“一张图”实施监督信息系统
商用密码应用差距分析

江西智慧云测安全检测中心股份有限公司

2024 年 07 月 17 日

声　明

本文档是”一张图”实施监督信息系统密评差距分析，本文档的编制依据”一张图”实施监督信息系统现场评估情况进行分析，并结合现有的密码产品、密码技术和密码服务，参照 GB/T 39786-2021 《信息安全技术信息系统密码应用基本要求》和《信息系统密码应用高风险判定指引》的相关要求，在不触发高风险的前提下，尽量考虑改进的可实施性。本差距分析不作为测评报告使用。

江西智慧云测安全检测中心股份有限公司

2024 年 07 月 17 日

1. 项目概述

江西智慧云测安全检测中心股份有限公司受临沧市自然资源和规划局的委托，于2024 年 07 月 11 日至 2024 年 07 月 12 日，根据等保定级报告的测评范围，依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的第三级别要求，确认本次测评网络边界、测评系统范围，针对物理与环境、网络与通信、设备与计算、应用与数据安全及相关管理制度进行差距分析，目前”一张图”实施监督信息系统不符合 GB/T 39786《信息安全 信息系统密码应用基本要求》第三级要求。本差距分析总结了被测系统目前存在的安全问题并提出改进建议，为其信息资产安全和业务持续稳定运行提供保障。

2. 参考依据

- GB/T 39786-2021 《信息安全技术信息系统密码应用基本要求》
- GM/T 0115-2021《信息系统密码应用测评要求》
- 《信息系统密码应用高风险判定指引》
- 《商用密码应用安全性评估量化评估规则》
- GM/T 0014-2012《证书认证系统密码协议规范》
- GM/T 0022-2014《IPSEC VPN技术规范》
- GM/T 0023-2014《IPSEC VPN网关产规范》
- GM/T 0024-2014《SSL VPN 技术规范》
- GM/T 0025-2014《SSL VPN 网关产品规范》
- GM/T 0027-2014《智能密码钥匙技术规范》
- GM/T 0028-2014《密码模块安全技术要求》
- GM/T 0029-2014《签名验签服务器技术规范》
- GM/T 0030-2014《服务器密码机技术规范》

3. 网络拓扑结构

“一张图”实施监督信息系统部署在本地机房，各网络通道情况主要包括：

①业务专网非国密浏览器与应用系统之间的通信信道，系统用户在业务专网环境下通过非国密浏览器采用 HTTP 协议访问应用系统。

②业务专网运维终端与通用服务器之间的运维通信信道，运维用户在业务专网环

境下通过管理工具采用 SSH 协议访问通用服务器。

③业务专网运维终端与数据库管理系统（PgSQL 与 MongoDB）之间的运维通信信道，运维用户在业务专网环境下通过管理工具采用数据库协议访问数据库管理系统。

4. 密码应用技术层面差距分析

4.1. 物理安全和环境安全

4.1.1. 当前现状

①身份鉴别（高风险*）：”一张图”实施监督信息系统所在本地机房未部署具有商用密码产品认证证书的安全门禁系统、视频监控安全管理系统等物理安防基础设施，在物理访问身份鉴别采用口令/生物识别（指纹）/刷 ID 卡等方式实现身份鉴别，未采用密码技术保证机房进出人员的身份鉴别。

②电子门禁记录数据存储完整性：”一张图”实施监督信息系统所在本地机房未部署具有商用密码产品认证证书的安全门禁系统、视频监控安全管理系统等物理安防基础设施，未采用密码技术保证电子门禁记录数据的完整性。

③视频监控记录数据存储完整性：”一张图”实施监督信息系统所在本地机房未部署具有商用密码产品认证证书的安全门禁系统、视频监控安全管理系统等物理安防基础设施，未采用密码技术保证视频监控记录的存储完整性。

4.1.2. 改进建议

①建议在所属机房部署符合 GM/T 0036-2014 《采用非接触卡的门禁系统密码应用技术指南》的电子门禁系统，基于 SM4 算法进行密钥分散，实现门禁卡的“一卡一密”，为机房进出人员配发具有商用密码产品认证证书的身份识别卡，并基于 SM4 算法对人员身份进行鉴别。具体如下图所示：

