(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106295377 A
(43)申请公布日 2017.01.04

(21)申请号 201610722989.6

(22)申请日 2016.08.24

(71)申请人 成都万联传感网络技术有限公司
地址 610041 四川省成都市高新区紫荆北路55号

(72)发明人 李志蜀 金虎 杨春 邓仁彬

(74)专利代理机构 成都睿道专利代理事务所（普通合伙）51217
代理人 潘育敏

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/62(2013.01)

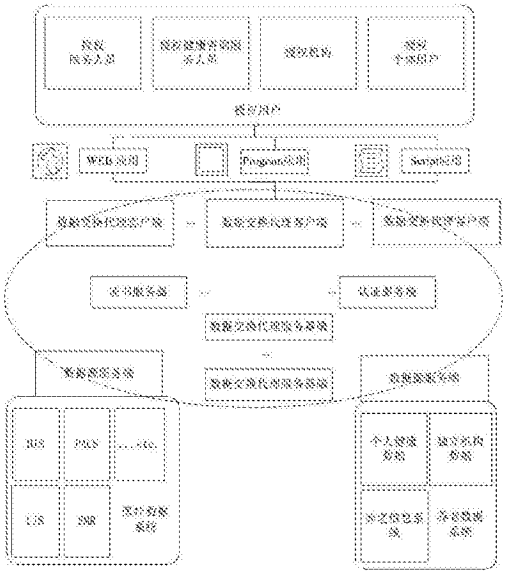
权利要求书6页 说明书13页 附图4页

(54)发明名称

一种医疗养老数据安全交换代理装置及其构建方法

(57)摘要

本发明公开了一种医疗养老数据安全交换代理装置及其构建方法。在医疗数据系统和养老数据系统之间构建第三方的医疗养老数据交换代理装置，装置由数据交换代理装置，认证代理装置，安全数据传输模块三部分构成。采用半双工服务模式进行数据的双向交换，有效隔离非授权数据的存取；通过数据交换代理服务器端形成医疗养老异构系统中数据交换隔离带，针对异构系统不同的分级存取权限形成映射关系，增强数据交换的灵活性和医疗、养老数据孤岛系统的互联；在处理流程的各步骤中，综合使用加密、认证、分级授权的技术手段。本发明将异构的医疗和养老数据系统安全整合在一起，对建立基于广域网的医疗养老服务应用扩展有非常积极的意义。



CN 106295377 A

1.一种医疗养老数据安全交换代理装置,其特征在于:

在医疗数据系统和养老数据系统之间构建第三方的医疗养老数据交换代理装置,在医疗数据系统和养老数据系统的异构数据系统之间形成隔离层;医疗养老数据安全交换代理装置采用单向的半双工服务模式,进行医疗养老数据的双向交换;

设置数据交换代理服务器端形成医疗养老异构系统中数据交换的数据交换代理服务器隔离带,设置数据交换映射表将数据服务源的存取从请求客户端独立出来,提高医疗、健康异构数据系统存取的安全性;

医疗养老数据安全交换代理装置由数据交换代理装置(20),认证代理装置(10),安全数据传输模块(30)构成;

数据交换代理装置(20)部件包括:数据交换代理服务器端(21)、数据交换代理客户端(22)、数据源服务端(24)、数据交换映射表(23);

认证代理装置(10)部件包括:证书服务器(11)、认证服务端(12)、节点信息库(13);

安全传输模块(30)部件包括:安全传输协议模块(31)、加解密子例程模块(32);

所述数据交换代理装置(20)中的部件为独立的运行节点,数据交换代理服务器端(21)一直保持网络在线,固定接收和响应特定的医疗养老数据服务请求,完成对授权客户端的数据请求响应;数据交换代理客户端(22)安装于实施医疗养老服务业务的客户端,业务应用程序向数据交换代理服务器端发起数据请求,并由数据交换代理客户端实现所需数据的接收并上传回业务应用程序;数据源服务端(24)分别安装在医疗数据系统和养老数据系统端,接受数据交换代理服务器的数据请求,建立起单向数据传输通道,将请求的应答数据发回数据交换代理客户端;数据交换映射表(23)根据医疗数据标准和健康数据标准制定内部的编码对应;

所述认证代理装置(10)中,证书服务器模块(11)负责为每一个合法的用户,包括数据交换代理客户端、数据交换代理服务器端、数据源服务端分配一个包含用户唯一识别号与用户公钥的证书,并负责证书的更新等相关服务;认证服务端模块(12)在本地服务器端数据库存储证书,作为证书认证服务代理,接收客户端的证书交换与验证请求,验证用户有效性,并将验证结果返回数据交换代理服务器节点;节点信息 库(13)根据医疗数据系统、养老数据系统提供的用户信息,形成企业级的用户信息表,以供认证服务器验证用户有效性时使用,并包含了用户间的数据存取权限的映射信息;

安全传输模块(30)中,安全传输协议模块(31)为企业内部制定的异构节点间采用的数据传输规则,设计并实现在网络通信的应用层上,用于获得面向状态连接的额外通信安全验证,包括逻辑通信链路的保持时间、校验设置、重传机制,加解密子例程模块(32)为公共服务进程,由医疗养老数据交换代理装置各个组件在进行网络数据通信过程中调用。

2.如权利要求1所述的医疗养老数据安全交换代理装置,其特征在于:所述数据交换代理装置(20)的安装部署按数据交换代理服务器端和数据交换代理客户端分别部署;数据源服务端(24)配置有数据缓存;认证服务端模块(12)配置有节点信息库维护内容。

3.如权利要求1所述的医疗养老数据安全交换代理装置,其特征在于:当医疗养老数据安全交换代理装置,应用在大规模的并发医疗养老数据交换处理时,数据交换代理装置(20)部件为多个的分布式服务结构。

4.一种采用如权利要求1所述的基于多安全防护的医疗养老数据安全交换代理装置的

构建方法，其特征在于：

在医疗数据系统和养老数据系统之间构建第三方的医疗养老数据交换代理装置，在医疗数据系统和养老数据系统的异构数据系统之间形成隔离层；通过第三方软件代理和企业认证方式，降低异构数据系统间数据的直接共享或交换的耦合性，提高医疗养老数据访问的灵活性，保证异构系统间数据存取的合法性和安全性验证；

医疗养老数据安全交换代理装置将医疗养老数据的双向交换模式，设计为单向的半双工服务模式，有效隔离非授权数据的存取，增强数据请求端的安全性；通过数据交换代理服务器端(20)形成医疗养老异构系统中数据交换隔离带，针对异构系统不同的分级存取权限形成映射关系，增强数据交换的灵活性和医疗、养老数据孤岛系统的互联；在处理流程的各步骤中，综合使用加密、认证、分级授权的技术手段，构建起医疗养老数据安全交换代理；

医疗养老数据安全交换代理装置为有医疗养老数据交换需求的业务应用，通过Script脚本、Program应用程序、Web应用方式激活数据交换代理客户端，用以代理数 据交换业务实施，数据交换代理客户端通过与应用系统进行验证，确认用户的合法性和有效性，并将数据交换请求发送至对应的数据交换代理服务器端，发起进一步的数据交换代理请求；数据交换代理服务器端将数据交换代理客户端信息一并提交认证服务端，验证数据交换代理请求的有效性；验证成功后，数据交换代理服务器端查找匹配的异构数据服务提供端，并与对应的数据源服务端进行协议验证，验证成功后数据交换代理客户端与数据源服务端形成安全数据传输通道，由数据源服务端从异构数据源系统中获取所需数据并发送至数据交换代理客户端；数据交换代理客户端取得所需数据后，馈入业务应用，完成医疗养老数据交换的代理流程；

医疗养老数据安全交换代理装置由数据交换代理装置(20)，认证代理装置(10)，安全传输模块(30)共同完成基于多安全防护的医疗养老数据交换代理：

在数据交换代理装置(20)中，数据交换代理服务器端(21)设计为一直保持网络在线，固定接收和响应特定的医疗养老数据服务请求，并负责完成对授权客户端的数据请求响应服务功能；数据交换代理客户端(22)设计安装于实施医疗养老服务业务的客户端，业务应用程序向数据交换代理服务器端发起数据请求，并由数据交换代理客户端实现所需数据的接收并上传回业务应用程序；数据源服务端(24)分别安装在医疗数据系统和养老数据系统端，接受数据交换代理服务器的数据请求，数据请求包含企业级认证确认、内部安全通信协议；建立起单向数据传输通道，将请求的应答数据发回数据交换代理客户端；数据交换映射表(23)按照医疗养老数据交换规则设定，根据医疗数据标准和健康数据标准制定内部的编码对应，根据业务需求，为新用户提供方便灵活的非标数据表达转换；

在认证代理装置(10)负责医疗养老数据安全交换中的合法节点认证相关工作，为数据交换代理装置的独立功能模块，包含了与其他功能模块中部件的交互；证书服务器模块(11)为自定义的企业级证书机构，负责为每一个合法的用户，包括数据交换代理客户端、数据交换代理服务器端、数据源服务端分配一个包含用户唯一识别号与用户公钥的证书，证书服务器除证书的发放外，还负责证书的更新相关服务；认证服务端模块(12)在本地服务器端数据库存储证书，作为证书认证服务代理，接收客户端的证书交换与验证请求，验证用户有效性，并将验证结果返回数据交换代理服务器节点；节点信息库模块(13)根据医疗信息系统、健康信息系统提供的用户信息，形成企业级的用户信息表，以供认证服务器验证用

