(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108055308 B
(45)授权公告日 2021.01.05

(21)申请号 201711280767.4
(22)申请日 2017.12.06
(65)同一申请的已公布的文献号
申请公布号 CN 108055308 A
(43)申请公布日 2018.05.18
(73)专利权人 北京航天计量测试技术研究所
地址 100076 北京市丰台区南大红门路一号
专利权人 中国运载火箭技术研究院
(72)发明人 张修建 高翌春 王兵 刘晓旭 张鹏程 靳硕 印朝辉 张铁犁
(74)专利代理机构 核工业专利中心 11007
代理人 吕岩甲
(51)Int.Cl.
*H04L 29/08*(2006.01)
*H04L 29/06*(2006.01)
*H04L 9/08*(2006.01)

(56)对比文件
CN 104506502 A,2015.04.08
CN 101355684 A,2009.01.28
CN 101136916 A,2008.03.05
US 2013073859 A1,2013.03.21
CN 105553927 A,2016.05.04
CN 102004969 A,2011.04.06
CN 102156844 A,2011.08.17

审查员 王曼

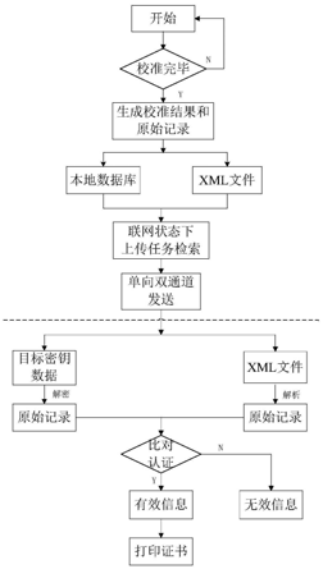
权利要求书1页 说明书3页 附图2页

(54)发明名称

一种用于离线校准无握手机制的证书上传方法

(57)摘要

本发明属于计量流程信息安全技术领域，具体涉及一种用于离线校准无握手机制的证书上传方法。校准装置在离线状态下对被校设备进行计量校准，生成校准结果和原始记录，加密后存储至本地数据库中；校准装置根据校准日期检索数据库未上传的原始记录，选择上传任务列表；校准装置对准备上传至计量信息系统的校准结果和原始记录生成目标密钥数据，然后传输至计量信息系统数据库服务器，同时包含校准结果和原始记录的文件传输至计量信息系统特定目录下；计量信息系统接收、解析文件数据以及解密目标密钥数据；计量信息系统根据被较设备类型和校准数据，自动生成打印证书。本发明可以确保证书原始记录的完整性和可靠性。




CN 108055308 B

1.一种用于离线校准无握手机制的证书上传方法,其特征在于:包括以下步骤:

步骤一、专用校准装置在离线状态下对被校设备进行计量校准,校准完成后生成校准结果和原始记录,以XML格式文件存在本地目录下,并加密后存储至本地数据库中;

步骤二、在专用校准装置具备联网条件下,根据校准日期检索数据库未上传的原始记录,选择上传任务列表;

步骤三、专用校准装置对准备上传至计量信息系统的校准结果和原始记录生成目标密钥数据,然后通过数据库网络协议传输至计量信息系统数据库服务器,同时,包含校准结果和原始记录的XML文件通过FTP协议传输至计量信息系统WEB服务器特定目录下;

步骤四、计量信息系统通过数据交互接口接收、解析XML文件数据以及解密目标密钥数据,通过双通道验证,确保无握手机制下证书信息的完整性,避免原始记录的丢失或者重复上传现象的发生;

步骤五、计量信息系统根据被较设备类型和校准数据,调用服务器内相应的计量证书模块,自动生成、打印证书。

2.根据权利要求1所述的用于离线校准无握手机制的证书上传方法,其特征在于:所述的专用校准装置是用来进行计量测试的设备、配件软硬件资源,其中软件安装在检定装置的控制器模块内,用于完成各类专用测试设备的检定任务,可实现检定过程的自动化控制及相应数据采集、处理、通信功能。

3.根据权利要求1所述的用于离线校准无握手机制的证书上传方法,其特征在于:所述的目标密钥数据包括口令字和随机密码Salt,在对校准结果和原始记录进行加密时,对于每一项原始记录,由随机数发生器生成一个随机密码Salt,并与该项原始记录对应的口令字结合生成加解密密钥,然后将对应的Salt与对应的原始记录密文一同发送,而将对应的口令字存储在计量信息系统数据库服务器口令字列表中,只有专用校准装置发出某项原始记录时,计量信息系统才能与数据库中的随机密码组合解密原始记录密文。

