ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0118—2015

金融电子认证规范

specification for financial electronic authentication

2015－10－27 发布　　2015－10－27 实施

中国人民银行　　发布

目　　次

前　言

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准由全国金融标准化技术委员会（SAC/TC 180）提出并归口。

本标准牵头起草单位：中国人民银行科技司、中国金融认证中心。

本标准参与起草单位：中国工商银行、中国农业银行、中国建设银行、招商银行、平安银行、农信银资金清算中心、北京数字认证股份有限公司、上海市数字证书认证中心有限公司、中国电子信息产业发展研究院。

本标准主要起草人：王永红、李晓枫、杨竑、陆书春、陈立吾、郭全明、王小青、王梅、吴金海、车珍、李阳、董贞良、张行、赵宇、龚喜杰、赵义斌、魏志杰、廖泉、赵乔伟、肖晗、闫晋国、黄薇、刘华军、仲海港、陈梦霄、李强、国枫、李珂、张晓东、吴玉洁、熊少军、陈曦、钟震江、时建军、林雪焰、李向锋、孙菲、刘权。

引　言

为保障金融交易安全和客户资金安全，电子认证服务在金融领域获得广泛应用，既有金融机构自建的电子认证系统的情况，也有由第三方电子认证服务机构（以下简称第三方CA）提供的电子认证服务。为了对在金融领域提供电子认证服务进行规范，提高行业应用水平，特制定本标准。

本标准严格遵循《电子签名法》、《电子认证服务管理办法》和《电子认证服务密码管理办法》的相关规定，同时根据金融行业的特点参考金融行业相关标准规范而制定。

行业主管部门另有规定的，遵循主管部门的相关规定。

金融电子认证规范

1 范围

本标准规定了金融电子认证机构及自建电子认证系统的机构所应遵循的要求，本标准第 5 章“金融电子认证管理”适用于在金融领域提供电子认证服务的机构，包含为金融机构提供电子认证服务的第三方电子认证机构、自建电子认证系统并为自身客户提供服务的金融机构和非银行支付机构。上述机构为内部员工提供电子认证服务的可参考本标准。

本标准第 6 章“金融电子认证应用”适用于应用电子认证服务的金融机构和非银行支付机构。

外资金融机构应用金融电子认证服务时可参考本标准。

行业主管部门另有规定的，遵循主管部门的相关规定。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 19713-2005 信息技术 安全技术 公钥基础设施 在线证书状态协议

