基于工业互联网标识解析体系的密码测试床

1.1 引言/导读

中国信息通信研究院作为工业和信息化部直属科研事业单位，致力于工业互联网领域技术研究工作，为我国工业互联网发展提供技术保障。同时，我院于2020年正式成立密码应用推进中心，推进我国商用密码基础科研能力建设。我国目前在加快构建工业和信息化领域完备的商用密码应用标准体系的同时，坚持创新驱动，围绕制造强国、网络强国战略重点领域，积极推动新兴技术与密码技术深度融合和协同创新。

工业互联网标识解析体系作为关键信息基础设施，遵循我国《关键信息基础设施安全保护条例》。随着条例的正式发布，国家对密码类安全产品的“安全可控”能力显得尤为必要，国产密码算法的验证研究迫在眉睫。中国信息通信研究院将国产密码算法融入到工业互联网标识解析体系中，形成对应用、推广、迭代的研究方案，并积极开展基础理论、创新模式、关键技术与标准、应用试验验证等技术研究，提升标识解析体系整体安全防护能力，切实保护工业互联网信息数据安全，为我国工业互联网发展保驾护航。

1.2 关键词

商用/国产密码算法、标识解析服务、递归解析服务

1.3 测试床项目承接主体

1.3.1 发起公司和主要联系人联系方式

发起公司：中国信息通信研究院

联系人：刘红炎，13810863339，liuhongyan@caict.ac.cn

1.3.2 合作公司

北京泰尔英福科技有限公司

北京市热力集团有限公司

江苏中天科技集团

1.4 测试床项目目标

国家高度重视工业互联网安全工作，《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》（以下简称《指导意见》）中从设备安全、控制安全、网络安全、平台安全和数据安全五个维度开展安全体系建设，其中，“自主可控，安全可靠”成为工业互联网发展的方向。目前，商用国产密码算法行业仍处于起步阶段，尚未形成密码企业集群发展之势，相对于国外商用密码市场软硬件产品分布较均衡，我国商用密码市场较为分散。工业互联网标识解析作为我国工业互联网关键信息基础设施，将会面对越来越严峻的安全风险。因此，亟需通过探索研究并制定技术方案，来验证国产密码算法在工业互联网标识解析体系中的可行性。

基于工业互联网标识解析体系的密码应用测试床目标是将国产密码算法应用在标识解析体系中，验证国产密码算法在标识注册、标识解析等应用场景中的方案是否可行。通过对国产密码算法在工业互联网标识解析体系中的验证研究，保证了标识数据的安全可信和标识服务身份合法可信，从而促成我国工业互联网的安全平稳发展。

