ICS 33.160.25
M 74
备案号：

SJ

中华人民共和国电子行业标准

SJ/T 11407.2—2009

数字接口内容保护系统技术规范
第2部分：数字证书测试规范

Content protection specifications for digital interface—
Part 2: Digital certificate test specification

2010-01-20 发布　　2010-03-01 实施

中华人民共和国工业和信息化部 发布

前　言

SJ/T 11407《数字接口内容保护系统技术规范》拟根据数字接口内容保护需求分为几个部分。

本部分为SJ 11407的第2部分。

请注意本部分的某些内容有可能涉及专利。本部分的发布机构不应承担识别这些专利的责任。

本部分由中华人民共和国工业和信息化部提出。

本部分由全国音频、视频及多媒体设备与系统标准化技术委员会归口。

本部分由中国电子技术标准化研究所、四川长虹电器股份有限公司、西安电子科技大学、北京浦奥得数码技术有限公司、TCL多媒体技术控股公司、青岛海信电器股份有限公司、深圳创维-RGB电子有限公司、深圳国微技术有限公司、厦门华侨电子股份有限公司、上海广电（集团）有限公司、数源科技股份有限公司，康佳集团股份有限公司等单位共同起草。

本部分主要起草人：范科峰、张素兵、王育民、葛建华、刘贤洪、张恩阳、高明、裴庆祺、詹阳、杨震，帅红宇等。

数字接口内容保护系统技术规范
第2部分：数字证书测试规范

1 范围

本部分规定了数字接口内容保护系统中数字证书的测试规范，测试内容为判断一个证书是否为数字接口内容保护系统认证机构颁发的合法证书，在确定为数字接口内容保护系统认证机构颁发的合法证书的基础上给出证书中各个字段的取值，并判断一致性。

本部分适用于有关单位研制、生产、销售、使用、检测和管理数字接口内容保护系统中的数字证书。

2 规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本也适用于本部分。

GB/T 20518—2006 信息安全技术 公钥基础设施 数字证书格式

3 缩略语

下列缩略语适用于本部分：

CA 证书认证机构

DICP 数字接口内容保护系统

ID 标识符

PKI 公钥基础设施

4 数字证书信任模型

公钥证书体系信任模型采用如图1所示的具有唯一根CA的树形结构。使用二级CA的PKI结构，即由DICP根CA给每一个子CA签发证书，再由相应的子CA签发设备中DICP安全模块所持的公钥证书（包括DICP识别管理单元所持有的设备证书和DICP接口模块所持的接口证书两种）。