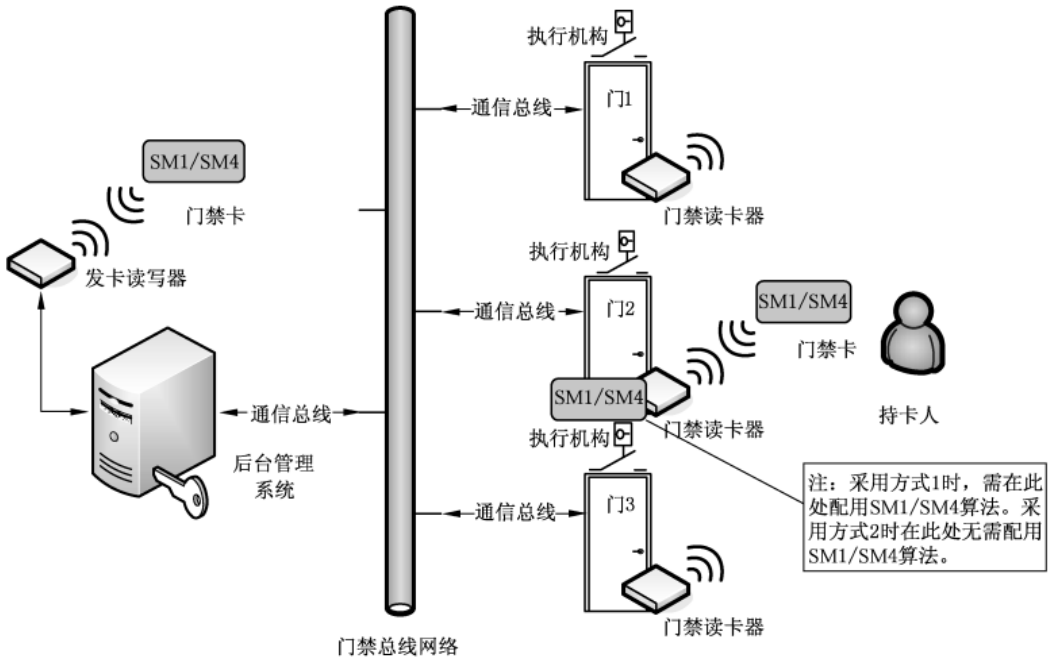

图4- 1门禁系统示意图

②建议调用合规的服务器密码机基于 HAMC-SM3 算法对电子门禁记录数据计算 MAC，并将 MAC 存储在数据库中，读取数据时再次调用服务器密码机计算 MAC 进行比对，以保证电子门禁记录数据存储完整性。

③建议调用合规的服务器密码机基于 HAMC-SM3 算法对视频监控记录数据计算 MAC，并将 MAC 存储在数据库中，读取数据时再次调用服务器密码机计算 MAC 进行比对，以保证视频监控记录数据存储完整性。

4.2. 网络和通信安全

4.2.1. 当前现状

①业务专网非国密浏览器与应用系统之间的通信信道未部署合规的 SSL VPN 设备，系统用户在业务专网环境下通过非国密浏览器采用 HTTP 协议访问应用系统，未采用密码技术保证通信实体身份真实性；未采用密码技术保证通信数据完整性、机密性；未采用密码技术保证网络边界访问控制信息的完整性。

②业务专网运维终端与通用服务器之间的运维通信信道未部署合规的 SSL VPN 设备，运维用户在业务专网环境下通过管理工具采用 SSH 协议访问通用服务器，未采用合规的密码技术保证通信实体身份真实性；未采用合规的密码技术保证通信数据完整性、机密性；未采用密码技术保证网络边界访问控制信息的完整性。

③业务专网运维终端与数据库管理系统（PgSQL 与 MongoDB）之间的运维通信信道

未部署合规的 SSL VPN 设备，运维用户在业务专网环境下通过管理工具采用数据库协议访问数据库管理系统（PgSQL 与 MongoDB），未采用符合密码相关国家标准或行业标准的密码技术保证通信实体身份真实性；未采用符合密码相关国家标准或行业标准的密码技术保证通信数据完整性、机密性；未采用密码技术保证网络边界访问控制信息的完整性。