1.5 测试床方案架构

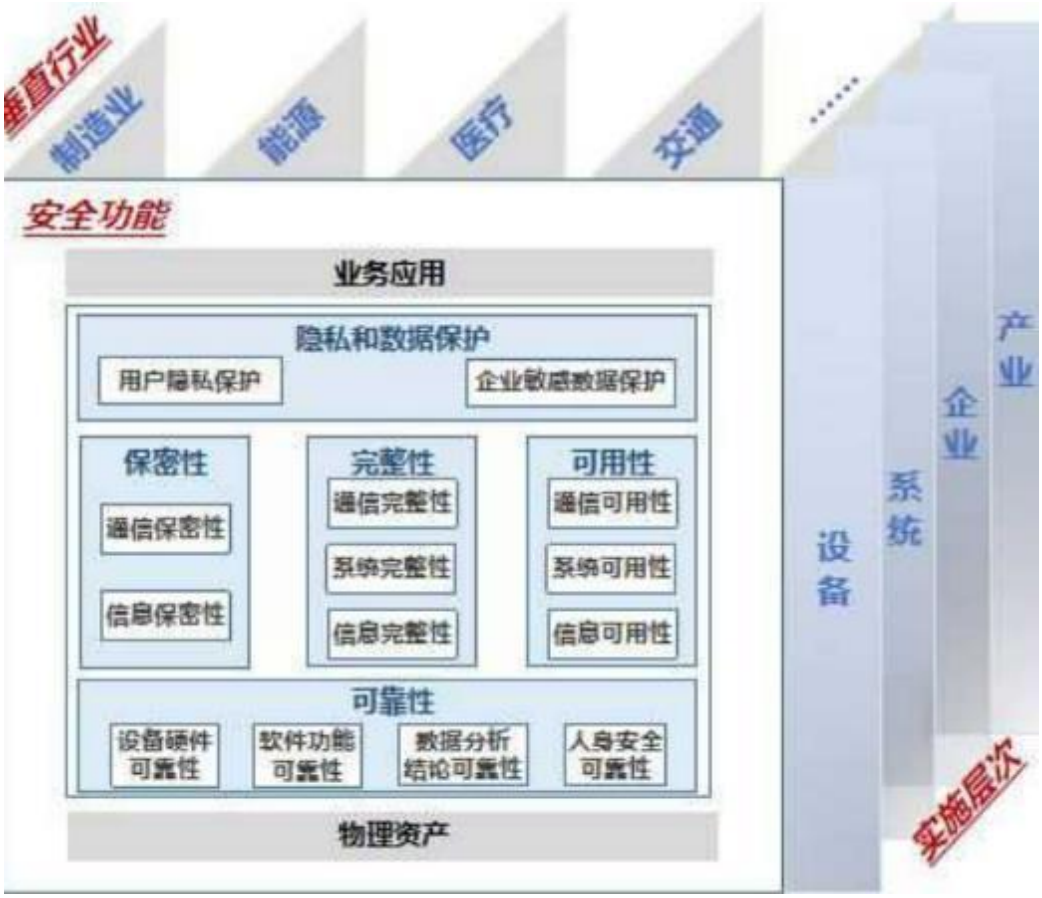
1.5.1 测试床应用场景

本测试床基于国家工业互联网标识解析体系，使用国产密码在标识注册、标识解析和标识数据同步的场景中进行验证。国家工业互联网标识解析体系由三层架构组成，分别为国家顶级、二级和企业。另外，还提供公共递归服务，为用户访问提供统一入口。目前网络标识数据传输中，由于数据敏感度较高，为保障数据隐私性，所有在数据传输

中使用了密码机制，但是目前使用的是国际上通用的密码体系，如RSA、DSA等公开密码算法，其在效率和安全性方面存在问题，而且是非自主独立可控的算法体系，因此需要能既保证数据安全可靠，又保证自主可控的解决方案。基于国产密码算法的应用能在保障数据可信使用的前提下，有效提高传输速率，提供用户体验，为保证我国工业互联网标识解析体系自主可控，安全可靠的建设奠定基石。

1.5.2 测试床架构

本测试床是为了验证国产密码算法与标识解析体系结合，以保证标识解析数据可信且可靠。在AII总体架构中属于安全功能视图中的保密性、完整性、隐私和数据保护部分内容，即标识数据在数据提供方安全自主可控制的范围内传递给使用方，并知晓数据安全情况，安全体系框架如下图所示。



