报告编号：15000045005-20003-23-01

**基于全员人口数据库的计划生育综合服务管理系统**

**商用密码应用安全性评估报告**

|  |  |
| --- | --- |
| **委托单位：** | **内蒙古自治区大数据中心** |
| **被测单位：** | **内蒙古自治区卫生健康委员会** |
| **密评机构：** | **内蒙古信元网络安全技术股份有限公司** |
| **报告时间：** | **2023年03月30日** |

# **声 明**

本报告是基于全员人口数据库的计划生育综合服务管理系统系统的商用密码应用安全性评估报告，报告模板为2023年版。

本报告评估结论的有效性建立在被测单位提供相关证据的真实性基础之上。

本报告中给出的评估结论仅对被测信息系统当时的安全状态有效。被测信息系统发生变更后，应重新对其进行评估，本报告不再适用。

本报告中给出的评估结论不能作为对被测信息系统内部署的相关系统构成组件（或产品）的评估结论。

在任何情况下，若需引用本报告中的评估结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

内蒙古信元网络安全技术股份有限公司（盖章）

2023年 03月30日

# **被测信息系统基本信息表**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 被测单位 | | | | | | | | |
| 单位名称 | 内蒙古自治区卫生健康委员会 | | | | | | | |
| 单位地址 | 内蒙古自治区呼和浩特市新华大街63号院 | | | | | 邮政编码 | | 010050 |
| 所属省部密码管理部门 | 内蒙古自治区国家密码管理局 | | | | | | | |
| 联系人 | 姓名 | 乌健鑫 | | 职务/职称 | | 工程师 | | |
| 所属部门 | 大数据中心九部 | | 办公电话 | | —— | | |
| 移动电话 | 13624713007 | | 电子邮件 | | —— | | |
| **被测信息系统** | | | | | | | | |
| 系统名称 | 基于全员人口数据库的计划生育综合服务管理系统 | | | | | | | |
| 是否为关键信息基础设施 | □已认定，所属安全保护工作部门：  🗹未认定 | | | | | | | |
| 网络安全等级保护定级和备案情况 | 🗹已定级备案，第 三 级（一至四），S 3 A 3 G 3  备案证明编号：15000045005-20003  本次被测信息系统与等级保护定级系统是否一致：  🗹是 □否，变化情况说明： | | | | | | | |
| □未定级，本次密评依据GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》第 级（一至四）信息系统要求 | | | | | | | |
| 网络安全等级测评情况 | 🗹已测评  测评机构名称：内蒙古信元网络安全技术股份有限公司  测评时间：2020年10月23日  测评结论：良 | | | | □正在测评  测评机构名称： | | □未测评 | |
| 系统服务情况 | 服务范围 | □全国　　□跨省（区、市）跨 个  🗹全省（区、市）　　□跨地（市、区）跨 个  □地（市、区）内　　□其他 | | | | | | |
| 服务领域 | □电信　□广电　□经营性公众互联网　□铁路　□银行　□海关　□税务　□民航　□电力　　□证券　□保险　　□国防科技工业　□公安　□财政　□人事劳动和社会保障　　□审计　□商业贸易　□国土资源　□能源　□交通　□统计　□工商行政管理　□邮政　□教育　□文化　🗹卫生　□农业　□水利　□外交　□发展改革　□科技　□宣传  □质量监督检验检疫　　□其他 | | | | | | |
| 服务对象 | 🗹单位内部人员　　□社会公众人员  □两者均包括 □其他 | | | | | | |
| 系统网络平台 | 覆盖范围 | □局域网　　🗹城域网　□广域网　□其他 | | | | | | |
| 网络性质 | 🗹业务专网　□互联网　□其他 | | | | | | |
| 系统服务用户数量 | 10000+ | | | | | | | |
| 系统是否已投入运行 | 🗹是，投入运行时间： 2021年03月  □否，目前情况：未验收 | | | | | | | |
| 系统互联情况 | □与其他行业系统连接 □与本行业其他单位系统连接  □与本单位其他系统连接　🗹其他 未与其他系统互联  互联系统名称： | | | | | | | |
| 系统是否依赖不在本系统范围内的云平台运行 | 🗹是，云平台名称：电子政务外网系统 | | □云平台已评估 □云平台正在评估 🗹云平台未评估  密评机构名称：  评估时间： 评估结论： | | | | | |
| □否 | | | | | | | |
| 系统是否具有密码应用方案 | □有密码应用方案，且通过密评，通过时间：  密评方式：□自行评估　□委托密评机构评估，密评机构名称： | | | | | | | |
| □有密码应用方案，但未通过密评 | | | | | | | |
| 🗹无密码应用方案 | | | | | | | |
| 系统使用的密码产品情况 | 🗹系统使用的密码产品1（台／套），独立使用0（台／套），共享使用1（台／套）；其中，取得认证证书的产品数量0（台／套），未取得认证证书的国内产品数量1（台／套），国外产品数量0（台／套）。 □系统未使用密码产品 | | | | | | | |
| 系统使用的密码算法 | 分组算法：□SM1 □SM4 □SM7 🗹AES □DES □3DES □其他  非对称算法：□SM2 □SM9 □RSA1024 🗹RSA2048 □其他  杂凑算法：□SM3 □SHA-1 🗹SHA-256 🗹SHA-384 □SHA-512  🗹MD5 □其他  序列算法：□ZUC □其他  其他算法： | | | | | | | |
| **密评机构** | | | | | | | | |
| 单位名称 | 内蒙古信元网络安全技术股份有限公司 | | | | | | | |
| 通信地址 | 内蒙古自治区呼和浩特市新城区南店街33号信元网安大楼 | | | | | 邮政编码 | | 010050 |
| 联系人 | 姓名 | 王红艳 | | 职务/职称 | | 市场部经理 | | |
| 所属部门 | 市场部 | | 办公电话 | | 0471-4599666 | | |
| 移动电话 | 13754010880 | | 电子邮件 | | - | | |
| 审核批准 | 编制人 |  | | 编制日期 | |  | | |
| 审核人 |  | | 审核日期 | |  | | |
| 批准人 |  | | 批准日期 | |  | | |

# **商用密码应用安全性评估结论**

|  |  |  |  |
| --- | --- | --- | --- |
| 系统名称 | 基于全员人口数据库的计划生育综合服务管理系统 | | |
| **系统简介** | 基于全员人口数据库的计划生育综合服务管理系统主要承载的业务是：综合管理人口信息、处理计生业务。内蒙古自治区卫生健康委员是该系统定级的责任单位，该系统安全保护等级是三级。该系统托管在联通政务云机房电子政务外网系统，电子政务外网系统采用云计算技术。 | | |
| **测评情况简介** | 受内蒙古自治区大数据中心委托，内蒙古信元网络安全技术股份有限公司于2023年02月08日-2023年03月30日对基于全员人口数据库的计划生育综合服务管理系统系统的业务应用系统、主机操作系统、数据库管理系统、相关人员、密钥及密码管理等方面进行密码应用安全性评估，提交密码应用安全性评估报告。评估内容统包括：物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行、应急处置等八个方面。在密码应用安全性评估的基础上，梳理基于全员人口数据库的计划生育综合服务管理系统系统的密码应用需求，对该系统密码应用保障体系的资源配置、整改建设和后续运维工作提出指导建议。 | | |
| **评估结论** | 不符合 | **综合得分** | 27.81分 |
| **不适用项数目/**  **总测评指标项数目** | 4/41 | **高风险项数目** | 9 |

# **总体评价**

本次信息系统商用密码应用安全性评估依据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，选取的测评指标总数为41项，其中不适用项为4项，特殊指标0项。测评结果为：符合项16项，部分符合项4项，不符合项17项。其中，在部分符合和不符合项中：高风险项9项，中风险项11项，低风险项1项。

1. 在物理和环境安全方面，被测系统部署于中国联通呼和浩特云数据中心DC2。进入机房时，通过门禁卡、电子门禁系统对进入人员进行身份鉴别，但电子门禁系统对进入人员进行身份鉴别时未采用商用密码技术实现；电子门禁系统进出记录、视频监控记录未采用商用密码技术进行完整性保护。

测评结果：符合项0项，部分符合项0项，不符合项3项，不适用项0项。

1. 在网络和通信安全方面，网络和通信安全层面有2个测评对象，分别是政务外网非国密浏览器与应用系统之间的通信信道、互联网VPN客户端与运维SSL VPN之间的运维通信信道。互联网VPN客户端与运维SSL VPN之间的运维通信信道采用TLSv1.2通信协议进行加密通信，并通过sha256RSA算法的数字证书进行身份认证，数字证书为自签发的数字证书，通信过程协商的密码套件为TLS\_ECDHE\_RSA\_WITH\_ AES\_256\_GCM\_SHA384，未采用合规的密码算法保证该信道通信过程中数据的机密性和完整性；政务外网非国密浏览器与应用系统之间的通信信道采用HTTP明文协议传输，未采用密码算法保证该信道通信过程中数据的机密性和完整性；以上的通信信道网络边界处的网络安全设备均为通用型产品，采用系统资产自有协议进行通信和身份认证，未采用密码技术保证通信实体身份的真实性。系统网络没有使用密码技术保护访问控制信息完整性。

测评结果：符合项0项，部分符合项3项，不符合项1项，不适用项1项。

1. 在设备和计算安全方面，登录应用服务器（虚拟机-Windows Server 2012）、数据库服务器（虚拟机-Windows Server 2012）、系统数据库（Oracle 11g）、运维SSL VPN使用“用户名+静态口令”的方式，未使用密码技术进行身份鉴别；应用服务器（虚拟机-Windows Server 2012）、数据库服务器（虚拟机-Windows Server 2012）采用TLSv1.2协议进行管理，数据库远程管理使用默认TNS协议进行明文通信， 应用服务器（虚拟机-Windows Server 2012）、数据库服务器（虚拟机-Windows Server 2012）、运维SSL VPN通信过程协商的密码套件为TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM \_SHA384，未采用合规的密码算法进行机密性和完整性保护，未使用国家核准的密码技术对系统资源访问控制信息完整性、日志记录完整性和重要可执行程序进行保护。

测评结果：符合项0项，部分符合项1项，不符合项4项，不适用项1项。

不适用项：宜采用密码技术保证设备中的重要信息资源安全标记的完整性。

不适用原因：被测信息系统不涉及安全标记数据，本项不适用。

1. 在应用和数据安全方面，基于全员人口数据库的计划生育综合服务管理系统用户登录方式为“用户名+口令”，未使用密码技术进行身份鉴别；系统重要业务数据在传输过程中未使用密码技术进行保护，用户鉴别数据采用明文传输；系统访问控制信息存储在数据库，未采用密码技术保证业务应用系统访问控制信息的完整性。管理用户口令在数据库中使用MD5算法加密存储；重要业务数据在数据库明文存储，未采用核准的密码技术保证鉴别信息和重要业务数据存储过程的完整性、机密性。

