(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115001697 B
(45)授权公告日 2024.04.02

(21)申请号 202210449556.3

(22)申请日 2022.04.26

(65)同一申请的已公布的文献号
申请公布号 CN 115001697 A

(43)申请公布日 2022.09.02

(73)专利权人 互联网域名系统北京市工程研究中心有限公司
地址 101408 北京市怀柔区雁栖经济开发区兴科南二街3号院1号楼322室

(72)发明人 邵晴 詹子林 马迪 毛伟

(74)专利代理机构 北京市万慧达律师事务所 11111
专利代理师 黄玉东

(51)Int.Cl.
H04L 9/32(2006.01)

(56)对比文件
CN 111262683 A,2020.06.09
CN 112865979 A,2021.05.28
CN 105141681 A,2015.12.09
CN 104980438 A,2015.10.14
US 10547457 B1,2020.01.28
US 2010115267 A1,2010.05.06
US 2018102904 A1,2018.04.12
G. Huston;R. Loomans;G. Michaelson;APNIC.A Profile for Resource Certificate Repository Structure.IETF .2012,全文.
许圣明;马迪;毛伟;王伟.基于有序哈希树的RPKI资料库数据同步方法.计算机系统应用.2016,(第06期),全文.

审查员 张长梅

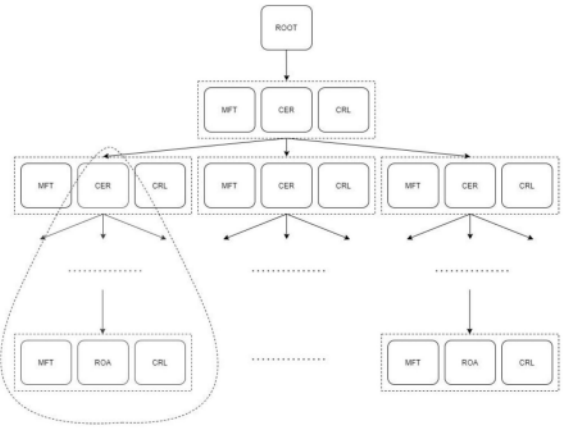
权利要求书2页 说明书5页 附图4页

(54)发明名称

基于RPKI的证书链局部验证方法、系统及存储介质

(57)摘要

本申请提供了一种基于RPKI的证书链局部验证方法、系统及存储介质。该方法包括:构建证书链的验证树结构,所述的验证树结构具有多个层级,各层级记录有多种存储证书文件,包括:CER公钥证书文件、证书撤销列表文件、路由起源授权文件、资料清单文件中的多种;RPKI的依赖方在检测到某层级的存储证书文件有更新时,对需更新的所述存储证书关联的同层级和/或其它各子节点的存储证书文件进行局部的验证和更新。本申请提出的一种证书链的局部验证方法,能够有效优化RP验证证书时的性能,提高RP效率。



CN 115001697 B

1.一种基于RPKI的证书链局部验证方法,其特征在于,包括:

构建证书链的验证树结构,所述的验证树结构具有根节点和多个层级,从根节点之后按照层级划分,每一层级形成一组或多组子节点,且各层级记录有一或多组存储证书文件,包括:CER公钥证书文件、证书撤销列表文件、路由起源授权文件以及资料清单文件中的多种,其中,最末级节点包括路由起源授权文件、资料清单文件以及证书撤销列表文件,除根节点和最末级节点外,其它层级均包括资料清单文件、CER公钥证书文件以及证书撤销列表文件;

RPKI的依赖方在检测到某层级的存储证书文件有更新时,对需更新的所述存储证书关联的同组和/或其它各子节点的存储证书文件进行局部的验证和更新;

其中,所述的局部的验证和更新包括:

当检测到有CER公钥证书文件更新时,先在所述证书链的验证树结构中查询定位到需更新CER公钥证书文件所在的组,验证和更新对应的CER公钥证书文件,以及验证和更新由所述CER公钥证书文件签发的其它各子节点的存储证书文件;

当检测到有资料清单文件更新时,先在所述证书链的验证树结构中查询定位到需更新资料清单文件所在的组,验证和更新对应的资料清单文件,以及同组的CER公钥证书文件和证书撤销列表文件;

当检测到有证书撤销列表文件更新时,先在所述证书链的验证树结构中查询定位到需更新撤销列表文件所在的组,验证和更新对应的撤销列表文件,以及同组的CER公钥证书文件和资料清单文件;

当检测到有路由起源授权文件更新时,先在所述证书链的验证树结构中查询定位到需更新路由起源授权文件所在的组,验证和更新对应的路由起源授权文件。

2.如权利要求1所述的方法,其特征在于,若对资料清单文件和证书撤销列表文件进行更新时,同层级的CER公钥证书文件出现变化,则对所述CER公钥证书文件签发的其它各子节点的存储证书文件也进行验证更新。