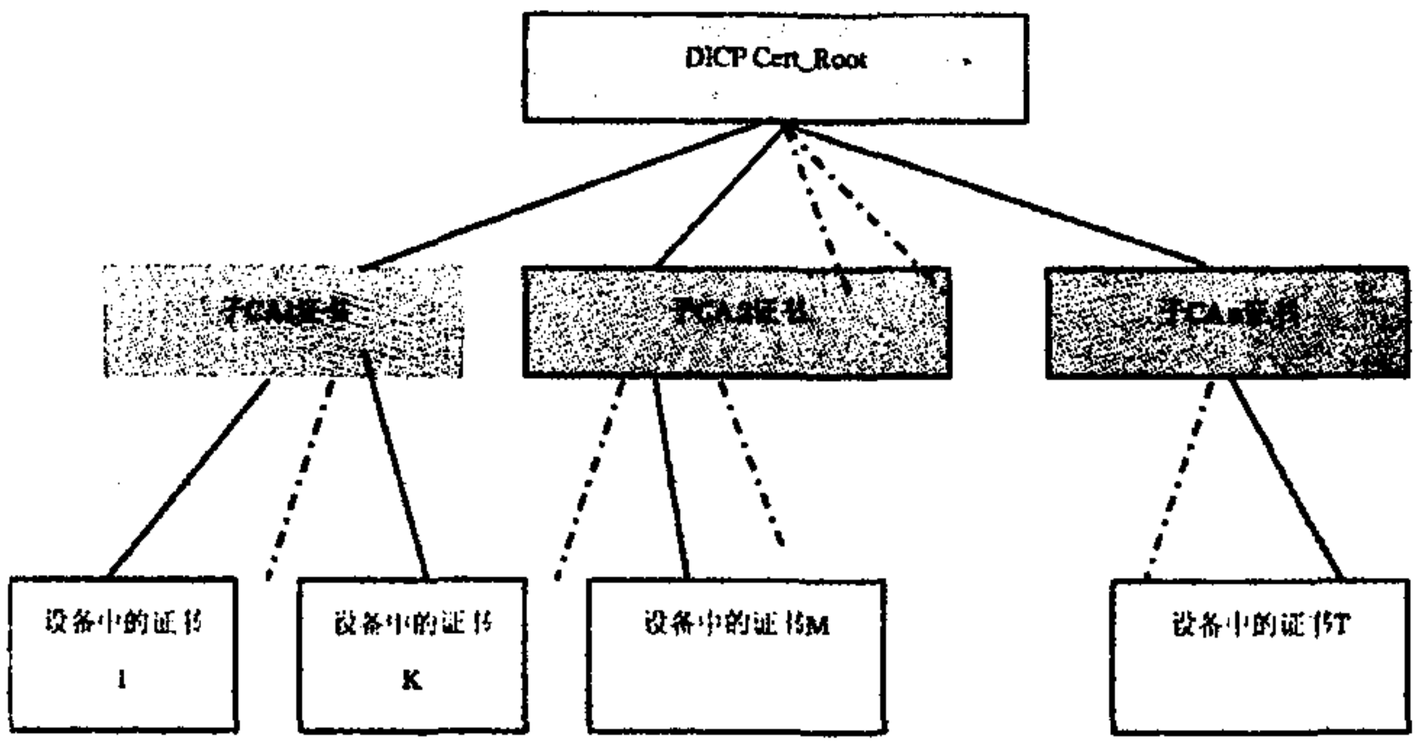


图1 二级CA的PKI信任模型

5 DICP数字证书格式

5.1 CA 证书格式

CA证书（包括DICP根CA证书和子CA证书）格式如下：

DICP标识（8 bit）||证书类型（4 bit）||证书版本号（4 bit）||保留（10 bit）||持有者ID（22 bit）||持有者公钥（384 bit）||持有者功能标识字段说明（10 bit）||证书签发者标识（22 bit）||签发日期（16 bit）||签名（384 bit） ——— （合计864 bit，即108字节）

CA证书字段格式说明见表1。

表1 CA 证书字段格式说明

序号	证书字段	字段说明
1	DICP 标识	标示此证书是哪一个公钥证书体系中的证书。此标识符为“0x5f”表示这是一个 DICP 体系中的公钥证书
2	证书类型	证书的类型，在 CA 所持证书中此字段值为 0；在 DICP 设备证书中此字段值为 1；在 DICP 接口证书中此字段值为 2；其余值先保留
3	证书版本号	标示证书的版本，现在仅使用版本号 0（表示第 1 版）。在版本号为 0 的证书里面采用 SHA－256 和本规范中规定的椭圆曲线签名体制。在以后的版本中，可以按照需要，采用不同的签名算法和不同的证书格式，与现有的第一版以版本号相区别
4	保留	全部置 0，留作以后备用
5	持有者 ID	持有者在本系统中的唯一标识，同时作为本证书的唯一标识符
6	持有者公钥	证书持有 CA 的公钥
7	持有者功能标识	指明证书中公钥的用途功能。 相应比特位含义： LSB0==1 表示证书中的公钥可以用于验证设备证书； LSB1==1 表示证书中的公钥可以用于验证接口证书； LSB2==1 表示证书中的公钥可以用于验证吊销列表； LSB3==1 表示证书中的公钥可以用于验证 CA 证书，其余比特位暂时保留，全部置零。
8	证书签发者标识	在 DICP 根证书中就是 DICP 根 CA 的唯一标识（即在根证书中，证书持有者和证书的签发者同为 DICP 根 CA 的）；在第二级 CA 所持证书中就是 DICP 根 CA 的唯一标识
9	签发日期	即签发年（7 bit）月（4 bit）日（5 bit）。其中年份的 7 bit 数转化为十进制若为 y，则实际表示年份为公元（2000+y）年。例如“0000101||0100||11110”表示签发日期为 2005 年 4 月 30 日
10	签名	证书签发者对证书以上所有信息的有效签名

5.2 设备证书和接口证书格式

设备中所持有的证书有设备证书和接口证书两种，其格式如下：

DICP标识（8 bit）||证书类型（4 bit）||证书版本号（4 bit）||保留（10 bit）||持有者ID（54 bit）||持有者公钥（384 bit）||持有者功能标识（10 bit）||证书签发者标识（22 bit）||签发日期（16 bit）||签名（384 bit） ——— （合计896 bit，即112字节）

