中国计算机学会团体标准

《零信任网络隐身协议规范（征求意见稿）》编制说明

1、 标准“范围”内容：

零信任体系架构和技术是当今网络信息安全领域的前沿技术，主要解决云计算网络架构中的数据安全问题。零信任体系架构中软件定义边界（SDP）的重要支撑即单包授权（SPA）和 SDP 协议，国外已经制定了相应的规范。我国也必须制定适合我国国情的自主可控标准规范。

《零信任网络隐身协议规范》定义了零信任网络隐身协议的基本概念、实现原则、技术架构、加密算法原理、交互协议及其验证方法，提供一个可实施、可评估、可扩展的技术框架，用于开发基于零信任架构的数据安全系统或者在此基础上的扩展功能。本规范定义的零信任网络隐身协议可作为零信任安全架构中的一个通用基础组件，不仅可以用于南北向流量的安全防护，也可用于东西向流量的安全防护，并且支持与任意第三方身份认证与访问权限管理（IAM）系统对接，也支持通过下一代防火墙（NGFWs）进行逻辑微隔离。

除了安全能力，本规范定义的零信任网络隐身协议还支持与第三方日志审计或区块链平台对接，以满足数据流通的监管合规要求。

2、 工作简况，主要包括：任务来源、主要工作过程、各起草单位和起草人及其在起草标准过程中所承担的工作等情况、对标准草案进行会议讨论范围、征求意见的范围、审查范围：

（1） 任务来源

标准工作组发起单位在开发零信任软件定义边界（SDP）相关产品期间，针对 SDP2.0 标准中现有的 SPA 单包授权协议的不足，提出了一套新的网络隐身及授权访问框架，即零信任网络隐身协议（NHP 协议），从安全、性能、可靠性与兼容性上进行了全面提升。鉴于国内业界还没有关于网络隐身方面的详细标准，所以由中国计算机学会抗恶劣环境计算机专业委员会牵头，组织各起草单位对《零信任网络隐身协议规范》草案进行研究与探讨，将其提交至学会标准工作委员会进行标准化流程。

（2） 工作流程

2023 年 3 月 23 日《网络资源超隐身协议规范》标准研究组正式启动成立。

2023 年 3 月 31 日召开《网络资源超隐身协议规范》技术研讨会第一次会议，开始对协议规范及其文本进行研究与编写工作，并于此后每两周定期举行研讨会进行草案的研究与完善。

2023 年 6 月 26 日《网络资源超隐身协议规范》草案通过 CCF 标准工作委员会评审，研究组升级为工作组，进入标准发布流程。工作组技术研讨会仍继续进行并持续对协议文本进行调整与补充。

2023 年 11 月 20 日 CCF 标准工作委员会召开《网络资源超隐身协议规范》专家委员会评审会，对协议标准的范围、行文规范、技术内容及验证方法进行详细探讨并提出修改建议。并将《网络资源超隐身协议规范》更名为《零信任网络隐身协议规范》。

2023 年 12 月 4 日《零信任网络隐身协议规范》通过专家委员会评审.

（3） 起草单位

西塞数字安全研究院、中国电子科技集团公司第十五研究所、中电科发展规划研究院有限公司、航天科工 706 所、中电科太极计算机股份有限公司、中科院空天信息研究院、中科边缘智慧信息科技（苏州）有限公司、中移（苏州）软件技术有限公司、中电科人大金仓信息技术股份有限公司、联通数字科技有限公司、中国电信上海研究院、中国电子科技集团公司第五十四研究所、苏州云至深技术有限公司、 北京芯盾时代科技有限公司、北京蔷薇灵动科技有限公司、北京天空卫士网络安全技术有限公司、南昌大学网络空间安全学院、中信云网有限公司、中国铁塔信息研究院、北京大学、中电科普华基础软件股份有限公司、华为技术有限公司、麒麟软件有限公司、统信软件技术有限公司、浪潮电子信息产业股份有限公司、湖州市安全运营中心、北京航空航天大学软件学院、上海交通大学、中国科技大学网络安全学院、中国信息通信研究院、公安部第三研究所、中国电子信息产业发展研究院（赛迪研究院）、北京邮电大学网络安全学院、中国软件评测中心、中广宽带网络有限公司、北京交通大学、北京双湃智安科技有限公司、山东大学、浙江大学