测评结果：符合项0项，部分符合项0项，不符合项6项，不适用项2项。

不适用项：宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性。

不适用原因：该系统没有重要信息资源的安全标记数据，无需保证重要信息资源安全标记的完整性。

不适用项：在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。

不适用原因：经访谈并核查，系统不涉及需要法律认定的重要操作的不可否认性。

1. 在管理制度方面，现有的管理制度体系中包含有密码应用安全管理制度、密码人员管理、密钥管理、密码建设运行、密码应急处置、密码软硬件管理等制度。

测评结果：符合项6项，部分符合项0项，不符合项0项，不适用项0项。

1. 在人员管理方面，系统的相关人员了解并遵守密码相关法律法规，学习过密码相关国家要求。已有制度体系中具有密码应用岗位责任制度、上岗人员培训制度、人员考核制度等。

测评结果：符合项5项，部分符合项0项，不符合项0项，不适用项0项。

1. 在建设运行方面，在信息系统规划阶段，没有依据密码相关标准和信息系统密码应用需求，制定密码应用方案、实施方案。系统定期开展系统攻防对抗演习，并形成攻防对抗演习报告；且已制定密钥管理制度及策略类文档、密码实施方案。

测评结果：符合项2项，部分符合项0项，不符合项3项，不适用项0项。

1. 在应急处置方面，制定了信息安全体系应急预案框架，明确了安全事件的级别，安全事件的处置流程及报告流程；截止本次测评结束系统未发生过安全事件，信息安全体系应急预案框架明确了密码应用安全事件的应急处置策略。

测评结果：符合项3项，部分符合项0项，不符合项0项，不适用项0项。

通过对基于全员人口数据库的计划生育综合服务管理系统系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行和应急处置等方面的测评，该系统不符合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。

# **安全问题及改进建议**

本次信息系统商用密码应用安全性评估依据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，发现被测信息系统存在以下安全问题。建议被测信息系统根据实际情况和以下给出的建议进行整改。

1. 物理和环境安全

**问题描述：**

1） 机房电子门禁系统未采用密码技术对访问人员进行身份鉴别。

2） 未使用密码技术保护电子门禁系统进出记录存储的完整性。

3） 未使用密码技术保护视频监控系统的音像记录存储的完整性。

**改进建议：**

1） 建议采用具有商密产品认证证书的电子门禁系统，并且配置合规、正确的密码算法对进入机房的人员进行身份鉴别。

2） 建议采用国密电子门禁系统，PCI-E密码卡（配合门禁日志审计系统使用），采用基于SM3的HMAC机制实现对门禁日志记录数据的完整性保护。

3） 建议采用国密NVR、国密摄像机、PCI-E密码卡，采用基于SM3国密算法的HMAC机制，实现音像记录数据的完整性保护。

1. 网络和通信安全

**问题描述：**

1）身份鉴别：政务外网非国密浏览器与应用系统之间的通信信道,互联网VPN客户端与运维SSL VPN之间的运维通信信道未使用合规的密码技术对通信实体进行身份鉴别，无法保证通信实体身份的真实性。**建议优先整改**。

2）通信数据完整性：政务外网非国密浏览器与应用系统之间的通信信道,互联网VPN客户端与运维SSL VPN之间的运维通信信道未使用密码技术保证通信过程中数据的完整性。

3）通信过程中重要数据的机密性：政务外网非国密浏览器与应用系统之间的通信信道,互联网VPN客户端与运维SSL VPN之间的运维通信信道未使用合规的密码技术保证通信过程中重要数据的机密性。**建议优先整改**。

4）网络边界访问控制信息的完整性 ：政务外网非国密浏览器与应用系统之间的通信信道,互联网VPN客户端与运维SSL VPN之间的运维通信信道网络边界设备未采用合规的密码技术对访问控制信息进行完整性保护。

**改进建议：**

1）政务外网非国密浏览器与应用系统之间的通信信道,互联网VPN客户端与运维SSL VPN之间的运维通信信道: 建议信道采用GMTLS通信协议，身份鉴别采用的签名算法是基于SM2算法和SM3算法的签名，数字证书由电子政务电子认证服务机构目录的签发机构签发。

2）政务外网非国密浏览器与应用系统之间的通信信道,互联网VPN客户端与运维SSL VPN之间的运维通信信道: 建议网络通信信道采用GMTLS通信协议，协商的密码套件为ECC\_SM4\_SM3，保证该信道通信过程中数据的完整性。

3）政务外网非国密浏览器与应用系统之间的通信信道,互联网VPN客户端与运维SSL VPN之间的运维通信信道: 建议网络通信信道采用GMTLS通信协议，协商的密码套件为ECC\_SM4\_SM3保证该信道通信过程中数据的机密性。

4）政务外网非国密浏览器与应用系统之间的通信信道,互联网VPN客户端与运维SSL VPN之间的运维通信信道: 建议通过在网络边界部署具有由国家密码管理局商用密码检测中心颁发的商用密码产品认证证书安全设备，实现对内部的网络边界控制机制，网络边界访问控制信息存储在该安全设备中，设备内部使用 HMAC-SM3等密码技术保障访问控制信息的完整性。

1. 设备和计算安全

**问题描述：**

1）身份鉴别：应用服务器（虚拟机-Windows Server 2012）,数据库服务器（虚拟机-Windows Server 2012）,系统数据库（Oracle 11g）,运维SSL VPN未使用密码技术对登录系统相关设备的用户进行身份鉴别。**建议优先整改**。

2）远程管理通道安全：应用服务器（虚拟机-Windows Server 2012）,数据库服务器（虚拟机-Windows Server 2012）,系统数据库（Oracle 11g）,运维SSL VPN未采用合规的密码技术建立安全的信息传输通道。**建议优先整改**。

3）系统资源访问控制信息完整性：应用服务器（虚拟机-Windows Server 2012）,数据库服务器（虚拟机-Windows Server 2012）,系统数据库（Oracle 11g）,运维SSL VPN未采用密码技术来保证系统资源访问控制信息的完整性。

4）日志记录完整性：应用服务器（虚拟机-Windows Server 2012）,数据库服务器（虚拟机-Windows Server 2012）,系统数据库（Oracle 11g）,运维SSL VPN未采用密码技术来保证日志记录的完整性。

5）重要可执行程序完整性、重要可执行程序来源真实性：应用服务器（虚拟机-Windows Server 2012）,数据库服务器（虚拟机-Windows Server 2012）,系统数据库（Oracle 11g）,运维SSL VPN未采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。

**改进建议：**

1）应用服务器（虚拟机-Windows Server 2012）,数据库服务器（虚拟机-Windows Server 2012）,系统数据库（Oracle 11g）,运维SSL VPN: 建议为运维管理员通过合规的第三方电子认证服务机构颁发智能密码钥匙，登录具有商用密码产品认证证书的SSL VPN安全网关，建立安全的传输通道，实现基于密码技术对运维管理员身份鉴别。

2）应用服务器（虚拟机-Windows Server 2012）,数据库服务器（虚拟机-Windows Server 2012）,系统数据库（Oracle 11g）,运维SSL VPN: 建议远程运维数据安全通过GMTLS协议建立安全传输通道，保障从运维端到实现设备远程管理通道信息传输的完整性和机密性。

3）应用服务器（虚拟机-Windows Server 2012）,数据库服务器（虚拟机-Windows Server 2012）,系统数据库（Oracle 11g）,运维SSL VPN: 建议关联设备通用计算设备可通过定制化开发调用服务器密码机签名验证/HMAC-SM3算法保证访问控制信息完整性。

4）应用服务器（虚拟机-Windows Server 2012）,数据库服务器（虚拟机-Windows Server 2012）,系统数据库（Oracle 11g）,运维SSL VPN: 建议关联设备可通过定制化开发调用服务器密码机签名验证/HMAC-SM3算法保证设备日志数据的完整性。

5）应用服务器（虚拟机-Windows Server 2012）,数据库服务器（虚拟机-Windows Server 2012）,系统数据库（Oracle 11g）,运维SSL VPN: 建议对重要可执行程序通过SM2算法数字证书对重要应用程序的操作员身份进行鉴别，确保仅具备权限的操作员才可以对重要应用程序执行加载和卸载操作；通过HMAC-SM3算法对重要应用程序在加载内容时进行完整性校验，确保重要应用程序内容未被非法篡改。这些功能可由应用程序进行二次开发提供，也可由操作系统或运行环境提供。

1. 应用和数据安全

**问题描述：**

1）身份鉴别：系统用户系统使用用户名口令进行身份鉴别，不能保证应用系统用户身份的真实性。**建议优先整改**。

2）访问控制信息完整性：基于全员人口数据库的计划生育综合服务管理系统未采用密码技术来保证应用系统访问控制信息的完整性。

3）重要数据传输机密性：系统用户鉴别数据，人口信息数据未采用密码技术保证信息系统应用系统的重要数据传输的机密性。**建议优先整改**。

4）重要数据存储机密性：系统用户鉴别数据，人口信息数据未采用核准的密码技术保证信息系统应用的重要数据存储的机密性。**建议优先整改**。

5）重要数据传输完整性：系统用户鉴别数据,人口信息数据重要数据传输完整性：应用层面未采用密码技术保证信息系统应用的重要数据传输的完整性。**建议优先整改**。

6）重要数据存储完整性：系统用户鉴别数据,人口信息数据,操作日志数据未采用密码技术保证信息系统应用的重要数据存储的完整性。**建议优先整改**。

**改进建议：**

1）系统用户: 建议关联用户类型通过身份鉴别登录应用系统，对其进行管理或使用。身份鉴别方式应为用户名+口令+智能密码钥匙/移动终端密码模块（用于产生“挑战一响应”中的SM2数字签名）的双因素身份鉴别。

2）基于全员人口数据库的计划生育综合服务管理系统: 建议应用系统通过部署服务器密码机，采用HMAC-SM3对其访问控制策略、数据库表访问控制信息进行完整性保护。

3）系统用户鉴别数据，人口信息数据: 建议通过部署安全认证网关建立的安全通信信道，访问业务系统通过安全认证网关建立SSL连接，并采用SM2/SM3/SM4算法套件，且SSL VPN安全网关中具有关联本业务系统的合规第三方电子认证服务机构颁发的SM2 SSL证书。

4）系统用户鉴别数据,人口信息数据: 建议部署服务器密码机，采用SM4算法对用户鉴别数据实现存储机密性。

5）系统用户鉴别数据,人口信息数据: 建议通过部署安全认证网关建立的安全通信信道，访问业务系统通过安全认证网关建立SSL连接，并采用SM2/SM3/SM4算法套件，且SSL VPN安全网关中具有关联本业务系统的合规第三方电子认证服务机构颁发的SM2 SSL证书。

6）系统用户鉴别数据,人口信息数据,操作日志数据: 建议部署服务器密码机，采用HMAC-SM3算法对业务系统重要数据实现存储完整性。

1. 建设运行

**问题描述：**

1） 在信息系统规划阶段，没有依据密码相关标准和信息系统密码应用需求，制定密码应用方案。**建议优先整改**。

2）在信息系统规划阶段，没有密码应用方案制定密码实施方案。

3）系统投入运行前未进行密码应用安全性评估。

**改进建议：**

1）建议在信息系统规划阶段，没有依据密码相关标准和信息系统密码应用需求，制定密码应用方案。

2）建议制定密码实施方案，方案内容应包括但不少于信息系统概述、安全需求分析、商用密码系统设计方案、商用密码产品清单（包括产品资质、功能及性能列表和产品生产单位等）、商用密码系统安全管理与维护策略、商用密码系统实施计划等。