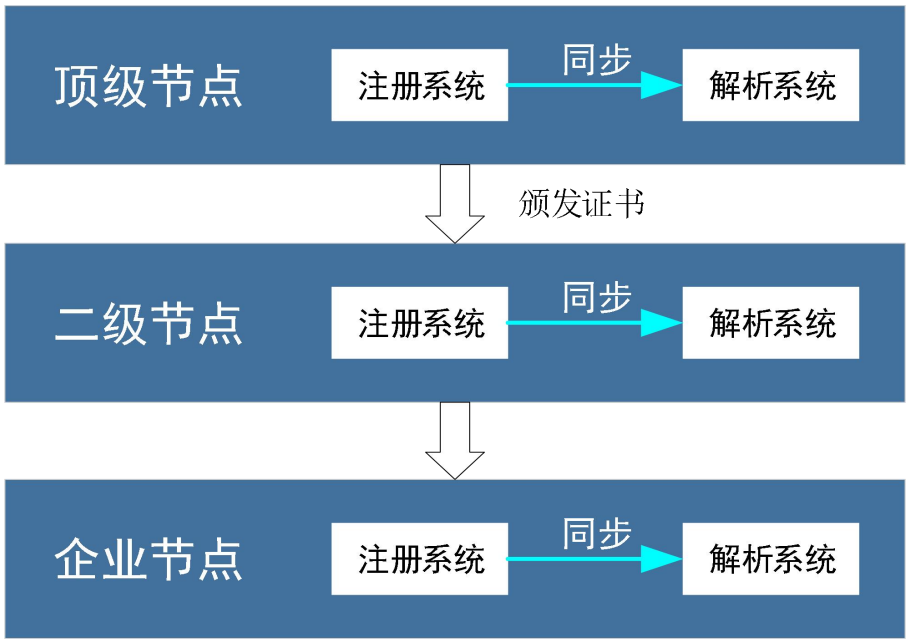
工业互联网功能视图安全体系框架

1.5.3 测试床方案

工业互联网标识解析体系由三层架构组成，分别为国家顶级、二级和企业，其中标识公共递归解析应用在标识解析体系的全流程中。国家顶级包括国家级标识的注册和解析节点，数据同步节点，实现国家二级前缀的注册、解析和数据同步功能。二级包括企业标识前缀的注册和解析节点，为企业提供标识前缀的注册和解析功能。企业包括企业节点的注册和解析，为企业具体标识提供注册和解析功能，以上三层架构和功能通过公共标识递归节点提供公共查询入口，对外提供工业互联网标识解析功能。

（1）标识注册解析系统

标识注册解析系统包括注册系统和解析系统，注册系统负责标识数据写入，解析系统输出标识数据查询结果，标识注册系统主动向标识解析系统做数据同步。注册系统和解析系统共同协作，实现对机器、物品等进行唯一性的定位和信息查询，是实现全球供应链系统和企业生产系统精准对接、产品全生命周期管理和智能化服务的前提和基础。



标识注册解析系统

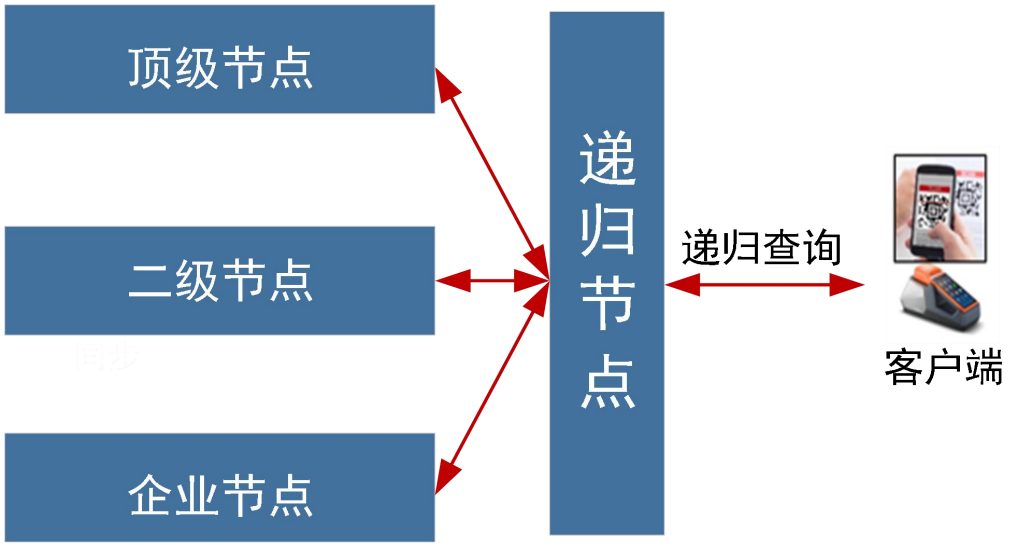
如上图所示，在标识注册解析系统中，工业互联网标识解析体系由国家顶级节点、二级节点和企业节点组成三层体系架构组成。其中，国家顶级节点完成所有二级节点的标识前缀分配和注册，二级节点完成其下的所有企业节点接入功能。企业节点可以实现企业内部标识产品的注册和解析，完成企业的实际需求。

国产密码算法在标识注册解析系统的测试验证，具体描述如下：

- 标识国家顶级节点制作自签名证书，在启用可信解析的情况下，顶级节点给二级节点颁发证书，二级节点对企业节点进行签名。在各级标识节点之间，使用国产密码算法 SM2、 SM3 算法，采用数字证书可信验证机制核验节点身份，实现节点身份可信。
- 标识权威注册系统和解析系统之间，使用全信道来同步数据，安全信道使用 SM2、SM3、SM4 国产密码算法进行加密传输。

（2）递归标识解析系统

公共递归节点是标识解析体系中客户端请求的第一环节，提供标识解析的统一入口，通过分别向国家顶级节点、二级节点、企业节点进行相应解析请求，最终获取标识的详细信息反馈给客户端。