GB/T 20520-2006 信息安全技术 公钥基础设施 时间戳规范

GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范

GB/T 25061-2010 信息安全技术 公钥基础设施 XML 数字签名语法与处理规范

GB/T 25064-2010 信息安全技术 公钥基础设施 数字签名格式规范

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GM/T 0009-2012 SM2 密码算法使用规范

GM/T 0005-2012 随机性检测规范

GM/T 0015-2012 基于 SM2 密码算法的数字证书格式规范

GM/T 0034-2014 基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范

3 术语与定义

下列术语和定义适用于本文件。

3.1

电子认证 electronic authentication

基于 PKI 的数字签名认证技术。

3.2

电子认证机构 certification authority

电子认证服务机构 certification authority

对数字证书进行全生命周期管理的实体。

3.3

注册机构　registration authority

受理数字证书的申请、更新、恢复和注销等业务的实体。

3.4

电子认证系统　certificate authentication system

对数字证书的签发、发布、更新、撤销等数字证书全生命周期进行管理的系统。

3.5

电子认证业务规则　certification practice statement

关于 CA 在整个数字证书服务生命周期中的业务实践（如签发、注销、更新）所遵循规范的详细描述和声明，并提供相关业务、法律和技术方面的细节。

3.6

电子认证服务　electronic certification service

为数字签名相关各方提供真实性、可靠性验证的活动。

3.7

私钥　private key

非对称密码算法中只能由拥有者使用的不公开密钥。

3.8

公钥　public key

非对称密码算法中可以公开的密钥。

3.9

证书策略　certificate policy

一套指定的规则集，用以指明证书对一个特定团体和(或)具有相同安全需求的应用类型的适用性；或用以指明证书对于具有相同安全需求的某类应用的适用性。

3.10

数字证书　digital certificate

公钥证书　digital certificate

由证书认证机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

3.11

数字签名　digital signature

数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

3.12

证书注销列表　certificate revocation list

由证书认证机构签发并发布的被撤销证书的列表。

3.13

依赖方　relying party

使用证书中的数据进行决策的用户或代理。

3.14

证书更新　certificate renewal

在证书所载信息不变的情况下，延长证书的有效期。

3.15

证书注销　certificate revocation

将用户的证书标记为CA永远不再信任的状态，并放置于证书注销列表中供依赖方查询。

3.16

证书挂起　certificate suspension

将用户的证书标记为CA暂时不信任的状态，并放置于证书注销列表中供依赖方查询。

3.17

证书解挂　certificate unsuspension

将已经挂起的证书标记为CA重新信任的状态，并从证书注销列表中删除其挂起信息供依赖方查询。

4　缩略语

下列缩略语适用于本文件。

CA　电子认证机构（certification authority）

COS　片内操作系统（chip operating system）

CPS　电子认证业务规则（certification practice statement）

CRL　证书注销列表（certificate revocation list）

KMC　密钥管理中心(key manage center)

PKI　公钥基础设施（public key infrastructure）

RA　注册机构　registration authority

SSL　安全套接层协议（secure sockets layer）

5 金融电子认证管理

5.1 基本要求

5.1.1 对第三方 CA 的基本要求

第三方CA应符合以下基本要求：

a) 应取得工业和信息化部颁发的《电子认证服务许可证》，并符合工业和信息化部的各项管理要求；
b) 信息系统安全保护等级原则上应为三级或更高级别；
c) 应制定针对金融领域的 CPS 和证书策略，并在网站上公开发布；
d) 应采用国家密码管理部门批准使用的算法，符合国家密码相关行业标准的要求，取得国家密码管理部门颁发的《电子认证服务密码使用许可证》，接入国家电子认证根 CA；
e) 符合国家其它相关法律法规及主管部门有关管理要求。

5.1.2 对金融机构自建 CA 的基本要求

金融机构自建CA的，应符合以下基本要求：

a) 信息系统安全保护等级原则上应为三级或更高级别，行业主管部门另有规定的，可遵循主管部门的相关规定；
b) 应制定相应的 CPS 和证书策略，并向用户公开发布；
c) 应采用国家密码管理部门批准使用的算法，符合国家密码相关行业标准的要求，并适时接入国家电子认证根 CA；
d) 符合国家其它相关法律法规及主管部门有关管理要求。

5.2 技术要求

5.2.1 格式及名称

5.2.1.1 证书格式要求

对于采用 SM 系列算法的证书应符合 GM/T 0015-2012 相关要求。

5.2.1.2 名称的含义要求

一般情况下，证书中载明的证书所有者名称要有实际意义。标识个人身份的证书（简称个人证书）命名至少应包括或对应自然人名称信息；标识机构身份的证书（简称机构证书）命名至少应包括或对应机构主体名称信息。

5.2.1.3 名称唯一性要求

CA 不能将同一证书主体名称的证书签发给不同的用户。

5.2.2 身份鉴别

5.2.2.1 证书申请个人身份鉴别

RA 在对个人用户进行身份鉴别时应检查并通过必要手段验证能够表明其真实身份的有效身份证件。有效身份证件应符合以下要求：

a) 中国居民，应出具居民身份证或临时身份证。
b) 对于 16 岁以下的中国公民，应由监护人代理进行证书申请，应出具监护人的有效身份证件以及账户使用人的居民身份证或户口簿。
c) 中国人民解放军军人，应出具军人身份证件。
d) 中国人民武装警察，应出具武警身份证件。
e) 香港、澳门居民，应出具港澳居民往来内地通行证；台湾居民，应出具台湾居民来往大陆通行证或者其他有效旅行证件。
f) 外国公民，应出具护照。
g) 法律、法规和国家有关文件规定的其他有效证件。

在身份鉴别过程中需要个人用户申请人到达证书申请现场时，RA 应要求个人用户出示以上所列示的至少一种个人实名身份证件原件；当个人用户授权他人代为办理时，RA 应要求代理人同时出示代理人与被代理人的身份证件，以及被代理人亲自签署的书面授权证明；RA 应仔细查验实名身份证件及授权证明。

5.2.2.2 证书申请机构身份鉴别

RA 在对机构申请者进行身份鉴别时应查验其有效证件，有效证件应符合以下要求：

a) 企业法人，应出具企业法人营业执照正本。
b) 非法人企业，应出具企业营业执照正本。
c) 机关和实行预算管理的事业单位，应出具政府人事部门或编制委员会的批文或登记证书和财政部门同意其开户的证明；非预算管理的事业单位，应出具政府人事部门或编制委员会的批文或登记证书。
d) 军队、武警团级(含)以上单位以及分散执勤的支(分)队，应出具军队军级以上单位财务部门、武警总队财务部门的开户证明。
e) 社会团体，应出具社会团体登记证书，宗教组织还应出具宗教事务管理部门的批文或证明。
f) 民办非企业组织，应出具民办非企业登记证书。
g) 外地常设机构，应出具其驻在地政府主管部门的批文。
h) 外国驻华机构，应出具国家有关主管部门的批文或证明；外资企业驻华代表处、办事处应出具国家登记机关颁发的登记证。
i) 个体工商户，应出具个体工商户营业执照正本。
j) 居民委员会、村民委员会、社区委员会，应出具其主管部门的批文或证明。
k) 独立核算的附属机构，应出具其主管部门的基本存款账户开户登记证和批文。
l) 其他组织，应出具政府主管部门的批文或证明。