（4） 征求意见范围

包括协议起草各单位、CCF 标准工作委员会专家委员会、CCF 抗恶劣环境计算机专家委员会。

3、 标准制定的必要性、编制原则和确定标准主要内容（如技术指标、参数、公式、性能要求、试验方法、检验规则等）的依据（包括试验、统计数据）：

近年来，国外针对零信任安全已提出了多项标准，而国内在此方面也亟需建立自己的标

准体系。《零信任网络隐身协议规范》作为面向解决网络隐身问题的解决方案框架，为其上位标准《信息安全技术 零信任参考体系架构》（国标报批稿）提供了支持。同时，该标准积极响应了国家提出的《信息安全技术 关键信息基础设施安全保护要求》，为减小网络关键设施暴露面与防御软件供应链漏洞攻击提供了一种零信任解决方案。因此有必要将该协议规范上升至标准层面，明确其与上位标准框架的关系及其所起到的作用，丰富国内的零信任安全标准体系。

标准工作组在编写标准时，以自主可控、全面提升为原则，重新制定了用于零信任网络隐身与验证授权访问的框架体系，并针对隐身能力、高性能、高可用、可扩展性与兼容性提出了验证方法。

（1） 隐身能力验证

NHP 协议的隐身能力可以通过以下两个方面验证且必须同时满足：

1） 资源请求方未经过身份认证前，被保护的资源的主机 IP 是否对其已知。

2） 资源请求方未经过身份认证前，被保护的资源的主机端口是否可以扫描到。

（2） 高性能验证

NHP 协议的高安全、高性能源于其基于噪声协议的身份认证机制。为验证噪声协议的实现及性能，可以通过以下两个方面验证且必须同时满足：

1） NHP 代理和 NHP 服务器输出基于噪声协议的密钥协商及校验每个步骤的日志，通过检查日志记录可以验证噪声协议的实现步骤是否符合规范。

2） NHP 代理和 NHP 服务器输出各自的公私钥，检查是否采用 ECC 密钥。

（3） 高可用验证

NHP 协议的高可用架构可以通过以下三个方面验证且必须同时满足：

1） 敲门验证的 NHP 服务器与 NHP 门禁服务不在同一个主机上。

2） 敲门验证服务可以横向弹性扩展成多台主机，选择其中任何一个服务器发送敲门数据包都可以完成同一个业务会话的敲门验证。

3） 门禁与被保护资源的所在主机 IP 地址由 NHP 敲门验证服务动态返回给 NHP 代理，而不是静态的，利于实现多台服务器之间的负载均衡。

（4） 扩展性验证

NHP 协议的可扩展架构可以通过以下四个方面验证且必须同时满足：

1） NHP 代理与 NHP 服务器的通信是双向的。

2） 身份认证与权限鉴定可由外部授权服务提供商 ASP 来完成，ASP 接受来自 NHP 服务器的 NHP 代理信息数据之后，对身份认证与权限鉴定做出判别，NHP 代理将收到 ASP 的判别结果。

3） NHP 消息的类型是可扩展的，新的扩展消息可以交由 ASP 处理之后并把处理结果返回给 NHP 代理。

4） 数据资源服务器的标识可以是任意字符串，而不是局限于域名形式。NHP 服务器可以根据标识字符串返回正确的数据资源服务器 IP 地址。

（5） 兼容性验证

NHP 协议的信创兼容性可以通过以下几个方面验证且必须同时满足：

1）NHP 协议同时支持国际加密算法与国密加密算法进行验证。使用上述不同算法的时候，数据包头的长度不同，加密的时间也不同。

2）NHP 协议的实现代码必须同时支持至少一种信创生态的 CPU 硬件和操作系统平台。

4、主要试验（或验证）的分析、综述报告：

零信任安全的重要理念为“持续验证、用不信任”，所以零信任网络隐身协议重点之一为提升验证环节中的计算性能与降低传输延时。协议要求通信双方进行身份的互相验证与消息的随机加密，标准工作组对此进行了详细的测试与验证，对比传统的直接使用 RSA 非对称加密和签名算法，证明了零信任网络隐身协议中噪声算法具有更高的性能，更强的安全性与更低的报文尺寸开销。