3.如权利要求1所述的方法,其特征在于,若对证书撤销列表文件进行更新时,同组的资料清单文件若出现变化,则对同层级的所述资料清单文件也进行更新。

4.一种基于RPKI的证书链局部验证系统,其特征在于,包括:

证书链构建模块,用于构建证书链的验证树结构,所述的验证树结构具有根节点和多个层级,从根节点之后按照层级划分,每一层级形成一组或多组子节点,且各层级记录有多组存储证书文件,包括:CER公钥证书文件、证书撤销列表文件、路由起源授权文件以及资料清单文件中的多种,其中,最末级节点包括路由起源授权文件、资料清单文件以及证书撤销列表文件,除根节点和最末级节点外,其它层级均包括资料清单文件、CER公钥证书文件以及证书撤销列表文件;

检测更新模块,用于RPKI的依赖方在检测到某层级的存储证书文件有更新时,对需更新的所述存储证书关联的同层级和/或其它各子节点的存储证书文件进行局部的验证和更新;

其中,检测更新模块还用于:

当检测到有CER公钥证书文件更新时,先在所述证书链的验证树结构中查询定位到需更新CER公钥证书文件所在的组,验证和更新对应的CER公钥证书文件,以及验证和更新由

所述CER公钥证书文件签发的其它各子节点的存储证书文件;当检测到有资料清单文件更新时,先在所述证书链的验证树结构中查询定位到需更新资料清单文件所在的组,验证和更新对应的资料清单文件,以及同组的CER公钥证书文件和证书撤销列表文件;当检测到有证书撤销列表文件更新时,先在所述证书链的验证树结构中查询定位到需更新撤销列表文件所在的组,验证和更新对应的撤销列表文件,以及同组的CER公钥证书文件和资料清单文件;当检测到有路由起源授权文件更新时,先在所述证书链的验证树结构中查询定位到需更新路由起源授权文件所在的组,验证和更新对应的路由起源授权文件。

5.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,所述计算机程序被处理器执行时实现权利要求1至3中任一项所述的方法的步骤。

基于RPKI的证书链局部验证方法、系统及存储介质

技术领域

[0001] 本申请涉及DNS服务技术领域,特别是涉及一种基于RPKI的证书链局部验证方法、系统及存储介质。

背景技术

[0002] 随着互联网规模的不断扩大,互联网性质的不断演变,互联网码号资源分配需求的不断增长,资源分配体系也在不断变革。IETF(The Internet Engineering Task Force,国际互联网工程任务组)于1990年成立IANA(The InternetAssignedNumbers Authority,互联网数字分配机构),以确保互联网码号资源得到公平且有效的分配。截至目前,世界范围内共有五个正在运作的RIR(Regional Internet Registry,互联网注册机构),负责特定地理区域内码号资源的分配和指定,从而实现IP地址和AS(Autonomous System,自治系统)号在可控范围内的管理自治。图1列举了五大RIR的相关信息,包括成立时间和服务管辖范围。RPKI(Resource Public Key Infrastructure,互联网码号资源公钥基础设施)资料库负责存储这些承载了INR(Internet Number Resource,互联网码号资源)分配/授权信息的RC(Resource Certificate,资源证书)/ROA(Route OriginAuthorization,路由起源声明)等数字对象,供全球的RP下载。

[0003] RPKI由三大基本组件组成:CA(Certificate Authority,认证权威)、RP(Relying Party,依赖方)和repository(资料库)。这三大组件通过签发、传送、存储、验证各种数字对象来彼此协作,共同完成RPKI的功能。CA通过签发RC来表达INR分配关系,签发ROA来授权某个ISP(Internet Service Providers,互联网服务提供商)针对自己的一部分IP地址前缀发起源路由通告;RPKI资料库负责存储这些承载了INR分配/授权信息的RC/ROA等数字对象,供全球的RP下载;RP同步并验证RPKI证书和签名对象,并将其处理成IP地址前缀与ASN(autonomous system number,自治系统号)的真实授权关系并下放至AS边界路由器指导路由过滤,如图2所示。随着RPKI部署率越来越高,RPKI的数据量也逐渐增大,给RP的同步下载和验证传输等流程提出了效率挑战。

[0004] 目前主流RP采用的证书验证算法为全局验证。由于各种证书是有上下级的验证关系的、证书同级间的彼此也存在验证关系,一个证书修改可能会影响其他证书,所以当前主流证书验证算法是进行全局验证,即无论哪个证书有更新,都要把全部证书验证一遍,随着RPKI部署率提高,将会大大影响整个RP服务器效率。