户有效性时使用,并包含了用户间 的数据存取权限的映射信息;

在安全传输模块(30)中:安全传输协议模块(32)采用企业内部制定的异构节点间的数据传输规则,设计并实现在网络通信的应用层上,用于获得面向状态连接的额外通信安全验证,包括逻辑通信链路的保持时间、校验设置、重传机制;加解密子例程模块(31)为公共服务进程,由医疗养老数据交换代理装置中各个组件在进行网络数据通信过程中调用。

5.如权利要求4所述的医疗养老数据安全交换代理装置的构建方法,其特征在于:所述数据交换代理装置(20)中,数据交换代理服务器端(21)处理流程是:

步骤1.数据交换代理服务器端为服务器节点式配置;

步骤2.数据交换代理服务器端获取证书;

若本地已有证书则转入步骤3;

步骤2.1查找网络上企业认证(CA)节点;

步骤2.2向企业证书服务器节点发起证书请求;

a.若请求成功则转入步骤2.3,

b.若请求失败则重复步骤2.2;

步骤2.3传输本节点的唯一标记UID至认证服务器;

a.若获得证书则本地存储,以供服务重启后使用,并转入步骤3,

b.若证书获取失败则标记失效状态,生成错误日志并退出;

步骤3.启动医疗养老数据监听服务直到有数据交换代理客户端接入;

///处理数据交换代理工作

步骤3.1启动子进程执行数据代理服务;

步骤3.2对数据交换代理客户端的CA验证;

a.验证成功进入步骤3.3,

b.验证失败生成错误日志,重置连接,转入步骤3;

步骤3.3查找对应数据源服务端并发起连接请求

a.连接成功进入步骤3.4,

b.连接失败生成错误日志,向数据交换代理客户端发送错误信息,并重置连接,转入步骤3;

步骤3.4与数据源服务端交换证书,双方验证合法性;

a.验证成功转入步骤3.5,

b.验证失败生成错误日志,重置与数据源服务端连接,向数据交换代理客户端发送错误信息,并重置连接,转入步骤3;

步骤3.5解析数据交换代理客户端报文信息,包括密文数据和解密,查找医疗养老数据交换映射表,按转换规则组装异构系统数据请求所需报文信息,向数据源服务端发送数据请求;

a.响应成功转入步骤4;

b.响应失败生成错误日志,重置与数据源服务端连接,向数据交换代理客户端发送错误信息,并重置连接,转入步骤3;

步骤4.进入安全传输处理流程;

步骤5.安全传输结束,终止当前子进程,转入步骤3;

数据交换代理客户端(22)的处理流程如下:

步骤1.数据交换代理客户端获取证书;

若本地已有证书则转入步骤1.1;

步骤1.1查找网络上企业认证(CA)节点,

步骤1.2向企业认证节点发起证书请求:

a.若请求成功则转入步骤1.3,

b.若请求失败则重复步骤1.1;

步骤1.3传输本节点的唯一标记UID至认证服务器;

a.若获得证书则本地存储,以供服务重启后使用,并转入步骤2,

b.若证书获取失败则标记失效状态,生成错误日志并退出;

步骤2.处理医疗养老数据交换请求的客户端工作:

步骤2.1接受本地用户登录请求:

步骤2.2本地验证用户的身份和数据存取权限;

a.验证成功进入步骤2.3,

b.验证失败生成错误日志,转入步骤2.1;

步骤2.3接受用户的异构数据请求;

步骤2.4查找数据交换映射表,将用户信息与数据请求信息按转换规则组装异构系统数据请求所需报文信息;

步骤2.5查找数据交换代理服务器端并发起连接请求:

a.连接成功则进入步骤2.6,

b.连接失败生成错误日志,转入步骤2;

步骤2.6与数据交换代理服务端交换证书验证:

a.验证成功进入步骤2.7,

b.验证失败生成错误日志,转入步骤2;

步骤2.7向数据交换代理服务器端提交加密后的报文信息;

步骤2.8接收数据交换代理服务器端的响应:

a.响应成功转入步骤3,

b.响应失败生成错误日志,转入步骤2;

步骤3进入安全传输处理流程;

步骤4安全传输结束,转入步骤2;

数据源服务端(24)提供下述几方面的功能:(1).接受数据交换服务代理的数据请求;(2).与本地数据库或数据服务进程交互,获得所需应用数据;(3).以安全传输模式向数据交换代理客户端实施单向数据传输服务,具体的处理流程如下:

步骤1数据源服务端在数据源端作为服务进程启动;

步骤2数据源服务端获取证书;

若本地已有证书则转入步骤3;

步骤2.1查找网络上企业认证(CA)节点;

步骤2.2向企业证书服务器节点发起证书请求:

a.若请求成功则转入步骤2.3,

b.若请求失败则重复步骤2.2：

步骤2.3传输本节点的唯一标记UID至认证服务器：

a.若获得证书则本地存储,以供服务重启后使用,并转入步骤3,

b.若证书获取失败则标记失效状态,生成错误日志并退出；

步骤3启动医疗养老数据监听服务直到有数据交换代理服务器端接入；

步骤3.1启动子进程执行数据代理服务；

步骤3.2对数据交换代理服务器端交换证书：

a.验证成功进入步骤3.3,

b.验证失败生成错误日志,向请求端发送错误消息,重置与数据交换代理服务器端的连接,并转入步骤3；

步骤3.3接收数据交换代理服务器端的数据请求,解析报文：

a.在数据缓存区搜索数据,获得数据后转入步骤3.4,

b.向源数据库或本地数据服务进程请求数据,获得数据后转入步骤3.4

c.从数据源获取数据失败,生成错误日志,向请求端发送错误消息,重置连接,转入步骤3

步骤3.4向数据交换代理客户端发起验证协议

a.验证成功转向步骤4

b.验证失败生成错误日志,重置与数据交换代理服务器端的连接,转入步骤3；

步骤4与数据交换代理客户端建立单向数据传输通路,调用加密子例程向数据交换代理客户端发送数据；

步骤5数据传输结束,终止当前子进程,转入步骤2；

所述数据交换映射表(23)设定医疗数据数据系统和养老数据系统互通的交换规则,分别对数据规范和数据格式进行了设定;该映射表分为标准映射和扩展映射两个部分;标准映射是按照遵从“HLV7”和“健康档案基本架构与数据标准”的医疗信息系统数据源和健康数据源进行内部编码;扩展映射则是针对非上述标准的数据源进行的内部编码。

6.如权利要求4所述的基于多安全防护的医疗养老数据交换代理装置的构建方法,其特征在于:所述认证代理装置(10)中证书服务器(11)的处理流程如下:

步骤1.监听网络证书服务请求；

步骤2.查找节点信息库,验证是否是授权用户节点；

若非授权用户则生成错误日志,重置连接,转至步骤1

步骤3.证书生成处理：

a.获得用户UID及相关信息并为其制作证书(.CER)《

b.将证书发送至证书请求节点,转入步骤1；

认证服务端(12)处理流程如下：

步骤1.监听认证服务请求；

步骤2.生成子进程响应数据交换代理服务器端的验证请求信息：

a.验证请求信息中证书的有效性,

b.验证不通过生成错误日志,向数据交换代理服务器端发送错误信息,重置连接,转入步骤1,

c.验证通过向数据交换代理服务器端发送确认信息，

d.继续响应数据交换代理服务器端后续的用户权类型和数据存取权限的验证请求。

7.如权利要求4所述的医疗养老数据安全交换代理装置的构建方法，其特征在于：所述安全传输模块(30)设置在网络应用层之上，用以保证通信链路上医疗养老数据传输的安全：在安全传输协议模块(32)制定异构节点间点到点的传输状态规则，传输节点间协商临时通信信道上的可靠数据传输的应用规则；加解密子例程模块(31)提供多种公开的密码算法代码库，包括DES算法、3DES算法、AES算法、RSA算法，以供通信双方在传输协议确定后执行具体的加解密操作，其中，公钥RSA算法用于密钥管理、证书管理功能模块中。

一种医疗养老数据安全交换代理装置及其构建方法

一、技术领域

[0001] 本发明涉及异构医疗养老信息系统之间的数据安全交换，特别是针对开放个人医疗养老数据与严格分级访问的医疗数据间的信息交换，涉及安全的认证管理与分级数据交换的保护方法，具体是一种医疗养老数据安全交换代理装置及其构建方法。