设备证书和接口证书字段格式说明见表2。

表2 设备/接口证书字段格式说明

序号	证书字段	字段说明
1	DICP 标识	标示此证书是哪一个公钥证书体系中的证书。本规范中为“0x5f”，表示这是 DICP 体系中的公钥证书
2	证书类型	详见 CA 证书字段说明，在 DICP 设备证书中此字段值为 1；在 DICP 接口证书中此字段值为 2
3	证书版本号	标示证书的版本，现在仅使用版本号 0，详细说明见 CA 证书字段说明中。
4	保留	全部置 0，留作以后备用
5	持有者 ID	证书持有设备的唯一标识符，即设备 ID
6	持有者公钥	证书持有设备的公钥
7	持有者功能标识	设备功能标识。 LSB0 —— 证书的持有者是桥设备；其余比特位暂时保留，全部置 0
8	证书签发者标识	证书签发者（相应 CA）的标识符
9	签发日期	即签发年（7 bit）月（4 bit）日（5 bit）。详见 CA 证书字段说明
10	签名	证书签发者对证书以上所有信息的有效签名

6 DICP 数字证书测试

6.1 DICP 数字证书测试一般要求

6.1.1 DICP 数字证书测试工作条件

DICP数字证书测试软件的硬件工作平台：根据软件运行占用资源来选择测试计算机（1台）。硬件配置：内存大于256 MB（主频高于266 MHz）、硬盘容量大于20 GB、网卡所支持的速度大于10 Mbps、主板支持USB2.0传输协议。

DICP数字证书测试软件的软件工作平台：选用比较普及的操作系统和软件平台，工作平台支持“Windows9X/ME/NT Workstation/2000 professional”和“MS Office 97/2000/XP”，采用“Windows 2000professional+MS Office 2003”的流行环境。