发明内容

[0005] 基于此,有必要针对上述技术问题,本申请提供一种基于RPKI的证书链局部验证方法、系统及存储介质,根据证书间的特点,将证书链全局验证优化为局部验证,有效提升了RP服务器的性能。

[0006] 本发明的第一方面,提供了一种基于RPKI的证书链局部验证方法,包括:构建证书链的验证树结构,所述的验证树结构具有多个层级,各层级记录有一或多组存储证书文件,

包括:CER公钥证书文件、证书撤销列表文件、路由起源授权文件、资料清单文件中的多种;

[0007] RPKI的依赖方在检测到某组的存储证书文件有更新时,对需更新的所述存储证书关联的同组和/或其它各子节点的存储证书文件进行局部的验证和更新。

[0008] 进一步地,所述的局部的验证和更新包括:当检测到有CER公钥证书文件更新时,先在所述证书链的验证树结构中查询定位到需更新CER公钥证书文件所在的组,验证和更新对应的CER公钥证书文件,以及验证和更新由所述CER公钥证书文件签发的其它各子节点的存储证书文件。

[0009] 进一步地,所述的局部的验证和更新包括:当检测到有资料清单文件更新时,先在所述证书链的验证树结构中查询定位到需更新资料清单文件所在的组,验证和更新对应的资料清单文件,以及同组的CER公钥证书文件和证书撤销列表文件。

[0010] 进一步地,所述的局部的验证和更新包括:当检测到有证书撤销列表文件更新时,先在所述证书链的验证树结构中查询定位到需更新撤销列表文件所在的组,验证和更新对应的撤销列表文件,以及同组的CER公钥证书文件和资料清单文件。

[0011] 进一步地,所述的局部的验证和更新包括:当检测到有路由起源授权文件更新时,先在所述证书链的验证树结构中查询定位到需更新路由起源授权文件所在的组,验证和更新对应的路由起源授权文件。

[0012] 进一步地,若对资料清单文件和证书撤销列表文件进行更新时,同组的CER公钥证书文件出现变化,则对所述CER公钥证书文件签发的其它各子节点的存储证书文件也进行验证更新。

[0013] 进一步地,若对证书撤销列表文件进行更新时,同组的资料清单文件若出现变化,则对同组的所述资料清单文件也进行更新。

[0014] 本发明的第二方面,提供了一种基于RPKI的证书链局部验证系统,包括:

[0015] 证书链构建模块,用于构建证书链的验证树结构,所述的验证树结构具有多个层级,各层级记录有多组存储证书文件,包括:CER公钥证书文件、证书撤销列表文件、路由起源授权文件、资料清单文件中的多种;

[0016] 检测更新模块,RPKI的依赖方在检测到某层级的某组的存储证书文件有更新时,对需更新的所述存储证书关联的同组和/或其它各子节点的存储证书文件进行局部的验证和更新。

[0017] 本发明的第三方面,提供了一种计算机可读存储介质,其上存储有计算机程序,所述计算机程序被处理器执行时实现如本发明第一方面所述的方法之一。

[0018] 本发明所提供的基于RPKI的证书链局部验证方法、系统及存储介质,利用证书链的结构与树的结构十分相似的特点,通过构建证书链验证树与存储证书之间的关系,记录每个CER(存储公钥证书的文件格式,代表CA证书)、CRL(certificate revocation list,证书撤销列表),ROA(Route Origin Authorization,路由起源授权),MFT(Manifest,资料清单)文件,并在RP有证书更新时,只需进行局部验证更新,而无需进行全局验证更新,减少了所需验证的证书总数量,减少了验证时间,并且没有遗漏真正需要验证的证书,未降低验证质量,显著提升了RP服务器的性能。

附图说明

[0019] 图1为本现有技术中的五大RIR机构的列表图。

[0020] 图2为本现有技术中的RPKI整体架构及运行机制示意图

[0021] 图3为本发明实施例中的证书链的验证树结构的示意图。

[0022] 图4为本发明实施例中的当前RP依赖方采用的证书链全局验证方法的示意图。

[0023] 图5为本发明实施例中的更新CER文件的示意图。

[0024] 图6为本发明实施例中的更新MFT或CRL文件的示意图。

[0025] 图7为本发明实施例中的更新ROA文件的示意图。

具体实施方式

[0026] 为了使本申请的目的、技术方案及优点更加清楚明白,以下结合附图及实施例,对本申请进行进一步详细说明。应当理解,此处描述的具体实施例仅仅用以解释本申请,并不用于限定本申请。此外,为了清楚和简洁,省略对公知功能和结构的描述。