二、背景技术

[0002] 随着我国老龄化速度的急剧升高，老龄化人口规模增大，其中高龄、失能老龄化人口也迅速增加。在增长迅速的老龄人口基数下，老年人中患病率也逐年升高，各类典型老年慢性病，如心血管、高血压、糖尿病、老年退性关节病、眼疾、呼吸系统疾病等成为导致老年人生活质量下降的一个重要因素。在我国目前的养老服务体系中，“居家养老为基础、社区养老为依托、机构养老为支撑的社会养老服务体系”的核心纲领下，主要构建90％由家庭自我照顾，7％享受社区居家养老服务，3％由机构代为照顾养老的9073养老服务模式。而无论哪种养老服务模式，将医疗服务有效引入到养老服务中，都将是医疗养老结合需实现的主要目标。在信息基础建设已日益完善的现代社会，借助于信息化手段拓宽医疗服务的方式和服务范围是将医疗服务引入养老服务的有效途径。在专业医护人员参与下实施的远程医疗咨询服务、远程医护监控、远程医疗指导等都是医疗养老结合的典型方式。在信息化为基础的医疗养老结合服务模式中，医疗和养老数据的互通和共享也就成为信息化的关键问题。信息处理中，对数据的共享和交换一般都不存在技术问题，但对于医疗和养老数据则存有一定特殊性。(1)医疗、养老数据都具有很高的私密性；(2)事关个体的生命、健康安全，数据具有高可靠性、完整性和有效性要求；(3)医疗养老服务数据使用有较强的分级存取权限设定；(4)多样化养老服务模式与集中式医疗服务模式二者的数据管理上有较大差异，且医疗、养老数据一般从属于独立机构，有较强的性质壁垒和数据孤岛性。因此，构建一种多重安全防护的医疗养老数据交换代理装置，有效解决医疗养老一体化服务的数据共享问题已十分必要和紧迫。

三、发明内容

[0003] 本发明的目的是针对现有医疗养老结合信息化服务中，医疗、养老异构数据系统间缺乏有效、安全的数据共享和数据交换方法，提供一种医疗养老数据安全交换代理装置，通过第三方软件代理和企业认证方式，降低异构数据系统间数据的直接共享或交换的耦合性，提高医疗养老数据访问的灵活性，并保证异构系统间数据存取的合法性和安全性验证。交换代理装置将医疗养老数据的双向交换模式，设计为单向的半双工服务模式，形成安全的数据传输防护，以提升通信链路上数据的可靠性和安全性。交换代理服务装置在处理流程的各步骤中，综合使用加密、认证、分级授权的技术手段，进一步提升医疗养老数据交换的安全性。

[0004] 本发明的基本思路是在医疗、养老数据系统之间建立第三方的交换代理层，用于在异构信息系统之间形成隔离层，避免数据的直接耦合式共享和交换，降低直接耦合可能

导致的数据泄露风险。采用第三方的交换代理装置，还易于针对异构系统不同的分级存取权限形成映射关系，增强数据交换的灵活性，更适于医疗、养老这类传统上数据孤岛系统的互联。交换代理装置还考虑到医疗、养老数据交换往往具有不对称性。沿用该思路，将双向的数据交换采用单向的半双工传输结构代替，该设计思路可有效隔离非授权的数据存取，并增强数据请求端的安全性。

[0005] 发明的目的是这样达到的：在医疗数据系统和养老数据系统之间构建第三方的医疗养老数据交换代理装置，在医疗数据系统和养老数据系统的异构数据系统之间形成隔离层；医疗养老数据安全交换代理装置采用单向的半双工服务模式，进行医疗养老数据的双向交换。设置数据交换代理服务器端形成医疗养老异构系统中数据交换的数据交换代理服务器隔离带，设置数据交换映射表将数据服务源的存取从请求客户端独立出来，提高医疗、健康异构数据系统存取的安全性。

[0006] 医疗养老数据安全交换代理装置由数据交换代理装置，认证代理装置，安全数据传输模块构成。

[0007] 数据交换代理装置部件包括：数据交换代理服务器端、数据交换代理客户端、数据源服务端、数据交换映射表。认证代理装置部件包括：证书服务器、认证服务端、节点信息库。安全传输模块部件包括：安全传输协议模块、加解密子例程模块。

[0008] 所述数据交换代理装置中的部件为独立的运行节点，数据交换代理服务器端一直保持网络在线，固定接收和响应特定的医疗养老数据服务请求，完成对授权客户端的数据请求响应；数据交换代理客户端安装于实施医疗养老服务业务的客户端，业务应用程序向数据交换代理服务器端发起数据请求，并由数据交换代理客户端实现所需数据的接收并上传回业务应用程序；数据源服务端分别安装在医疗数据系统和养老数据系统端，接受数据交换代理服务器的数据请求，建立起单向数据传输通道，将请求的应答数据发回数据交换代理客户端；数据交换映射表根据医疗数据标准和健康数据标准制定内部的编码对应。

[0009] 所述认证代理装置中，证书服务器模块负责为每一个合法的用户，包括数据交换代理客户端、数据交换代理服务器端、数据源服务端分配一个包含用户唯一识别号与用户公钥的证书，并负责证书的更新等相关服务；认证服务端模块在本地服务器端数据库存储证书，作为证书认证服务代理，接收客户端的证书交换与验证请求，验证用户有效性，并将验证结果返回数据交换代理服务器节点；节点信息库根据医疗数据系统、养老数据系统提供的用户信息，形成企业级的用户信息表，以供认证服务器验证用户有效性时使用，并包含了用户间的数据存取权限的映射信息。

[0010] 安全传输模块中，安全传输协议模块为企业内部制定的异构节点间采用的数据传输规则，设计并实现在网络通信的应用层上，用于获得面向状态连接的额外通信安全验证，包括逻辑通信链路的保持时间、校验设置、重传机制，加解密子例程模块为公共服务进程，由医疗养老数据交换代理装置各个组件在进行网络数据通信过程中调用。

[0011] 所述数据交换代理装置的安装部署，按数据交换代理服务器端和数据交换代理客户端分别部署；数据源服务端配置有数据缓存；认证服务端模块配置有节点信息库维护内容。

[0012] 当医疗养老数据安全交换代理装置应用在大规模的并发医疗养老数据交换处理时，数据交换代理装置部件为多个的分布式服务结构。

[0013] 一种医疗养老数据安全交换代理装置的构建方法，其特征在于：在医疗数据系统和养老数据系统之间构建第三方的医疗养老数据交换代理装置，在医疗数据系统和养老数据系统的异构数据系统之间形成隔离层；通过第三方软件代理和企业认证方式，降低异构数据系统间数据的直接共享或交换的耦合性，提高医疗养老数据访问的灵活性，保证异构系统间数据存取的合法性和安全性验证。

[0014] 医疗养老数据安全交换代理装置将医疗养老数据的双向交换模式，设计为单向的半双工服务模式，有效隔离非授权数据的存取，增强数据请求端的安全性；通过数据交换代理服务器端形成医疗养老异构系统中数据交换隔离带，针对异构系统不同的分级存取权限形成映射关系，增强数据交换的灵活性和医疗、养老数据孤岛系统的互联；在处理流程的各步骤中，综合使用加密、认证、分级授权的技术手段，构建起基于多安全防护的医疗养老数据交换代理。

[0015] 医疗养老数据安全交换代理装置为有医疗养老数据交换需求的业务应用，通过Script脚本、Program应用程序、Web应用方式激活数据交换代理客户端，用以代理数据交换业务实施，数据交换代理客户端通过与应用系统进行验证，确认用户的合法性和有效性，并将数据交换请求发送至对应的数据交换代理服务器端，发起进一步的数据交换代理请求；数据交换代理服务器端将数据交换代理客户端信息一并提交认证服务端，验证数据交换代理请求的有效性；验证成功后，数据交换代理服务器端查找匹配的异构数据服务提供端，并与对应的数据源服务端进行协议验证，验证成功后数据交换代理客户端与数据源服务端形成安全数据传输通道，由数据源服务端从异构数据源系统中获取所需数据并发送至数据交换代理客户端；数据交换代理客户端取得所需数据后，馈入业务应用，完成医疗养老数据交换的代理流程。

[0016] 医疗养老数据安全交换代理装置由数据交换代理装置，认证代理装置，安全传输模块共同完成基于多安全防护的医疗养老数据交换代理。

[0017] 在数据交换代理装置中，数据交换代理服务器端设计为一直保持网络在线，固定接收和响应特定的医疗养老数据服务请求，并负责完成对授权客户端的数据请求响应服务功能；数据交换代理客户端设计安装于实施医疗养老服务业务的客户端，业务应用程序向数据交换代理服务器端发起数据请求，并由数据交换代理客户端实现所需数据的接收并上传回业务应用程序；数据源服务端分别安装在医疗数据系统和养老数据系统端，接受数据交换代理服务器的数据请求，数据请求包含企业级认证确认、内部安全通信协议；建立起单向数据传输通道，将请求的应答数据发回数据交换代理客户端；数据交换映射表按照医疗养老数据交换规则设定，根据医疗数据标准和健康数据标准制定内部的编码对应，根据业务需求，为新用户提供方便灵活的非标数据表达转换。

[0018] 在认证代理装置负责医疗养老数据安全交换中的合法节点认证相关工作，为数据交换代理装置的独立功能模块，包含了与其他功能模块中部件的交互；证书服务器模块为自定义的企业级证书机构，负责为每一个合法的用户，包括数据交换代理客户端、数据交换代理服务器端、数据源服务端分配一个包含用户唯一识别号与用户公钥的证书，证书服务器除证书的发放外，还负责证书的更新相关服务；认证服务端模块在本地服务器端数据库存储证书，作为证书认证服务代理，接收客户端的证书交换与验证请求，验证用户有效性，并将验证结果返回数据交换代理服务器节点；节点信息库模块根据医疗信息系统、健康信