标识递归解析系统

如上图标识递归解析系统所示：客户端向递归发起请求，递归节点第一跳指向国家顶级节点，国家顶级节点接收到标识请求后，根据前缀信息返回递归节点二级节点HS_SITE信息，递归节点继续向二级节点HS_SITE站点发起标识查询，二级节点根据请求前缀返回企业节点的HS_SITE信息，递归节点继续向企业节点HS_SITE站点发起标识查询，获取到标识解析最终结果，并将该结果返回至请求客户端。在该环节中，为了保证数据可信，可靠的传递到客户端。在整个解析过程中，验证了国产密码算法在全流程中实施的可行性，具体如下：

- 在递归节点向顶级、二级和企业查询时，使用了 SM2、SM3 国产密码算法来进行签名和验证签名，保证了消息的来源可信和内容可信。
- 在递归解析的过程中，为了保证国家顶级、二级和企业节点身份可信，需要对其身份进行验证，并将验证后的结果返回给客户端。此环节使用了国产密码 SM2 和 SM3 算法。

1.5.4 方案重点技术

目前，在工业互联网标识数据交互中，为了保证数据在网络上安全可靠的传输，广泛采用了比较成熟的国际标准密码体系进行安全防护，如DSA、RSA加解密算法。本测试床在现有的标识解析技术基础之上，使用国产密码算法在标识解析各个环节中进行安全加固。国产密码算法在安全性、签名速度和存贮资源占用上，都明显优于国际标准算法。

- 安全性：基于 ECC 的 SM2 证书普遍采用 256 位密钥长度，加密强度等同于 3072 位 RSA 证书，安全性远高于业界普遍采用的 2048 位 RSA 证书。
- 签名速度：SM2 在私钥运算上，速度远比 RSA 快得多。
- 存贮空间：SM2 算法的密码一般使用 192-256 位，RSA 算法密码一般需要使用 2048-4096 位。这意味着 SM2 算法的证书字节数更少，在高并发的情况下消耗资源更少，速度更快。

技术验证如下表所示：

技术验证项	描述
安全信道	安全信道是信息以加密的形式经过网络传播,网络破坏者虽然可以截获网络上传输的所有数据,但他无法得到数据中包含的真正信息.安全信道的建立主要有两项任务：一是通过验证身份确立相互的信任关系；二是协商确定安全信道中所使用的加密密钥。 使用国产密码算法构建安全信道，应用在标识注册、数据同步等环节。

消息凭据	消息凭据是为了保证标识解析数据不被篡改，通过密码算法对解析数据进行签名，将签名结果附加在解析内容尾部。用户在收到该数据时，可以通过签名结果对收到的数据进行验证。 消息凭据应用在标识解析环节中。
可信解析	可信解析是应用在分布式标识解析架构下对各个标识解析层级进行身份验证的一种机制。用户在进行迭代查询时，自上而下，逐级对每个解析节点进行身份验证。国家顶级节点作为工业互联网标识解析体系中的信任锚点，向二级节点颁发数字证书，确定其合法身份；二级节点向企业节点授权，确定企业合法身份。 可信解析应用在标识递归解析环节中。数字证书颁发及授权应用在标识注册环节。

1.5.5 方案自主研发性、创新性及先进性

本测试床方案是中国信息通信研究院基于工业互联网标识解析技术体系，将国产密码算法应用到工业互联网标识解析的研究验证。测试床的实施方案经过需求分析、关键技术验证和可行性分析后得出。相关软件系统由中国信息通信研究院自主研发，以上工作均体现了本测试床方案的自主研发性。

基于工业互联网标识解析体系，采用国产密码算法加固了该体系安全性。同时，拓展到标识解析应用环节，安全指标得到较大提升，完成了标识网络技术探索实践，因此本测试床方案具有创新性和技术运用的先进性。

1.5.6 方案安全风险控制

本测试床是基于国产密码算法在工业互联网标识解析体系中的一个测试验证，在测试方案中使用了国产密码算法来加固标识数据的安全性。这样，虽然比起国际通用算法DSA、RSA性能有所提高，但是加固安全确实影响服务器解析性能。为了防止DDOS攻击，在传输层开启了最大连接数，超过该数值，则链接关闭。而且还应用LVS技术，实现负载均衡，提升高可靠，高可用性。在态势网络感知方面，使用了自主研发的标识监测系统，通过主动探测、被动探测等技术，实时对工业互联网标识解析体系的相关服务进行监控。对异常服务情况做到了实时监控，报警并推送负责人，以便及时处理。