3）建议对系统进行商用密码改造，且定期开展密码应用安全性评估工作。

**目录**

[**声 明** I](#_Toc133220843)

[**被测信息系统基本信息表** I](#_Toc133220844)

[**商用密码应用安全性评估结论** III](#_Toc133220845)

[**总体评价** V](#_Toc133220846)

[**安全问题及改进建议** IX](#_Toc133220847)

[1 **测评项目概述** 1](#_Toc133220848)

[1.1 测评目的 1](#_Toc133220849)

[1.2 测评依据 1](#_Toc133220850)

[1.2.1 依据标准和规范 1](#_Toc133220851)

[1.2.2 参考标准和规范 1](#_Toc133220852)

[1.2.3 术语和缩略语 1](#_Toc133220853)

[1.3 测评过程 1](#_Toc133220854)

[1.3.1 测评准备阶段 2](#_Toc133220855)

[1.3.2 方案编制阶段 3](#_Toc133220856)

[1.3.3 现场测评阶段 3](#_Toc133220857)

[1.3.4 分析与报告编制阶段 3](#_Toc133220858)

[1.4 报告分发范围 4](#_Toc133220859)

[2 **被测系统情况** 5](#_Toc133220860)

[2.1 承载的业务情况 5](#_Toc133220861)

[2.2 网络拓扑图及描述 5](#_Toc133220862)

[2.2.1 物理和环境安全密码应用情况 5](#_Toc133220863)

[2.2.2 网络和通信安全密码应用情况 6](#_Toc133220864)

[2.2.3 设备和计算安全密码应用情况 6](#_Toc133220865)

[2.2.4 应用和数据安全密码应用情况 6](#_Toc133220866)

[2.3 系统资产 6](#_Toc133220867)

[2.3.1 物理环境 7](#_Toc133220868)

[2.3.2 物理安防设施 7](#_Toc133220869)

[2.3.3 密码产品 7](#_Toc133220870)

[2.3.4 服务器/存储设备 7](#_Toc133220871)

[2.3.5 网络及安全设备 8](#_Toc133220872)

[2.3.6 数据库管理系统 8](#_Toc133220873)

[2.3.7 关键业务应用 8](#_Toc133220874)

[2.3.8 重要数据 9](#_Toc133220875)

[2.3.9 安全管理文档 9](#_Toc133220876)

[2.3.10 人员 10](#_Toc133220877)

[2.4 密码服务 10](#_Toc133220878)

[2.5 安全威胁 10](#_Toc133220879)

[2.6 前次测评情况 11](#_Toc133220880)

[3 **测评范围与方法** 11](#_Toc133220881)

[3.1 测评指标 11](#_Toc133220882)

[3.1.1 基本指标 11](#_Toc133220883)

[3.1.2 特殊指标 14](#_Toc133220884)

[3.1.3 不适用指标 14](#_Toc133220885)

[3.2 测评方法及工具 15](#_Toc133220886)

[3.2.1 现场测评方法 15](#_Toc133220887)

[3.2.2 测评工具 16](#_Toc133220888)

[3.2.3 测评工具检查点 16](#_Toc133220889)

[3.3 测评对象和对应测评方式 17](#_Toc133220890)

[3.3.1 测评对象确定方法 17](#_Toc133220891)

[3.3.2 测评对象确定结果 17](#_Toc133220892)

[4 **单元测评** 20](#_Toc133220893)

[4.1 密码技术应用要求 20](#_Toc133220894)

[4.1.1 物理和环境安全 20](#_Toc133220895)

[4.1.2 网络和通信安全 20](#_Toc133220896)

[4.1.3 设备和计算安全 21](#_Toc133220897)

[4.1.4 应用和数据安全 23](#_Toc133220898)

[4.2 安全管理 24](#_Toc133220899)

[4.2.1 管理制度 24](#_Toc133220900)

[4.2.2 人员管理 25](#_Toc133220901)

[4.2.3 建设运行 26](#_Toc133220902)

[4.2.4 应急处置 27](#_Toc133220903)

[5 **整体测评** 27](#_Toc133220904)

[5.1 测评结果修正 27](#_Toc133220905)

[5.2 整体测评结果和量化评估 28](#_Toc133220906)

[6 **风险分析** 30](#_Toc133220907)

[7 **评估结论** 37](#_Toc133220908)

[**附录A测评结果记录** 38](#_Toc133220909)

[A.1 物理和环境安全 38](#_Toc133220910)

[A.2 网络和通信安全 51](#_Toc133220911)

[A.3 设备和计算安全 58](#_Toc133220912)

[A.4 应用和数据安全 69](#_Toc133220913)

[A.5 管理制度 75](#_Toc133220914)

[A.6 人员管理 77](#_Toc133220915)

[A.7 建设运行 79](#_Toc133220916)

[A.8 应急处置 82](#_Toc133220917)

[**附录B密评活动有效性证明记录** 83](#_Toc133220918)

[B.1 密评委托证明 83](#_Toc133220919)

[B.2 密评活动证明 84](#_Toc133220920)

[B.3 密评活动质量文件 88](#_Toc133220921)

[B.4 密评人员资格证明 92](#_Toc133220922)

[B.5 系统定级匹配证明 94](#_Toc133220923)

# **测评项目概述**

## 测评目的

内蒙古信元网络安全技术股份有限公司受内蒙古自治区卫生健康委员会的委托，于2023年01月05日至2023年03月30日，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，对内蒙古自治区卫生健康委员会的基于全员人口数据库的计划生育综合服务管理系统从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行和应急处置等方面进行商用密码应用安全性评估，通过测评项目的实施，根据被测信息系统当前的安全状况，给出测评结果并提出改进建议，以确保被测信息系统达到GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》的要求，也为其信息资产安全和业务持续稳定运行提供保障。

## 测评依据

### 依据标准和规范

* 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》
* GM/T 0116—2021《信息系统密码应用测评过程指南》
* 《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》

### 参考标准和规范

* 《GM/T 0024 2014 SSL VPN 技术规范》

### 术语和缩略语

无。

## 测评过程

商用密码应用安全性评估过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动。测评双方之间的沟通与洽谈贯穿整个密码应用安全性评估过程。测评工作流程如图1‑1所示。



**图1‑1测评工作流程**

### 测评准备阶段

根据测评双方签订的委托测评协议书和被测信息系统规模，密评机构组建测评项目组，从人员方面做好准备，并编制项目计划书。密评机构通过查阅被测系统已有资料并使用调查表格的方式，了解整个系统的构成和密码保护情况，为编写密评方案和开展现场测评工作奠定基础。测评项目组成员在进行现场测评之前，熟悉与被测信息系统相关的各种组件、调试测评工具、准备各种表单等。

测评准备阶段时间：2023年01月05日- 2023年01月09日。

测评项目组成员如表1‑1所示：

**表1‑1测评项目组成员**

| 角色 | 姓名 | 任务分工 | 是否通过密评人员考核 |
| --- | --- | --- | --- |
| 项目负责人 | 李世昌 | 报告编制、设备和计算安全测评、应用和数据安全测评 | 是 |
| 测评项目组成员 | 蔡子航 | 网络和通信安全测评，物理和环境安全测评 | 是 |
| 冶占猛 | 管理测评 | 否 |

### 方案编制阶段

根据已经了解到的被测信息系统情况，分析整个被测系统及其涉及的业务应用系统，以及与此相关的密码应用情况，确定出本次测评的测评对象；根据已经了解到的被测系统定级结果，确定出本次测评的测评指标；确认测评过程中需要现场检查的关键安全点，并且充分考虑到检查的可行性和风险，最大限度的避免对被测系统，尤其是在线运行业务系统的影响；确定现场测评的具体实施内容；最终完成测评方案的编制。

方案编制阶段时间：2023年01月10日- 2023年01月12日。

### 现场测评阶段

现场测评准备：召开测评现场首次会，密评机构介绍测评工作，交流测评信息，进一步明确测评计划和测评方案中的内容，说明测评过程中具体的实施工作内容，测评时间安排，测评过程中可能存在的安全风险等，以便于后面的测评工作开展。测评双方确认现场测评需要的各种资源，包括被测单位的配合人员和需要提供的测评条件等，确认被测信息系统已备份过系统及数据。被测单位签署现场测评授权书。密评人员根据会议沟通结果，对测评结果记录表单和测评程序进行必要的更新。

测评项目组根据密评方案以及现场测评准备的结果，安排密评人员在现场完成测评工作，汇总现场测评的测评记录；召开测评现场结束会，测评双方对测评过程中发现的问题进行现场确认；密评机构归还测评过程中借阅的所有文档资料，并由被测单位文档资料提供者签字确认。

现场测评阶段时间：2023年01月13日- 2023年03月10日。

### 分析与报告编制阶段

在现场测评工作结束后，密评机构对现场测评获得的测评结果进行汇总分析，形成评估结论，并编制评估报告。

密评人员在初步判定各测评单元涉及的各个测评对象的测评结果后，还需进行单元测评、整体测评、量化评估和风险分析。经过整体测评后，有的测评对象的测评结果可能会有所变化，需进一步修订测评结果，而后进行量化评估和风险分析，最后形成评估结论。

分析与报告编制阶段时间：2023年03月13日- 2023年03月31日。

## 报告分发范围

本报告一式3份，其中1份提交密码管理部门，1份提交委托单位，1份由密评机构留存。

# **被测系统情况**

## 承载的业务情况

基于全员人口数据库的计划生育综合服务管理系统主要承载的业务是：综合管理人口信息、处理计生业务。内蒙古自治区卫生健康委员是该系统定级的责任单位，该系统安全保护等级是三级。该系统托管在联通政务云机房电子政务外网系统，电子政务外网系统采用云计算技术。该系统通过互联网远程接入VPN对系统资产进行远程运维，通过政务外网为本单位管理人员提供业务服务。