息系统提供的用户信息，形成企业级的用户信息表，以供认证服务器验证用户有效性时使用，并包含了用户间的数据存取权限的映射信息。

[0019] 在安全传输模块中：安全传输协议模块采用企业内部制定的异构节点间的数据传输规则，设计并实现在网络通信的应用层上，用于获得面向状态连接的额外通信安全验证，包括逻辑通信链路的保持时间、校验设置、重传机制；加解密子例程模块为公共服务进程，由医疗养老数据交换代理装置中各个组件在进行网络数据通信过程中调用。

[0020] 所述数据交换代理装置中，数据交换代理服务器端处理流程是：

[0021] 步骤1.数据交换代理服务器端为服务器节点式配置；

[0022] 步骤2.数据交换代理服务器端获取证书；

[0023] 若本地已有证书则转入步骤3；

[0024] 步骤2.1查找网络上企业认证(CA)节点；

[0025] 步骤2.2向企业证书服务器节点发起证书请求；

[0026] a.若请求成功则转入步骤2.3，

[0027] b.若请求失败则重复步骤2.2；

[0028] 步骤2.3传输本节点的唯一标记UID至认证服务器；

[0029] a.若获得证书则本地存储，以供服务重启后使用，并转入步骤3，

[0030] b.若证书获取失败则标记失效状态，生成错误日志并退出；

[0031] 步骤3.启动医疗养老数据监听服务直到有数据交换代理客户端接入；

[0032] ///处理数据交换代理工作

[0033] 步骤3.1启动子进程执行数据代理服务；

[0034] 步骤3.2对数据交换代理客户端的CA验证；

[0035] a.验证成功进入步骤3.3，

[0036] b.验证失败生成错误日志，重置连接，转入步骤3；

[0037] 步骤3.3查找对应数据源服务端并发起连接请求：

[0038] a.连接成功进入步骤3.4，

[0039] b.连接失败生成错误日志，向数据交换代理客户端发送错误信息，并重置连接，转入步骤3；

[0040] 步骤3.4与数据源服务端交换证书，双方验证合法性；

[0041] a.验证成功转入步骤3.5，

[0042] b.验证失败生成错误日志，重置与数据源服务端连接，向数据交换代理客户端发送错误信息，并重置连接，转入步骤3；

[0043] 步骤3.5解析数据交换代理客户端报文信息，包括密文数据和解密，查找医疗养老数据交换映射表，按转换规则组装异构系统数据请求所需报文信息，向数据源服务端发送数据请求；

[0044] a.响应成功转入步骤4；

[0045] b.响应失败生成错误日志，重置与数据源服务端连接，向数据交换代理客户端发送错误信息，并重置连接，转入步骤3；

[0046] 步骤4.进入安全传输处理流程；

[0047] 步骤5.安全传输结束，终止当前子进程，转入步骤3。

[0048] 数据交换代理客户端(22)的处理流程如下：

[0049] 步骤1.数据交换代理客户端获取证书；

[0050] 若本地已有证书则转入步骤1.1；

[0051] 步骤1.1查找网络上企业认证(CA)节点，

[0052] 步骤1.2向企业认证节点发起证书请求：

[0053] a.若请求成功则转入步骤1.3，

[0054] b.若请求失败则重复步骤1.1；

[0055] 步骤1.3传输本节点的唯一标记UID至认证服务器；

[0056] a.若获得证书则本地存储,以供服务重启后使用,并转入步骤2，

[0057] b.若证书获取失败则标记失效状态,生成错误日志并退出；

[0058] 步骤2.处理医疗养老数据交换请求的客户端工作：

[0059] 步骤2.1接受本地用户登录请求：

[0060] 步骤2.2本地验证用户的身份和数据存取权限；

[0061] a.验证成功进入步骤2.3，

[0062] b.验证失败生成错误日志,转入步骤2.1；

[0063] 步骤2.3接受用户的异构数据请求；

[0064] 步骤2.4查找数据交换映射表,将用户信息与数据请求信息按转换规则组装异构系统数据请求所需报文信息；

[0065] 步骤2.5查找数据交换代理服务器端并发起连接请求：

[0066] a.连接成功则进入步骤2.6，

[0067] b.连接失败生成错误日志,转入步骤2；

[0068] 步骤2.6与数据交换代理服务端交换证书验证：

[0069] a.验证成功进入步骤2.7，

[0070] b.验证失败生成错误日志,转入步骤2；

[0071] 步骤2.7向数据交换代理服务器端提交加密后的报文信息；

[0072] 步骤2.8接收数据交换代理服务器端的响应：

[0073] a.响应成功转入步骤3，

[0074] b.响应失败生成错误日志,转入步骤2；

[0075] 步骤3进入安全传输处理流程；

[0076] 步骤4安全传输结束,转入步骤2。

[0077] 数据源服务端提供下述几方面的功能:(1).接受数据交换服务代理的数据请求；(2).与本地数据库或数据服务进程交互,获得所需应用数据;(3).以安全传输模式向数据交换代理客户端实施单向数据传输服务,具体的处理流程如下：

[0078] 步骤1数据源服务端在数据源端作为服务进程启动；

[0079] 步骤2数据源服务端获取证书；

[0080] 若本地已有证书则转入步骤3；

[0081] 步骤2.1查找网络上企业认证(CA)节点；

[0082] 步骤2.2向企业证书服务器节点发起证书请求：

[0083] a.若请求成功则转入步骤2.3，

[0084] b.若请求失败则重复步骤2.2：

[0085] 步骤2.3传输本节点的唯一标记UID至认证服务器：

[0086] a.若获得证书则本地存储,以供服务重启后使用,并转入步骤3，

[0087] b.若证书获取失败则标记失效状态,生成错误日志并退出；

[0088] 步骤3启动医疗养老数据监听服务直到有数据交换代理服务器端接入；

[0089] 步骤3.1启动子进程执行数据代理服务；

[0090] 步骤3.2对数据交换代理服务器端交换证书：

[0091] a.验证成功进入步骤3.3，

[0092] b.验证失败生成错误日志,向请求端发送错误消息,重置与数据交

[0093] 换代理服务器端的连接,并转入步骤3；

[0094] 步骤3.3接收数据交换代理服务器端的数据请求,解析报文：

[0095] a.在数据缓存区搜索数据,获得数据后转入步骤3.4，

[0096] b.向源数据库或本地数据服务进程请求数据,获得数据后转入步骤3.4

[0097] c.从数据源获取数据失败,生成错误日志,向请求端发送错误消息,重置连接,转入步骤3；

[0098] 步骤3.4向数据交换代理客户端发起验证协议

[0099] a.验证成功转向步骤4，

[0100] b.验证失败生成错误日志,重置与数据交换代理服务器端的连接,转入

[0101] 步骤3；

[0102] 步骤4与数据交换代理客户端建立单向数据传输通路,调用加密子例程向数据交换代理客户端发送数据；

[0103] 步骤5数据传输结束,终止当前子进程,转入步骤2。

[0104] 所述数据交换映射表(23)设定医疗数据数据系统和养老数据系统互通的交换规则,分别对数据规范和数据格式进行了设定;该映射表分为标准映射和扩展映射两个部分;标准映射是按照遵从“HLV7”和“健康档案基本架构与数据标准”的医疗信息系统数据源和健康数据源进行内部编码;扩展映射则是针对非上述标准的数据源进行的内部编码。

[0105] 所述认证代理装置中证书服务器的处理流程如下：

[0106] 步骤1.监听网络证书服务请求；

[0107] 步骤2.查找节点信息库,验证是否是授权用户节点；

[0108] 若非授权用户则生成错误日志,重置连接,转至步骤1

[0109] 步骤3.证书生成处理：

[0110] a.获得用户UID及相关信息并为其制作证书(.CER)《

[0111] b.将证书发送至证书请求节点,转入步骤1。

[0112] 认证服务端(12)处理流程如下：

[0113] 步骤1.监听认证服务请求；

[0114] 步骤2.生成子进程响应数据交换代理服务器端的验证请求信息：

[0115] a.验证请求信息中证书的有效性，

[0116] b.验证不通过生成错误日志,向数据交换代理服务器端发送错误信息,重置连接,转入步骤1，

[0117] c.验证通过向数据交换代理服务器端发送确认信息，

[0118] d.继续响应数据交换代理服务器端后续的用户权类型和数据存取权限的验证请求。

[0119] 所述安全传输模块设置在网络应用层之上，用以保证通信链路上医疗养老数据传输的安全：在安全传输协议模块制定异构节点间点到点的传输状态规则，传输节点间协商临时通信信道上的可靠数据传输的应用规则；加解密子例程模块提供多种公开的密码算法代码库，包括DES算法、3DES算法、AES算法、RSA算法，以供通信双方在传输协议确定后执行具体的加解密操作，其中，公钥RSA算法用于密钥管理、证书管理功能模块中。

[0120] 本发明的积极效果是：

[0121] 1医疗养老数据安全交换代理装置能够将网络上异构的医疗和养老数据系统整合在一起，提供授权条件下的网络数据交换请求服务。该数据交换代理可解决传统的医疗、养老管理系统的数据孤岛问题，在保证数据私密性条件下，为授权用户提供跨系统的数据读取服务，对建立基于广域网的医疗养老服务应用扩展有非常积极的数据支撑作用。同时，该装置可降低异构系统的数据耦合性，提高数据访问的灵活性和可扩展性，便于实现按需的异构数据服务功能。