注1:营造相对简单、独立的软件测试环境。除了操作系统，测试机上只安装软件运行和测试必需的软件，以免不相关的软件影响测试实施。

注2:无毒的环境指利用有效的正版杀毒软件检测软件环境，保证测试环境中没有病毒。

6.1.2 环境条件

在下列测试用标准大气条件下进行测试：

——环境温度：15 ℃～35 ℃；

——相对湿度：25%～75%；

——大气压力：86 kPa～106 kPa 。

6.1.3 电源

DICP数字证书的测试应在额定电源电压条件下，测试时的电源电压的变化为±2%；当采用交流电网供电时，电源频率的波动为±2%，谐波分量不超过5% 。

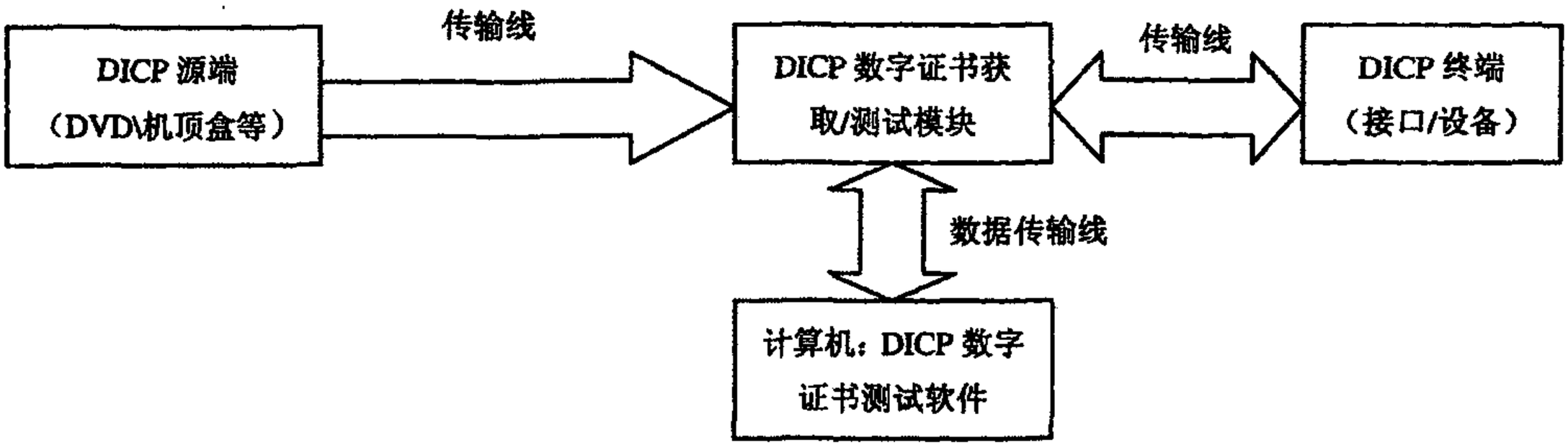
6.1.4 稳定时间

为了确保在测量开始后，DICP数字证书测试的功能不随时间而有明显的变化，搭建的整个系统应在额定测试条件下工作30 min，以使整个系统性能稳定。

6.1.5 测试场地

测试应在不受来自外界电磁场干扰的室内进行。如果干扰影响测试结果，测试应在屏蔽室内进行。

6.1.6 证书测试系统模型（见图 2）



注1:传输线可以是HDMI、DisplayPort等传输线，源端、终端与DICP数字证书测试模块上的接口同样可以是HDMI、DisplayPort等数字传输接口。

注2:只有在源端与终端之间有内容传输过程中DICP数字证书获取/测试模块才可以读取固化在DICP终端内的数字证书。

图2　证书测试系统模型

6.2　DICP 数字证书测试目的

1)　测试待测证书是否为DICP证书；
2)　测试待测证书是否是DICP机构颁发的合法证书；
3)　测试待测证书的类型：设备证书还是接口证书；
4)　测试待测证书的版本；
5)　测试待测证书的ID；
6)　测试待测证书的功能标识；
7)　测试待测证书的签发日期；
8)　测试待测证书的签发者标识。

在第1）项检测出是DICP的证书后才进行第2）项检测。在第2）项检测后确定是合法的DICP机构颁发的证书后，对于CA证书进行第4）项到第7）项的检测，对于设备证书或接口证书进行第3）项到第8）项的检测。

6.3　DICP 数字证书测试说明

进行证书测试时，分以下2种情况：

a)　如果待测证书是CA证书，则首先测试所提供的DICP根证书是否合法。如果合法，则对待测CA证书进行测试；
b)　如果待测证书是设备证书或者接口证书，则首先测试所提供的DICP根证书是否合法。如果根证书合法，则对颁发该设备证书或接口证书的CA证书进行测试。如果CA证书合法，则开始对待测的设备证书或接口证书进行测试。

6.4　DICP 数字证书测试软件使用方法

本条主要介绍DICP数字证书测试软件的使用方法以及导致证书测试失败的各种原因分析。

a)　待测证书为CA证书：确保DICP的根证书和待测CA证书在“DICP数字证书测试软件”安装目录下，并且DICP的根证书名称为“Cert_Root”。运行程序，按照程序提示输入待测CA证书的文件名称就可以得到测试结果。
　1)　如果待测CA证书合法，则会给出“待测CA证书是合法的DICP CA证书”提示，并且同时给出该CA证书的证书版本、证书ID号、证书的功能标识以及证书的签发日期。
　2)　如果待测CA证书非法则会给出“CA证书非法”提示。

导致没有完成证书测试整个流程的主要原因有以下几种情况，如表3所示。

表3　测试软件测试提示及导致证书测试失败原因分析（待测证书为CA证书）

序号	未完成测试情况	系统提示	失败原因分析
1	找不到相应的证书文件	没有找到文件	找不到根证书文件或者待测CA证书文件
2	待测CA证书与根证书不匹配	CA证书与根证书不匹配，无法进行进一步检测，程序退出	待测的CA证书并不是该DICP根证书所签发的
3	待测CA证书版本错误	所提供的CA证书版本错误，无法进行进一步检测，程序退出	待测CA证书的版本不是DICP的第一版证书
4	待测CA证书并非一个真正的CA证书	CA证书不是DICP系统证书，退出检测程序	用户要检测的CA证书并不是DICP机构所颁发的证书
5	待测CA证书不是DICP系统的证书	CA证书不是DICP系统证书，退出检测程序	用户要检测的CA证书并不是DICP机构所颁发的证书

a）　待测证书为设备（接口）证书：确保DICP的根证书和待测设备（接口）证书以及颁发待测设备（接口）证书的CA证书在“DICP数字证书测试软件”安装目录下，并且DICP的根证书名称为“Cert_Root”。运行程序，按照程序提示分别输入待测设备（接口）证书以及相应的CA证书的文件名称就可以得到测试结果。

