《自主可控网络安全技术——机密计算安全服务接口规范》

（征求意见稿）编制说明

一、工作简况

（一）任务来源

本团体标准由中关村华安关键信息基础设施安全保护联盟提出并归口。旨在针对自主可控网络安全技术中的机密计算安全服务接口规范相关问题制定标准，以满足网络安全防护在自主可控方面不断增长的需求。

（二）协作单位

本标准的起草单位包括麒麟软件有限公司、奇安信科技集团股份有限公司、飞腾信息技术有限公司、中关村华安关键信息基础设施安全保护联盟、北京源堡科技有限公司、中电（海南）联合创新研究院有限公司、华北电力大学等。这些单位在网络安全、信息技术、自主可控技术研发等领域具有丰富的经验和技术实力，涵盖了从软件到硬件、从科研机构到企业的多个层面，为标准的起草提供了广泛的技术和专业支持。

（三）主要工作过程

1. **预研阶段**
   - 各起草单位对自主可控网络安全技术领域的现状进行了深入调研，特别是针对机密计算安全服务接口方面存在的问题进行了梳理。研究发现，随着信息技术的发展，自主可控网络安全面临着诸如信息技术产品“后门”、供应链不可控等风险，而机密计算安全服务接口的标准化对于解决这些问题至关重要。
   - 对国内外相关标准和技术文献进行收集和分析，了解机密计算安全服务接口在不同地区和行业的应用情况以及相关标准的制定情况，为标准的制定奠定了坚实的理论基础。
2. **起草小组组建**
   - 根据各单位的专业优势和技术特长，组建了由网络安全专家、软件开发工程师、硬件技术人员等多学科背景人员构成的起草小组。起草小组成员包括于博、纪胜龙、张大朋、战茅、靳佑鼎、王震、王舒、姬一文、张帆、岳佳圆、杨诏钧、吴彤、于晴晴、张建林、杨伟平、张坤、陈晓峰、常凯翔、郦文琪、廖菁菁等。
   - 明确了起草小组各成员的职责和分工，确保标准起草工作有序进行。
3. **标准起草**

- 起草小组依据 GB/T 1.1 - 2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定，结合前期调研成果和实际需求，开始起草《自主可控网络安全技术 - 机密计算安全服务接口规范》（征求意见稿）。
- 在起草过程中，充分考虑了自主可控网络安全技术的特点以及机密计算安全服务接口在不同应用场景下的需求，重点对安全服务接口的定义、功能要求、接口参数、版本管理等方面进行了规范。
- 针对安全模块实现所需的系统接口、不同系统安全功能协同、跨平台互联互通以及用户应用程序迁移和维护等涉及机密计算安全服务接口的一致性和统一性问题进行了详细的规定，以确保通过该标准能够实现机密计算安全服务的标准化，为上层应用程序提供统一的机密计算服务接口及安全服务。

4. **内部评审与修改**
   - 起草小组完成初稿后，组织内部评审会议。各起草单位代表和起草小组成员对标准初稿进行了细致的审查，从技术准确性、内容完整性、条款合理性、语言规范性等多个方面提出了修改意见和建议。
   - 根据内部评审意见，起草小组对标准进行了认真修改完善，进一步优化了标准的结构和内容，提高了标准的质量。

二、标准编制原则和确定标准主要内容的依据

（一）编制原则

1. **科学性原则**
   - 本标准以科学的网络安全理论和自主可控技术原理为基础，确保标准内容准确反映机密计算安全服务接口的技术内涵和要求。在标准起草过程中，参考了大量国内外权威的网络安全研究成果和技术文献，借鉴了相关领域的科学研究方法和实践经验。
2. **实用性原则**
   - 标准的制定紧密结合实际应用需求，重点关注解决自主可控网络安全技术在实际应用中面临的问题，如不同系统之间的安全功能协同、跨平台互联互通、用户应用程序迁移和维护等。通过规范机密计算安全服务接口，提高网络安全防护的效率和能力，为相关企业和机构在自主可控网络安全建设方面提供切实可行的技术依据和操作指南。
3. **协调性原则**
   - 充分考虑与现有国家标准、行业标准以及国际标准的协调性。在制定过程中，对相关标准进行了深入研究，避免与现有标准产生冲突，并尽量采用已有的通用技术术语和定义，确保本标准能够与其他相关标准相互衔接、配套使用。
4. **前瞻性原则**

- 在满足当前自主可控网络安全技术需求的基础上，适当考虑未来技术发展趋势，为机密计算安全服务接口的技术创新和应用拓展预留一定的空间。例如，在接口参数的定义和版本管理方面，采用了较为灵活的设计方式，以便能够适应未来可能出现的新技术和新应用场景。