4.根据权利要求1所述的用于离线校准无握手机制的证书上传方法,其特征在于:所述的计量信息系统包括数据库服务器、WEB服务器和客户端;数据库服务器与Web服务器相连传输数据请求及应答信息,数据库服务器存储被较设备的原始记录、校准结果、证书信息、操作日志及用户信息,实现对数据库的管理;Web服务器以网页的形式完成与客户端的动态交互,通过响应客户的HTTP请求,从数据库中获取被较设备的计量数据信息,实现对专用计量设备有关的原始数据、任务、证书信息、规程、标准、设备状态及操作者权限信息的统一管理。

5.根据权利要求1所述的用于离线校准无握手机制的证书上传方法,其特征在于:该方法采用基于B/S和C/S混合架构实现,包括便携式校准系统和计量信息系统;便携式校准系统包括专用校准装置和被较设备,专用校准装置选择便携式PXI机箱,其控制器内安装校准软件,用于完成各类专用测试设备的检定任务,可实现检定过程的自动化控制及相应数据采集处理功能;计量信息系统包括数据库服务器和WEB服务器,完成检定任务后,各检定装置将数据回传到计量信息系统,由计量信息系统统一进行数据管理、证书管理、资源管理、数据交互,实现对专用计量设备有关的原始数据、任务、证书信息、规程、标准、设备状态及操作者权限信息的统一管理。

# 一种用于离线校准无握手机制的证书上传方法

## 技术领域

[0001] 本发明属于计量流程信息安全技术领域，具体涉及一种用于离线校准无握手机制的证书上传方法。

## 背景技术

[0002] 在国防军工计量领域，大多数专用校准装置在离线状态下对被校设备进行计量检定，而生成的原始记录需要在联网状态下，通过以太网上传至计量信息系统，而使用密码验证或者FTP上传的手段很难保证数据的可靠性、完整性和准确性。另一方面，用于证书打印的计量信息系统为Web服务器软件，通常状态下，与校准软件的数据交互不具备实时握手通信的条件，无法满足航天型号发展计量保证需求，因此提出一种用于离线校准无握手机制的证书上传方法，来确保证书原始记录的完整性和可靠性，避免原始记录的丢失、篡改或者重复等现象的发生。

## 发明内容

[0003] 本发明的目的在于提供一种用于离线校准无握手机制的证书上传方法，为校准数据的上传提供一种简单有效的手段，以确保证书原始记录的完整性和可靠性。

[0004] 为达到上述目的，本发明所采取的技术方案为：

[0005] 一种用于离线校准无握手机制的证书上传方法，包括以下步骤：

[0006] 步骤一、专用校准装置在离线状态下对被校设备进行计量校准，校准完成后生成校准结果和原始记录，以XML格式文件存在本地目录下，并加密后存储至本地数据库中；

[0007] 步骤二、在专用校准装置具备联网条件下，根据校准日期检索数据库未上传的原始记录，选择上传任务列表；

[0008] 步骤三、专用校准装置对准备上传至计量信息系统的校准结果和原始记录生成目标密钥数据，然后通过数据库网络协议传输至计量信息系统数据库服务器，同时，包含校准结果和原始记录的XML文件通过FTP协议传输至计量信息系统WEB服务器特定目录下；

[0009] 步骤四、计量信息系统通过数据交互接口接收、解析XML文件数据以及解密目标密钥数据，通过双通道验证，确保无握手机制下证书信息的完整性，避免原始记录的丢失或者重复上传现象的发生；

[0010] 步骤五、计量信息系统根据被较设备类型和校准数据，调用服务器内相应的计量证书模块，自动生成、打印证书。

[0011] 所述的专用校准装置是用来进行计量测试的设备、配件软硬件资源，其中软件安装在检定装置的控制器模块内，用于完成各类专用测试设备的检定任务，可实现检定过程的自动化控制及相应数据采集、处理、通信功能。

[0012] 所述的目标密钥数据包括口令字和随机密码Salt，在对校准结果和原始记录进行加密时，对于每一项原始记录，由随机数发生器生成一个随机密码Salt，并与该项原始记录对应的口令字结合生成加解密密钥，然后将对应的Salt与对应的原始记录密文一同发送，

而将对应的口令字存储在计量信息系统数据库服务器口令字列表中，只有专用校准装置发出某项原始记录时，计量信息系统才能与数据库中的随机密码组合解密原始记录密文。

[0013] 所述的计量信息系统包括数据库服务器、WEB服务器和客户端；数据库服务器与Web服务器相连传输数据请求及应答信息，数据库服务器存储被较设备的原始记录、校准结果、证书信息、操作日志及用户信息，实现对数据库的管理；Web服务器以网页的形式完成与客户端的动态交互，通过响应客户的HTTP请求，从数据库中获取被较设备的计量数据信息，实现对专用计量设备有关的原始数据、任务、证书信息、规程、标准、设备状态及操作者权限信息的统一管理。