1）　如果待测设备（接口）证书合法，则会给出“待测的设备（接口）证书是合法的DICP证书”提示，并且同时给出待测设备（接口）证书的证书类型号（该字段说明待测证书是设备证书还是接口证书）、证书版本、证书ID号、证书的功能标识、证书的签发日期和证书的签发者标识。

2）　如果待测设备（接口）证书非法则会给出“设备（接口）证书非法”提示。

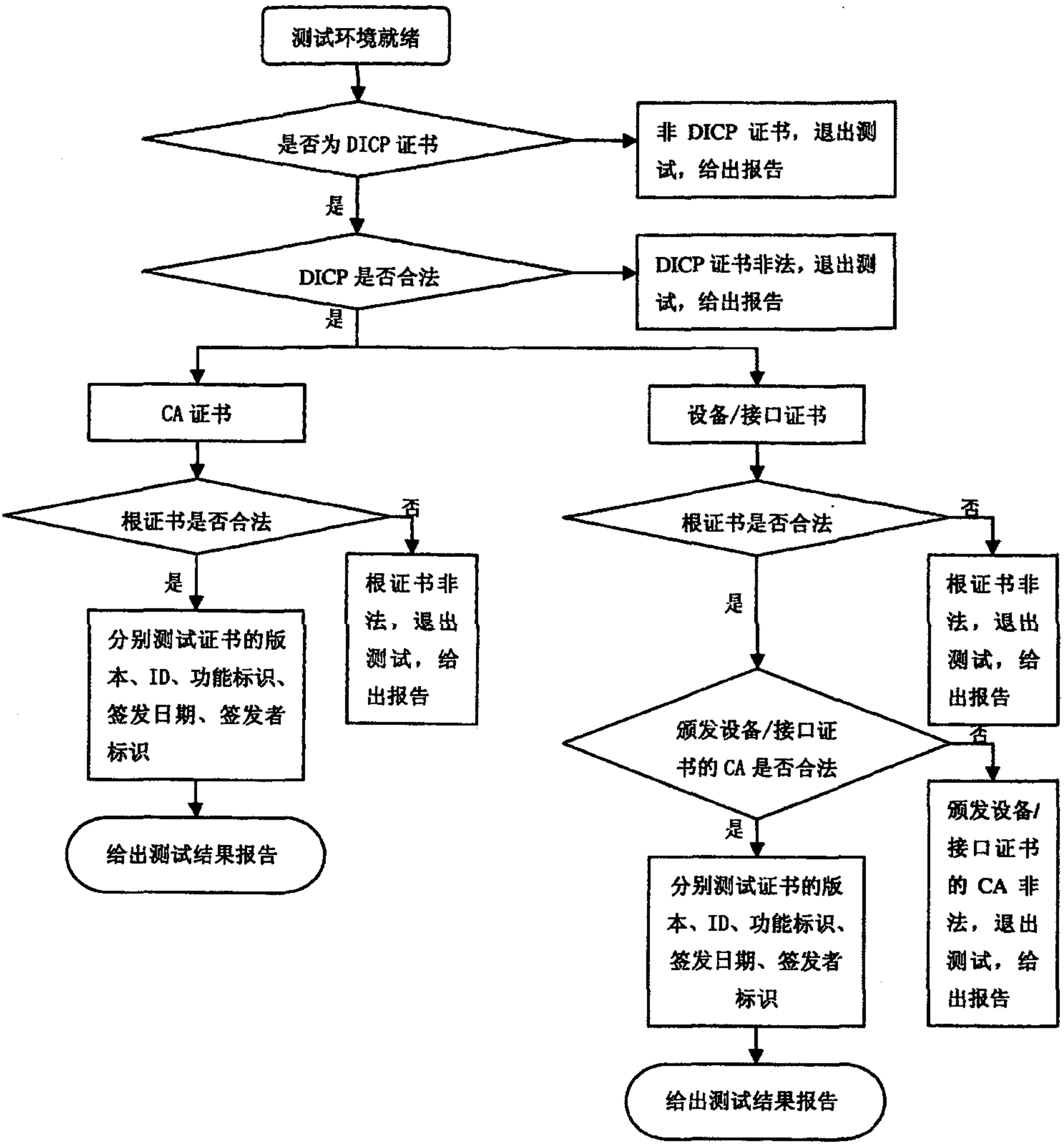
导致没有完成证书测试整个流程的主要原因有以下几种情况，如表4所示。

表4　测试软件测试提示及导致证书测试失败原因分析（待测证书为设备/接口证书）

序号	未完成测试情况	系统提示	失败原因分析
1	找不到相应的证书文件	没有找到文件	找不到根证书文件或者待测设备（接口）证书文件或者签发待测设备（接口）证书的 CA 证书文件
2	对应 CA 证书与根证书不匹配	CA 证书与根证书不匹配，无法进行进一步检测，程序退出	待测的 CA 证书并不是该 DICP 根证书所签发的
3	签发待测设备（接口）证书的 CA 证书版本错误	所提供的 CA 证书版本错误，无法进行进一步检测，程序退出	签发待测设备（接口）证书的 CA 证书的版本不是 DICP 的第一版证书
4	签发待测设备（接口）证书的 CA 证书并非一个真正的 CA 证书	该证书不是一个 CA 证书，无法进行进一步检测，程序退出	用户把设备（接口）证书当作签发待测设备（接口）证书的 CA 证书
5	签发待测设备（接口）证书的 CA 证书不是 DICP 系统的证书	CA 证书不是 DICP 系统证书，退出检测程序	签发待测设备（接口）证书的 CA 证书并不是 DICP 机构所颁发的证书
6	签发待测设备（接口）证书的 CA 证书非法	检测结果：CA 证书非法	用户提供的签发待测设备（接口）证书的 CA 证书本身就是一个非法的 DICP 证书
7	签发待测设备（接口）证书的 CA 证书功能受限情况 1	所提供的 CA 证书不能用于验证设备证书，无法进行进一步检测，程序退出	系统已经检测出待测证书是设备证书，但是用户提供的签发待测设备（接口）证书的 CA 证书并不具备签发设备证书的功能