4.2.2. 改进建议

①建议业务专网非国密浏览器与应用系统之间的通信信道，通过在终端部署国密浏览器与合规的 SSL VPN 网关设备建立 TLCP 协议通道，通过 SSL VPN 网关代理转发 TLCP 协议访问应用系统，TLCP 协议基于数字证书实现通信实体身份鉴别，涉及相关数字证书由合规的第三方 CA 机构颁发国密双证书，以保证通信实体身份的真实性；将 SSL VPN 网关后台配置密码套件为 ECC_SM4_SM3，通过 HMAC-SM3 算法保证通信数据完整性，通过 SM4 算法保证通信数据机密性，通过 SSL VPN 网关自身机制实现网络边界访问控制信息的完整性。

②+③建议业务专网运维终端与通用服务器之间的运维通信信道、业务专网运维终端与数据库管理系统（PgSQL 与 MongoDB）之间的运维通信信道，通过在终端部署 VPN 客户端与合规的 SSL VPN 网关设备建立 TLCP 协议通道，通过 SSL VPN 网关代理转发 TLCP 协议访问堡垒机（需新增堡垒机设备进行统一运维管理通用服务器及数据库管理系统），TLCP 协议基于数字证书实现通信实体身份鉴别，涉及相关数字证书由合规的第三方 CA 机构颁发国密双证书，以保证通信实体身份的真实性；将 SSL VPN 网关后台配置密码套件为 ECC_SM4_SM3，通过 HMAC-SM3 算法保证通信数据完整性，通过 SM4 算法保证通信数据机密性，通过 SSL VPN 网关自身机制实现网络边界访问控制信息的完整性。

Ps：当前与第三方系统之间的通信信道暂未启用，本次不纳入测评范围内，建议提前准备 IPSec 网关，以备后续与第三方系统间通道启用时可通过 IPSec 网关与第三方系统所在机房间 IPSec 网关建立国密 IPSec 协议实现通道加密。

4.3. 设备和计算安全

4.3.1. 当前现状

①身份鉴别（高风险*）：运维用户在运维终端通过管理工具采用账号+口令的方式管理通用服务器、数据库管理系统（PgSQL 与 MongoDB），未采用密码技术保证登

录设备用户身份的真实性。

②远程管理通道安全（高风险*）：通用服务器运维时，采用 SSH 协议连接，未采用符合密码相关国家标准或行业标准的密码技术保证远程管理通道安全；数据库管理系统运维时，采用数据库协议连接，未采用符合密码相关国家标准或行业标准的密码技术保证远程管理通道安全。

③系统资源访问控制信息完整性：通用服务器、数据库管理系统的系统资源访问控制信息存储时未进行完整性保护，未采用密码技术保证系统资源访问控制信息完整性。

④日志记录完整性：通用服务器、数据库管理系统的日志在记录存储时未进行完整性保护，未采用密码技术保证日志记录完整性。

⑤重要可执行程序完整性、重要可执行程序来源真实性：未采用密码技术对通用服务器、数据库管理系统的重要可执行程序的完整性和真实性进行保护。

4.3.2. 改进建议

①

1）建议所有设备均通过堡垒机（新增合规堡垒机）统一运维，采用账号+口令+UKEY 方式进行登录，为运维用户配发 UKEY 采用 SM2 数字签名机制实现登录人员身份鉴别，在 UKEY 中内置国密签名加密双证书，涉及的数字证书均由具有电子认证服务许可资质的单位颁发签名加密双证书，客户端向服务端请求随机数，服务端调用签名验签服务器生成随机数后传输到客户端，在客户端调用 UKEY 对随机数进行签名，将签名值和证书发送给服务端，服务端调用签名验签服务器，签名验签服务器对证书和签名值依次验证，若验证通过，则用户登录成功，可以保证登录设备用户身份的真实性。【优点：前端采用硬件设备，密钥存储方面更加安全；缺点：需随身携带 UKEY，用户使用不方便，牺牲便利性】