1.6 测试床实施部署

1.6.1 测试床实施规划

序号	阶段名称	进度计划	主要工作内容
1	需求调研、可行性研究和需求分析阶段	5个月	调研密码测试床的需求，并产出相关需求说明书和可行性分析报告。
2	设计开发阶段	6个月	针对测试需求，对其进行设计和开发。
3	调试并上线试运行	2个月	施工部署并调测
4	正式上线运行并验收	2个月	根据需求，完成所有功能并正式上线运行。
5	宣传推广	3个月	宣传推广，并发展整个生态。

1.6.2 测试床实施的技术支撑及保障措施

本测试床实施所需要的支撑保障，主要是由目标主机提供适用于测试床部署的软硬件环境及网络通信环境，具体细节要求如下：

硬件环境：5台服务器（ 32核 CPU， 128G 内存，1T 硬盘）；

系统环境：CentOS 7.5及以上；

网卡：千兆网卡；

编译环境：GCC4.8.5或以上，Eclipse 等。

1.6.3 测试床实施的自主可控性

基于国产密码算法的工业互联网标识解析体系，从整个技术架构到代码实现，核心系统使用C/C++编程，G++编译，完成研发并上线运行。

综上所述，基于工业互联网标识解析体系的密码应用测试床验证方案从源码、编译、调试、测试，到实施部署试运行，再到调整上线正式运行的全生命周期都具备自主可控性。

1.7 测试床预期成果

1.7.1 测试床的预期可量化实施结果

输出国产密码算法在工业互联网标识解析体系中的标识权威解析服务、标识注册服务和标识递归解析查询服务等相关系统及软件著作权。

1.7.2 测试床的商业价值、经济效益

本测试床构建完成后，既验证了国产密码算法在保障工业互联网标识解析体系全流程安全方面的可行性，降低了工业互联网标识产业经济损失风险，又带动我国商业密码产业规模发展，进一步促进国产密码算法的推广。

1.7.3 测试床的社会价值

密码直接关系到国家政治安全、经济安全、国防安全和网络安全，同时也关系到社会组织和公民个人的合法权益。将国产密码算法应用到工业互联网标识解析体系中进行测试验证，对保障我国工业互联网关键信息基础设施的自主可控、安全可靠具有里程碑的意义。

1.7.4 测试床初步推广应用案例

本测试床项目在北京市热力集团有限公司和江苏中天科技股份有限公司两家企业间进行探索应用。两家企业在工业互联网标识解析国产密码应用方面有较强的需求，这也是测试床验证的主要应用案例。

北京热力集团嵌入式终端在标识注册及终端发起的标识解析中使用国产加密算法；江苏中天科技股份有限公司，在标识解析应该过程中使用国产加密算法，保障标识注册和解析数据可以安全可靠的传输。

1.8 测试床成果验证

1.8.1 测试床成果验证计划

拟根据测试床在工业互联网标识解析体系适用的生产环境内，基于国产密码算法的技术要点，通过对安全信道、可信解析和消息凭据，三个维度来验证本测试床实际使用效果。

1.8.2 测试床成果验证方案

在开发满足本测试床的相关需求后，搭建一套完整的OTE环境，并测试标识的注册、解析流程，以便验证国产密码算法在该测试床中的应用。

在标识注册系统中验证国产密码算法TLS、证书的颁发，用于评价数据的可信可靠传输，二级节点和企业节点的身份的授权认证。

在标识解析系统中来验证基于国产密码算法加固数据的完整性和不可篡改性，用于评价标识数据的传输安全效果。

在标识递归解析流程中，使用递归系统来验证整改解析流程数据的真实可信，用于评价标识 数据内容可信，身份可信。

通过以上的整个流程的验证测试，可以完全实现标识注册、标识解析、标识数据同步的各个环节自主可控，并验证了工业互联网标识解析体系全流程自主可控。

1.9 与已存在 AII 测试床的关系

本测试床属于工业互联网安全领域，具有较高的研究、应用和推广价值。

1.10 测试床成果交付

1.10.1 测试床成果交付件

本测试床最后提供的交付件为一套基于国产密码算法的工业互联网标识解析系统试验证平台，验证的成功标准是可以把该平台应用到工业互联相关的产业中，如北京热

力集团嵌入式终端在标识注册及终端发起的标识解析中应用，预计要完成30万热计量表、室内温控设备终端上线应用。可以实现对计量表、室内温控设备终端数据的全程监控。

1.10.2 测试床可复制性

本测试床用可应用在工业互联网的基础设施建设中，如船舶、集装箱、石化、食品、医疗器械等多个领域，未来更多的行业会逐步加入。其主要测试应用场景为工业互联网数据的安全加固，实现标识数据的可信可靠流转。