[0122] 2、多安全防护：充分考虑医疗养老数据的私密性、可靠性及这类数据应用的安全性，设计和实施采用了大量网络认证和数据安全传输的方法，保证医疗养老数据交换的信息安全性。

[0123] 3、本发明的数据交换代理结构设计，充分适应当前医疗、养老数据源具有较强的区域和行政壁垒特征，采用了数据交换映射表方式，形成中间件式的代理网关，适合于渐进式的数据源之间数据交换应用建设。

[0124] 4、装置设计简单、可靠、实用，易于企业级的医疗养老数据服务提供。

四、附图说明

[0125] 图1示出了一个完整的应用系统示意图。

[0126] 图2为本发明的医疗养老数据安全交换代理装置的框架结构图。

[0127] 图3为本发明的医疗养老数据安全交换代理装置的工作原理图。

[0128] 图4为本发明的医疗养老数据安全交换代理装置在实施例中的部署图。

[0129] 图5为本发明的医疗养老数据交换映射表图。

五、具体实施方式

[0130] 本发明在医疗数据系统和养老数据系统之间构建第三方的医疗养老数据交换代理装置，在医疗数据系统和养老数据系统的异构数据系统之间形成隔离层；医疗养老数据安全交换代理装置采用单向的半双工服务模式，进行医疗养老数据的双向交换。医疗养老数据安全交换代理装置将网络上异构的医疗和养老数据系统整合在一起，提供授权条件下的网络数据交换请求服务。

[0131] 设置数据交换代理服务器端形成医疗养老异构系统中数据交换的数据交换代理服务器隔离带，设置数据交换映射表将数据服务源的存取从请求客户端独立出来，提高医疗、健康异构数据系统存取的安全性。

[0132] 附图给出了本实施例的实现方式。

[0133] 图1示出了本发明基于医疗养老数据安全交换代理装置的一个完整应用系统示意图。包括业务应用系统为授权用户系用户端数据交换存取的接入载体，数据交换代理客户端，数据交换代理服务器端，证书服务器，认证服务端，数据源服务端，以及异构的医疗数据源和养老信息数据源。在本实施例中，应用系统为有医疗养老数据交换需求的业务应用，可通过Script脚本、Program应用程序、Web应用方式激活数据交换代理客户端，用以代理数据交换业务实施。数据交换代理客户端通过与应用系统进行验证，确认用户的合法性和有效性，并将数据交换请求发送至对应的数据交换代理服务器端，发起进一步的数据交换代理请求。数据交换代理服务器端将数据交换代理客户端信息一并提交认证服务端，验证数据交换代理请求的有效性。验证成功后，数据交换代理服务器端查找匹配的异构数据服务提供端，并与对应的数据源服务端进行协议验证，验证成功后数据交换代理客户端与数据源服务端形成安全数据传输通道，由数据源服务端从异构数据源系统中获取所需数据并发送至数据交换代理客户端。数据交换代理客户端取得所需数据后，馈入业务应用，完成医疗养老数据交换的代理流程。

[0134] 图2为本发明的医疗养老数据安全交换代理装置的框架结构图。

[0135] 参照图2，医疗养老数据安全交换代理装置由数据交换代理装置20，认证代理装置10，安全数据传输模块30构成。

[0136] 数据交换代理装置由4个单元组成，分别为：数据交换代理客户端22、数据交换代理服务器端21、数据源服务端24、和数据交换映射表23。

[0137] 认证代理装置10由3个部分组成，分别为证书服务器11、认证服务端12、节点信息库13。

[0138] 安全传输模块30包括2个部分，分别为安全验证协议31、加解密子例程32。

[0139] 数据交换代理装置20主要形成独立于应用的数据服务代理层。该构造方法具有应用独立性的优点，在应用与数据之间形成中间层，易于适应不同应用的业务需求，并可避免应用层对医疗养老数据交换的直接耦合，提升数据交换存取的安全性。通过面向应用的存取权限分级设计，能灵活扩展数据服务代理层的服务模式，使得代理层有良好的可扩展性。

[0140] 图3为本发明的医疗养老数据安全交换代理装置的工作原理图。

[0141] 参照图3，在开放网络环境下一个医疗养老数据交换请求的实施，是以委托代理方法进行。交换代理对于请求方是一黑盒，更好地屏蔽了用户对数据服务的细节了解，除提升了访问安全性，同时也可方便请求方实现数据存取结构无关的上层应用，为开发面向业务的数据服务提供方便。作为交换代理的黑盒，数据交换代理客户端为对外的唯一接口。在黑盒内部，采用内部编码，映射授权的异构节点，以及异构节点中的用户类型和数据存取权限的对应关系；数据交换代理客户端、数据交换代理服务器端、数据源服务端采用认证技术，确保通信节点的安全性；通信的对等节点间则采用了加密、解密模块，提高网络数据报文的安全性。由数据交换代理客户端、数据交换代理服务器端、数据源服务端应用安全传输协议，验证数据请求的合法性。最终由数据源服务端为数据交换代理客户端提供所需数据。

[0142] 图4为本发明的医疗养老数据安全交换代理装置在实施例中的部署图。

[0143] 参照图4，单点数据服务请求用户往往也是数据服务提供用户。根据医疗养老数据的特殊性和现行的实际情况，仅在两两异构数据系统之间搭成互访协议才能提供数据交换

服务。因此，在部署图中将请求客户与数据源的表达放置于同一处。实际上，不同数据源分属于不同机构，数据源服务端部署于用户端不同服务器设备之上。企业应用服务器部署在公网上，安装证书服务器、认证服务器端、数据交换代理服务器端等应用进程，用以提供各相应的服务功能。逻辑上，医疗养老数据交换服务客户端划分在交换代理层，在实施部署上则作为客户端进程安装在用户端。

[0144] 本实施例中，在数据交换代理装置20中的数据交换代理服务器端21设计为一直保持网络在线，固定接收和响应特定的医疗养老数据服务请求，并负责完成对授权客户端的数据请求响应服务功能。数据交换代理客户端22设计安装于实施医疗养老服务业务的客户端，业务应用程序向数据交换代理服务器端发起数据请求，并由数据交换代理客户端实现所需数据的接收并上传回业务应用程序。数据源服务端24安装在原医疗数据、养老数据系统端，接受数据交换代理服务器的数据请求(包含企业级认证确认、内部安全通信协议)，并建立起单向数据传输通道，将请求的应答数据发回数据交换代理客户端。数据源服务端配置有数据缓存，是为了提高数据交换服务效率，对关联性数据进行本地预取和缓存，减少源数据库的访问。数据交换映射表23是企业内部的医疗养老数据交换规则设定，可根据医疗数据标准和健康数据标准制定内部的编码对应，该实施方式可以降低外部针对数据攻击的危险性。同时，也可以根据业务需求，为新用户提供方便灵活的非标数据表达转换。

[0145] 数据交换代理装置是医疗养老数据安全交换代理模型的核心部件，该部件设计成独立的运行节点。该设计方式还有利于调整为分布式服务结构，可服务于大规模的并发医疗养老数据交换处理。

[0146] 数据交换代理装置的安装部署按数据交换代理服务器端和数据交换代理客户端别部署。其中，数据交换代理服务器端负责处理多项医疗养老数据交换的关键处理工作，并与认证代理装置和安全传输模块均有交互，其工作原理见附图3，主要处理流程表述如下：

[0147] 步骤1.数据交换代理服务器端为服务器节点式配置；

[0148] 步骤2.数据交换代理服务器端获取证书；

[0149] 若本地已有证书则转入步骤3；

[0150] 步骤2.1查找网络上企业认证(CA)节点

[0151] 步骤2.2向企业证书服务器节点发起证书请求

[0152] a.若请求成功则转入步骤2.3

[0153] b.若请求失败则重复步骤2.2

[0154] 步骤2.3传输本节点的唯一标记UID至认证服务器。

[0155] a.若获得证书则本地存储，以供服务重启后使用，并转入步骤3

[0156] b.若证书获取失败则标记失效状态，生成错误日志并退出

[0157] 步骤3.启动医疗养老数据监听服务直到有数据交换代理客户端接入；

[0158] ///处理数据交换代理工作

[0159] 步骤3.1启动子进程执行数据代理服务

[0160] 步骤3.2对数据交换代理客户端的CA验证

[0161] a.验证成功进入步骤3.3

[0162] b.验证失败生成错误日志，重置连接，转入步骤3

[0163] 步骤3.3查找对应数据源服务端并发起连接请求

[0164] a.连接成功进入步骤3.4

[0165] b.连接失败生成错误日志，向数据交换代理客户端发送错误信息，并重置连接，转入步骤3

[0166] 步骤3.4与数据源服务端交换证书，双方验证合法性

[0167] a.验证成功转入步骤3.5

[0168] b.验证失败生成错误日志，重置与数据源服务端连接，向数据交换代理客户端发送错误信息，并重置连接，转入步骤3

[0169] 步骤3.5解析数据交换代理客户端报文信息(密文数据、解密)，查找医

[0170] 疗养老数据交换映射表，按转换规则组装异构系统数据请求所需报文信息，向数据源服务端发送数据请求

[0171] a.响应成功转入步骤4

[0172] b.响应失败生成错误日志，重置与数据源服务端连接，向数据交换代理客户端发送错误信息，并重置连接，转入步骤3

[0173] 步骤4.进入安全传输处理流程；

[0174] 步骤5.安全传输结束(含正常、异常结束情况)，终止当前子进程，转入步骤3.