[0027] 本文使用的术语仅用于描述本发明的各种实施例,而不旨在限制本发明。除非上下文另有明确指示,否则单数形式旨在包括复数形式。在本发明中,应理解,术语“包括”或“具有”指示特征、数字、步骤、操作、元件、部件或其组合的存在,并且不排除一个或更多个其它特征、数字、步骤、操作、元件、部件或其组合的存在,或添加一个或更多个其它特征、数字、步骤、操作、元件、部件或其组合的可能性。

[0028] 实施例一

[0029] 考虑到证书链的结构与树的结构十分相似,所以可以构建证书链验证树以存储证书之间的关系,记录每个CER、MFT、CRL、ROA文件,如图3所示的为本申请所构建的证书链的验证树结构,其具有根节点root,从根节点之后按照层级划分,而每一层级则形成一组或多组子节点,如二级节点包括MFT(Manifest,资料清单)文件、CER(存储公钥证书的文件格式,代表CA证书)、CRL(certificate revocation list,证书撤销列表)文件,除根节点和最末级节点外,其它层级均由CER、CRL、MFT文件组成,末级节点包含ROA文件、MFT和CRL文件,其中,ROA文件仅存在于最末级层级中。由于下级的子节点所签发的一些存储证书文件依赖上一层级所在组的CER证书文件,由此可形成树状的多层级验证结构。目前主流RP采用的证书验证算法为全局验证。由于各种证书是有上下级的验证关系的、证书同级间的彼此也存在验证关系,一个证书修改可能会影响其他证书,所以当前主流证书验证算法是进行全局验证,即无论哪个证书有更新,都要把全部证书验证一遍,如图4所示,当某层级的CER文件有更新时,其上的节点、同级的节点、其下的节点中包含的各个存储证书文件全部一一进行更新,如此大大增加了验证时间。

[0030] 本发明的实施例一提供了一种基于RPKI的证书链局部验证方法,旨在根据存储证书间的特点,发现在某存储证书更新时,其实并不需要对整个证书链进行全局验证,而是可以通过与该更新存储证书有关的局部证书间的更新验证即可完成,故提出一种证书链验的局部验证方法,将证书链全局验证优化为局部验证,进而减少验证时间,以有效提升RP服务器的性能。

[0031] 参照图3所示,构建完成的证书链的验证树结构具有多个层级,各层级记录有多种存储证书文件,包括:CER公钥证书文件、证书撤销列表文件、路由起源授权文件、资料清单

文件中的多种;

[0032] RPKI的依赖方(RP)在检测到某层级的存储证书文件有更新时,对需更新的所述存储证书关联的同组和/或其它各子节点的存储证书文件进行局部的验证和更新。

[0033] 具体来说,证书的更新涉及到四种情况,也即CER公钥证书文件的更新、证书撤销列表文件的更新、路由起源授权文件的更新、资料清单文件的更新,针对不同的存储证书更新,进行不同情况的局部更新。

[0034] 如图5所示,假设检测到某层级的某组的CER(存储公钥证书的文件格式)文件更新,因为CER代表CA证书,所以当某CER文件更新时不仅涉及到它自身,还涉及到它所签发的子CER/CRL/ROA/MFT文件,则先在证书链验证树中找到该层级对应组的CER文件,验证并更新对应CER文件,同时验证并更新由其签发的其他层级的CER/CRL/ROA/MFT文件即可,与该CER文件同层级的其它组的CER/CRL/ROA/MFT文件则无需更新,如图5中三角形虚线框的部分为需要更新的部分。

[0035] 如图6所示,假设检测到某层级的某组的MFT(Manifest,资料清单)文件更新,因为MFT代表资料清单,其中包含存储库发布点中与负责在存储库中发布的机构关联的所有已签名对象(文件)的列表。即当有MFT文件更新时,先在证书链验证树中找到某层级某组对应的MFT文件,验证并更新对应MFT文件及其同级同组的CER和CRL文件(MFT文件的更新通常会带来CER文件和CRL文件的更新),若同级CER文件发生变化后,则和图5所示的CER文件更新过程相同,也即更新该组下的对应CER文件及其签发的其它各子节点的CER/CRL/ROA/MFT文件,此外,若同层级的同组的CRL文件有变化则更新本组对应的CRL文件即可,如图6中椭圆形虚线框的部分为需要更新的部分。