[0014] 该方法采用基于B/S和C/S混合架构实现，包括便携式校准系统和计量信息系统；便携式校准系统包括专用校准装置和被较设备，专用校准装置选择便携式PXI机箱，其控制器内安装校准软件，用于完成各类专用测试设备的检定任务，可实现检定过程的自动化控制及相应数据采集处理功能；计量信息系统包括数据库服务器和WEB服务器，完成检定任务后，各检定装置将数据回传到计量信息系统，由计量信息系统统一进行数据管理、证书管理、资源管理、数据交互，实现对专用计量设备有关的原始数据、任务、证书信息、规程、标准、设备状态及操作者权限信息的统一管理。

[0015] 本发明所取得的有益效果为：

[0016] 本发明通过FTP原始记录文件的解析和目标密钥数据的双通道验证，解决了无握手机制下校准数据常规上传方法带来的问题，提高了证书原始记录上传的安全性和完整性。

## 附图说明

[0017] 图1为用于离线校准无握手机制的证书上传方法流程图；

[0018] 图2为实现图1所述方法的系统结构图。

## 具体实施方式

[0019] 下面结合附图和具体实施例对本发明进行详细说明。

[0020] 如图1所示，本发明所述用于离线校准无握手机制的证书上传方法包括以下步骤：

[0021] 步骤一、专用校准装置在离线状态下对被校设备进行计量校准，校准完成后生成校准结果和原始记录，以XML格式文件存在本地目录下，并加密后存储至本地数据库中。

[0022] 所述的专用校准装置是用来进行计量测试的设备、配件等软硬件资源，其中软件安装在检定装置的控制器模块内，用于完成各类专用测试设备的检定任务，可实现检定过程的自动化控制及相应数据采集、处理、通信等功能。

[0023] 步骤二、在专用校准装置具备联网条件下，在系统数据上传模块内，根据校准日期检索数据库未上传的原始记录，选择上传任务列表。

[0024] 步骤三、专用校准装置对准备上传至计量信息系统的校准结果和原始记录通过口令字和随机密码Salt生成目标密钥数据，然后通过数据库网络协议传输至计量信息系统数据库服务器，同时，包含校准结果和原始记录的XML文件通过FTP协议传输至计量信息系统WEB服务器特定目录下。

[0025] 所述的目标密钥数据由两部分组成，即口令字和随机密码Salt。在对校准结果和

原始记录进行加密时，对于每一项原始记录，由随机数发生器生成一个随机密码Salt，并与该项原始记录对应的口令字结合生成加解密密钥。然后将对应的Salt与对应的原始记录密文一同发送，而将对应的口令字存储在计量信息系统数据库服务器口令字列表中。只有专用校准系统发出某项原始记录(含对应的口令字)时，计量信息系统才能与数据库中的随机密码组合解密原始记录密文，从而保证原始记录的安全性。

[0026] 所述的计量信息系统包括数据库服务器、WEB服务器和客户端。其中，数据库服务器与Web服务器相连传输数据请求及应答信息，数据库服务器存储被较设备的原始记录、校准结果、证书信息、操作日志及用户信息等，实现对数据库的管理。Web服务器以网页的形式完成与客户端的动态交互，通过响应客户的HTTP请求，从数据库中获取被较设备的计量数据信息，实现对专用计量设备有关的原始数据、任务、证书信息、规程、标准、设备状态及操作者权限等信息的统一管理。

[0027] 步骤四、计量信息管理系统通过数据交互接口接收、解析XML文件数据以及解密目标密钥数据，通过双通道验证，来确保无握手机制下证书信息的完整性，避免原始记录的丢失或者重复上传等现象的发生。

[0028] 步骤五、计量信息管理系统根据被较设备类型和校准数据，调用服务器内相应的计量证书模块，自动生成、打印证书。

[0029] 如图2所示，实现用于离线校准无握手机制的证书上传方法的系统结构图，采用基于B/S和C/S混合架构设计，包括：便携式校准系统和计量信息系统两部分。便携式校准系统包括专用校准装置和被较设备，专用校准装置选择便携式PXI机箱，其控制器内安装校准软件，用于完成各类专用测试设备的检定任务，可实现检定过程的自动化控制及相应数据采集、处理等功能。计量信息系统以数据库服务器和WEB服务器等组成的专用计量信息系统为业务处理核心，完成检定任务后，各检定装置将数据回传到专用计量信息系统，由专用计量信息系统统一进行数据管理、证书管理、资源管理、数据交互等，实现对专用计量设备有关的原始数据、任务、证书信息、规程、标准、设备状态及操作者权限等信息的统一管理。

[0030] 本实施例方法可行，系统基于B/S和C/S混合架构，专用校准装置选择便携式PXI机箱，利用无握手机制的证书上传方法，保证了证书原始记录的完整性，提高了整个系统的安全性和易用性。