## 网络拓扑图及描述

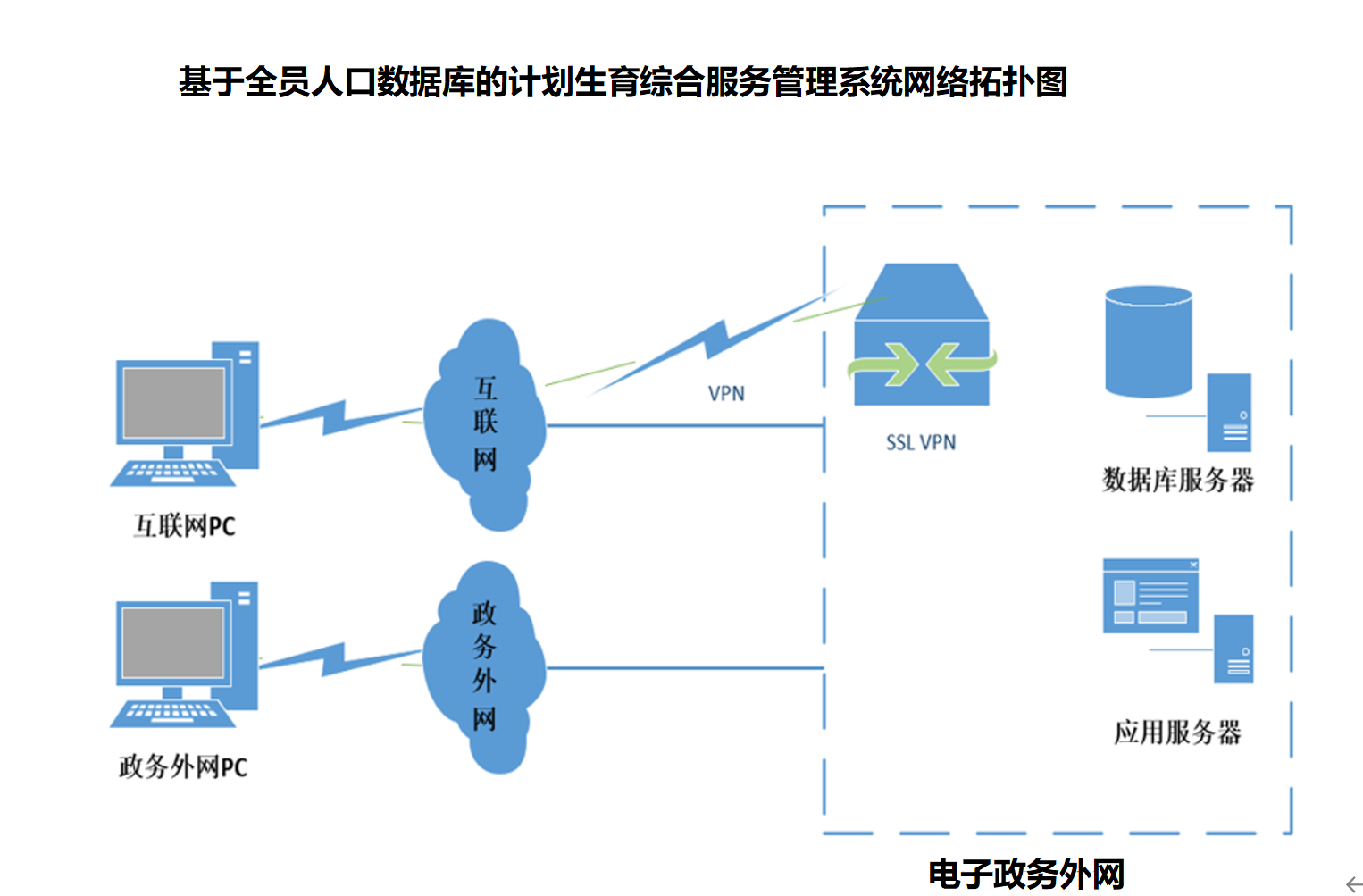


图2.1 网络拓扑图

如图2.1 网络拓扑图所示，被测系统部署于中国联通呼和浩特云数据中心DC2。进入机房时，通过门禁卡、电子门禁系统对进入人员进行身份鉴别，但电子门禁系统对进入人员进行身份鉴别时未采用商用密码技术实现；电子门禁系统进出记录、视频监控记录未采用商用密码技术进行完整性保护。通信信道分为：政务外网非国密浏览器与应用系统之间的通信信道、互联网VPN客户端与运维SSL VPN之间的运维通信信道。

### 物理和环境安全密码应用情况

被测系统部署于中国联通呼和浩特云数据中心DC2。进入机房时，通过门禁卡、电子门禁系统对进入人员进行身份鉴别，但电子门禁系统对进入人员进行身份鉴别时未采用商用密码技术实现；电子门禁系统进出记录、视频监控记录未采用商用密码技术进行完整性保护。

### 网络和通信安全密码应用情况

网络和通信安全层面有2个测评对象，分别是政务外网非国密浏览器与应用系统之间的通信信道、互联网VPN客户端与运维SSL VPN之间的运维通信信道。互联网VPN客户端与运维SSL VPN之间的运维通信信道采用TLSv1.2通信协议进行加密通信，并通过sha256RSA算法的数字证书进行身份认证，数字证书为自签发的数字证书，通信过程协商的密码套件为TLS\_ECDHE\_RSA\_WITH\_ AES\_256\_GCM\_SHA384，未采用合规的密码算法保证该信道通信过程中数据的机密性和完整性；政务外网非国密浏览器与应用系统之间的通信信道采用HTTP明文协议传输，未采用密码算法保证该信道通信过程中数据的机密性和完整性；以上的通信信道网络边界处的网络安全设备均为通用型产品，采用系统资产自有协议进行通信和身份认证，未采用密码技术保证通信实体身份的真实性。系统网络没有使用密码技术保护访问控制信息完整性。

### 设备和计算安全密码应用情况

登录应用服务器（虚拟机-Windows Server 2012）、数据库服务器（虚拟机-Windows Server 2012）、系统数据库（Oracle 11g）、运维SSL VPN使用“用户名+静态口令”的方式，未使用密码技术进行身份鉴别；应用服务器（虚拟机-Windows Server 2012）、数据库服务器（虚拟机-Windows Server 2012）采用TLSv1.2协议进行管理，数据库远程管理使用默认TNS协议进行明文通信，应用服务器（虚拟机-Windows Server 2012）、数据库服务器（虚拟机-Windows Server 2012）、运维SSL VPN通信过程协商的密码套件为TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM \_SHA384，未采用合规的密码算法进行机密性和完整性保护，未使用国家核准的密码技术对系统资源访问控制信息完整性、日志记录完整性和重要可执行程序进行保护。

### 应用和数据安全密码应用情况

基于全员人口数据库的计划生育综合服务管理系统用户登录方式为“用户名+口令”，未使用密码技术进行身份鉴别；系统重要业务数据在传输过程中未使用密码技术进行保护，用户鉴别数据采用明文传输；系统访问控制信息存储在数据库，未采用密码技术保证业务应用系统访问控制信息的完整性。管理用户口令在数据库中使用MD5算法加密存储；重要业务数据在数据库明文存储，未采用核准的密码技术保证鉴别信息和重要业务数据存储过程的完整性、机密性。

## 系统资产

### 物理环境

**表2‑1物理环境**

| 序号 | 物理环境名称 | 物理位置 | 重要程度 |
| --- | --- | --- | --- |
| 1 | 政务云中心机房 | 中国联通呼和浩特云数据中心DC2 | 非常重要 |

### 物理安防设施

**表2‑2****物理安防设施**

| 序号 | 产品名称 | 生产厂商和型号 | 所在物理环境名称 | 重要程度 |
| --- | --- | --- | --- | --- |
| 1 | 电子门禁系统 | HID | 中国联通呼和浩特云数据中心DC2 | 非常重要 |
| 2 | 视频监控系统 | 优网通 | 中国联通呼和浩特云数据中心DC2 | 非常重要 |

### 密码产品

**表2‑3密码产品**

| 序号 | 产品  名称 | 生产厂商 | 商密产品认证证书编号 | 使用的密码算法 | 数量 | 用途 |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 运维 SSL VPN | 深信服 | 无 | RSA2048/AES256/ SHA384 | 1台 | 互联网远程系统运维接入 |

### 服务器/存储设备

**表2‑4服务器/存储设备**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 生产厂商 | 型号 | 操作系统版本 | 是否为虚拟设备 | 用途 | 数量 | 重要程度 |
| 1 | 数据交互服务器 | 虚拟机 | 虚拟机 | Windows Server 2012 | 是 | 系统支撑 | 1 | 非常重要 |
| 2 | 数据库服务器 | 虚拟机 | 虚拟机 | Windows Server 2012 | 是 | 系统支撑 | 1 | 非常重要 |
| 3 | 前置服务器 | 虚拟机 | 虚拟机 | Windows Server 2012 | 是 | 系统支撑 | 1 | 非常重要 |
| 4 | 平台应用服务器 | 虚拟机 | 虚拟机 | Windows Server 2012 | 是 | 系统支撑 | 1 | 非常重要 |
| 5 | 公众应用服务器 | 虚拟机 | 虚拟机 | Windows Server 2012 | 是 | 系统支撑 | 1 | 非常重要 |

### 网络及安全设备

**表2‑5网络及安全设备**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 生产厂商 | 型号 | 用途  （包括涉及的密码技术） | 数量 | 重要程度 |
| 本系统部署在联通政务云机房电子政务外网系统，网络及安全设备内蒙古政务云中心负责，本次密评不涉及。 | | | | | | |

### 数据库管理系统

**表2‑6数据库管理系统**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 数据库管理系统  名称 | 版本 | 部署位置 | 主要功能 | 重要  程度 |
| 1 | 系统数据库（Oracle 11g） | Oracle 11g | 数据库服务器 | 数据存储 | 非常重要 |

### 关键业务应用

**表2‑7关键业务应用**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 应用名称 | 版本 | 部署位置 | 主要功能 |
| 1 | 基于全员人口数据库的计划生育综合服务管理系统 | - | 应用服务器（虚拟机-Windows Server 2012） | 综合管理人口信息、处理计生业务 |

### 重要数据

**表2‑8重要数据**

| 序号 | 数据 | 描述 | 所属应用 | 存储位置 | 安全需求 |
| --- | --- | --- | --- | --- | --- |
| 1 | 系统用户鉴别数据 | 用户登录鉴别信息 | 基于全员人口数据库的计划生育综合服务管理系统 | 系统数据库（Oracle 11g） | 机密性/真实性/完整性 |
| 2 | 人口信息数据 | 人口信息数据（公民姓名、身份信息、健康信息等） | 基于全员人口数据库的计划生育综合服务管理系统 | 系统数据库（Oracle 11g） | 机密性/完整性 |
| 3 | 操作日志数据 | 重要业务操作记录 | 基于全员人口数据库的计划生育综合服务管理系统 | 系统数据库（Oracle 11g） | 完整性 |

### 安全管理文档

**表2‑9安全管理文档**

|  |  |  |
| --- | --- | --- |
| 序号 | 文档名称 | 主要内容 |
| 1 | 《密码建设要求》 | 信息系统密码建设应符合密码相关法律与行业相关政策要求进行建设。 |
| 2 | 《密码人员管理要求》 | 结合系统建设具体现状明确本管理机构内密码管理人员组成与智能，明确管理责任，做到责任到部门责任到人。 |
| 3 | 《密钥管理制度》 | 管理内容包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档、销毁等环节进行管理和策略制定的全过程。 |
| 4 | 《商用密码人员管理制度》 | 依据本单位《商用密码安全管理制度》设立本管理制度，主要用于对人员的相关合规性要求、培训、奖惩制度的说明和建立。 |
| 5 | 《密码安全管理小组》 | 依据《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》中对密码管理以及人员的要求，成立密码安全管理小组，密码安全管理小组依托于本单位内安全管理小组进行人员的重新设定、复用等成立。 |
| 6 | 《密码安全操作规范》 | 密码设备操作应严格遵守相关规章制度和操作规范。 |
| 7 | 《商用密码应用安全性评估管理制度汇编》 | 包括有密码人员管理、密钥管理、建设运行、应急处置、介质管理制度等方面的制度。 |