[0175] 其中，数据交换代理服务器端形成了医疗养老异构系统中数据交换的隔离带。通过医疗养老数据映射表，将对数据服务源的存取从请求客户端独立出来，进一步提高了异构数据存取的安全性。医疗养老数据映射表的格式如图5中所示，其主要字段的解释如下：

[0176] 图5字段中包含了数据请求端所属机构信息，对应于数据源1ID字段；数据请求存取端所属机构信息为数据源2ID字段。异构数据源之间的用户角色权限的设定规定了从数据请求端到存取端的映射法则，即数据请求方是否具有有效的异构数据存取权限。该设计方式可对异构存取法则提供很好的灵活性，便于点对点的数据交换扩展。用户的基本信息以角色为主，用户ID不是必选项，但对受限的用户或特殊的用户，可通过该字段的扩展，制定更细粒度的存取规则。映射规则除前述字段，还包括数据存取权限与数据请求编码，数据存取权限是将数据服务源的数据服务转换为位图映射的字段信息，设定本规则下的有效数据范围。数据请求编码在代理端形成了对请求端的屏蔽，该编码为代理端与数据服务端之间的内部协议。

[0177] 数据交换代理客户端的处理流程如下：

[0178] 步骤1.数据交换代理客户端获取证书；

[0179] 若本地已有证书则转入步骤

[0180] 步骤1.1查找网络上企业认证(CA)节点；

[0181] 步骤1.2向企业认证节点发起证书请求；

[0182] a.若请求成功则转入步骤1.3

[0183] b.若请求失败则重复步骤1.1

[0184] 步骤1.3传输本节点的唯一标记UID至认证服务器；

[0185] a.若获得证书则本地存储，以供服务重启后使用，并转入步骤2

[0186] b.若证书获取失败则标记失效状态，生成错误日志并退出；

[0187] 步骤2.处理医疗养老数据交换请求的客户端工作；

[0188] 步骤2.1接受本地用户登录请求

[0189] 步骤2.2本地验证用户的身份和数据存取权限

[0190] a.验证成功进入步骤2.3

[0191] b.验证失败生成错误日志,转入步骤2.1;

[0192] 步骤2.3接受用户的异构数据请求

[0193] 步骤2.4查找数据交换映射表,将用户信息与数据请求信息按转换规则组装异构系统数据请求所需报文信息

[0194] 步骤2.5查找数据交换代理服务器端并发起连接请求

[0195] a.连接成功则进入步骤2.6

[0196] b.连接失败生成错误日志,转入步骤2

[0197] 步骤2.6与数据交换代理服务端交换证书验证

[0198] a.验证成功进入步骤2.7

[0199] b.验证失败生成错误日志,转入步骤2

[0200] 步骤2.7向数据交换代理服务器端提交加密后的报文信息

[0201] 步骤2.8接收数据交换代理服务器端的响应

[0202] a.响应成功转入步骤3

[0203] b.响应失败生成错误日志,转入步骤2

[0204] 步骤3.进入安全传输处理流程;

[0205] 步骤4.安全传输结束(含正常、异常结束情况),转入步骤2。

[0206] 本处理流程中,步骤1可归类到证书的应用子例程。步骤2一般以服务响应方式激活,即异构数据请求端用户通过事件或信号方式激活数据交换代理客户端应用程序。

[0207] 数据源服务端部署于授权提供交换数据的数据源端,通常从属于独立的用户机构,拥有对该数据源完全的所有权。该数据源服务端作为数据源面向网络提供的应用服务进程,主要提供下述几方面的功能:(1).接受数据交换服务代理的数据请求;(2).与本地数据库或数据服务进程交互,获得所需应用数据;(3).以安全传输模式向数据交换代理客户端实施单向数据传输服务。具体的处理流程如下:

[0208] 步骤1.数据源服务端在数据源端作为服务进程启动;

[0209] 步骤2.数据源服务端获取证书;

[0210] 若本地已有证书则转入步骤3;

[0211] 步骤2.1查找网络上企业认证(CA)节点;

[0212] 步骤2.2向企业证书服务器节点发起证书请求:

[0213] a.若请求成功则转入步骤2.3

[0214] b.若请求失败则重复步骤2.2

[0215] 步骤2.3传输本节点的唯一标记UID至认证服务器;

[0216] a.若获得证书则本地存储,以供服务重启后使用,并转入步骤3,

[0217] b.若证书获取失败则标记失效状态,生成错误日志并退出;

[0218] 步骤3.启动医疗养老数据监听服务直到有数据交换代理服务器端接入;

[0219] 步骤3.1启动子进程执行数据代理服务;

[0220] 步骤3.2对数据交换代理服务器端交换证书:

[0221] a.验证成功进入步骤3.3

[0222] b.验证失败生成错误日志，向请求端发送错误消息，重置与数据交换代理服务器端的连接，并转入步骤3；

[0223] 步骤3.3接收数据交换代理服务器端的数据请求，解析报文：

[0224] a.在数据缓存区搜索数据，获得数据后转入步骤3.4，

[0225] b.向源数据库或本地数据服务进程请求数据，获得数据后转入步骤3.4

[0226] c.从数据源获取数据失败，生成错误日志，向请求端发送错误消息，重置连接，转入步骤3；

[0227] 步骤3.4向数据交换代理客户端发起验证协议：

[0228] a.验证成功转向步骤4

[0229] b.验证失败生成错误日志，重置与数据交换代理服务器端的连接，转入步骤3；

[0230] 步骤4.与数据交换代理客户端建立单向数据传输通路，调用加密子例程向数据交换代理客户端发送数据；

[0231] 步骤5.数据传输结束(含正常、异常结束情况)，终止当前子进程，转入步骤3。

[0232] 数据交换映射表，设定了医疗-健康数据互通的交换规则，分别对数据规范和数据格式进行了设定；该映射表分为标准映射和扩展映射两个部分。标准映射是按照遵从“HLV7”和“健康档案基本架构与数据标准”的医疗信息系统数据源和健康数据源进行内部编码；扩展映射则是针对非上述标准的数据源进行的内部编码。映射表使得代理节点间的数据信息更加规范，且具可扩展性。

[0233] 图5表字段中包含了数据请求端所属机构信息，对应于数据源1ID字段；数据请求存取端所属机构信息为数据源2ID字段。异构数据源之间的用户角色权限的设定规定了从数据请求端到存取端的映射法则，即数据请求方是否具有有效的异构数据存取权限。该设计方式可对异构存取法则提供很好的灵活性，便于点对点的数据交换扩展。用户的基本信息以角色为主，用户ID不是必选项，但对受限的用户或特殊的用户，可通过该字段的扩展，制定更细粒度的存取规则。映射规则除前述字段，还包括数据存取权限与数据请求编码，数据存取权限是将数据服务源的数据服务转换为位图映射的字段信息，设定本规则下的有效数据范围。数据请求编码在代理端形成了对请求端的屏蔽，该编码为代理端与数据服务端之间的内部协议。

[0234] 认证代理装置10负责医疗养老数据安全交换中的合法节点认证相关工作。该部件在逻辑上设计为数据交换代理装置的独立功能模块，在实现上包含了与其他功能模块中部件的交互。证书服务器11为自定义的企业级证书机构，负责为每一个合法的用户(数据交换代理客户端、数据交换代理服务器端、数据源服务端)分配一个包含用户唯一识别号与用户公钥的证书。证书结构参照基于X.509证书格式，针对医疗养老数据交换代理服务进行了修改。证书服务器除证书的发放外，还负责证书的更新等相关服务。认证服务端12在本地服务器端数据库存储证书。作为证书认证服务代理，接收客户端的证书交换与验证请求，验证用户有效性，并将验证结果返回数据交换代理服务器节点。节点信息库13根据各用户信息系统(医疗信息系统、健康信息系统)提供的用户信息，形成企业级的用户信息表，以供认证服务器验证用户有效性时使用，并包含了用户间的数据存取权限的映射信息。其中，认证服务端模块替换传统的网络数据证书存储，增设节点信息库维护内容。该设计充分考虑长远情况下，跨区用户、授权个体用户的存取可能性。

[0235] 证书服务器主要处理流程如下：

[0236] 步骤1.监听网络证书服务请求

[0237] 步骤2.查找节点信息库，验证是否是授权用户节点；

[0238] 若非授权用户则生成错误日志，重置连接，转至步骤1

[0239] 步骤3.证书生成处理

[0240] c.获得用户UID及相关信息并为其制作证书(.CER)

