方。
b) 可使用函证服务平台提供的 SDK 开发工具包建立密钥对，或自行研发符合 GB/T 32918 要求的算法。采用自行研发符合 GB/T 32918 要求算法应用程序的，应确保随机数的生成规律不能为其他方所获知。
c) 按 GB/T 35276—2017 中 9.1 的要求生成接入方密钥对。
d) 接入方密钥对中的私钥，不准许以明文存储在计算机的硬盘上，宜存储于采取了安全措施的独立介质中。
e) 在具备条件时，接入方密钥对中的私钥宜分解为两个或更多分离的密钥组件形式，分别存储于采取了安全措施的独立介质中，且采取分别存储和存取访问管理等控制措施。
f) 接入方密钥对中的公钥,可通过电子邮件或其他可达方式传递到银行函证服务平台及业务相关场景中的非自身接入方。
g) 接入方可根据自身需求，定期更新接入方密钥对。

5.3 文件密钥

银行函证服务平台中，文件密钥仅由产生或接收文件的接入方生成或使用，不产生文件且不需阅读所传输文件明文的银行函证服务平台本身和其他参与方不需要生成和使用文件密钥。文件密钥建立过程如下。

a) 可使用函证服务平台提供的 SDK 开发工具包或加解密工具包建立文件密钥，或自行研发符合 GB/T 32907—2016 要求的算法。采用自行研发符合 GB/T 32907—2016 要求算法应用程序的，应确保产生文件密钥的生成规律不能为其他方所获知。
b) 文件密钥仅在使用时生成，且每个密钥仅使用一次。
c) 文件密钥在传输时，采用文件接收方密钥公钥加密保护。

6 函证传输加密与解密

6.1 标识约定

密钥采用 6 位英文字母与数字标识，规则为：

a) 第 1 位以英文字母标识密钥的生成方；
b) 第 2～5 位以英文字母标识密钥的种类，其中不同种类密钥英文缩写首字母相同的，引入后继的小写字母区分；
c) 第 6 位以数字标识密钥的使用场景。

6.1.1 密钥生成方标识

密钥生成方标识如下：

a) 由发送方生成的密钥，用“A”表示；
b) 由平台生成的密钥，用“B”表示；
c) 由接收方生成的密钥，用“C”表示。

6.1.2 密钥种类标识

密钥种类标识如下：

a) 非对称密钥对中的公钥，用“PubK”表示；
b) 非对称密钥对中的私钥，用“PriK”表示；
c) 文件密钥，用“DocK”表示。

6.1.3 密钥使用场景标识

密钥使用场景标识如下：

a) 在浏览器接入模式下，发送方向平台传输文件的场景，用“1”表示；
b) 在浏览器接入模式下，接收方从平台获取文件的场景，用“2”表示；
c) 在应用系统接入模式下，发送方向平台发送业务报文的场景，用“3”表示；
d) 在应用系统接入模式下，平台向接收方发送业务报文的场景，用“4”表示；
e) 在应用系统接入模式下，发送方向平台传输文件的场景，用“5”表示；
f) 在应用系统接入模式下，接收方从平台获取文件的场景，用“6”表示。

6.2 浏览器接入

6.2.1 适用业务场景

浏览器接入方式适用如下业务场景：

a) 会计师事务所发送银行函证申请文件；
b) 银行业金融机构接收银行函证申请文件；
c) 银行业金融机构发送银行回函文件；
d) 会计师事务所接收银行回函文件。