表B. 1　RSA 与 ECC 安全强度与密钥长度

	最小公钥长度（比特）		密钥长度比	
安全强度（比特）	DSA/RSA	ECC	ECC 比 DSA/RSA	有效性
80	1024	160-223	1:6	到 2010 年
112	2048	224-255	1:9	到 2030 年
128	3072	256-383	1:12	2031 年以后
192	7680	384-511	1:20	
256	15360	512+	1:30	

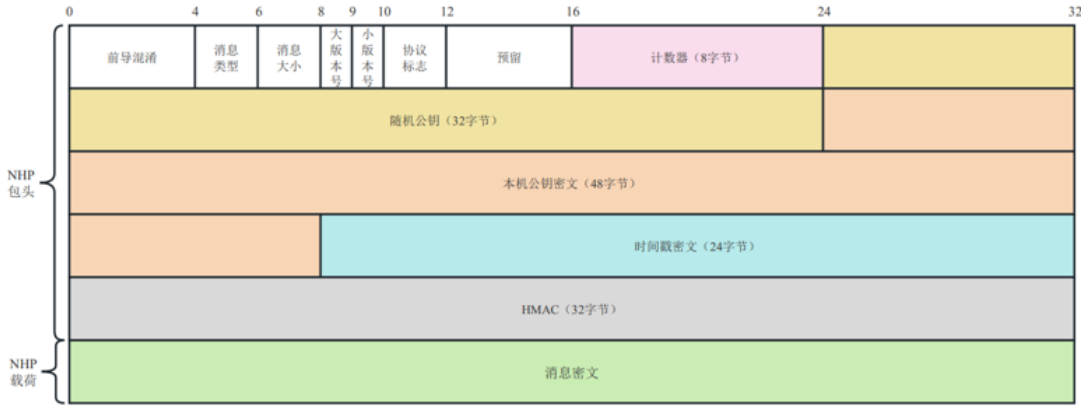


图3 NHP 协议包头（标准长度）

协议	计算步骤	运算次数	耗时（微秒）@intel-i7 Win10	性能比
SPA协议	使用RSA2048生成公私钥对、 使用私钥对189字节数据进行哈希并签名， 使用公钥对签名进行验证	10	4373992	1.00
NHP噪声协议（国际算法）	使用Curve25519生成公私钥对A、B、 A私钥与B公钥交叉、 对189字节数据进行AES256加密形成密文、 A公钥与B私钥交叉、 对密文进行AES256解密获取原文	10	3733	1171.00
NHP噪声协议（国密算法）	使用SM2生成公私钥对A、B、 A私钥与B公钥交叉、 对189字节数据进行SM4加密形成密文、 A公钥与B私钥交叉、 对密文进行SM4解密获取原文	10	3926	1141.00

5、标准在起草过程中遇到的问题及解决办法、重大分歧意见的处理经过和依据、有无重要技术问题需要说明：

在历次协议起草技术研讨会中，标准工作组组织并记录各起草单位专家发表的问题、意见与建议，并对协议文档进行必要的修订与完善，修改完成后会形成新的文稿版本，并在发布时对专家提出的每条建议进行逐一回复。

在工程实践方面，标准工作组对在复杂应用网络场景中实际产生的一系列问题提供了具体消息流程与解决办法，例如公钥分发、服务发现、防御 DDoS 攻击、报文中继、日志上传等，并将其内容收录于附录中。