（二）确定标准主要内容的依据

1. **技术需求分析**
   - 通过对自主可控网络安全技术的深入研究和实际应用场景的分析，明确了机密计算安全服务接口在自主可控网络安全体系中的关键地位和作用。例如，安全模块的实现依赖于系统提供的接口，而不同系统之间的安全功能协同等需求要求解决机密计算安全服务接口的一致性和统一性问题，这成为确定标准中关于接口一致性、参数规范等内容的重要依据。
2. **行业最佳实践**
   - 借鉴了行业内在自主可控网络安全技术应用方面的最佳实践经验。各起草单位在实际工作中积累了丰富的网络安全建设和管理经验，这些经验在标准制定过程中得到了充分体现。例如，在安全服务接口的功能要求方面，参考了部分企业在机密计算安全服务实际应用中的功能需求和实现方式，确保标准内容具有可操作性和实用性。
3. **相关标准参考**
   - 参考了国内外相关的网络安全标准、信息技术标准以及标准化文件的结构和起草规则等标准。如 GB/T 1.1 - 2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》为本标准的结构和起草提供了规范依据；同时，还参考了部分国际网络安全标准中关于机密计算安全服务接口的相关规定，使本标准在内容上与国际标准接轨，提高了标准的通用性和国际认可度。

三、主要试验（或验证）的分析、综述，技术经济论证，预期的经济效果

（一）主要试验（或验证）的分析、综述

1. **接口功能验证**
   - 在标准起草过程中，部分起草单位对机密计算安全服务接口的功能进行了初步的试验验证。通过构建模拟的自主可控网络安全环境，采用不同的硬件平台和软件系统，对标准中规定的安全服务接口功能进行测试。结果表明，按照标准定义的接口功能能够满足基本的机密计算安全服务需求，如数据加密、访问控制、安全审计等功能在不同平台和系统之间能够实现有效的协同。
   - 在接口功能验证过程中，发现了一些在实际应用中可能出现的问题，如部分接口在跨平台调用时存在性能损耗的情况。针对这些问题，起

草小组对标准中的接口参数和调用方式进行了优化调整，以提高接口的性能和稳定性。

2. **接口一致性验证**
   - 为验证标准中关于机密计算安全服务接口一致性的要求，起草单位采用了多组不同的安全模块和应用程序进行测试。在测试过程中，确保这些安全模块和应用程序分别基于不同的硬件架构和软件系统开发，以模拟实际应用中的多样性。测试结果显示，当按照标准规定的接口一致性要求进行开发和集成时，不同的安全模块和应用程序能够实现有效的互联互通，验证了标准中关于接口一致性要求的合理性和可行性。

（二）技术经济论证

1. **技术可行性**
   - 从技术角度来看，本标准所涉及的机密计算安全服务接口规范是在充分调研和试验验证的基础上制定的。起草单位具备丰富的网络安全技术研发和应用经验，在标准起草过程中充分考虑了当前自主可控网络安全技术的发展水平和实际应用需求。通过对接口功能、一致性等方面的验证，证明了标准内容在技术上是可行的，能够为自主可控网络安全技术中的机密计算安全服务提供有效的技术规范。
2. **经济合理性**
   - 在经济方面，本标准的实施将有助于降低自主可控网络安全建设的成本。通过实现机密计算安全服务接口的标准化，能够减少不同系统和平台之间的兼容性问题，提高安全模块和应用程序的复用性，降低开发和维护成本。例如，企业在进行自主可控网络安全系统建设时，无需针对不同的硬件和软件平台重新开发安全服务接口，可直接按照本标准进行接口的对接和集成，从而节省大量的人力、物力和财力资源。

（三）预期的经济效果

1. **提高产业竞争力**
   - 本标准的发布实施将有助于提升我国自主可控网络安全产业的整体竞争力。标准的统一将促进产业链上下游企业之间的协同发展，提高产品的兼容性和互操作性，有利于企业扩大市场份额，增强在国内外市场的竞争力。
2. **推动行业发展**
   - 预期本标准将对自主可控网络安全技术行业的发展产生积极的推动作用。通过规范机密计算安全服务接口，将吸引更多的企业和机构投入到自主可控网络安全技术的研发和应用中，促进技术创新和产业升级，推动整个行业朝着更加规范化、标准化的方向发展。
3. **降低社会成本**

- 在社会层面，本标准的实施将有助于降低整个社会在网络安全建设方面的成本。随着不同企业和机构按照标准建设自主可控网络安全系统，将减少因接口不统一而导致的重复开发和资源浪费现象，提高网络安全资源的利用效率，为社会节约大量的经济成本。

四、采用国际标准和国外先进标准的程度，以及与国际、国内同类标准水平的对比情况

（一）采用国际标准和国外先进标准的程度

在本标准起草过程中，对国际标准和国外先进标准进行了广泛的研究和参考。虽然目前尚未直接采用某一特定的国际标准或国外先进标准，但在标准的技术内容方面，借鉴了国际上关于机密计算安全服务接口相关的先进理念和技术方法。例如，在接口参数的定义、安全功能的设计等方面，参考了部分国际网络安全标准中的通用做法，以确保本标准在技术水平上与国际接轨。