### 人员

**表2‑10人员**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 姓名 | 岗位/角色 | 职责说明 | 联系方式 |
| 1 | 乌健鑫 | 项目对接人 | 项目协调 | 13624713007 |

## 密码服务

**表2‑11密码服务**

|  |  |  |
| --- | --- | --- |
| 序号 | 密码服务名称 | 密码服务提供商 |
| 系统未使用密码服务 | | |

## 安全威胁

**表2‑12安全威胁**

|  |  |  |
| --- | --- | --- |
| 序号 | 安全层面 | 威胁分类 |
| TP1 | 物理和环境 | 非法人员进入物理环境，对软硬件设备和数据进行直接破坏 |
| TP2 | 物理进出记录和视频记录遭到篡改，以掩盖非法人员进出情况 |
| TN1 | 网络和通信 | 非法通信实体接入网络 |
| TN2 | 通信数据在信息系统外部被非授权的截取、篡改 |
| TN3 | 非法设备从外部接入内部网络，或网络边界被破坏 |
| TD1 | 设备和计算 | 设备被非法人员登录 |
| TD2 | 搭建的远程管理通道被非法使用，或传输的管理数据被非授权获取和篡改 |
| TD3 | 设备资源被登录设备的其他用户获取 |
| TD4 | 重要信息资源安全标记被非授权获取和篡改 |
| TD5 | 设备日志记录被非法篡改，以掩盖非法操作 |
| TD6 | 设备内重要程序和文件的来源不可信 |
| TA1 | 应用和数据 | 应用被非法人员登录 |
| TA2 | 应用资源被登录应用的其他用户获取 |
| TA3 | 重要信息资源安全标记被非授权获取和篡改 |
| TA4 | 传输或存储的数据被外部攻击者非法获取和/或篡改 |
| TA5 | 某个应用传输或存储的数据被其他应用获取 |
| TA6 | 数据发送者或接收者不承认发送或接受到数据，或者否认所做的操作和交易 |
| TK1 | 密钥管理和安全管理 | 生成的密钥缺少随机性，被攻击者猜测 |
| TK2 | 密钥被非法获取 |
| TK3 | 密钥被非法篡改，或密钥与实体之间的关联关系被非法篡改 |
| TK4 | 密钥被非法使用 |
| TK5 | 密钥备份和归档机制不健全，导致密钥泄露，或密钥被恢复到非法的设备中 |
| TK6 | 密钥销毁不及时导致密钥泄露，或销毁的密钥被恶意恢复 |
| TK7 | 安全管理制度和密钥管理策略等不完善，管理流程不健全，执行不到位，职责不明确，导致密钥泄露、数据泄露等风险 |

## 前次测评情况

本次测评是被测信息系统进行的第 1 次商用密码应用安全性评估。

# **测评范围与方法**

## 测评指标

### 基本指标

**表3‑1GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》{第三级别}要求基本指标**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测评指标 | | | 测评指标描述 | 应用要求 |
| 技术  要求 | 物理和环境安全 | 身份鉴别 | 8.1 a）宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性； | 宜 |
| 电子门禁记录数据存储完整性 | 8.1 b）宜采用密码技术保证电子门禁系统进出记录数据的存储完整性； | 宜 |
| 视频监控记录数据存储完整性 | 8.1 c）宜采用密码技术保证视频监控音像记录数据的存储完整性。 | 宜 |
| 网络和通信安全 | 身份鉴别 | 8.2 a）应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性； | 应 |
| 通信数据完整性 | 8.2 b）宜采用密码技术保证通信过程中数据的完整性； | 宜 |
| 通信过程中重要数据的机密性 | 8.2 c）应采用密码技术保证通信过程中重要数据的机密性； | 应 |
| 网络边界访问控制信息的完整性 | 8.2 d）宜采用密码技术保证网络边界访问控制信息的完整性； | 宜 |
| 安全接入认证 | 8.2 e）可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。 | 可 |
| 设备和计算安全 | 身份鉴别 | 8.3 a）应采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性； | 应 |
| 远程管理通道安全 | 8.3 b）远程管理设备时，应采用密码技术建立安全的信息传输通道； | 应 |
| 系统资源访问控制信息完整性 | 8.3 c）宜采用密码技术保证系统资源访问控制信息的完整性； | 宜 |
| 重要信息资源安全标记完整性 | 8.3 d）宜采用密码技术保证设备中的重要信息资源安全标记的完整性； | 宜 |
| 日志记录完整性 | 8.3 e）宜采用密码技术保证日志记录的完整性； | 宜 |
| 重要可执行程序完整性、重要可执行程序来源真实性 | 8.3 f）宜采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。 | 宜 |
| 应用和数据安全 | 身份鉴别 | 8.4 a）应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性； | 应 |
| 访问控制信息完整性 | 8.4 b）宜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； | 宜 |
| 重要信息资源安全标记完整性 | 8.4 c）宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性； | 宜 |
| 重要数据传输机密性 | 8.4 d）应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性； | 应 |
| 重要数据存储机密性 | 8.4 e）应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性； | 应 |
| 重要数据传输完整性 | 8.4 f）宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性； | 宜 |
| 重要数据存储完整性 | 8.4 g）宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性； | 宜 |
| 不可否认性 | 8.4 h）在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。 | 宜 |
| 管理  要求 | 管理  制度 | 具备密码应用安全管理制度 | 8.5 a）应具备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； | 应 |
| 密钥管理规则 | 8.5 b）应根据密码应用方案建立相应密钥管理规则； | 应 |
| 建立操作规程 | 8.5 c）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； | 应 |
| 定期修订安全管理制度 | 8.5 d）应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订； | 应 |
| 明确管理制度发布流程 | 8.5 e）应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制； | 应 |
| 制度执行过程记录留存 | 8.5 f）应具有密码应用操作规程的相关执行记录并妥善保存。 | 应 |
| 人员  管理 | 了解并遵守密码相关法律法规  和密码管理制度 | 8.6 a）相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度； | 应 |
| 建立密码应用岗位责任制度 | 8.6 b）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，其中密码安全审计员岗位不可与密钥管理员、密码操作员兼任；  4）相关设备与系统的管理和使用账号不得多人共用。 | 应 |
| 建立上岗人员培训制度 | 8.6 c）应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能； | 应 |
| 定期进行安全岗位人员考核 | 8.6 d）应定期对密码应用安全岗位人员进行考核； | 应 |
| 建立关键岗位人员保密制度和调离制度 | 8.6 e）应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。 | 应 |
| 建设  运行 | 制定密码应用方案 | 8.7 a）应依据密码相关标准和密码应用需求，制定密码应用方案； | 应 |
| 制定密钥安全管理策略 | 8.7 b）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，各环节安全管理要求参照《信息安全技术 信息系统密码应用基本要求》附录B； | 应 |
| 制定实施方案 | 8.7 c）应按照应用方案实施建设； | 应 |
| 投入运行前进行密码应用安全性评估 | 8.7 d）投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行； | 应 |
| 定期开展密码应用安全性评估及攻防对抗演习 | 8.7 e）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整改。 | 应 |
| 应急  处置 | 应急策略 | 8.8 a）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； | 应 |
| 事件处置 | 8.8 b）事件发生后，应及时向信息系统主管部门进行报告； | 应 |
| 向有关主管部门上报处置情况 | 8.8 c）事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。 | 应 |
| **测评指标合计** | | 41项 | | |

### 特殊指标

本系统不涉及特殊指标。

### 不适用指标

鉴于信息系统的复杂性和特殊性，GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》的第三级要求中的个别项可能不适用于被测信息系统，对于这些不适用项及其不适用原因如表3‑2所示：

**表3‑2不适用指标及说明**

|  |  |  |  |
| --- | --- | --- | --- |
| 安全层面 | 测评指标 | 测评指标描述 | 不适用原因 |
| 网络和通信 | 安全接入认证 | 可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。 | 该系统不涉及从外部设备连接到内部网络进行的工作场景。 |
| 设备和计算 | 重要信息资源安全标记完整性 | 宜采用密码技术保证设备中的重要信息资源安全标记的完整性； | 被测信息系统不涉及安全标记数据，本项不适用。 |
| 应用和数据安全 | 重要信息资源安全标记完整性 | 宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性； | 该系统没有重要信息资源的安全标记数据，无需保证重要信息资源安全标记的完整性。本项不适用。 |
| 应用和数据安全 | 不可否认性 | 在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。 | 经访谈并核查，系统不涉及需要法律认定的重要操作的不可否认性，本项不适用。 |
| **不适用项合计** | | 4 | |

## 测评方法及工具

### 现场测评方法

本次商用密码应用安全性评估使用的测评方法包括：

* 访谈：通过与被测单位的相关人员进行交谈和问询，了解被测信息系统技术和管理方面的一些基本信息，并对一些测评内容进行确认；
* 文档审查：审核被测单位提交的有关信息系统安全的各个方面的文档，如：被测系统总体描述文件，被测系统密码总体描述文件，安全管理制度文件，密钥管理制度，各种密码安全规章制度及相关过程管理记录、配置管理文档，被测单位的信息化建设与发展状况以及联络方式；密码应用方案及评审意见，安全保护等级定级报告，系统验收报告，安全需求分析报告，安全总体方案，自查或上次评估报告等等。通过对这些文档的审核与分析确认测评的相关内容是否达到安全保护等级的要求；
* 实地查看：现场查看测评对象所处的环境、外观等情况；
* 配置检查：查看测评对象的相关配置；
* 工具测试：根据被测信息系统的实际情况，密评人员使用适合的技术工具对其进行测试。

### 测评工具

本次商用密码应用安全性评估使用的测评工具如表3‑3所示：

**表3‑3测评工具**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 工具名称 | 版本 | 生产厂商 | 工具说明 |
| 1 | wireshark | Version 3.3.0-gm | 开源 | 对被测系统网络和通信安全、设备和计算安全、应用和数据安全方面进行检测分析｡通过对通信双方、用户身份鉴别等通信数据包进行抓取，分析系统应用的密码技术的完整性、机密性服务是否有效。 |
| 2 | 数字证书规范性检测工具 | 1.0 | 开源 | 查看数字证书是否符合规范性要求。 |
| 3 | burpsuite | 1.7.3 | portswigger | 分析、重放、篡改http请求包。 |