金融机构已查验过有效证件的机构客户，通过该金融机构 RA 申请证书的，可以不再提供相关证件。

机构申请者应委派授权申请人办理证书申请。

需要机构证书的授权申请人到达证书申请现场时，RA 应要求授权申请人出示以上所列示的至少一种机构证件原件或加盖公章的影印件、授权申请人的个人实名身份证件、机构授予申请人的书面授权证明（应加盖公章）；RA 应仔细查验授权申请人出示的身份证件及授权证明，验证其真实性及有效性。

5.2.2.3 证书更新身份鉴别

RA 受理用户的证书更新请求时应采取与证书生命周期管理中证书申请相同的身份鉴别过程。

5.2.2.4 证书挂起身份鉴别

RA 受理用户的证书挂起请求时，应验证用户申请证书时预留的身份信息。

CA 也可通过电话呼叫中心受理用户提出的证书挂起请求，应验证用户在申请证书时预留的身份信息。

5.2.2.5 证书解挂身份鉴别

RA 在受理证书解挂请求时应至少采取与证书挂起相同的身份鉴别过程。

5.2.2.6 证书注销身份鉴别

RA 在受理证书注销请求时应验证用户在该机构预留的身份信息。

5.2.3 证书生命周期操作

5.2.3.1 证书申请处理

RA 应书面告知用户使用证书服务的权利和义务以及 CA 应承担的责任。

用户应按照 CPS 规定的要求填写证书申请相关信息，并准备相关的身份证明材料。由 CA 或 RA 依据本标准 5.2.2 条对证书申请人的身份进行鉴别，并决定是否受理申请。

5.2.3.2 证书签发及交付

5.2.3.2.1 证书的签发

CA 应基于审核通过的用户实名信息签发数字证书，同时需从技术和制度上保证在证书生成时，用于签名的证书相对应的私钥只留存在安全的硬件介质中(用户有特殊要求并自行采取其它措施保护私钥安全的除外)，CA 不应留存任何私钥备份。用于加密的证书，应在电子认证系统中归档保留加密证书的私钥。

5.2.3.2.2 证书的交付

CA 应在 CPS 中明确证书交付的方式、证书下载的期限和环境安全性要求。

5.2.3.3 证书更新

用户证书在到期前 3 个月内可进行更新操作，CA 或 RA 应及时提醒用户进行证书更新。

证书更新可根据业务需要提供在线更新和离线更新两种方式,用户证书在有效期内且未被注销或挂起的情况下，用户可通过互联网在 CA 提供的在线更新服务平台上完成证书的更新。

客户端进行证书更新时，应使用私钥对证书请求进行签名，CA 在受理用户的证书更新时，应验证证书更新请求中的签名，并保存此签名信息。

CA 在受理用户的证书更新之前应验证证书的有效性，对于未记载证书持有者实名信息的证书还应验证证书信息与证书所有者真实身份信息关联关系的有效性。

CA 应在收到证书更新申请后的 5 个工作日内处理完成。通过证书更新申请的予以更新证书，拒绝用户的证书更新申请的，应在 5 个工作日内通知用户并告知其原因。

CA 应知会用户使用证书服务的权利和义务以及 CA 应承担的责任。

CA 应制定在线证书更新的业务规则。当 CA 认为用户密钥存在安全隐患时，应主动提醒用户进行更新。

对于个人用户数字证书的更新，应立即撤销旧证书。对于机构客户的数字证书更新，CA 应根据客户需要提供特殊服务，不立即注销旧证书，使得新、旧证书并行一段时间，以保证某些系统的业务连续性要求。

5.2.3.4 证书挂起

CA 应根据业务安全需求在其 CPS 中规定挂起请求生效的最大时限。

CA 应明确证书挂起的审核过程、权利与义务。

CA 对于验证通过的挂起请求，应立即处理完成，并有义务将证书挂起情况及时通知用户。

5.2.3.5 证书解挂

对于验证通过的解挂请求，应立即处理完成，并有义务将证书解挂情况及时通知用户。

5.2.3.6 证书注销

CA 应根据业务安全需求在其 CPS 中规定证书注销生效的最大时限，超过时限的责任由 CA 承担。CPS 应规定用户申请证书注销的条件和 CA 注销用户证书的条件。