1.10.3 测试床开放性

本测试床是对国产密码算法在工业互联网标识解析体系中的一种测试验证。与现有的企业内部系统，如ERP、MES等完全独立，没有耦合性。可以在各企业部署并完成测试验证，因此具有很高的开放性。

1.11 其他信息

1.11.1 测试床使用者

中国信息通信研究院负责具体代码编写、解决方案部署、后续运营技术支持等工作。只有通过申请，且申请成功的二级节点和企业节点方可接入工业互联网体系中，这些接入工业互联网体系的企业方可进行多场景的可信测试。

1.11.2 测试床知识产权说明

中国信息通信研究院对测试床的建设、运营以及使用拥有软件自主产权。

1.11.3 测试床运营及访问使用

本测试床将部署于工业互联网产业联盟，由中国信息通信研究院运营，并提供相关技术支持。对测试床的访问使用需经过申请同意，并通过付费、知识产权共享等方式有条件使用。

1.11.4 测试床资金

测试床建设资金来源于发起方中国信息通信研究院。

1.11.5 测试床时间轴

任务描述		时间进度	详情
沟通交流，行业调研		2022.03.31	调研当前的密码算法体系，包括国际通用算法和国密算法，并产出文档国密算法调研文档。
需求分析、可行性分析，积极探索示范试点场景讨论		2022.05.31	根据调研结果，分析当前的使用环境，进行可行性分析，并产出可行性分析报告。
产品开发	安全信道功能	2022.11.31	完成在标识权威系统中使用基于国密算法TLS通信，实现标识解析各环节在网络中使用国产密码进行数据加密传输。
	消息凭据功能		完成在标识权威系统中使用基于国密算法的消息凭据，实现标识解析数据在传输过程中不被防篡改。
	可信解析功能		完成在标识递归系统中使用基于国密算法证书可信验证链，实现标识数据内容可信及身份可信。
系统联调测试，并试运行		2023.01.31	系统联调测试
正式上线运行和验收		2023.03.31	上线并验收
宣传推广		2023.06.30	宣传推广，扩大应用范围

1.11.6 附加信息

该测试床的建设面向对象工业互联网的多个行业，可逐步应用到船舶、集装箱、石化、食品、医疗器械等领域，为各行业数据流通共享提供全新的解决方案，充分促进数据价值释放。

1.12 测试床进展

基于测试床的规划，测试床项目分为前期调研，需求和可行性分析阶段、产品设计和开发阶段、联调试运行阶段、正式上线验收阶段和宣传推广阶段。目前已经完成了需求、调研和可行性分析，产出了相关文档。组织了多次产品的设计和研讨，最终方案通过评审。现在进入产品设计、开发和调试阶段，2022年08月31日完成在标识权威系统中使用基于国密算法TLS通信，实现标识解析各环节在网络中使用国产密码进行数据加密传输，后续按计划进行其他功能的开发。

1.12.1 需求调研和可行性分析

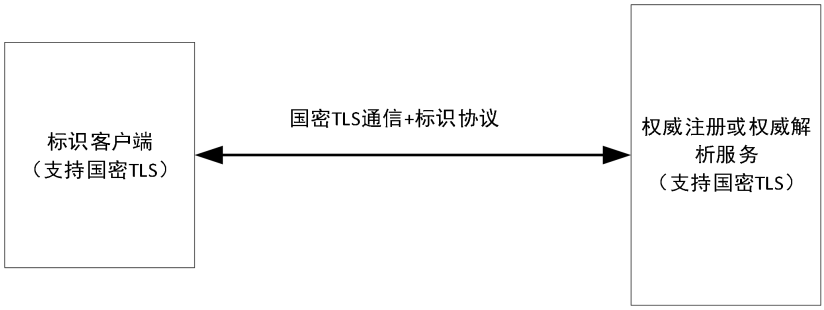
调研了国产密码的发展历程，对国际通用密码算法与国产密码算法进行了对比，总结并分析了它们之间的优缺点。并对国产密码算法进行了总结，结合工业互联网标识解析体系，找到适合当前解析体系的算法，并分析其适合场景以及效率。