[0036] 再请参照如图6所示,和前述更新MFT文件类似的,当检测到某层级的某组的CRL(certificate revocation list,证书撤销列表)文件更新,因为CRL代表证书撤销列表,它列出存储库中被认为不能再使用的证书的序列号,所以当有CRL文件更新时,先在证书链验证树中找到对应的CRL文件,验证并更新对应CRL文件及其同级同组的CER和MFT文件(CRL文件的更新通常会带来CER文件和MFT文件的更新),若同级CER文件有变化,则和图5所示的CER文件更新过程相同,也即更新该组下的对应CER文件及其签发的其它各子节点的CER/CRL/ROA/MFT文件,此外,若同级同组的MFT文件有变化则更新对应MFT文件即可。

[0037] 参照图7所示,当检测到是ROA(Route OriginAuthorization,路由起源授权)文件更新时,ROA是一种加密签名的对象,表示授权哪个自治系统(AS)来生成特定IP地址前缀或一组前缀。它的更新不会影响其它证书文件,所以当有ROA文件更新时,只需在证书链验证树中找到对应的ROA文件并进行验证更新即可,如图7中仅对最末级圆形虚线框出的部分为需要更新的部分。

[0038] 本申请实施例一提供的基于RPKI的证书链局部验证方法,通过构建证书链验证树以存储证书之间的关系,存储证书之间的上下级以及同级之间的关系,使得在证书插入删除或者更新时,更快找到需要插入删除或者更新的证书,消耗的资源和代价更小,每个层级通过记录的CER、CRL、ROA、MFT文件,并在RP有证书更新时,只需根据证书链验证树结构关系,进行局部验证更新,而无需进行全局验证更新,减少了所需验证的证书总数量,减少了验证时间,并且没有遗漏真正需要验证的证书,未降低验证质量,显著提升了RP服务器的性能。

[0039] 实施例二

[0040] 本发明的实施例二提供了一种基于RPKI的证书链局部验证系统,包括:

[0041] 证书链构建模块,用于构建证书链的验证树结构,所述的验证树结构具有多个层级,各层级记录有一或多组存储证书文件,每组包括:CER公钥证书文件、证书撤销列表文件、路由起源授权文件、资料清单文件中的多种,其中,路由起源授权文件仅存在于最末级;

[0042] 检测更新模块,RPKI的依赖方在检测到某层级的某组的存储证书文件有更新时,对需更新的所述存储证书关联的同组和/或其它各子节点的存储证书文件进行局部的验证和更新。

[0043] 关于本实施例基于RPKI的证书链局部验证系统的具体限定可以参见上文中对于基于RPKI的证书链局部验证方法的限定,在此不再赘述。上述基于RPKI的证书链局部验证系统中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中,也可以以软件形式存储于计算机设备中的存储器中,以便于处理器调用执行以上各个模块对应的操作。

[0044] 实施例三

[0045] 本发明的实施例三,提供了一种计算机可读存储介质,存储有计算机程序,计算机程序被处理器执行时,使得处理器执行上述基于RPKI的证书链局部验证方法的步骤。此处基于RPKI的证书链局部验证方法的步骤可以是上述各个实施例的基于RPKI的证书链局部验证方法中的步骤:构建证书链的验证树结构,所述的验证树结构具有多个层级,各层级记录有一或多组存储证书文件,包括:CER公钥证书文件、证书撤销列表文件、路由起源授权文件、资料清单文件中的多种;RPKI的依赖方在检测到某组的存储证书文件有更新时,对需更新的所述存储证书关联的同组和/或其它各子节点的存储证书文件进行局部的验证和更新。

[0046] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程,是可以通过计算机程序来指令相关的硬件来完成,所述的计算机程序可存储于一非易失性计算机可读取存储介质中,该计算机程序在执行时,可包括如上述各方法的实施例的流程。其中,本申请所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用,均可包括非易失性和/或易失性存储器。非易失性存储器可包括只读存储器(ROM)、可编程ROM(PROM)、电可编程ROM(EPROM)、电可擦除可编程ROM(EEPROM)或闪存。易失性存储器可包括随机存取存储器(RAM)或者外部高速缓冲存储器。作为说明而非局限,RAM以多种形式可得,诸如静态RAM(SRAM)、动态RAM(DRAM)、同步DRAM(SDRAM)、双数据率SDRAM(DDRSDRAM)、增强型SDRAM(ESDRAM)、同步链路(Synchlink)DRAM(SLDRAM)、存储器总线(Rambus)直接RAM(RDRAM)、直接存储器总线动态RAM(DRDRAM)、以及存储器总线动态RAM(RDRAM)等。

[0047] 以上所述实施例仅表达了本申请的几种实施方式,其描述较为具体和详细,但并不能因此而理解为对发明专利范围的限制。应当指出的是,对于本领域的普通技术人员来说,在不脱离本申请构思的前提下,还可以做出若干变形和改进,这些都属于本申请的保护范围。因此,本申请专利的保护范围应以所附权利要求为准。