对于验证通过的注销请求，应立即处理，并有义务将证书注销情况通知用户。RA 应提醒用户在发生下列情形之一时，用户应申请注销证书：

a) 数字证书私钥泄露；
b) 数字证书中的信息发生重大变更；
c) 认为本人不能履行CPS。

发生下列情形之一的，CA 应注销其签发的数字证书：

a) 用户申请注销数字证书；
b) 用户提供的信息不真实；
c) 用户没有履行双方合同规定的义务；
d) 数字证书的安全性得不到保证；
e) 法律、行政法规规定的其它情形。

5.2.3.7 证书注销列表服务

CA 应在满足机构的业务安全需求的前提下在其 CPS 中规定 CRL 生成与发布的频率和有效时限，并及时发布。CPS 应规定因 CA 原因导致 CRL 更新不及时或 CRL 不可用而造成用户损失的处理条款。

5.2.3.8 在线证书查询服务

CA 的在线证书查询服务应符合 GB/T 19713-2005 的要求。

5.2.3.9 时间戳服务

CA 提供时间戳服务的，时间戳服务应遵循 GB/T 20520-2006 的要求。

5.2.3.10 证书有效期规定

CA 应在满足机构的业务安全需求的前提下为不同类型的证书指定合理的有效期，并在 CPS 中提示用户根据密钥长度、使用频度和业务场景选择合适的证书有效期，但 CA 签发的个人证书、企业证书和设备证书，其有效期最长不得超过 5 年。

5.2.4 授权管理

CA 可使用自身的 RA 进行证书注册。

各机构也可接受 CA 委托，作为 RA 处理用户证书的申请、更新、挂起、解挂、注销请求。 CA 应在 CPS 中明确被委托对象与 CA 的关系，应明确 CA 与被委托对象各自的权利、责任与义务。

RA 将用户证书的申请、更新、挂起、解挂、注销请求信息发送给电子认证系统时，请求信息中应包含经 RA 签名的身份标识信息，并应采取相应的安全保密措施，确保请求在传输时不被篡改。电子认证系统获得 RA 的请求信息后，应对此信息进行鉴别与解密，仅对有效的请求信息进行处理。

CA 应在与 RA 签订的合作协议中，明确 CA 给予 RA 的授权事项、RA 在处理授权事项时应符合的相应要求以及双方的权利与义务。

CA 应定期对 RA 的职责履行情况进行检查，同时也可根据需要不定期进行检查。

5.2.5 技术安全控制

5.2.5.1 证明持有私钥的方法

CA 应使用证书请求中所包含的数字签名来证明用户持有与注册公钥对应的私钥。在 CA 证书体系中，签名私钥应在客户端生成，证书请求信息中包含用户用签名私钥进行的数字签名，CA 应验证这个签名。

5.2.5.2 密钥对的生成

CA 应要求用户的签名密钥对由用户终端密码设备生成。

CA 应提供适当技术手段，配合终端密码设备确保用户的证书申请中所使用的密钥对在用户的终端密码设备中生成。

5.2.5.3 密钥长度

CA 应在 CPS 中规定证书的密钥长度，且密钥长度应符合国家密码管理部门的要求。

5.2.5.4 私钥保护和密码模块工程控制

- 私钥的多人控制

电子认证系统私钥的生成、更新、注销、备份和恢复等操作应采用多人控制机制，用户的私钥由用户自己通过终端密码设备控制。

- 密码模块

电子认证系统的密码模块或设备应获得国家密码管理部门核准证书。

5.2.5.5 计算机安全控制

CA 应建立电子认证系统内设备的保管和维护制度。

5.2.5.6 电子认证系统密钥管理

5.2.5.6.1 密钥生命周期管理

电子认证系统密钥的生命周期管理包括根密钥的产生、恢复、更新、废除及销毁，其管理要求应符合 GM/T 0034-2014 中 8.2.4.2 与 8.2.4.3 的规定。

5.2.5.6.2 密钥泄露的应急处理

CA 应制定私钥泄露应急预案，明确私钥泄露的内部处理流程、人员分工及对外通知处理流程。

当电子认证系统的私钥信息被窃取或被未授权使用时，则其私钥信息被泄露。电子认证系统发生私钥泄露，或者怀疑发生私钥泄露的情况，应立即注销此电子认证系统证书、由此私钥签发的公钥证书，停止签发新的用户证书，并立即通报运营监管机构和使用本电子认证系统服务的相关机构，要求相关机构通知证书用户及依赖方不得再使用原有证书。