2）建议所有设备均通过堡垒机（新增合规堡垒机）统一运维，采用账号+口令+动态令牌方式进行登录，为运维用户配发具有商用密码产品认证证书的动态令牌（移动端 APP），配合后端具有商用密码产品认证证书的动态令牌认证系统采用合规的密码算法实现登录人员身份鉴别，可以保证登录设备用户身份的真实性。【优点：用户可通过移动端 APP 获取动态口令，无需携带硬件设备，便利性更好一些；缺点：软件密码模块密钥存储安全性略低于硬件设备（密码模块等级足够，安全性也可以拿满分）】

②建议使用具有商用密码产品认证证书的SSL VPN代理转发HTTPS协议，通过国密浏览器访问堡垒机，使用核准的密码技术，提高堡垒机与各运维设备通信时，通信协议的版本及密码套件的安全强度，保证远程管理通道安全。

③建议调用合规的服务器密码机，采用HMAC-SM3算法对所有被测设备的系统资源访问控制信息计算MAC值，并将MAC值存储在数据库中，调用系统资源访问控制信息时，重新计算MAC值与数据库中的MAC值进行比对，以保证系统资源访问控制信息完整性。

④建议调用合规的服务器密码机，采用HMAC-SM3算法对所有被测设备的日志记录计算MAC值，并将MAC值存储在数据库中，调用日志记录时，重新计算MAC值与数据库中的MAC值进行比对，以保证日志记录完整性。

⑤建议通过调用合规的服务器密码机对所有被测设备的重要可执行程序，使用HMAC-SM3算法进行完整性保护，并在执行或查看重要可执行程序时进行二次校验对比；调用合规的签名验签服务器的SM2算法采用数字签名机制对其来源真实性进行验证，保证重要可执行程序来源真实性。

4.4. 应用和数据安全

4.4.1. 应用与数据层面保护对象

本次差距分析评估涉及最小范围的关键数据如下所示，建议严格按照本表格进行改造。

表 5- 1 应用和数据安全层面保护对象

应用名称	类别	具体保护对象	安全需求
“一张图”实施监督信息系统	应用用户	系统用户	真实性
		管理员用户	真实性
	重要数据	身份鉴别信息（登录口令）	☑传输机密性 ☑存储机密性 ☑传输完整性 ☑存储完整性
		个人隐私信息（身份证号、手机号、邮箱）	☑传输机密性 ☑存储机密性

			☑传输完整性 ☑存储完整性
		重要业务数据（地图二维数据）	☐传输机密性 ☐存储机密性 ☑传输完整性 ☑存储完整性
		日志数据（登录日志、操作日志）	☐传输机密性 ☐存储机密性 ☑传输完整性 ☑存储完整性
	操作行为	无	不可否认性

4.4.2. 当前现状

①身份鉴别（高风险*）：系统用户、系统管理员通过非国密浏览器采用账号+口令的方式进行身份鉴别，未采用密码技术对登录用户进行身份鉴别，不能保证应用系统用户身份的真实性。