[0241] d.将证书发送至证书请求节点转入步骤1。

[0242] 认证服务器主要处理流程如下：

[0243] 步骤1.监听认证服务请求

[0244] 步骤2.生成子进程响应数据交换代理服务器端的验证请求信息

[0245] b.验证请求信息中证书的有效性

[0246] c.验证不通过生成错误日志，向数据交换代理服务器端发送错误信息，重置连接，转入步骤1

[0247] d.验证通过向数据交换代理服务器端发送确认信息

[0248] e.继续响应数据交换代理服务器端后续的用户权类型和数据存取权限的验证请求。

[0249] 在安全传输模块30是数据交换代理模型的数据传输基础模块，作为独立的逻辑功能设计，实施上涉及本装置中的多个组件。安全传输模块设计在网络应用层之上，用以保证通信链路上医疗养老数据传输的安全。安全传输协议制定了异构节点间点到点的传输状态规则，传输节点间协商临时通信信道上的可靠数据传输的应用规则。加解密子例程则提供了多种公开的密码算法代码库，主要包括DES算法、3DES算法、AES算法、RSA算法等，以供通信双方在传输协议确定后执行具体的加解密操作。其中，公钥RSA算法主要用于密钥管理、证书管理功能模块中。安全传输协议32为企业内部制定的异构节点间采用的数据传输规则，设计并实现在网络通信的应用层上，用于获得面向状态连接的额外通信安全验证，包括逻辑通信链路的保持时间、校验设置、重传机制。加解密子例程31为公共服务进程，由本模型中各个组件在进行网络数据通信过程中调用。

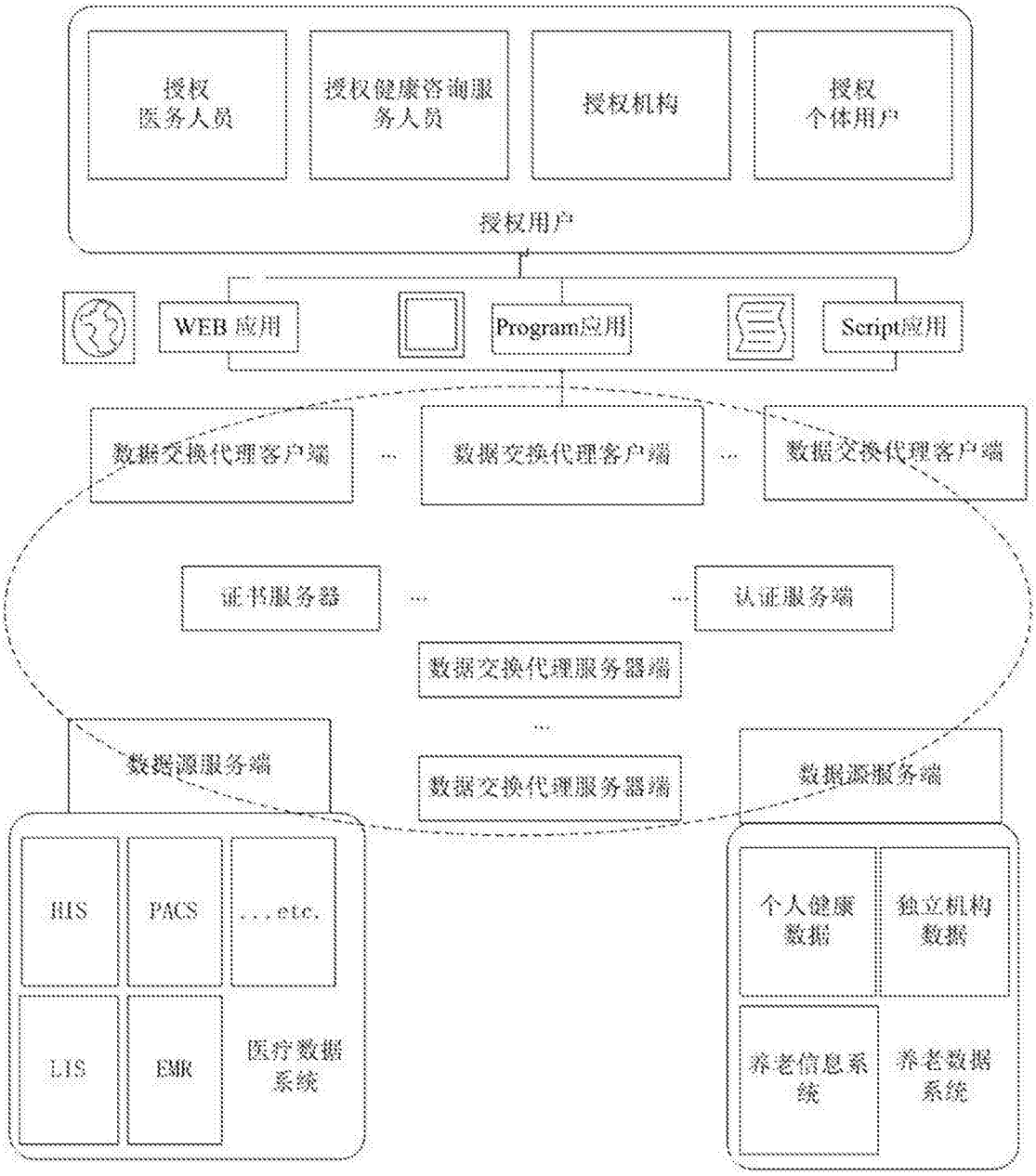

授权
医务人员
授权健康咨询服务人员
授权机构
授权
个体用户
授权用户
WEB 应用
Program应用
Script应用
数据交换代理客户端
数据交换代理客户端
数据交换代理客户端
证书服务器
认证服务端
数据交换代理服务器端
数据交换代理服务器端
数据源服务端
数据源服务端
HIS
PACS
...etc.
LIS
EMR
医疗数据系统
个人健康数据
独立机构数据
养老信息系统
养老数据系统

图1

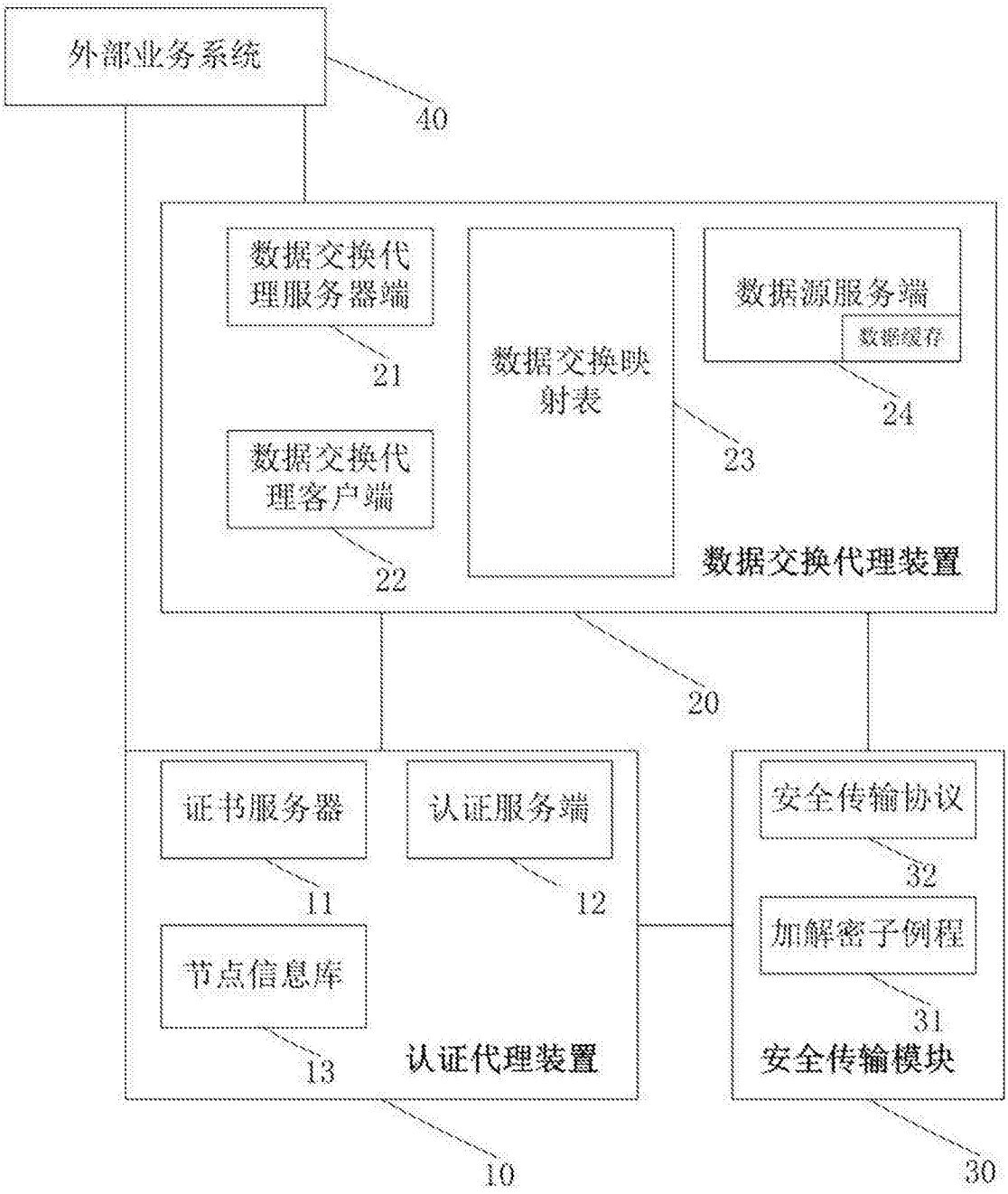

外部业务系统
40
数据交换代理服务器端
21
数据交换代理客户端
22
数据交换映射表
23
数据源服务端
数据缓存
24
数据交换代理装置
20
证书服务器
11
认证服务端
12
节点信息库
13
认证代理装置
10
安全传输协议
32
加解密子例程
31
安全传输模块
30