5.2.5.7 KMC 密钥管理

5.2.5.7.1 密钥分管

应符合 GM/T 0034-2014 中 10.3 的相关规定。

5.2.5.7.2 数据备份

应符合 GM/T 0034-2014 中 8.3 的相关规定。

5.2.6 数字签名验证服务

5.2.6.1 提供验证服务的情形

当用户或者数字签名依赖方对数字签名信息产生质疑时，CA 应为证书用户和依赖方提供数字签名数据的验证服务，即对数字证书对应私钥所做的数字签名文件进行验证。

必要时，可由司法鉴定机构给出验证结论。

5.2.6.2 验证申请材料

CA 提供签名验证服务时，应向用户或依赖方告知需要提交的相关材料，包括但不限于：

a) 已签字或盖章的书面申请；
b) 签名证书；
c) 签名原文；
d) 签名结果。

5.2.6.3 验证内容

CA 应验证如下内容：

a) 验证该张数字证书是否为电子认证系统签发的有效数字证书；
b) 验证该张数字证书在签名时，是否在电子认证系统发布的CRL内；
c) 对数字证书、数字签名、时间戳（若存在）的真实性、有效性进行技术确认。

5.2.6.4 验证结果交付

CA 应在用户或依赖方提交验证申请后的 1 个工作日内完成签名有效性验证，并将验证结果返回给验证申请者。

5.3 管理要求

5.3.1 人员管理

5.3.1.1 人员数量要求

CA 应配备 3 个或 5 个密钥管理人员，应至少有 3 名安全管理人员，3 名证书业务办理人员，以满足本标准规定的业务持续服务承诺。行业主管部门另有规定的，可遵循主管部门的相关规定。

5.3.1.2 关键岗位要求

a) 密钥管理人员

CA 应设置密钥管理人员，负责按照 CA 密钥管理策略，对 CA 的密钥进行统一管理。

b) 安全管理人员

CA 应设置专职安全管理人员，负责物理环境安全、人员安全、信息系统安全、通信系统安全及重要 IT 资产安全，进行日常管理和监控。

c) 业务办理人员

RA 应设置证书办理人员岗位。

证书办理人员包括：证书申请材料接收人员、证书申请材料鉴证人员、证书申请信息录入人员、证书申请信息审核人员，其中证书申请材料鉴证人员、证书申请信息审核人员不能由客户服务人员兼任，证书申请信息录入人员与证书申请信息审核人员不能由同一人兼任。

5.3.1.3 人员任职资格要求

CA 应制定人员录用的相关制度，对人员录用进行严格管理，在录用人员之前应进行背景审查，不得录用有犯罪记录的人员。

CA 应与所有录用人员签订录用协议及保密协议。

5.3.1.4 人员培训

CA 应建立人员培训制度。

员工正式上岗之前，应进行入职培训，培训内容包括本岗位职责、公司制度、必要的业务信息、保密制度、安全意识等。

CA 应不定期地对员工进行内部培训，并应根据岗位职责要求对员工进行相应的外部专业培训，确保其知识水平和业务技能不断提升。

5.3.1.5 关键岗位人员离职管理

CA 应制定人员离职的相关制度，对关键岗位人员的离职进行严格管理。关键岗位人员离职时，CA 应立即取消该人员的内部访问权限。CA 应安排专人监督关键岗位离职人员的工作移交过程。移交介质、密钥、文档等内容应进行书面记录，交接双方签字确认。