②访问控制信息完整性：被测系统由权限管理和角色管理进行访问控制，本系统未采用密码技术保证信息系统应用的访问控制信息的完整性。

③重要数据传输机密性（高风险*）：被测系统身份鉴别数据、个人隐私数据目前以明文形式进行传输，未采用密码技术保证系统的重要数据在传输过程中的机密性。

④重要数据存储机密性（高风险*）：被测系统身份鉴别数据目前使用哈希算法实现存储机密性；个人隐私数据明文存储，未采用密码技术实现重要数据存储机密性保护。

⑤重要数据传输完整性：被测系统身份鉴别数据、个人隐私数据、重要业务数据、日志数据目前以明文形式进行传输，未采用密码技术保证系统的重要数据在传输过程中的完整性。

⑥重要数据存储完整性（高风险*）：被测系统身份鉴别数据、个人隐私数据、重要业务数据、日志数据目前未采用密码技术实现重要数据存储完整性。

4.4.3. 改进建议

①在身份鉴别方面

1）建议系统用户、管理员用户采用账号+口令+UKEY 方式进行登录，为用户配发 UKEY 采用 SM2 数字签名机制实现登录人员身份鉴别，在 UKEY 中内置国密签名加密双证书，涉及的数字证书均由合规第三方 CA 机构颁发国密签名加密双证书，客户端向服务端请求随机数，服务端调用数字签名服务器生成随机数后传输到客户端，在客户端调用 UKEY 对随机数进行签名，将签名值和证书发送给服务端，服务端调用数字签名服务器，数字签名服务器对证书和签名值依次验证，若验证通过，则用户登录成功，可以保证登录系统用户身份的真实性。【优点：前端采用硬件设备，密钥存储方面更加安全；缺点：需随身携带 UKEY，用户使用不方便，牺牲便利性】

2）建议系统用户、管理员用户采用账号+口令+动态令牌方式进行登录，为用户配发具有商用密码产品认证证书的动态令牌（移动端 APP），配合后端具有商用密码产品认证证书的动态令牌认证系统采用合规的密码算法实现登录人员身份鉴别，可以保证登录系统用户身份的真实性。【优点：用户可通过移动端 APP 获取动态口令，无需携带硬件设备，便利性更好一些；缺点：软件密码模块密钥存储安全性略低于硬件设备（密码模块等级足够，安全性也可以拿满分）】

②在访问控制信息完整性方面，建议调用合规的服务器密码机或数据库透明加解密系统，采用 HMAC-SM3 算法对访问控制信息采用 HMAC-SM3 算法进行完整性保护，后期系统使用到相关访问控制信息时，需再次调用服务器密码机的 HMAC-SM3 算法对重要数据计算哈希值，并通过比对方式验证与数据库存储的哈希值是否一致，以保证访问控制信息存储的完整性。

③数据传输机密性安全方面，被测系统重要数据在传输前应调用具有商用密码产品认证证书的密码模块采用 SM4-CBC 加密，加密完成后再对密文进行数据传输，服务器后端接收到加密传输的数据后，存储在本地数据库服务器中。

④数据传输完整性安全方面，被测系统重要数据在传输前应调用具有商用密码产品认证证书的密码模块采用 HMAC-SM3 实现完整性保护，完成后再对数据进行数据传输，服务器后端接收到数据后，需调用服务器密码机对报文进行完整性验证，以保证重要数据在传输过程中的完整性。

⑤数据存储机密性安全方面，被测系统重要数据在存入数据库之前应调用合规的服务器密码机或数据库透明加解密系统采用 SM4-CBC 算法对关键数据进行加密存储，

以保证重要数据存储的机密性。【服务器密码机：常规加密方式，针对各个字段调用加密机加解密接口进行分别改造，改造工作量稍大；数据库加解密系统：新型加密方式，应用系统与数据库之间部署数据库加解密系统，通过在数据库加解密系统中进行字段配置，实现数据存储机密性、完整性保护，改造工作量会更小】

⑥数据存储完整性安全方面，被测系统重要数据在存入数据库之前应调用合规的服务器密码机或数据库透明加解密系统采用 HMAC-SM3 算法进行计算后对哈希值进行存储，后期系统使用到此类重要数据时，需再次调用服务器密码机的 HMAC-SM3 算法对重要数据计算哈希值，并通过比对方式验证与数据库存储的哈希值是否一致，以保证重要数据存储的完整性。【服务器密码机：常规加密方式，针对各个字段调用加密机加解密接口进行分别改造，改造工作量稍大；数据库加解密系统：新型加密方式，应用系统与数据库之间部署数据库加解密系统，通过在数据库加解密系统中进行字段配置，实现数据存储机密性、完整性保护，改造工作量会更小】