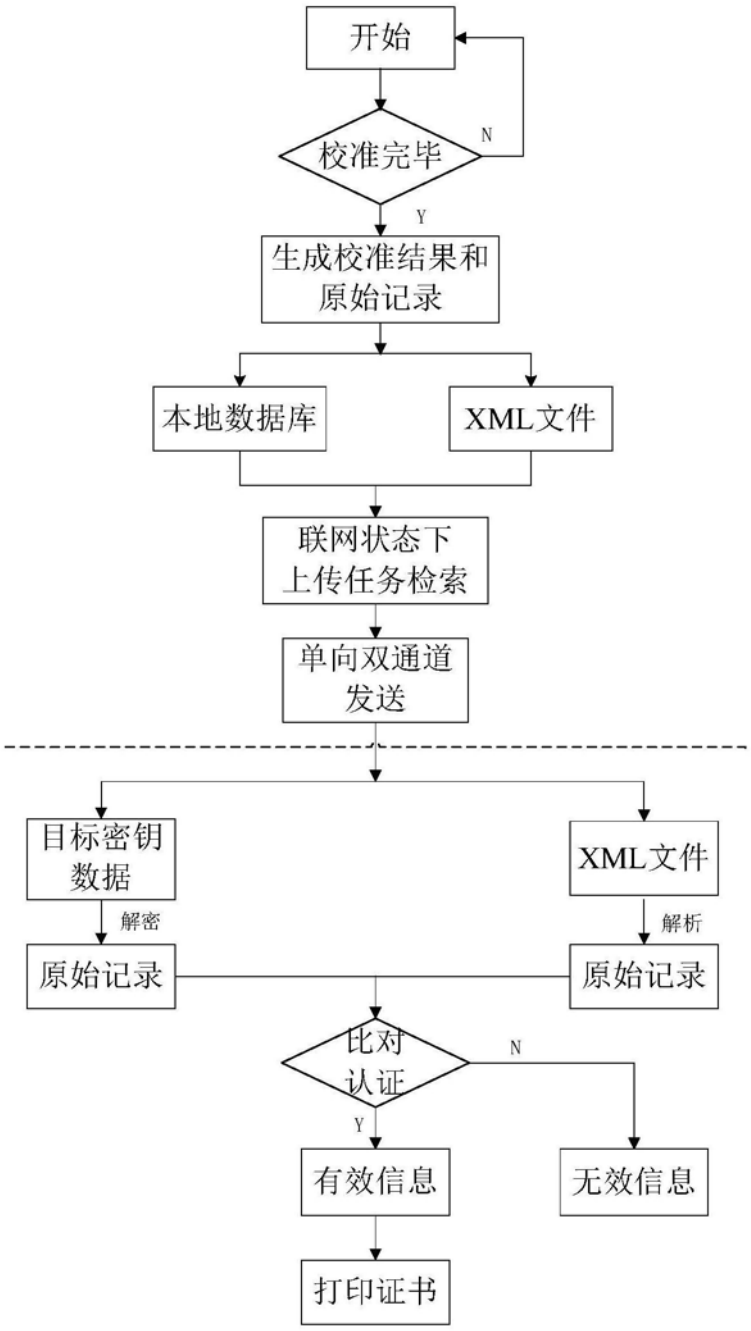

开始
校准完毕
N
Y
生成校准结果和
原始记录
本地数据库
XML文件
联网状态下
上传任务检索
单向双通道
发送
目标密钥
数据
解密
原始记录
XML文件
解析
原始记录
比对
认证
N
Y
有效信息
无效信息
打印证书

图1

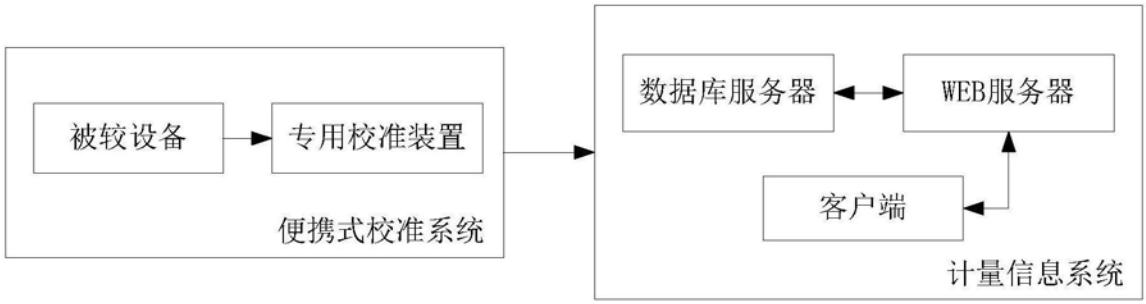



图2