ICS 35.220.20
A 90

GA

中华人民共和国公共安全行业标准

GA/T 977—2012

取证与鉴定文书电子签名

Electronic signature of forensic and identification document

2012-02-01 发布　　2012-02-01 实施

中华人民共和国公安部　发布

中华人民共和国公共安全
行 业 标 准
取证与鉴定文书电子签名
GA/T 977—2012
*
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(100013)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
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 0.5 字数 9千字
2012年4月第一版 2012年4月第一次印刷
*
书号:155066·2-23319 定价 14.00元

前　言

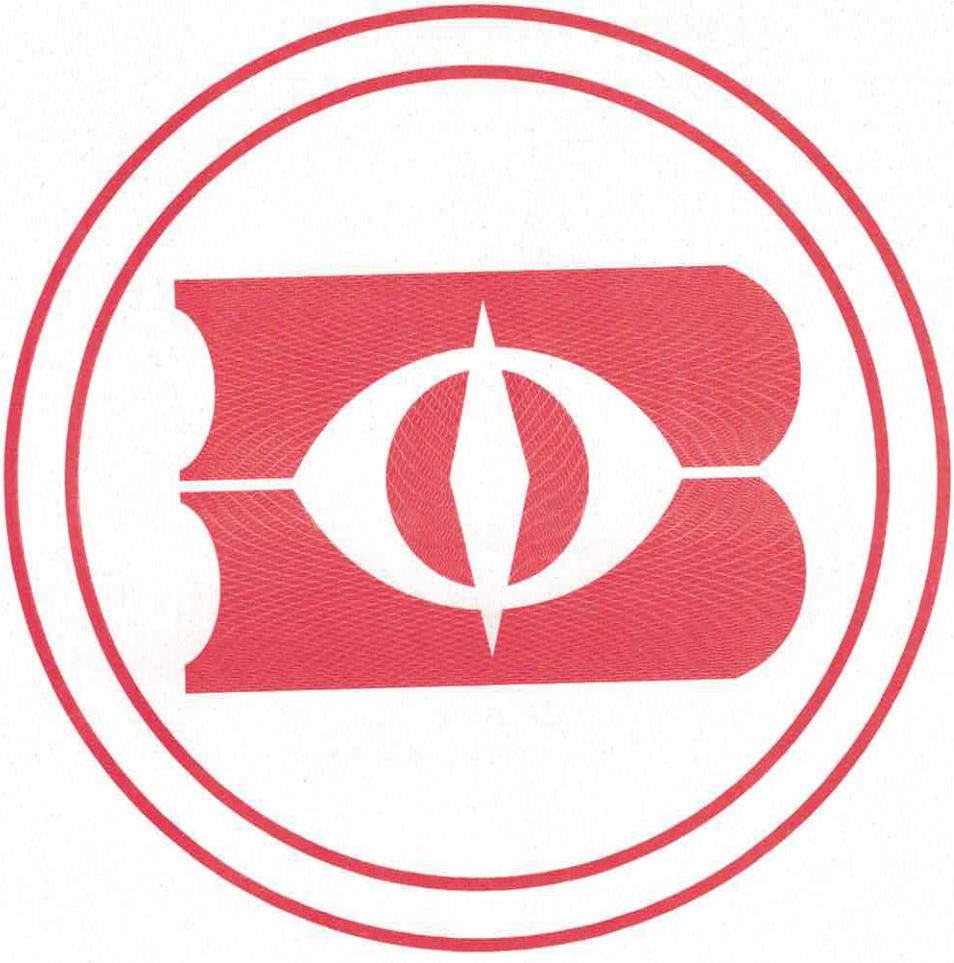
本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部网络安全保卫局，公安部第三研究所。

本标准主要起草人：许剑卓、卢涛、王婷、李勋、金波、徐隽。



取证与鉴定文书电子签名

1 范围

本标准规定了取证与鉴定文书电子文档中的电子签名。

本标准适用于基于 PKI 的取证与鉴定文书的电子文档的电子签名。

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。

ITU-T X.509 电子证书国际标准

RFC 3075 xml-signature syntax and processing

RFC 3280 因特网 X.509 公钥基础设施证书和 CRL 轮廓

3 术语和定义

ITU-T X.509、RFC 3075、RFC 3280 界定的以及下列术语和定义适用于本文件。

3.1

电子文档 electronic document

以电子形式表现的信息的混合，能被计算机识别与处理。

3.2

电子签名 electronic signature

电子文档中以电子形式所含、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。

3.3

数字证书 digital certification

经过数字证书签发机构签名的包括证书持有人信息和公钥的文件。

3.4

签名算法 signature algorithm

对信息摘要进行加密的非对称加密算法。

4 电子签名

4.1 电子文档

取证与鉴定文书电子文档应载有能够识别鉴定委托人、鉴定人、鉴定时间的内容以及鉴定结论，并应能够有效地表现取证与鉴定文书所载内容，可供随时调取查用。取证与鉴定文书电子文档格式应符合司法鉴定相关规定。