图2

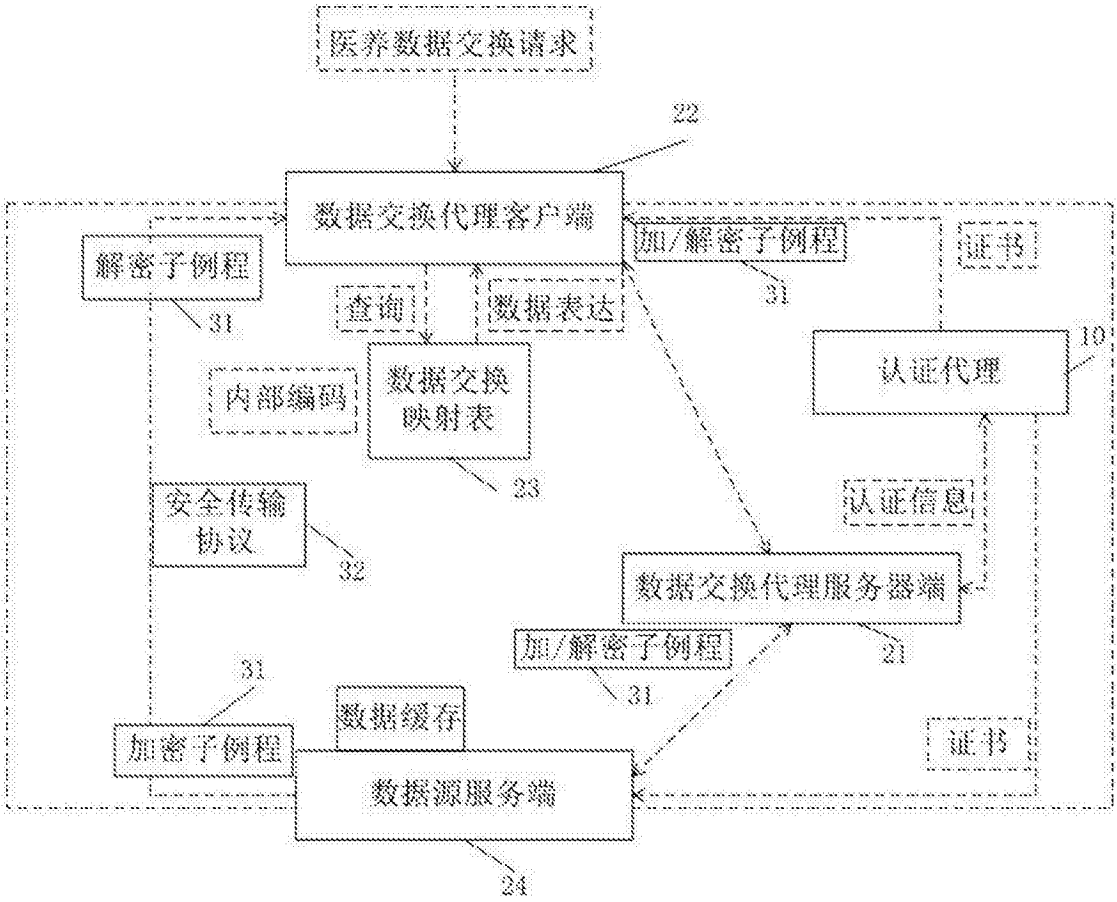

医养数据交换请求
22
数据交换代理客户端
解密子例程
31
查询
数据表达
加/解密子例程
31
证书
内部编码
数据交换
映射表
23
认证代理
10
安全传输
协议
32
认证信息
数据交换代理服务器端
21
加/解密子例程
31
31
数据缓存
加密子例程
证书
数据源服务端
24

图3

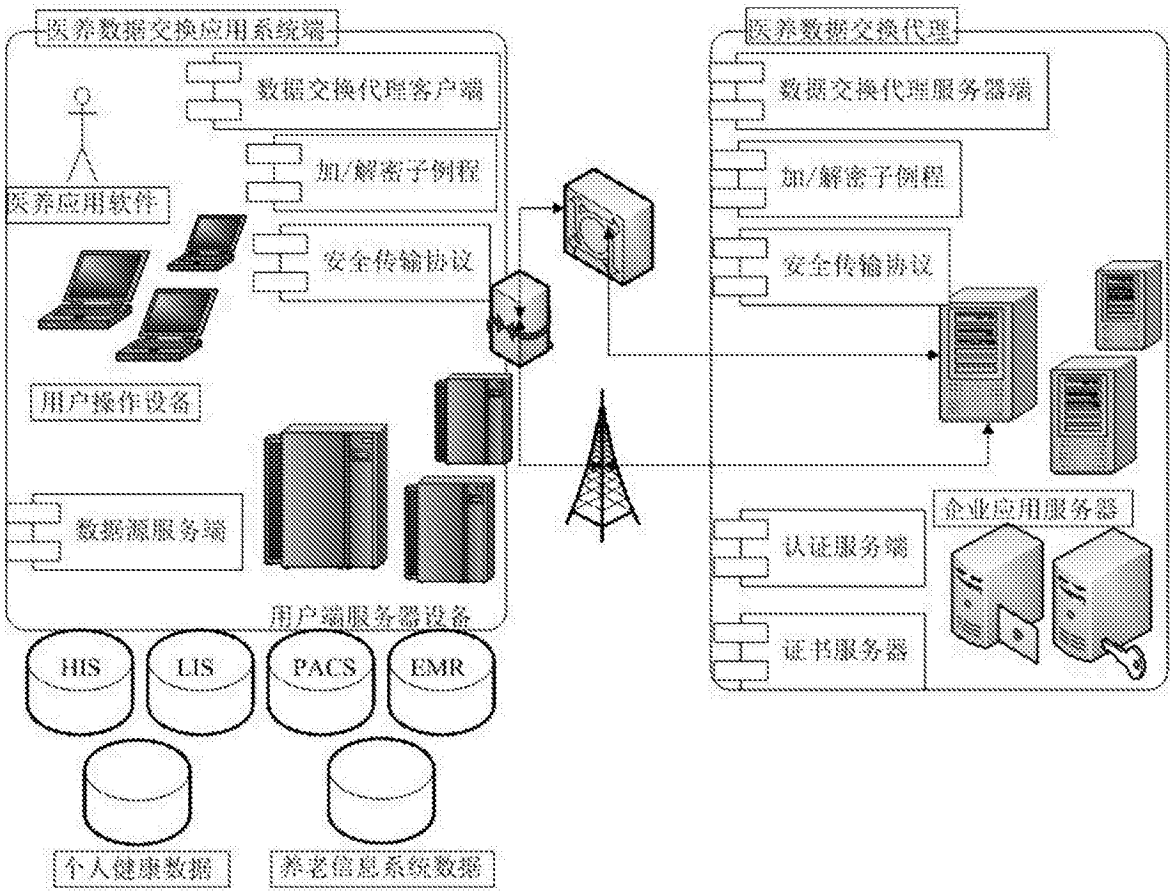

医养数据交换应用系统端
数据交换代理客户端
加/解密子例程
安全传输协议
医养应用软件
用户操作设备
数据源服务端
用户端服务器设备
HIS
LIS
PACS
EMR
个人健康数据
养老信息系统数据
医养数据交换代理
数据交换代理服务器端
加/解密子例程
安全传输协议
企业应用服务器
认证服务端
证书服务器

图4

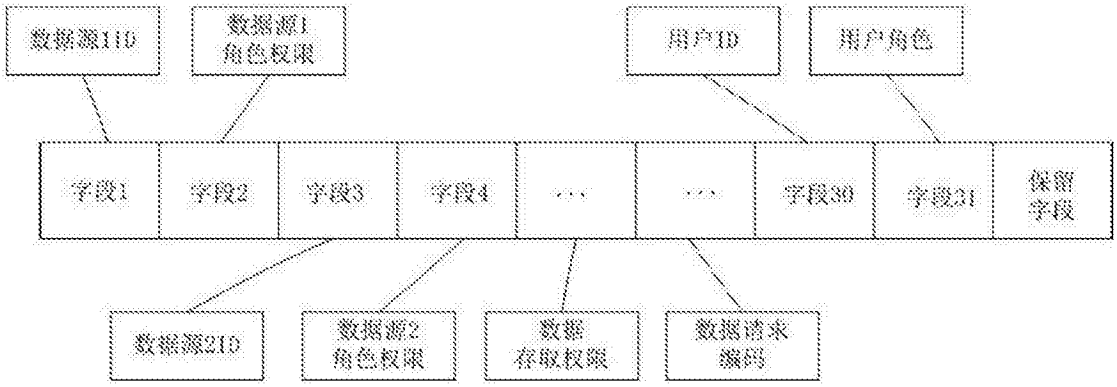

数据源1ID
数据源1
角色权限
用户ID
用户角色
字段1
字段2
字段3
字段4
…
…
字段30
字段31
保留
字段
数据源2ID
数据源2
角色权限
数据
存取权限
数据请求
编码

图5