5.3.2 归档管理

5.3.2.1 归档资料

CA 应对关键资料进行归档保存，包括但不限于：

a) 办理证书申请、证书更新、证书挂起、证书解挂、证书注销等业务时的用户申请材料；

b) 内、外部审计记录和报告；

c) 事件处理报告；

d) 数字签名验证报告。

5.3.2.2 归档资料保存期

CA 对于归档资料的保存期限应符合如下要求：

a) 证书办理的相关材料应至少保存至证书失效后五年；

b) 内、外部审计的记录和报告、事件处理报告、数字签名验证报告应至少保存十年。

5.3.2.3 归档资料保护

CA 应设置专门的档案管理人员对归档资料进行管理，并应制定防火、防盗、防潮、防光、防鼠、防虫、防尘等措施对归档资料进行保护。

CA 的重要电子资料应进行异地备份，如电子认证系统配置信息、系统数据等。

5.3.3 业务持续性保障

5.3.3.1 组织结构设置

CA 应设置安全策略委员会，其成员应包括管理人员及核心人员。委员会负责制定安全策略、规范和决策，其职责包括但不限于：

a) 主导制定安全策略，召开安全工作会议；
b) 制定并修订证书策略、CPS；
c) 批准、发布业务持续计划，根据实际情况决定启动灾难恢复等。

5.3.3.2 业务持续性服务承诺

CA 应提供 7*24 小时不间断服务，并提供 7*24 小时服务热线（对于业务系统不需要 7*24 小时不间断服务的情况，可视业务情况而定）。

对于核心服务，包括：证书签发服务、证书状态查询服务、证书注销服务等，CA 应保证在非不可抗力情况下的全年服务可用率达到 99.9%。

5.3.3.3 关键数据保护

对于关键的数据信息，例如根密钥备份信息、证书信息与证书所有者真实身份信息的关联关系信息，CRL 等应进行安全的异地备份管理。

5.3.3.4 应急预案

CA 应针对整个电子认证系统的连续性服务要求制定相应的应急预案。

CA 应定期对相关人员进行应急预案培训，培训应至少每年举办一次。

CA 应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期，应急预案的演练应至少每年举行一次；

CA 应规定应急预案需定期审查和根据实际情况更新的内容，并遵照执行。

5.3.3.5 事件处理

事件是指对认证机构安全策略、安全手段、系统、服务、制度和流程的破坏。根据事件对电子认证业务造成的影响可划分为普通信息安全事件与重大事件，如果因 CA 提供的认证服务故障导致各机构信息系统无法正常运行或数据安全受到损害，从而对国家安全、社会秩序、公众利益和金融机构造成特别严重影响的网络与信息安全事件，属于重大事件。

CA 应根据自身的情况，制定针对事件的处理方案，其中应包括：

a) 各类事件的定义；
b) 事件处理责任人；
c) 处理流程、方法与手段；
d) 对事件责任人的处理要求；
e) 事件处理记录报告要求。

CA 需开展内部整改，对重大事件进行评估和总结，并向受影响的相关机构提供整改总结报告。总结报告应包括的内容为：

a) 重大事件评估，应包括现象、影响范围、处理时间和过程以及造成的损失；
b) 处置工作总结，应评价应急预案的可用性，分析处置工作中存在的问题，总结处置工作的整体过程；
c) 症结分析和相应建议，应分析重大事件的深层次原因，反映存在的困难和问题，并提出改进措

施、计划及相关建议；

d) 对于认证机构所在行业对信息安全事件处理有另行规定的，可依照所在行业规定的要求处理。

5.3.3.6 灾难备份中心

CA 应设立灾难备份中心，重要信息系统灾难恢复能力原则上应达到 GB/T 20988-2007 中定义的灾难恢复等级第 3 级（含）以上。行业主管部门另有规定的，可遵循主管部门的相关规定。

当出现不能预见、不能避免和不能克服的客观情况导致电子认证系统中断服务时，CA 应启动相应的灾难应急预案，尽快恢复电子认证业务，保障业务系统服务连续性，对用户的影响降低到最低。

5.3.4 风险评估

CA 应定期开展风险评估，每年至少进行一次内部风险评估和外部风险评估，并将外部风险评估结果向使用其电子认证服务的各机构或个人进行公开，外部风险评估应由具有信息系统等级保护测评机构资质的机构进行。

各机构应根据本标准要求，对向其提供服务的 CA 机构定期进行评估结果检查。

5.3.5 终止业务

第三方 CA 不再从事电子认证服务或被电子认证服务主管部门吊销服务资质时应按照工业和信息化部最新发布的《电子认证服务管理办法》中的要求进行业务承接。

第三方 CA 不愿或不能为各机构继续提供电子认证服务时应履行如下义务：

a) 至少提前 90 天以书面形式告知各机构；

b) 向各机构提供电子认证业务切换方案；

c) 向电子认证业务承接方提供认证相关信息，包括但不限于：证书办理资料、证书信息库、最新的证书状态资料等。

6 金融电子认证应用

6.1 数字证书与应用的关联

用户申领数字证书后，各机构应将证书信息注册到业务应用系统中，并与业务应用中的账户信息进行关联。

应用系统中所注册的证书信息应是证书的唯一识别信息，如证书 DN、证书序列号、以及各机构认为有必要在其应用系统中记录的其他证书信息。

一张数字证书应只与一个用户关联。

6.2 数字证书及密钥安全

6.2.1 安全存储介质要求

各机构应使用硬件介质作为证书的安全存储设备，所选择的证书安全存储设备应符合以下基本要求（用户有特殊要求并自行采取其它措施保护私钥安全的除外）并在条件许可的情况下建议满足增强要求。