### 测评工具检查点

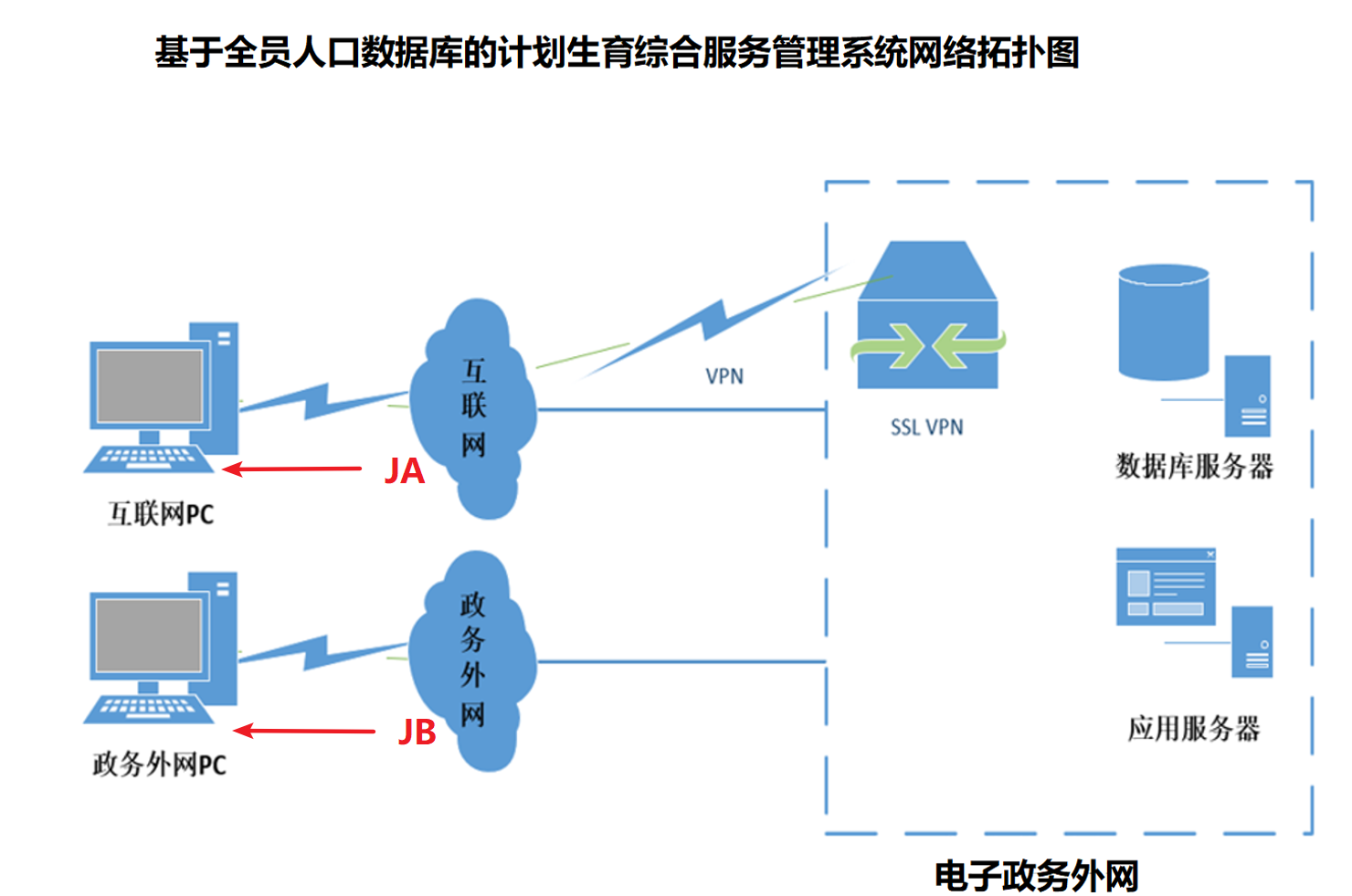


图3.1 测评工具检查点

检查点JA：在互联网PC端接入，在检查点JA进行抓包，查看互联网VPN客户端与运维SSL VPN之间的运维通信信道之间的通信报文是否是加密。

检查点JB：在政务外网PC端接入，在检查点JB进行抓包，查看政务外网非国密浏览器与应用系统之间的通信信道的通信报文是否是加密。

## 测评对象和对应测评方式

### 测评对象确定方法

依据《信息系统密码应用测评过程指南》的测评对象确定方法，根据被测信息系统的重要程度及其相关资产等的价值认定结果，明确核心资产在信息系统内的流转，从而确定与密码相关的测评对象。

### 测评对象确定结果

#### 密码技术应用测评

##### 物理和环境安全测评

**表3‑4物理和环境安全测评对象**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 测评对象 | 测评方式 | 说明 |
| 1 | 政务云中心机房 | 🗹访谈  🞏文档审查  🗹实地查看  🞏配置检查  🞏工具测试 |  |

##### 网络和通信安全测评

**表3‑5 网络和通信安全测评对象**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 测评对象 | 测评方式 | 说明 |
| 1 | 政务外网非国密浏览器与应用系统之间的通信信道 | 🗹访谈  🞏文档审查  🞏实地查看  🗹配置检查  🗹工具测试 |  |
| 2 | 互联网VPN客户端与运维SSL VPN之间的运维通信信道 | 🗹访谈  🞏文档审查  🞏实地查看  🗹配置检查  🗹工具测试 |  |

##### 设备和计算安全测评

**表3‑6设备和计算安全测评对象**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 测评对象 | 测评方式 | 说明 |
| 1 | 应用服务器（虚拟机-Windows Server 2012） | 🗹访谈  🗹文档审查  🗹实地查看  🗹配置检查  🗹工具测试 |  |
| 2 | 数据库服务器（虚拟机-Windows Server 2012） | 🗹访谈  🗹文档审查  🗹实地查看  🗹配置检查  🗹工具测试 |  |
| 3 | 系统数据库（Oracle 11g） | 🗹访谈  🗹文档审查  🗹实地查看  🗹配置检查  🗹工具测试 |  |
| 4 | 运维SSL VPN | 🗹访谈  🗹文档审查  🗹实地查看  🗹配置检查  🗹工具测试 |  |

##### 应用和数据安全测评

**表3‑7应用和数据安全测评对象**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 测评对象 | 测评方式 | 说明 |
| 1 | 基于全员人口数据库的计划生育综合服务管理系统 | 🗹访谈  🗹文档审查  🞏实地查看  🗹配置检查  🗹工具测试 |  |

#### 安全管理测评

**表3‑8安全管理测评对象**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 测评单元 | 测评对象 | 测评方式 | 说明 |
| 1 | 管理制度 | 管理体系（包括安全管理制度类文档、密码应用方案、密钥管理制度及策略类文档、操作规程类文档、记录表单类文档、系统相关人员） | 🗹访谈  🗹文档审查 |  |
| 2 | 人员管理 | 管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员） | 🗹访谈  🗹文档审查 |  |
| 3 | 建设运行 | 密码应用方案、密钥管理制度及策略类文档、密码实施方案、商用密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告、整改文档 | 🗹访谈  🗹文档审查 |  |
| 4 | 管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员） | 🗹访谈  🗹文档审查 |  |
| 5 | 应急处置 | 管理体系（包括密码应用应急处置方案、应急处置记录类文档、安全事件发生情况及处置情况报告、系统相关人员） | 🗹访谈  🗹文档审查 |  |

# **单元测评**

## 密码技术应用要求

### 物理和环境安全

#### 结果汇总

针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表4‑1所示：

**表4‑1物理和环境安全测评结果汇总**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 测评对象 | 测评指标符合情况（符合/部分符合/不符合/不适用） | | |
| **身份鉴别** | **电子门禁记录数据存储完整性** | **视频监控记录数据存储完整性** |
| 1 | 政务云中心机房 | 不符合 | 不符合 | 不符合 |
| 单元测评结果  （符合/部分符合/不符合/不适用） | | 不符合 | 不符合 | 不符合 |

#### 结果分析

被测系统部署于中国联通呼和浩特云数据中心。进入机房时，通过门禁卡、电子门禁系统对进入人员进行身份鉴别，但电子门禁系统对进入人员进行身份鉴别时未采用商用密码技术实现；电子门禁系统进出记录、视频监控记录未采用商用密码技术进行完整性保护。

### 网络和通信安全

#### 结果汇总

针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表4‑2所示：

**表4‑2网络和通信安全测评结果汇总**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 测评对象 | 测评指标符合情况（符合/部分符合/不符合/不适用） | | | | |
| **身份鉴别** | **通信数据完整性** | **通信过程中重要数据的机密性** | **网络边界访问控制信息的完整性** | **安全接入认证** |
| 1 | 政务外网非国密浏览器与应用系统之间的通信信道 | 不符合 | 不符合 | 不符合 | 不符合 | 不适用 |
| 2 | 互联网VPN客户端与运维SSL VPN之间的运维通信信道 | 部分符合 | 部分符合 | 部分符合 | 不符合 | 不适用 |
| 单元测评结果  （符合/部分符合/不符合/不适用） | | 部分符合 | 部分符合 | 部分符合 | 不符合 | 不适用 |

#### 结果分析

网络和通信安全层面有2个测评对象，分别是政务外网非国密浏览器与应用系统之间的通信信道、互联网VPN客户端与运维SSL VPN之间的运维通信信道。互联网VPN客户端与运维SSL VPN之间的运维通信信道采用TLSv1.2通信协议进行加密通信，并通过sha256RSA算法的数字证书进行身份认证，数字证书为自签发的数字证书，通信过程协商的密码套件为TLS\_ECDHE\_RSA\_WITH\_ AES\_256\_GCM\_SHA384，未采用合规的密码算法保证该信道通信过程中数据的机密性和完整性；政务外网非国密浏览器与应用系统之间的通信信道采用HTTP明文协议传输，未采用密码算法保证该信道通信过程中数据的机密性和完整性；以上的通信信道网络边界处的网络安全设备均为通用型产品，采用系统资产自有协议进行通信和身份认证，未采用密码技术保证通信实体身份的真实性。系统网络没有使用密码技术保护访问控制信息完整性。

### 设备和计算安全

#### 结果汇总

针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表4‑3所示：

**表4‑3设备和计算安全测评结果汇总**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 测评对象 | 测评指标符合情况（符合/部分符合/不符合/不适用） | | | | | |
| **身份鉴别** | **远程管理通道安全** | **系统资源访问控制信息完整性** | **重要信息资源安全标记完整性** | **日志记录完整性** | **重要可执行程序完整性、重要可执行程序来源真实性** |
| 1 | 应用服务器（虚拟机-Windows Server 2012） | 不符合 | 部分符合 | 不符合 | 不适用 | 不符合 | 不符合 |
| 2 | 数据库服务器（虚拟机-Windows Server 2012） | 不符合 | 部分符合 | 不符合 | 不适用 | 不符合 | 不符合 |
| 3 | 系统数据库（Oracle 11g） | 不符合 | 不符合 | 不符合 | 不适用 | 不符合 | 不符合 |
| 4 | 运维SSL VPN | 不符合 | 部分符合 | 不符合 | 不适用 | 不符合 | 不符合 |
| 单元测评结果  （符合/部分符合/不符合/不适用） | | 不符合 | 部分符合 | 不符合 | 不适用 | 不符合 | 不符合 |