6.2.2 机制描述

在浏览器接入模式下，加密与解密流程如图 1 所示。

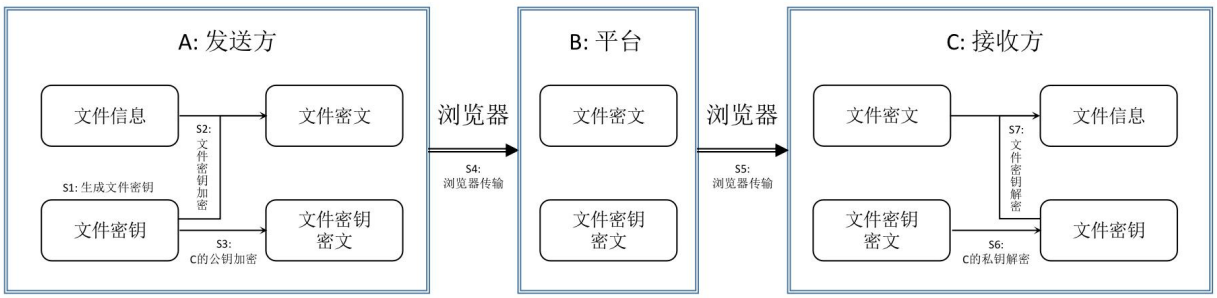

图 1 浏览器接入模式的文件传输加密解密概要流程

在浏览器接入模式下，用户通过身份认证后登陆平台，加密与解密流程概要描述如下。

a） 发送方通过浏览器方式向平台传输文件的场景：

1）步骤 S1：发送方生成文件密钥 ADocK1 明文；

2）步骤 S2：发送方使用文件密钥 ADocK1 对函证文件进行加密；

3）步骤 S3：发送方使用接收方的公钥 CPubK1，对文件密钥 ADocK1 进行加密形成 ADocK1 的密文；

4）步骤 S4：发送方通过浏览器方式，将文件密钥 ADocK1 密文和使用 ADocK1 加密后的函证文件密文发送给银行函证服务平台。

b） 接收方通过浏览器方式从平台获取文件的场景：

1）步骤 S5：银行函证服务平台通过浏览器方式，将发送方的文件密钥 ADocK2 密文（使用接收方公钥 CPubK2 加密后的文件密钥）和函证文件密文（使用 ADocK2 加密后的函证文件）发送给接收方；

2）步骤 S6：接收方使用本机构的私钥 CPriK2，对文件密钥 ADocK2 进行解密获得其明文；

3）步骤 S7：接收方使用文件密钥 ADocK2 明文，对函证文件解密，获得函证文件的明文。

6.3 应用系统接入

6.3.1 适用业务场景

应用系统接入方式适用如下业务场景：

a） 银行函证服务平台与银行或会计师事务所函证系统及其他接入方之间进行报文交互；

b） 本文件 6.2.1 描述的文件传输。

注：通过银行函证服务平台与银行或会计师事务所函证系统及其他接入方之间的报文交互，能够将银行函证业务中诸多由人工交互的信息转为应用系统的传递，提高工作的效率、安全性和便利性。