8	签发待测设备（接口）证书的 CA 证书功能受限情况 2	所提供的 CA 证书不能用于验证接口证书，无法进行进一步检测，程序退出	系统已经检测出待测证书是接口证书，但是用户提供的签发待测设备（接口）证书的 CA 证书并不具备签发接口证书的功能
9	签发待测设备（接口）证书的 CA 证书与待测设备（接口）证书不匹配	所提供的 CA 证书与设备（接口）证书不匹配，无法进行进一步检测，程序退出	待测设备（接口）证书并不是所提供的 CA 证书所签发的
10	待测设备（接口）证书不是 DICP 系统证书	设备（接口）证书不是 DICP 系统证书，退出检测程序	用户要检测的设备（接口）证书并不是 DICP 机构所颁发的证书
11	待测设备（接口）证书类型错误	待测证书类型错误，无法进行进一步检测，程序退出	待测设备（接口）证书既不是设备证书也不是接口证书
12	待测设备（接口）证书的证书版本错误	待测证书版本错误，无法进行进一步检测，程序退出	待测设备（接口）证书的证书版本不是 DICP 第一版证书

6.5　DICP 数字证书测试流程框图

根据测试结果要求和测试目的DICP数字证书测试流程见图3。



任何一次检测到证书非法退出测试后要给出提示：退出原因、测试进行到的环节、已经测得的各比特位的值。测试结果报告要以文本的形式显示出来，包括测试结果（数据表格的形式）、测试日期、测试负责人等信息。

在分别测试证书的版本、ID、功能标识、签发日期与签发者标识过程中，按此顺序依次测试这些内容，在任何一步骤中检测到非法或者不能识别证书都要退出检测程序，同时给出检测报告。

图3 DICP 数字证书测试流程

6.6 DICP 数字证书测试结果显示及汇总的方法

6.6.1 屏幕现实

将每个测试用例的测试结果情况显示在计算机屏幕上。

6.6.2 文本记录

将每个测试用例的测试结果输入到一个文件中，自动形成测试报告。

6.6.3 测试结果输出的内容

测试报告无论是屏幕显示还是文件显示，需要包括如下内容：

a) 证书通过测试需要给出以下测试结果：证书的类型、证书的版本、证书的ID、证书的功能标识、证书的签发日期与证书的签发者标识等；
b) 证书未通过测试需要给出以下测试结果：证书未通过测试的原因、证书测试进行到的环节、已经测得的数据（各比特位的值）等；
c) 数字证书测试输入的路径；
d) 其他数据：测试日期、测试负责人等信息。