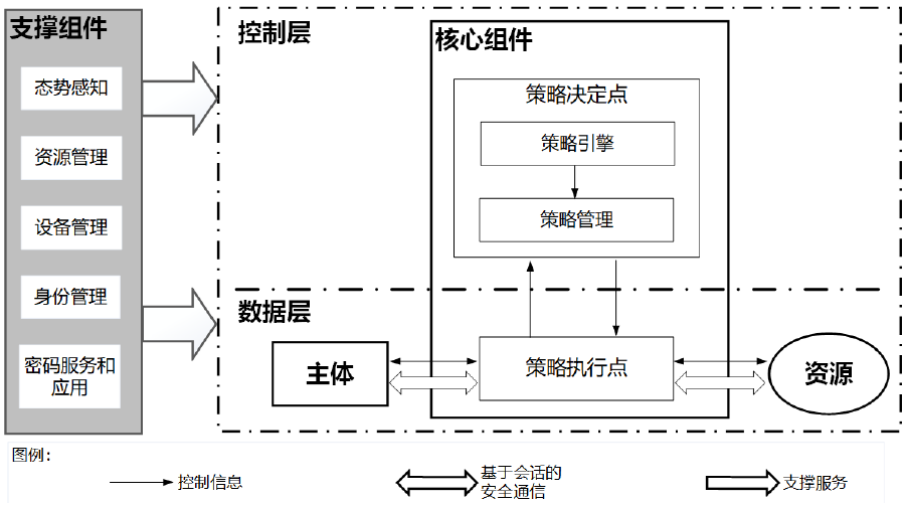
表A. 1　NHP 协议消息列表

名称	类型	描述
NHP-KPL	0	用于支持协议双方保活机制。
NHP-KNK	1	用于 NHP 代理向服务器发起敲门请求。
NHP-ACK	2	用于 NHP 服务器向 NHP 代理回应敲门结果。
NHP-QRY	N/A	用于 NHP 服务器向服务提供商查询 NHP 代理的授权（非 NHP 包头）。
NHP-AUT	N/A	用于服务提供商向 NHP 服务器回复 NHP 代理授权结果（非 NHP 包头）。
NHP-AOP	3	用于 NHP 服务器向 NHP 门禁请求开关门操作。
NHP-ART	4	用于 NHP 门禁向 NHP 服务器回复开关门结果。
NHP-LST	5	用于 NHP 代理或 NHP 门禁向 NHP 服务器发起服务发现查询。
NHP-LRT	6	用于 NHP 服务器向 NHP 代理或 NHP 门禁回复查询结果。
NHP-COK	7	用于 NHP 服务器向 NHP 代理发送 cookie。
NHP-RKN	8	用于 NHP 代理向 NHP 服务器发起二次敲门请求。
NHP-RLY	9	用于 NHP 中继向 NHP 服务器转发敲门或发现请求。
NHP-AOL	10	用于 NHP 门禁向 NHP 服务器报告自身在线状态。
NHP-AAK	11	用于 NHP 服务器向门禁确认连接成功。
NHP-OTP	12	用于 NHP 代理向服务器申请生成一次性验证码。
NHP-REG	13	用于 NHP 代理向服务器注册自身的公钥。
NHP-RAK	14	用于 NHP 服务器确认 NHP 代理注册成功。
NHP-ACC	15	用于 NHP 代理访问门禁的随机临时端口。
NHP-LOG	16	用于 NHP 门禁向 NHP 服务器上报日志。
NHP-LAK	17	用于 NHP 服务器向 NHP 门禁回复日志消息接收成功。

6、与国外标准、其他标准或文件的关系：包括：采用国际标准和国外先进标准的程度，与国外标准主要技术内容的差异、与有关的现行法律、法规和强制性国家标准的关系（可引用标准前言的内容）：

《零信任网络隐身协议》起源于国际云安全联盟《软件定义边界（SDP）标准规范 V2.0》中的单包授权协议（SPA），但自身采用了重新设计与优化的协议框架以实现按网络隐身与授权访问。国外尚未发布改进版的 SPA 协议。

零信任网络隐身协议也符合国家标准《信息安全技术 零信任参考体系架构》（报批稿）中规定的体系架构。



零信任网络隐身协议为 GB/T 39204-2022《信息安全技术 关键信息基础设施安全保护要求》提供了一种切实的解决方案。

零信任网络隐身协议在噪声协议算法中使用了商密国家标准 GB/T 32918.3-2016《信息安全技术 SM2 椭圆曲线公钥密码算法》、GB/T 32905-2016《信息安全技术 SM3 密码杂凑算法》、GB/T 32907-2016《信息安全技术 SM4 分组密码算法》，对应的国外算法标准为 RFC8422《Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier》、NIST FIPS 180-4《Secure Hash Standard (SHS)》、NIST FIPS 197《Advanced Encryption Standard》。

7、标准是否涉及知识产权的情况说明，如标准中含有自主知识产权，说明产品研发程度、产业化基础及进程：

暂无

8、贯彻标准的要求和措施建议：

暂无

9：其他应予说明的事项：

暂无