6.3.2 机制描述

6.3.2.1 业务报文传输

在应用系统接入模式下，业务报文传输时加密与解密流程如图 2 和图 3 所示。

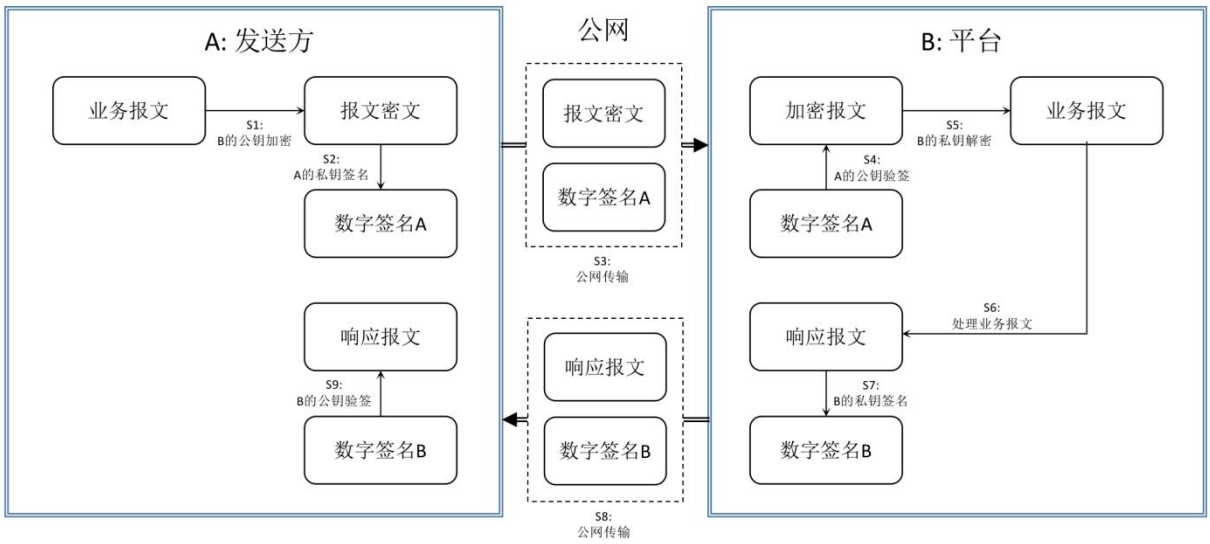

图 2 应用系统接入模式的业务报文加密解密概要流程（上行报文）

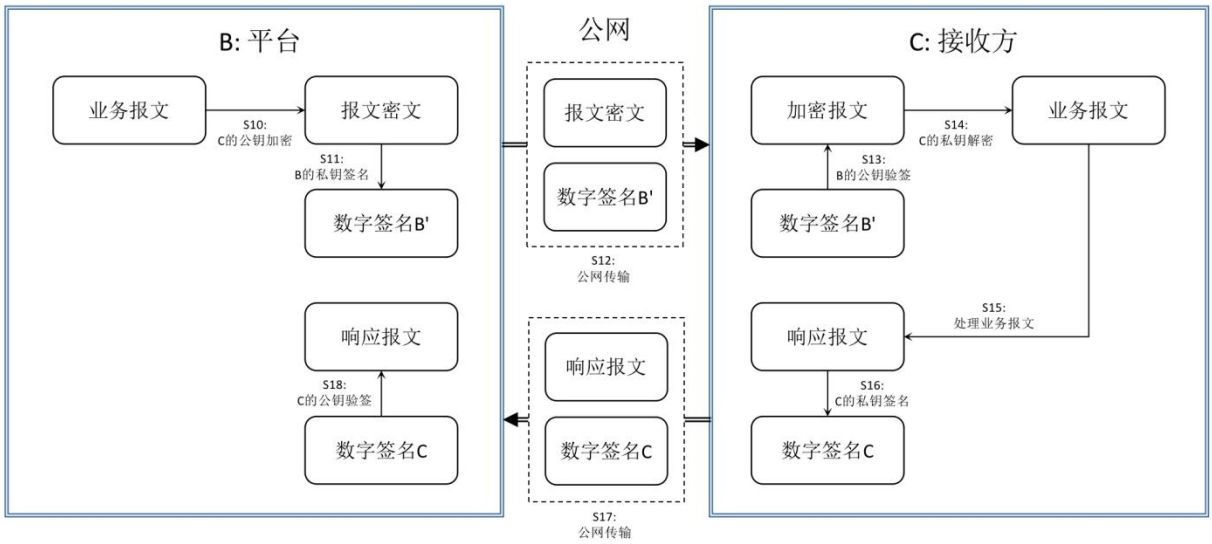

图 3　应用系统接入模式的业务报文加密解密概要流程（下行报文）

在应用系统接入模式下，业务报文传输时加密与解密流程概要描述如下。

a)　上行报文，此时接入方作为发送方，向银行函证服务平台发送业务报文：

1)　步骤 S1：发送方使用银行函证服务平台公钥 BPubK3，对业务报文进行加密；
2)　步骤 S2：发送方使用发送方私钥 APriK3，对业务报文进行数字签名；
3)　步骤 S3：发送方通过公网，向银行函证服务平台发送报文密文及发送方数字签名；
4)　步骤 S4：银行函证服务平台使用发送方公钥 APubK3，进行验签；
5)　步骤 S5：银行函证服务平台使用平台私钥 BPriK3，对业务报文解密；
6)　步骤 S6：银行函证服务平台处理该业务报文；
7)　步骤 S7：银行函证服务平台使用平台私钥 BPriK3，对响应数据进行签名；
8)　步骤 S8：银行函证服务平台通过公网，向发送方发送响应报文及平台数字签名；
9)　步骤 S9：发送方接收响应数据，使用平台公钥 BPubK3，进行验签。

