

《银行函证服务平台 加密体系》宣贯指南 V01

1 宣传范围

本标准将对外宣传。宣传对象包括：

- a) 全体银行业协会会员单位；
- b) 各相关会计师事务所；
- c) 各地方银行业协会。

2 宣传方法

本标准采用如下方式进行宣传。

- a) 在标准发布时发送中国银行业协会全体会员单位，并由地方银行业协会转发所属会员单位。
- b) 在中国银行业协会官网、“中国银协”公众号等网络途径进行宣传。
- c) 组织专门的培训班进行讲解。
- d) 向会计师事务所报送简报。

3 贯彻方法

所有应用银行函证系统处理银行函证业务的各方，包括银行函证服务平台、商业银行、会计师事务所和相关机构，均按照本文件的要求处理银行函证业务中的加密和解密。

4 检验方法

本标准采用如下方式进行检验。

- a) 银行函证业务报文及业务文件加密与解密流程是否满足本文要求。
- b) 银行函证业务文件是否仅在文件的发出方和接收方之间可见明文。
- c) 业务文件加密过程中使用的文件密钥，是否确保其他方无法获知其生成规律且每个文件密钥仅使用一次。
- d) 银行函证业务的文件密钥是否采用加密的方式传输。
- e) 文件密钥加密过程中使用的公钥，是否是接收方的公钥。
- g) 所有的加密过程是否采用了国密算法。
- f) 银行函证业务中涉及到的私钥，是否仅保存在非对称密钥对的生成方。
- h) 接入方密钥对中私钥在存储过程中，是否采取必要的安全管理措施。