5. 密码安全管理差距分析

5.1. 管理制度

5.1.1. 当前现状

①被测单位不具有密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；

②被测单位不具有密码应用方案，且未根据密码应用方案建立相应密钥管理规则；

③未对管理人员或操作人员执行的日常管理操作建立操作规程。

5.1.2. 改进建议

①应制定密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；

②应根据密码应用方案建立相应密钥管理规则；

③应对管理人员或操作人员执行的日常管理操作建立操作规程。

5.2. 人员管理

5.2.1. 当前现状

①未建立密码应用岗位责任制度，未明确各岗位在安全系统中的职责和权限；

②未建立上岗人员培训制度；

③未建立关键岗位人员保密制度和调离制度。

5.2.2. 改进建议

①应建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限：1） 根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位；2） 对关键岗位建立多人共管机制；3） 密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密钥管理员岗位不可与密码审计员、密码操作员等关键安全岗位兼任；4） 相关设备与系统的管理和使用账号不得多人共用；

②应建立上岗人员培训制度与考核制度；1）明确安全意识教育总则、安全教育的含义和方式以及安全教育制度和技能培训实施等相关内容；2）定期对密码应用安全岗位人员进行考核、对考核记录进行妥善保存；

③应建立关键岗位人员保密制度和调离制度：1）明确保密内容、双方的权利和义务、保密期限、保密津贴、违约责任、劳动争议处理；2）“人员离岗”，明确了对涉密信息系统访问授权的回收、文档材料的交接及归档等相关内容。

5.3. 建设运行

5.3.1. 当前现状

①被测单位未制定密码应用方案；

②未制定密钥安全管理策略；

③未制定实施方案；

④正式投入运行前未通过密码应用安全性评估；

⑤未定期开展攻防对抗演习。

5.3.2. 改进建议

①应依据密码相关标准和密码应用需求，制定密码应用方案，并邀请专家或密评机构进行评审；

②应根据密码应用方案，确定系统涉及的密钥种类、体系及其生命周期环节；

③应按照应用方案实施建设；

④正式投入运行前应通过密码应用安全性评估；

⑤在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行改进。

5.4. 应急处置

5.4.1. 当前现状

①未根据密码应用安全事件等级制定相应的密码应用应急策略；

②未定义安全事件发生时的处置措施等规定；

③未定义向有关主管部门上报处置情况等规定。

5.4.2. 改进建议

①应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置；

②事件发生后，应及时向信息系统主管部门进行报告；

③事件处置完成后，应及时向信息系统主管部门及所属地的密码管理部门报告事件发生情况及处置情况。

（以下内容为附录 A）

附录A 常见的密码产品部署建议

A.1. 编制目的

因商用密码应用安全性评估涉及各类密码产品及技术要求，江西智慧云测安全检测中心股份有限公司为推进密码应用的正确、合规、有效性，结合自身项目经验为被测系统建设单位提供具体的改进建议参考。

A.2. 免责声明

常见的密码产品部署要求仅适用于常见的密码应用安全问题，各信息系统建设单位需结合实际对被测系统网络、业务情况进行细化。

A.3. 适用范围

网络与通信安全层面、设备与计算层面、应用与数据安全层面常见的高风险问题。

A.4. 合规的VPN部署建议

A.4.1 SSL VPN

产品合规要求参考：符合 GM/T 0025-2014 《SSL VPN 网关产品规范》或GM/T 0026 《安全认证网关产品规范》、GM/T 0028 《密码模块安全技术要求》二级要求。

建议在需要保护的网络边界处部署具有商用密码产品认证证书的SSL VPN，并配置合规的数字证书，建议对SSL VPN配置为GMTLS协议，密码套件设置为ECC_SM4_SM3，结合实际情况统一为相关运维人员、设备管理员配发具有商用密码产品认证证书的USBKEY，并配置合规的数字证书。以保证通信实体身份的真实性及数据传输过程机密性、完整性。

A.4.2 IPSEC VPN

IPSEC VPN 产品合规要求参考：符合 GM/T 0023-2014 《IPSec VPN 网关产品规范》或GM/T 0026 《安全认证网关产品规范》、GM/T 0028 《密码模块安全技术要求》。

建议部署具有商用密码产品认证证书的IPSEC VPN设备，且配置为符合密码相关国家标准或行业标准的密码算法、配置合规的数字证书。以保证通信实体身份的真实性及数据传输过程机密性、完整性。