b)　下行报文，此时接入方作为接收方，从银行函证服务平台接收业务报文，：

1)　步骤 S10：银行函证服务平台使用接收方公钥 CPubK4，对业务报文进行加密；
2)　步骤 S11：银行函证服务平台使用平台私钥 BPriK4，对业务报文进行数字签名；
3)　步骤 S12：银行函证服务平台通过公网，向接收方发送报文密文及平台数字签名；
4)　步骤 S13：接收方使用银行函证服务平台公钥 BPubK4，进行验签；
5)　步骤 S14：接收方使用接收方私钥 CPriK4，对报文数据解密；
6)　步骤 S15：接收方处理该业务报文；
7)　步骤 S16：接收方使用接收方私钥 CPriK4，对响应数据进行数字签名；
8)　步骤 S17：接收方通过公网，向银行函证服务平台发送响应报文及接收方数字签名；
9)　步骤 S18：银行函证服务平台接收响应数据，使用接收方公钥 CPubK4，进行验签。

6.3.2.2　文件传输

在应用系统接入模式下，文件传输时加密与解密流程如图 4 所示。

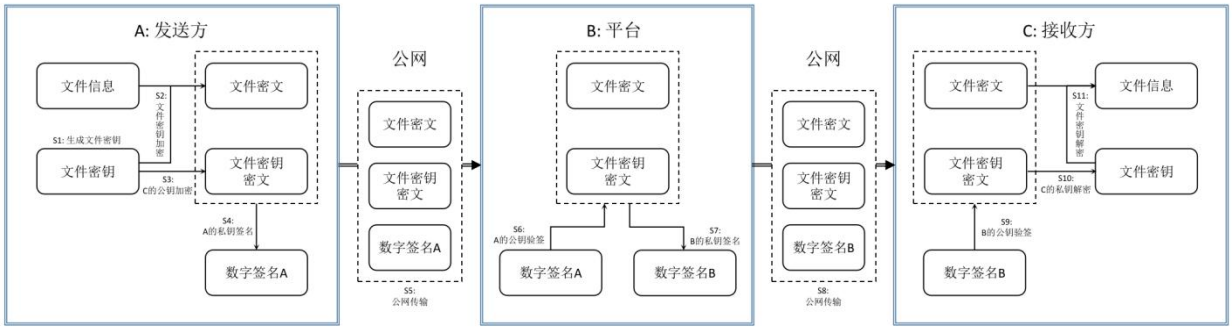

图 4　应用系统接入模式的文件传输加密解密概要流程

在应用系统接入模式下，文件传输时加密与解密流程概要描述如下。

a)　发送方通过应用系统方式向平台传输文件的场景：

1)　步骤 S1：发送方生成文件密钥 ADocK5；

2)　步骤 S2：发送方使用文件密钥 ADocK5 对函证文件进行加密；

3)　步骤 S3：发送方使用接收方的公钥 CPubK5，对文件密钥 ADocK5 进行加密；

4)　步骤 S4：发送方使用本机构的私钥 APriK5，进行数字签名；

5)　步骤 S5：发送方通过公网，将加密后的文件密钥 ADocK5 密文、使用 ADocK5 加密后的函证文件密文以及发送方数字签名发送给银行函证服务平台；

6)　步骤 S6：银行函证服务平台使用发送方的公钥 APubK5，进行验签；

7)　步骤 S7：银行函证服务平台使用平台私钥 BPriK5 进行数字签名。

b)　接收方通过应用系统方式从平台获取文件的场景：

1)　步骤 S8：银行函证服务平台通过公网，将发送方的文件密钥 ADocK6 密文（使用接收方公钥 CPubK6 加密后的文件密钥）、函证文件密文（使用 ADocK6 加密后的函证文件）以及平台数字签名（使用平台私钥 BPriK6 进行的数字签名）发送给接收方；

2)　步骤 S9：接收方使用银行函证服务平台公钥 BPubK6，进行验签；

3)　步骤 S10：接收方使用本机构的私钥 CPriK6，对加密后的文件密钥 ADocK6 进行解密；

4)　步骤 S11：接收方使用文件密钥 ADocK6 明文，对函证文件解密得到明文。

参 考 文 献

[1] GB/T 17901.1—2020 信息技术 安全技术 密钥管理 第1部分：框架
[2] GB/T 25068.1—2020 信息技术 安全技术 网络安全 第1部分：综述和概念
[3] GB/T 36624—2018 信息技术 安全技术 可鉴别的加密机制