1.12.2 设计、开发和测试

由于密码算法是一个基础框架，需要依赖于某个具体的体系，才能发挥其作用。把国产密码算法应用到工业互联网标识解析体系中，是对该体系创新应用。国产密码体系的在标识解析中的应用，具体如下：

（1）基于国产密码算法的安全加密传输功能框架

使用SM2、SM3和SM4算法，完成底层的TLS通信，通信信道建立后，双方可以进行加密通信，完成数据的加密传输，安全通道框图如下：

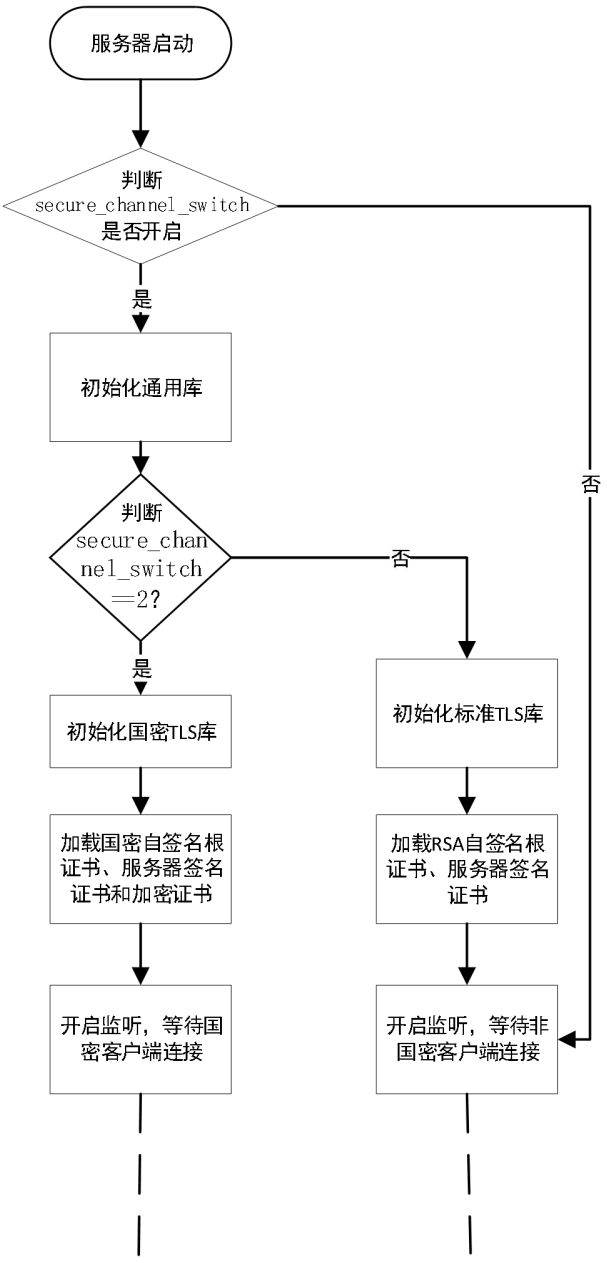


安全通道功能框图

如上图所示，在标识客户端与标识权威系统之间，进行数据安全加密传输，使用国密TLS协议。保证客户端与服务器之间数据，在传输过程中，使用了国密算法进行加密，保证数据不被篡改。

目前基于国产密码算法的TLS通信已经在标识权威和注册解析系统中设计完毕，功能已经调试完毕，可以完成标识数据的安全加密通信传输。

（2）基于国产密码算法的安全加密传输功能程序流程图



基于国密算法TLS功能流程图

如上图所示，在基于国产密码算法安全加密通信的标识权威系统中，通过开关来配置是否开启国密算法，同时也支持国际通用标准的算法。在设计时，考虑到兼容国密算法和国际标准算法。另外，基于国密算法的TLS通信时，使用了签名证书和加密证书，只有正确的配置了双证书才能完成通信。

（3）测试结果

基于国密算法TLS通信测试结果图

如上图所示，基于国密算法TLS在标识解析系统中的测试结果，从图中可以看出，通信过程中使用了国密SM2证书，以完成底层通信协议的建立，之后通过协商的密码进行加密通信。