#### 结果分析

登录应用服务器（虚拟机-Windows Server 2012）、数据库服务器（虚拟机-Windows Server 2012）、系统数据库（Oracle 11g）、运维SSL VPN使用“用户名+静态口令”的方式，未使用密码技术进行身份鉴别；应用服务器（虚拟机-Windows Server 2012）、数据库服务器（虚拟机-Windows Server 2012）采用TLSv1.2协议进行管理，数据库远程管理使用默认TNS协议进行明文通信，应用服务器（虚拟机-Windows Server 2012）、数据库服务器（虚拟机-Windows Server 2012）、运维SSL VPN通信过程协商的密码套件为TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM \_SHA384，未采用合规的密码算法进行机密性和完整性保护，未使用国家核准的密码技术对系统资源访问控制信息完整性、日志记录完整性和重要可执行程序进行保护*。*

### 应用和数据安全

#### 结果汇总

针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表4‑4所示：

**表4‑4应用和数据安全测评结果汇总**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 测评对象 | 测评指标符合情况（符合/部分符合/不符合/不适用） | | | | | | | |
| **身份鉴别[[1]](#footnote-1)** | **访问控制信息完整性** | **重要信息资源安全标记完整性** | **重要数据传输机密性[[2]](#footnote-2)** | **重要数据存储机密性** | **重要数据传输完整性** | **重要数据存储完整性** | **不可否认性[[3]](#footnote-3)** |
| 1 | 基于全员人口数据库的计划生育综合服务管理系统 | 不符合 | 不符合 | 不适用 | 不符合 | 不符合 | 不符合 | 不符合 | 不适用 |
| 单元测评结果  （符合/部分符合/不符合/不适用） | | 不符合 | 不符合 | 不适用 | 不符合 | 不符合 | 不符合 | 不符合 | 不适用 |

针对应用和数据安全层面身份鉴别情况进行说明和汇总，如表4‑5所示：

**表4‑5应用和数据安全身份鉴别测评结果汇总**

|  |  |  |
| --- | --- | --- |
| 序号 | 应用用户 | 身份鉴别 |
| 1 | 系统用户 | 不符合 |
| 单元测评结果  （符合/部分符合/不符合/不适用） | | 不符合 |

针对应用和数据安全层面重要数据的机密性和完整性保护情况进行说明和汇总，如表4‑6所示：

**表4‑6应用和数据安全重要数据测评结果汇总**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 重要数据 | 传输机密性 | 存储机密性 | 传输完整性 | 存储完整性 |
| 1 | 系统用户鉴别数据 | 不符合 | 不符合 | 不符合 | 不符合 |
| 2 | 人口信息数据 | 不符合 | 不符合 | 不符合 | 不符合 |
| 3 | 操作日志数据 | / | / | / | 不符合 |
| 单元测评结果  （符合/部分符合/不符合/不适用） | | 不符合 | 不符合 | 不符合 | 不符合 |

针对应用和数据安全层面不可否认性情况进行说明和汇总，如表4‑7所示：

**表4‑7应用和数据安全不可否认性测评结果汇总**

|  |  |  |
| --- | --- | --- |
| 序号 | 操作行为 | 不可否认性 |
| 1 | 系统不涉及需要法律认定的重要操作的不可否认性 | |
| 单元测评结果  （符合/部分符合/不符合/不适用） | | 不适用 |

#### 结果分析

基于全员人口数据库的计划生育综合服务管理系统用户登录方式为“用户名+口令”，未使用密码技术进行身份鉴别；系统重要业务数据在传输过程中未使用密码技术进行保护，用户鉴别数据采用明文传输；系统访问控制信息存储在数据库，未采用密码技术保证业务应用系统访问控制信息的完整性。管理用户口令在数据库中使用MD5算法加密存储；重要业务数据在数据库明文存储，未采用核准的密码技术保证鉴别信息和重要业务数据存储过程的完整性、机密性。

## 安全管理

### 管理制度

#### 结果汇总

针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表4‑8所示：

**表4‑8管理制度测评结果汇总**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 测评对象 | 测评指标符合情况（符合/部分符合/不符合/不适用） | | | | | |
| **具备密码应用安全管理制度** | **密钥管理规则** | **建立操作规程** | **定期修订安全管理制度** | **明确管理制度发布流程** | **制度执行过程记录留存** |
| 1 | 管理体系（包括安全管理制度类文档、密码应用方案、密钥管理制度及策略类文档、操作规程类文档、记录表单类文档、系统相关人员） | 符合 | 符合 | 符合 | 符合 | 符合 | 符合 |
| 单元测评结果  （符合/部分符合/不符合/不适用） | | 符合 | 符合 | 符合 | 符合 | 符合 | 符合 |

#### 结果分析

现有的管理制度体系中包含有密码应用安全管理制度、密码人员管理、密钥管理、密码建设运行、密码应急处置、密码软硬件管理等制度。

### 人员管理

#### 结果汇总

针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表4‑9所示：

**表4‑9人员管理测评结果汇总**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 测评对象 | 测评指标符合情况（符合/部分符合/不符合/不适用） | | | | |
| **了解并遵守密码相关法律法规**  **和密码管理制度** | **建立密码应用岗位责任制度** | **建立上岗人员培训制度** | **定期进行安全岗位人员考核** | **建立关键岗位人员保密制度和调离制度** |
| 1 | 管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员） | 符合 | 符合 | 符合 | 符合 | 符合 |
| 单元测评结果  （符合/部分符合/不符合/不适用） | | 符合 | 符合 | 符合 | 符合 | 符合 |

#### 结果分析

系统相关人员了解并遵守密码相关法律法规，学习过密码相关国家要求。已有制度体系中具有密码应用岗位责任制度、上岗人员培训制度、人员考核制度等。

### 建设运行

#### 结果汇总

针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表4‑10所示：

**表4‑10建设运行测评结果汇总**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 测评对象 | 测评指标符合情况（符合/部分符合/不符合/不适用） | | | | |
| **制定密码应用方案** | **制定密钥安全管理策略** | **制定实施方案** | **投入运行前进行密码应用安全性评估** | **定期开展密码应用安全性评估及攻防对抗演习** |
| 1 | 密码应用方案、密钥管理制度及策略类文档、密码实施方案、商用密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告、整改文档 | 不符合 | 不符合 | 不符合 | 符合 | 符合 |
| 2 | 管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员） | 不符合 | 不符合 | 不符合 | 符合 | 部分符合 |
| 单元测评结果  （符合/部分符合/不符合/不适用） | | 不符合 | 不符合 | 不符合 | 符合 | 部分符合 |

#### 结果分析

在信息系统规划阶段，没有依据密码相关标准和信息系统密码应用需求，制定密码应用方案、实施方案。系统定期开展系统攻防对抗演习，并形成攻防对抗演习报告；且已制定密钥管理制度及策略类文档。系统投入运行未前进行密码应用安全性评估。

### 应急处置

#### 结果汇总

针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表4‑11所示：

**表4‑11应急处置测评结果汇总**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 测评对象 | 测评指标符合情况（符合/部分符合/不符合/不适用） | | |
| **应急策略** | **事件处置** | **向有关主管部门上报处置情况** |
| 1 | 管理体系（包括密码应用应急处置方案、应急处置记录类文档、安全事件发生情况及处置情况报告、系统相关人员） | 不符合 | 不符合 | 不符合 |
| 单元测评结果  （符合/部分符合/不符合/不适用） | | 不符合 | 不符合 | 不符合 |

#### 结果分析

未制定信息安全体系应急预案框架，未明确安全事件的级别和安全事件的处置流程及报告流程，未规定发生严重安全事件时应向相关部门报告（公安厅、网信办、工业和信息化厅等）；截止本次测评结束系统未发生过安全事件据等*。*

# **整体测评**

## 测评结果修正

针对各个“部分符合”及“不符合”测评指标要求的测评对象，分析与其相关的其他单元、其他层面的测评对象能否和它发生关联关系，发生何种的关联关系，这些关联关系产生的作用是否可以“弥补”该测评对象的不足，以及该测评对象的不足是否会影响与其有关联关系的其他测评对象的测评结果。

**表5‑1测评结果修正**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 安全层面 | 测评单元 | 测评对象 | 经弥补前的测评结果/分值 | 经弥补后的测评结果/分值[[4]](#footnote-4) | 弥补原因及相关测评对象 |
| 无 | | | | | | |

## 整体测评结果和量化评估

修正后的整体测评结果和量化评估汇总如表5‑2所示。其中，测评单元得分的计算过程参见附录A。

**表5‑2****整体测评结果**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 层面（类） | 测评单元 | 符合情况 | | | | 测评单元得分 | 安全层面得分情况 |
| **符合** | **部分**  **符合** | **不符合** | **不适用** |
| 物理和环境安全 | 身份鉴别 |  |  | √ |  | 0 | 0 |
| 电子门禁记录数据存储完整性 |  |  | √ |  | 0 |
| 视频监控记录数据存储完整性 |  |  | √ |  | 0 |
| 网络和通信安全 | 身份鉴别 |  | √ |  |  | 0.125 | 0.1089 |
| 通信数据完整性 |  | √ |  |  | 0.125 |
| 通信过程中重要数据的机密性 |  | √ |  |  | 0.125 |
| 网络边界访问控制信息的完整性 |  |  | √ |  | 0 |
| 安全接入认证 |  |  |  | √ | 不适用 |
| 设备和计算安全 | 身份鉴别 |  |  | √ |  | 0 | 0.0536 |
| 远程管理通道安全 |  | √ |  |  | 0.1875 |
| 系统资源访问控制信息完整性 |  |  | √ |  | 0 |
| 重要信息资源安全标记完整性 |  |  |  | √ | 不适用 |
| 日志记录完整性 |  |  | √ |  | 0 |
| 重要可执行程序完整性、重要可执行程序来源真实性 |  |  | √ |  | 0 |
| 应用和数据安全 | 身份鉴别 |  |  | √ |  | 0 | 0 |
| 访问控制信息完整性 |  |  | √ |  | 0 |
| 重要信息资源安全标记完整性 |  |  |  | √ | 不适用 |
| 重要数据传输机密性 |  |  | √ |  | 0 |
| 重要数据存储机密性 |  |  | √ |  | 0 |
| 重要数据传输完整性 |  |  | √ |  | 0 |
| 重要数据存储完整性 |  |  | √ |  | 0 |
| 不可否认性 |  |  |  | √ | 不适用 |
| 管理  制度 | 具备密码应用安全管理制度 | √ |  |  |  | 1 | 1 |
| 密钥管理规则 | √ |  |  |  | 1 |
| 建立操作规程 | √ |  |  |  | 1 |
| 定期修订安全管理制度 | √ |  |  |  | 1 |
| 明确管理制度发布流程 | √ |  |  |  | 1 |
| 制度执行过程记录留存 | √ |  |  |  | 1 |
| 人员  管理 | 了解并遵守密码相关法律法规和密码管理制度 | √ |  |  |  | 1 | 1 |
| 建立密码应用岗位责任制度 | √ |  |  |  | 1 |
| 建立上岗人员培训制度 | √ |  |  |  | 1 |
| 定期进行安全岗位人员考核 | √ |  |  |  | 1 |
| 建立关键岗位人员保密制度和调离制度 | √ |  |  |  | 1 |
| 建设  运行 | 制定密码应用方案 |  |  | √ |  | 0 | 0.3864 |
| 制定密钥安全管理策略 | √ |  |  |  | 1 |
| 制定实施方案 |  |  | √ |  | 0 |
| 投入运行前进行密码应用安全性评估 |  |  | √ |  | 0 |
| 定期开展密码应用安全性评估及攻防对抗演习 | √ |  |  |  | 1 |
| 应急  处置 | 应急策略 | √ |  |  |  | 1 | 1 |
| 事件处置 | √ |  |  |  | 1 |
| 向有关主管部门上报处置情况 | √ |  |  |  | 1 |
| **合计** | | 16 | 4 | 17 | 4 | 27.81 | | |
| **符合情况** | | **符合** | **部分**  **符合** | **不符合** | **不适用** | **综合得分** | | |