4.2 数字证书签发机构

数字证书应由合法权威机构签发。

4.3 数字证书格式

取证与鉴定电子文书电子签名的认证证书应符合 ITU-T X.509 的规定。

4.4 电子签名过程

签名方在生成取证与鉴定电子文书后，应对电子文书的签名按图 1 表示的过程执行：

a) 将电子文书全文作为输入参数，用散列算法做电子文书摘要；

b) 对电子文书摘要使用数字证书持有者的签名私钥做非对称加密，生成电子签名内容；

c) 将取证与鉴定电子文书原文、生成的电子签名以及签名证书进行封装，形成签名结果。

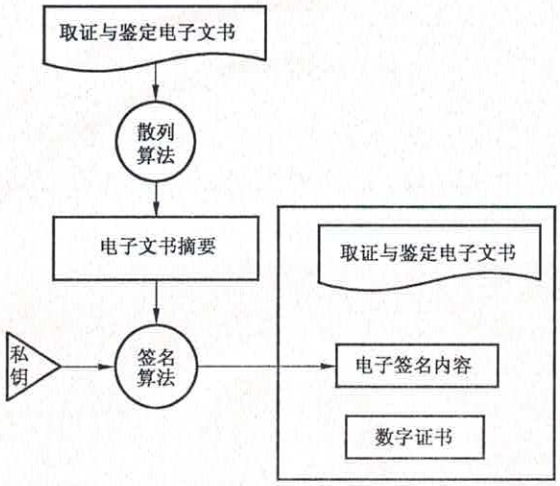


图 1 取证与鉴定电子文书电子签名过程

4.5 电子签名验证过程

取证与鉴定电子文书电子签名的结果，即待验证数据，包括电子签名内容、电子文书原文和签名方公钥。

取证与鉴定电子文书签名验证按照图 2 表示的过程执行：

a) 验证方首先将电子文书原文用散列算法得到电子文书摘要；

b) 对电子签名结果中的电子签名内容，用签名方数字证书解密签名内容，得到根据签名内容导出的电子文书摘要；

c) 将两个摘要进行验证比较，相同则电子文书原文有效，否则无效。

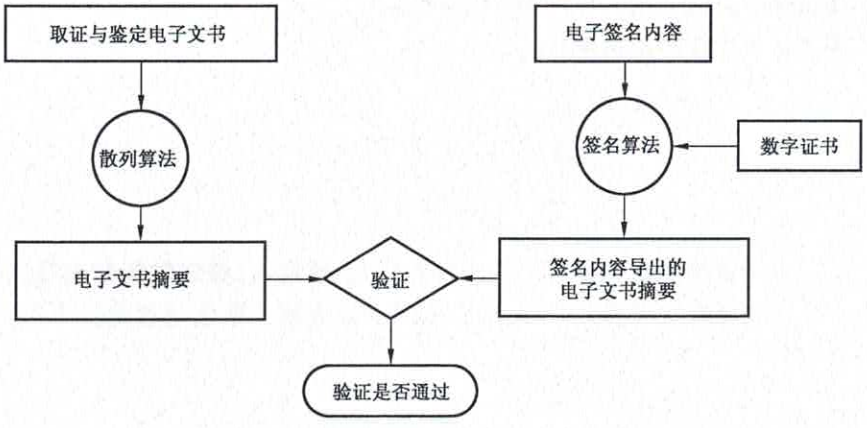


图 2 取证与鉴定电子文书电子签名验证过程

4.6 电子签名格式

取证与鉴定文书电子签名存取格式应按照 RFC 3075 和 RFC 3280 的要求进行存放，文字编码全部采用 UTF-8 格式。格式如下：

[L01]〈Signature Id=" "xmlns=""〉
[L02] 〈SignedInfo〉
[L03] 〈CanonicalizationMethod Algorithm=""/〉
[L04] 〈SignatureMethod Algorithm=""/〉
[L05] 〈Reference URI=""〉
[L06] 〈Transforms〉
[L07] 〈Transform Algorithm=""/〉
[L08] 〈/Transforms〉
[L09] 〈DigestMethod Algorithm=""/〉
[L10] 〈DigestValue〉〈/DigestValue〉
[L11] 〈/Reference〉
[L12] 〈/SignedInfo〉
[L13] 〈SignatureValue/〉
[L14] 〈CertInfo/〉
[L15]〈/Signature〉

其中，各个 xml 标签定义如下：

Signature 标签标明一个完整的 xml 签名，标识为电子文书编号，xml 的命名空间应唯一。

SignedInfo 标签标明待签名的信息。

CanonicalizationMethod 标签中的 Algorithm 属性指定 SignatureInfo 内容在签名前的规范化算法。

SignatureMethod 标签中的 Algorithm 属性指定签名过程中使用的散列算法和签名算法。

Reference 标签包括摘要算法和摘要值等。

Transforms 标签包括签名前的转换算法。

DigestMethod 标签标明摘要算法。

DigestValue 标签标明摘要值。

SignatureValue 标签标明签名结果。

CertInfo 标签标明签名中使用的证书信息。

4.7 电子签名管理系统

4.7.1 总则

取证与鉴定文书电子签名管理系统应具有系统管理和签名显示的功能。

4.7.2 系统管理

系统建立、修改、维保或传送取证与鉴定电子文书应使用能够保证记录真实性、完整性和适当的机密性的程序和控制，以保证签名者不能轻易地否认已经签署的记录是不真实的。这样的程序和控制应包括如下过程：

a) 系统应验证以保证准确、可靠、稳定地预期性能，有能力识别无效的和被改变的记录；

b) 确保产生的人们易读的和适合检查、回顾和拷贝的电子文档准确、完整；

c) 保护系统操作记录以使记录能够在整个的保存期内准确和易于检索；

d) 通过授权个人用户以限制系统的登录；

e) 使用安全的、计算机产生的、时间印记的审核跟踪以便独立地记录操作者登录和建立、修改、或删除电子记录的行为的日期和时间，记录的改变不能使先前的记录信息被覆盖。

4.7.3 签名的显示

签署的取证与鉴定电子文书应包含能清晰显示如下所有与签名相关的信息：

a) 用印刷体书写出签名者的名字；

b) 签名生效的日期和时间；

c) 和签名相关的涵意(例如“同意”)。

GA/T 977—2012

GA/T 977-2012

*

书号：155066·2-23319

定价： 14.00 元