RIR	成立时间	服务管辖范围
RIPE NCC：The Réseaux IP Européens Network Coordination Center	1992	欧洲、俄罗斯、中东和亚洲中部
APNIC：Asia-Pacific Network Information Center	1993	亚洲、澳大利亚、新西兰和邻接国家
ARIN：American Registry for Internet Numbers	1997	美国、加拿大、加勒比海部分地区以及南极洲
LACNIC：Latin America and the Caribbean Network Information Center	2002	拉丁美洲和加勒比海部分地区
AfriNIC：Africa Internet Network Information Center	2005	非洲

图1

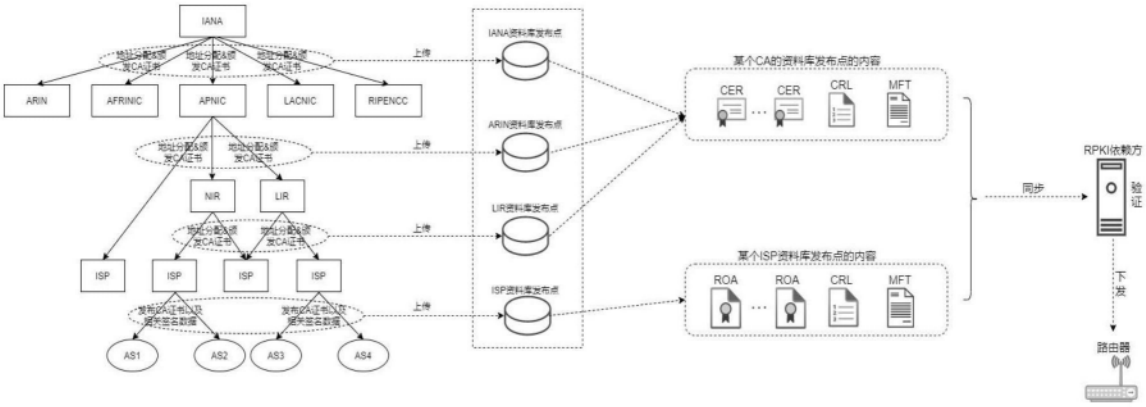


图2

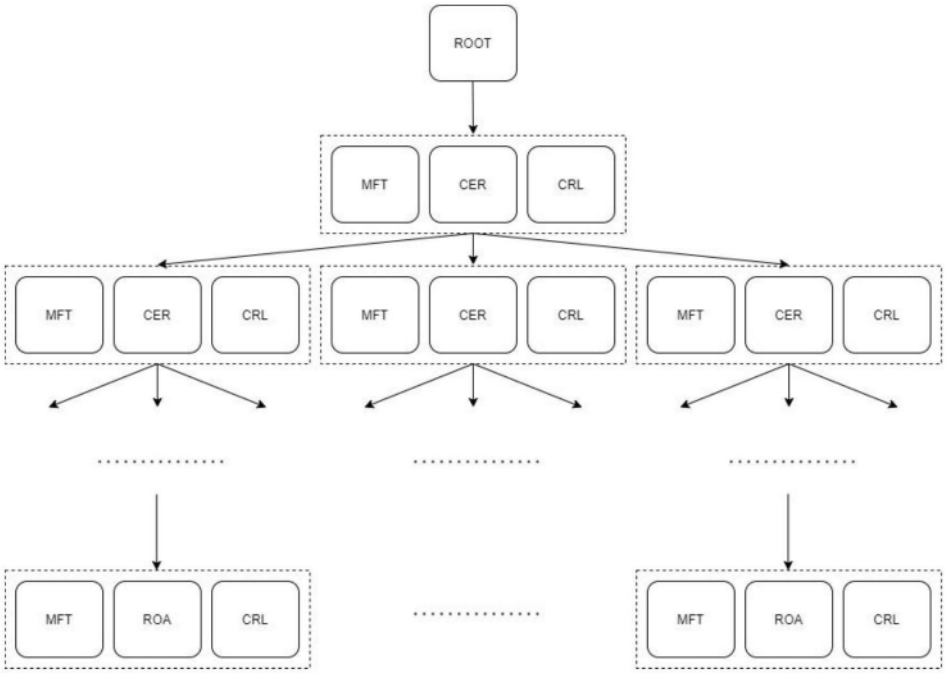

ROOT
MFT
CER
CRL
MFT
CER
CRL
MFT
CER
CRL
MFT
CER
CRL
MFT
ROA
CRL
MFT
ROA
CRL

图3

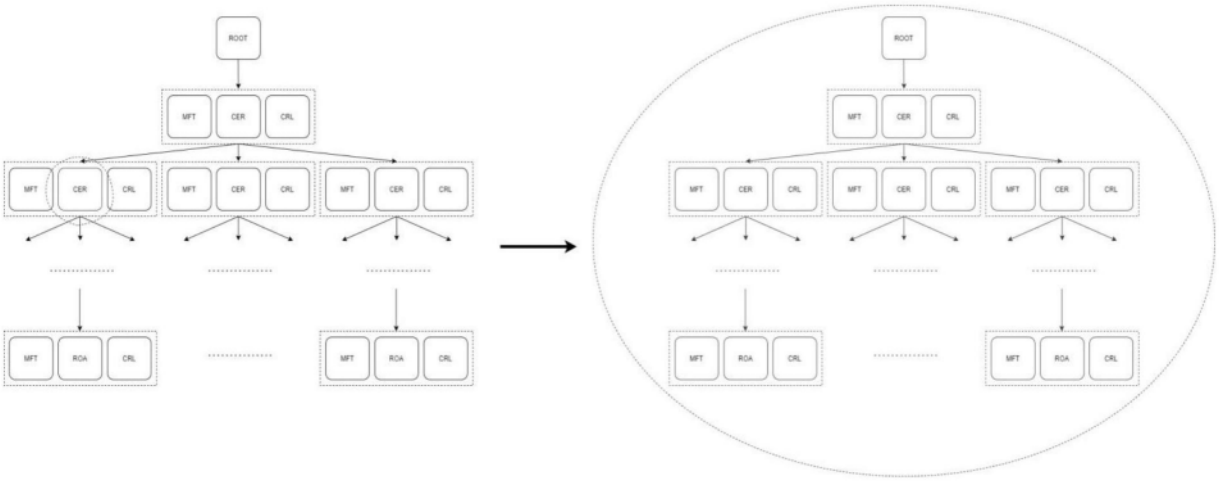


图4

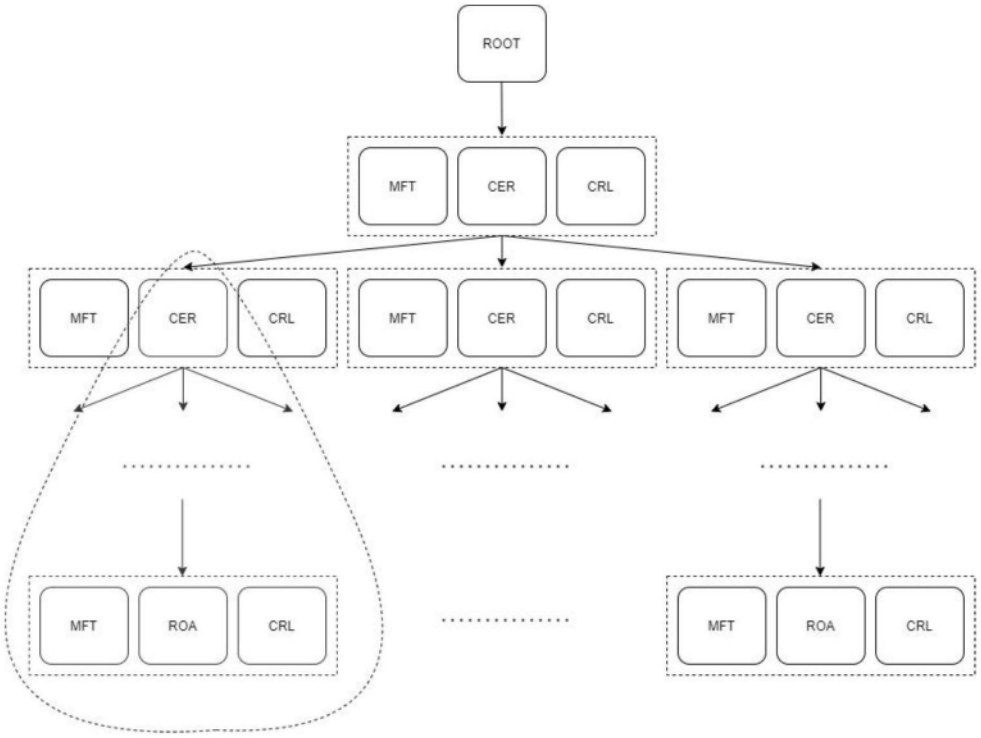

ROOT