应为设备管理员人员配发具有商用密码产品认证证书的USBKEY，并配置合规的数字证书。

A.4.3 SSL 安全认证网关

产品合规要求参考： GM/T 0026 《安全认证网关产品规范》、GM/T 0028 《密码模块安全技术要求》二级要求。

建议在需要保护的网络边界处部署具有商用密码产品认证证书的SSL 安全认证网关，并配置合规的数字证书，建议对SSL 安全认证网关配置为GMTLS协议，密码套件设置为ECC_SM4_SM3，并配置合规的数字证书，并结合实际情况统一为相关用户是否需要配发具有商用密码产品认证证书的USBKEY，完成双向认证，以保证通信实体身份的真实性及数据传输过程机密性、完整性。

A.5. 合规的签名验签服务器、服务器密码机部署建议

产品合规要求参考： GM/T 0029《签名验签服务器技术规范》、GM/T 0030 《服务器密码机技术规范》、GM/T 0028 《密码模块安全技术要求》二级要求。

建议部署具有商用密码产品认证证书的服务器密码机于机房内部网络，设备管理员应采用账号+口令+USBKey的方式进行身份鉴别。并配置合规的数字证书，运维用户通过SSL安全网关代理转发GMTLS协议访问服务器密码机的后台管理系统。

注意：不允许多个信息系统使用同一台服务器密码机，应结合实际情况考虑采购云服务器密码机、搭建密码服务资源池来进行统一管理。

A.6. 身份鉴别改进建议

A.6.1 建议通过部署具有商用密码产品认证证书的统一身份认证系统、智能密码钥匙，应采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对登录用户进行身份鉴别，并确保应用系统用户身份真实性实现机制正确和有效。

A.6.2 建议通过部署具有商用密码产品认证证书的签名验签服务器、智能密码钥匙、国密浏览器，为系统用户统一配发智能密码钥匙并采用合规的数字证书与用户身份进行有效绑定，具体建议流程如下：

1）系统用户通过国密浏览器访问信息系统登录页面，客户端请求信息系统服务器生成随机数。

2）后端签名验签服务器生成合规的随机数并下发至客户端。

3）客户端使用随机数+用户身份鉴别信息通过调用智能密码钥匙中的SM2私钥生成签名值，并将随机数、用户身份鉴别信息、该用户公钥数字证书及其他数据发送服务器后端；

4）服务器后端接收到客户端发送的请求，应通过调用签名验签服务器采用SM2公钥进行验签，并验证用户身份、数字证书真实性。

A.7. 应用与数据安全层重要数据传输建议

应根据被测系统关键数据安全需求在传输前客户端应调用具有商用密码产品认证证书的密码模块采用SM4-CBC算法进行机密性保护和采用HMAC-SM3算法进行完整性保护形成报文后再进行数据传输，服务器后端接收到数据后，需调用服务器密码机对报文进行完整性验证，根据被测系统业务需求是否解密或者落盘存储，以保证重要数据在传输过程中的机密性和完整性。

A.8. 应用与数据安全层重要数据存储建议

关键数据落盘前应根据被测系统关键数据安全需求，应调用合规的服务器密码机（附录A），采用SM4-CBC算法对关键数据进行加密存储，以保证重要数据存储的机密性；采用HMAC-SM3算法进行计算后对哈希值进行存储，后期系统使用到此类重要数据时，需再次调用服务器密码机的HMAC-SM3算法对重要数据计算哈希值，并通过比对方式验证与数据库存储的哈希值是否一致，以保证重要数据存储的完整性。

A.9. 合规的数字证书

数字证书认证系统产品合规要求参考:符合GM/T0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》、GM/T 0028《密码模块安全技术要求》二级要求。

在可能涉及法律责任认定的应用中涉及数字证书应由具有相关资质的第三方CA机构颁发国密双证书（加密证书、签名证书）；在不涉及法律责任认定的应用中且仅应用系统内部，可通过部署具有商用密码产品认证证书的数字证书认证系统（CA系统），进行签发国密双证书（加密证书、签名证书），并统一管理。

（文档已完结，以下空白）