（二）与国际、国内同类标准水平的对比情况

1. 与国际同类标准对比
   - 在国际上，虽然有一些关于网络安全和机密计算方面的标准，但专门针对自主可控网络安全技术下机密计算安全服务接口规范的标准尚未发现。本标准在结合我国自主可控网络安全技术发展需求的基础上，对机密计算安全服务接口进行了全面、系统的规范，在一定程度上填补了国际上在这一领域的空白。同时，本标准在接口一致性、跨平台互联互通等方面的规定具有一定的创新性，与国际同类标准相比，具有鲜明的特色和优势。
2. 与国内同类标准对比
   - 在国内，目前也存在一些网络安全相关的标准，但针对自主可控网络安全技术中的机密计算安全服务接口规范的标准较少。本标准与国内其他网络安全标准相互补充，重点聚焦于自主可控网络安全技术领域的机密计算安全服务接口问题，在内容上更加具体、细化，对推动我国自主可控网络安全技术的发展具有独特的意义。

五、与有关的现行法律、法规和强制性标准的关系

本标准在制定过程中，严格遵循我国现行的法律法规要求，确保标准内容不与法律法规相冲突。同时，本标准与现行的强制性标准保持协调一致。在网络安全领域，本标准是对现有标准体系的补充和完善，旨在针对自主可控网络安全技术中的机密计算安全服务接口规范问题提供具体的标准依据，与其他强制性和推荐性标准共同构建完整的网络安全标准体系，为我国网络安全建设提供全面的技术支持。

六、重大分歧意见的处理经过和依据

在本标准的起草过程中，未出现重大分歧意见。起草小组成员在标准的编制原则、主要内容、试验验证等方面基本达成一致。对于一些小的意见分歧，如部分接口参数的取值范围等问题，通过查阅相关技术文献、进行内部技术讨论以及参考实际应用经验等方式，最终达成了共识。

七、标准作为团体标准的必要性

1. **满足特定行业需求**
   - 在自主可控网络安全技术领域，机密计算安全服务接口的标准化是实现网络安全防护效率与能力提升的关键。本团体标准专门针对这一特定领域的需求制定，能够满足中关村标准化协会成员单位以及整个自主可控网络安全行业在机密计算安全服务接口规范方面的需求，为行业发展提供技术支持。
2. **促进技术创新与交流**
   - 作为团体标准，它将为自主可控网络安全技术领域的企业和机构提供一个统一的技术交流平台。通过制定和推广本标准，能够促进企业之间在机密计算安全服务接口技术方面的创新与交流，鼓励企业在遵循标准的基础上进行技术研发和应用实践，推动行业技术水平的不断提高。
3. **填补标准空白**
   - 在我国现行的标准体系中，针对自主可控网络安全技术下机密计算安全服务接口规范的标准相对较少。本团体标准的制定将填补这一空白，完善我国网络安全标准体系，为自主可控网络安全技术的发展提供更为全面、系统的标准依据。

八、贯彻标准的要求和措施建议

（一）贯彻标准的要求

1. **宣传推广**
   - 中关村标准化协会应积极开展本标准的宣传推广工作，通过举办标准宣贯会、技术研讨会等形式，向会员单位和相关企业、机构介绍本标准的内容、意义和作用，提高标准的知晓度和影响力。
2. **培训教育**
   - 组织开展针对本标准的培训教育活动，邀请标准起草专家对相关人员进行培训，使其深入理解标准的技术内容和实施要求，为标准的贯彻实施提供人员保障。
3. **示范应用**
   - 鼓励部分有条件的会员单位率先开展本标准的示范应用，通过实际应用案例展示标准的可行性和有效性，为其他企业和机构贯彻实施标准提供借鉴经验。

（二）措施建议

1. **建立监督机制**
   - 中关村标准化协会应建立对本标准贯彻实施情况的监督机制，定期对会员单位和相关企业的标准执行情况进行检查和评估，确保标准得到有效贯彻实施。
2. **反馈与改进**
   - 在标准贯彻实施过程中，建立反馈渠道，及时收集企业和机构在应用标准过程中遇到的问题和意见，以便对标准进行适时的修订和完善，提高标准的适应性和实用性。

九、废止现行有关标准的建议

本标准为新制定的团体标准，不存在废止现行有关标准的情况。

十、其他应予说明的事项

在本标准的起草过程中，虽然已经进行了广泛的调研、试验验证和内部评审等工作，但由于自主可控网络安全技术仍在不断发展，可能存在一些未考虑到的情况。随着技术的发展和实际应用的深入，本标准将适时进行修订和完善，以确保其始终能够适应行业发展的需求。同时，由于本文件的某些内容可能涉及专利，本文件的发布机构不承担识别专利的责任，各相关单位在使用本标准时应注意遵守相关的知识产权法律法规。