MFT
CER
CRL
MFT
CER
CRL
MFT
CER
CRL
MFT
CER
CRL
MFT
ROA
CRL
MFT
ROA
CRL

图5

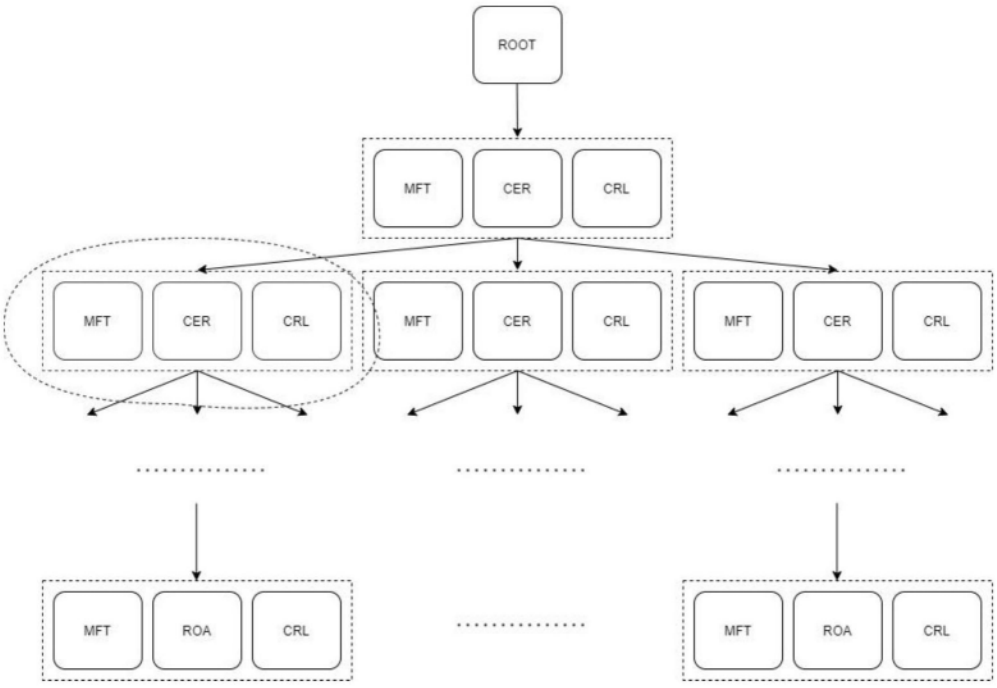

ROOT
MFT
CER
CRL
MFT
CER
CRL
MFT
CER
CRL
MFT
CER
CRL
MFT
ROA
CRL
MFT
ROA
CRL

图6

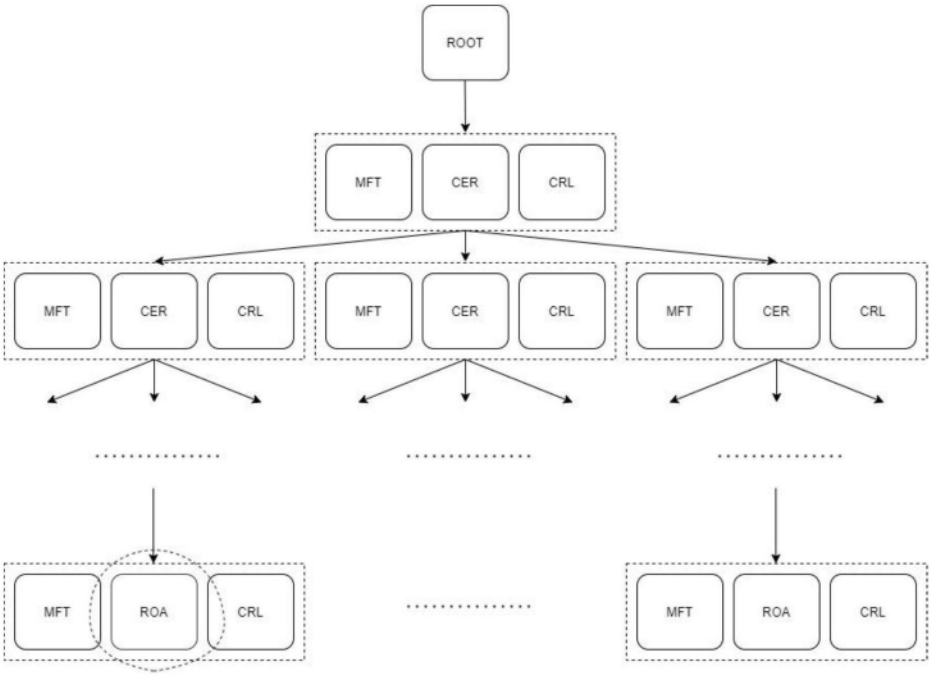

ROOT
MFT
CER
CRL
MFT
CER
CRL
MFT
CER
CRL
MFT
CER
CRL
MFT
ROA
CRL
MFT
ROA
CRL

图7