基本要求：

a) 应取得国家密码管理部门核准证书；

b) 金融机构应使用指定的第三方中立测试机构安全检测通过的硬件介质；

c) 应采取有效措施防范硬件介质被远程挟持，例如通过可靠的第二通信渠道要求用户确认交易信息等；

d) 应在安全环境下完成硬件介质的个人化过程；
e) 硬件介质应采用具有密钥生成和数字签名运算能力的智能卡芯片，保证敏感操作在硬件介质内进行；
f) 硬件介质的主文件应受到 COS 安全机制保护，保证用户无法对其进行删除和重建；
g) 应保证私钥在生成、存储和使用等阶段的安全：
   - 私钥应在硬件介质内部生成，不得固化密钥对和用于生成密钥对的素数。
   - 应保证私钥的唯一性。
   - 禁止以任何形式从硬件 Key 读取私钥或写入签名私钥。
   - 私钥文件应与普通文件类型不同，应与密钥文件类型相同或相似。
   - 硬件介质每次执行签名等敏感操作前均应经过用户身份鉴别。
   - 硬件介质在执行签名等敏感操作时，应具备操作提示功能，包括但不限于声音、指示灯、屏幕显示等形式。
h) 参与密钥、PIN 码运算的随机数应在硬件介质内生成，其随机性指标应符合 GM/T 0005-2012 的相关规定；
i) 密钥文件在启用期应封闭；
j) 签名交易完成后，状态机应立即复位；
k) 应保证 PIN 码和密钥的安全：
   - PIN 码应具有复杂度要求。
   - 采用安全的方式存储和访问 PIN 码、密钥等敏感信息。
   - PIN 码和密钥(除公钥外)不能以任何形式输出。
   - 经客户端输入进行验证的 PIN 码在其传输到硬件介质的过程中，应加密传输，并保证在传输过程中能够防范重放攻击。
   - PIN 码连续输错次数达到错误次数上限(不超过 10 次)，硬件介质应锁定。
l) 硬件介质使用的密码算法应经过国家密码管理部门认定；
m) 应设计安全机制保证硬件介质驱动的安全，防范被篡改或替换；
n) 对硬件介质固件进行的任何改动，都应经过归档和审计，以保证硬件介质中不含隐藏的非法功能和后门指令；
o) 硬件介质应具备抗旁路攻击的能力，包括但不限于：
   - 抗 SPA/DPA 攻击能力。
   - 抗 SEMA/DEMA 攻击能力。
p) 在外部环境发生变化时，硬件介质不应泄露敏感信息或影响安全功能，外部环境的变化包含但不限于：
   - 高低温。
   - 高低电压。
   - 强光干扰。
   - 电磁干扰。
   - 紫外线干扰。
   - 静电干扰。
   - 电压毛刺干扰。

增强要求：

a) 硬件介质应能够防远程挟持，具有屏幕显示或语音提示以及按键确认等确认功能，可对交易指令完整性进行校验、对交易指令合法性进行鉴别、对关键交易数据进行输入、确认和保护；
b) 硬件介质应能够自动识别待签名数据的格式，识别后在屏幕上显示或语音提示交易数据，保证

屏幕显示和语音提示的内容与硬件介质签名的数据一致；

c) 应采取有效措施防止签名数据在用户最终确认前被替换；

d) 未经按键确认，硬件介质不得签名和输出，在等待一段时间后，可自动清除数据，并复位状态；

e) 硬件介质应能够自动识别其是否与客户端连接，应具备在规定的时间与客户端连接而未进行任何操作时的语音提示、屏幕显示提醒等的功能；

f) 硬件介质在连接到终端设备一段时间内无任何操作，应自动关闭，宜重新连接才能继续使用，以防范远程挟持。

6.2.2 服务器证书保护

各机构在应用服务器证书时，应采取必要的安全手段保护服务器证书，满足如下要求：

a) 服务器证书密钥对应离线产生；

b) 服务器证书密钥对应由经国家密码管理部门审批的密码设备产生，私钥应不出该密码设备并设置有安全保护措施；

c) 服务器证书所有操作由专人负责及管理，对服务器证书所对应的私钥进行的任何操作应进行身份认证，防止未授权的操作。

6.3 电子认证技术实现

6.3.1 数字证书验证技术实现要求

验证证书的内容，应包括如下基本验证：

a) 证书的颁发者名称与颁发者证书的主体名称匹配；

b) 验证证书的签名，并确保签名算法是国家密码管理部门批准使用的算法；

c) 证书的有效期；

d) 证书的密钥用法与系统应用需求相符；

e) 正确构造证书链到受信任的颁发者；

f) 各机构应通过 CA 提供的 CRL、OCSP 或者其它可靠的方式查询证书或者验证证书的状态；

g) 各机构根据应用安全要求，验证证书中与应用相关的其它信息。

6.3.2 数字签名技术实现要求

使用数字签名技术产生数字签名，应满足如下要求：

a) 签名者证书的密钥用法应包含“数字签名”；

b) 验证签名者证书的有效性；

c) 在金融信息系统中应使用标准的签名结构，签名结果根据应用的不同可使用不同的格式，包括但不限于 GB/T 25064-2010 中定义的签名格式、CMS 定义的签名格式和 GB/T 25061-2010 中定义的 XML 签名格式。

6.3.3 用户身份认证技术实现要求

各机构采用数字证书验证用户的身份，应符合如下要求：

a) 用户的数字签名作为各机构鉴别用户身份的必要因素；

b) 各机构应验证用户证书有效性；

c) 各机构应验证用户签名的有效性；

d) 各机构应验证产生签名的数字证书与用户关联的关联关系。

6.3.4 系统身份认证技术实现要求

各机构应采用服务器证书标识网站的真实性。

6.3.5 代码保护技术实现要求

各机构应采用代码签名技术实现对所提供程序组件的正确性与真实性保护。

6.4 数字证书应用要求

6.4.1 数字证书要求

各机构确定在业务中使用证书的，数字证书的存储应符合 GM/T 0034-2014 7.2 的相关要求。

6.4.2 用户身份认证

各机构可在业务中采用数字证书鉴别用户身份。

6.4.3 系统身份认证

各机构应使用服务器证书标识交易网站的真实性。

6.4.4 操作完整性及抗抵赖保证

对于风险级别较高的业务操作，各机构应明确用户对业务操作进行数字签名并对用户提交的签名进行验证，以保证用户操作的完整性和抗抵赖性（交易业务在集中清算托管机构进行集中清算的可不做抗抵赖设计），该过程应满足如下要求：

- 生成数字签名要求

应对业务所涉及的关键要素进行数字签名。

- 验证数字签名要求
  1) 验证用户证书有效性；
  2) 验证数字签名的有效性；
  3) 验证签名所使用的签名算法是否符合要求；
  4) 验证签名所使用的数据摘要算法是否符合要求；
  5) 验证产生签名的数字证书与用户的关联关系。

6.4.5 机密性

各机构可根据业务需求采用基于内容的数据加密技术或基于 SSL 通道的数据加密技术实现数据的机密性保护。

6.4.6 数字签名时间戳要求

对于时间敏感且业务双方认为需要采用可信时间标识的业务：

a) 各机构应向电子认证系统申请对“交易行为”加盖时间戳；
b) 时间戳数据可嵌入到数字签名中，或单独分离出来保存。

6.4.7 数字签名保存要求

对于长时间保存的业务，除了需要满足数字签名基本要求和时间戳要求，还应满足如下要求：

a) 各机构可选择 GB/T 25064-2010 中定义的签名格式、CMS 定义的签名格式和 GB/T 25061-2010 中定义的 XML 签名格式；
b) 各机构应妥善保存业务的数字签名数据，保存期限为数字签名证书失效后至少 5 年；

c） 对于已有法律、规章规定业务凭证保存期的，数字签名保存期限应与该保存期一致。

参 考 文 献

[1] GB/T 9361-2011 计算机场地安全要求
[2] GB/T 20518-2006 信息安全技术 公钥基础设施 数字证书格式
[3] GB/T 25069-2010 信息安全技术 术语
[4] GB/T 50174 电子信息系统机房设计规范
[5] GM/T 0003.1-2012 SM2 椭圆曲线公钥密码算法 第1部分：总则
[6] GM/T 0003.2-2012 SM2 椭圆曲线公钥密码算法 第2部分：数字签名算法
[7] GM/T 0003.3-2012 SM2 椭圆曲线公钥密码算法 第3部分：密钥交换协议
[8] GM/T 0003.4-2012 SM2 椭圆曲线公钥密码算法 第4部分：公钥加密算法
[9] GM/T 0003.5-2012 SM2 椭圆曲线公钥密码算法 第5部分：参数定义
[10] GM/T 0006-2012 密码应用标识规范
[11] GM/T 0010-2012 SM2 密码算法加密签名消息语法规范
[12] RFC 3852 加密消息语法（Cryptographic Message Syntax(CMS)）
[13] RFC 5280 互联网 X.509 公钥基础设施 证书和证书注销列表（Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile）
[14] AICPA/CICA 电子认证服务机构认证服务原则与标准（Trust Service Principles and Criteria for Certification Authorities）