# **风险分析**

具体地，根据威胁类型和威胁发生频率，判断测评结果汇总中部分符合项或不符合项所产生的安全问题被威胁利用的可能性，可能性的取值范围为高、中和低。根据资产价值的高低，判断测评结果汇总中部分符合项或不符合项所产生的安全问题被威胁利用后，对被测系统的业务信息安全造成的影响程度，影响程度取值范围为高、中和低。综合以上的结果，密评机构根据自身经验和相关国家标准要求，对被测系统面临的安全风险进行赋值，风险值的取值范围为高、中和低。结合被测系统的安全保护等级对风险分析结果进行评价，即对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的风险。如果存在高风险项，则认为信息系统面临高风险；同时也需要考虑多个中低风险叠加可能导致的高风险问题。

经风险分析，系统存在高风险9项，中风险11项，低风险1项，具体见表6‑1：

**表6‑1风险分析**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 安全层面 | 问题描述 | 关联威胁 | 风险分析 | 风险等级 | | |
| **高** | **中** | **低** |
| 1 | 物理和环境安全 | 身份鉴别：政务云中心机房电子门禁系统未采用密码技术对访问用户进行身份鉴别。 | TP1 | 电子门禁系统未采用密码技术对用户进行身份鉴别，可能导致非法人员进入机房，对软硬件设备和数据进行直接破坏的风险，但机房部署了视频监控系统，另外进入机房需要提前申请并进行身份登记，该威胁利用身份鉴别漏洞的可能性不高，结合信息系统密码应用高风险判定指引，判定该问题的风险级别为中。 | 0 | 1 | 0 |
| 2 | 电子门禁记录数据存储完整性：政务云中心机房未使用密码技术保护电子门禁系统进出记录存储的完整性。 | TP2 | 电子门禁系统的出入登记记录未采用密码技术进行存储完整性保护，可能导致记录被篡改或删除的风险，但其存储位置位于机房内，机房部署了视频监控系统，另外进入机房需要进行身份登记，进入机房的登记记录被篡改的可能性不高，因此判定该问题的风险级别为中 | 0 | 1 | 0 |
| 3 | 视频监控记录数据存储完整性：政务云中心机房未使用密码技术保护视频监控系统的音像记录存储的完整性。 | TP2 | 视频监控系统的音像记录未采用密码技术进行存储完整性保护，可能导致记录被篡改或删除的风险，但其存储位置位于机房内，另外进入机房需要进行身份登记，音像记录被篡改的可能性不高，因此判定该问题的风险级别为低。 | 0 | 0 | 1 |
| 4 | 网络和通信安全 | 身份鉴别：政务外网非国密浏览器与应用系统之间的通信信道,互联网VPN客户端与运维SSL VPN之间的运维通信信道未使用合规的密码技术对通信实体进行身份鉴别，无法保证通信实体身份的真实性。 | TN1 | 可能导致非法用户设备接入系统网络的风险，综合分析该威胁发生的频率为高，威胁利用该漏洞实施破坏的可能性为高，结合信息系统密码应用高风险判定指引，判定该问题的风险级别为高。 | 1 | 0 | 0 |
| 5 | 通信数据完整性：政务外网非国密浏览器与应用系统之间的通信信道,互联网VPN客户端与运维SSL VPN之间的运维通信信道未使用密码技术保证通信过程中数据的完整性。 | TN2 | 在通信过程未采用密码技术保证通信数据的完整性，可能导致重要数据被非法篡改的风险，综合分析该威胁利用该漏洞实施破坏的可能性为中，结合信息系统密码应用高风险判定指引，判定该问题的风险级别为中。 | 0 | 1 | 0 |
| 6 | 通信过程中重要数据的机密性：政务外网非国密浏览器与应用系统之间的通信信道,互联网VPN客户端与运维SSL VPN之间的运维通信信道未使用合规的密码技术保证通信过程中重要数据的机密性 | TN2 | 在通信过程未采用密码技术保证通信数据的机密性，可能导致业务数据被非法获取的风险，但是数据传输的线路为单位内网，在一定程度上降低了数据被非法获取的风险，结合信息系统密码应用高风险判定指引，判定该问题的风险级别为中。 | 1 | 0 | 0 |
| 7 | 网络边界访问控制信息的完整性 ：政务外网非国密浏览器与应用系统之间的通信信道,互联网VPN客户端与运维SSL VPN之间的运维通信信道网络边界设备未采用合规的密码技术对访问控制信息进行完整性保护。 | TN1 | 可能导致非授权人员破坏网络边界的风险，综合分析该威胁发生的频率不高，威胁利用漏洞，导致资产被破坏的可能性不高，结合信息系统密码应用高风险判定指引，判定该问题的风险级别为中。 | 0 | 1 | 0 |
| 8 | 安全计算环境 | 身份鉴别：应用服务器（虚拟机-Windows Server 2012）,数据库服务器（虚拟机-Windows Server 2012）,系统数据库（Oracle 11g）,运维SSL VPN未使用密码技术对登录系统相关设备的用户进行身份鉴别 | TD1 | 未使用密码技术对登录系统关联设备的用户进行身份鉴别，无法保证用户身份的真实性，存在设备被非法人员登录的风险，结合信息系统密码应用高风险判定指引，威胁严重程度为高，因此风险等级为高。 | 1 | 0 | 0 |
| 9 | 远程管理通道安全：应用服务器（虚拟机-Windows Server 2012）,数据库服务器（虚拟机-Windows Server 2012）,系统数据库（Oracle 11g）,运维SSL VPN未采用合规的密码技术建立安全的信息传输通道。 | TD2 | 关联设备未使用合规密码技术建立安全的信息传输通道，存在身份鉴别数据被非法获取的风险，结合信息系统密码应用高风险判定指引，威胁严重程度为高，因此风险等级为高。 | 1 | 0 | 0 |
| 10 | 系统资源访问控制信息完整性：应用服务器（虚拟机-Windows Server 2012）,数据库服务器（虚拟机-Windows Server 2012）,系统数据库（Oracle 11g）,运维SSL VPN未采用密码技术来保证系统资源访问控制信息的完整性。 | TD3 | 当前系统资源访问控制信息没有完整性保护措施，存在设备资源被登录设备的其他用户篡改的风险，但由于网络环境相对可控，威胁发生频率为中，威胁严重程度为中，因此风险等级为中。 | 0 | 1 | 0 |
| 11 | 日志记录完整性：应用服务器（虚拟机-Windows Server 2012）,数据库服务器（虚拟机-Windows Server 2012）,系统数据库（Oracle 11g）,运维SSL VPN未采用密码技术来保证日志记录的完整性。 | TD5 | 关联设备的日志记录在设备本机存储，日志记录没有完整性保护措施，存在日志记录被非法篡改的风险，威胁发生频率为中，威胁严重程度为中，因此风险等级为中。 | 0 | 1 | 0 |
| 12 | 重要可执行程序完整性、重要可执行程序来源真实性：应用服务器（虚拟机-Windows Server 2012）,数据库服务器（虚拟机-Windows Server 2012）,系统数据库（Oracle 11g）,运维SSL VPN未采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。 | TD6 | 关联设备重要可执行程序没有完整性保护措施，存在被篡改的风险，程序都由软件开发商提供，威胁发生频率为低，威胁严重程度为高，因此风险等级为中。 | 0 | 1 | 0 |
| 13 | 应用和数据安全 | 身份鉴别：系统用户系统使用用户名口令进行身份鉴别，不能保证应用系统用户身份的真实性。 | TA1 | 应用系统用户采用用户名口令进行身份鉴别，存在被非法人员登录系统的风险，威胁发生频率为高，问题严重程度为高，而且该问题容易被利用，被利用后给组织带来严重影响，因此风险等级为高。 | 1 | 0 | 0 |
| 14 | 访问控制信息完整性：基于全员人口数据库的计划生育综合服务管理系统未采用密码技术来保证应用系统访问控制信息的完整性。 | TA2 | 当前应用系统访问控制信息没有完整性保护措施，存在应用资源被其他用户获取的风险，威胁发生频率为低，问题严重程度为中，因此风险等级为中。 | 0 | 1 | 0 |
| 15 | 重要数据传输机密性：系统用户鉴别数据,人口信息数据未采用密码技术保证信息系统应用系统的重要数据传输的机密性。 | TA4、TA5 | 系统业务数据明文传输，存在传输数据被攻击者非法获取的风险，威胁发生频率为中，问题严重程度为高，而且该问题容易被利用，被利用后给组织带来严重影响，因此风险等级为高。 | 1 | 0 | 0 |
| 16 | 重要数据存储机密性：系统用户鉴别数据,人口信息数据未采用核准的密码技术保证信息系统应用的重要数据存储的机密性。 | TA4、TA5 | 当前系统重要业务信息为明文存储，用户身份鉴别信息使用不合规的MD5算法存储在数据库，存在存储数据被攻击者非法获取的风险，威胁发生频率为中，问题严重程度为高，而且该问题容易被利用，被利用后给组织带来严重影响，因此风险等级为高。 | 1 | 0 | 0 |
| 17 | 重要数据传输完整性：系统用户鉴别数据,人口信息数据重要数据传输完整性：应用层面未采用密码技术保证信息系统应用的重要数据传输的完整性。 | TA4、TA5 | 当前系统重要业务数据、用户鉴别数据传输存在传输数据被外部攻击者非法获取篡改的风险，威胁发生频率为中，问题严重程度为中，而且该问题容易被利用，被利用后给组织带来一般影响，因此风险等级为中。 | 0 | 1 | 0 |
| 18 | 重要数据存储完整性：系统用户鉴别数据,人口信息数据,系统操作日志数据未采用密码技术保证信息系统应用的重要数据存储的完整性。 | TA4、TA5、 | 当前重要业务数据、用户鉴别数据存储没有采用密码算法进行完整性保护，存在数据被篡改的风险，威胁发生频率为中，问题严重程度为高，而且该问题容易被利用，被利用后给组织带来严重影响，因此风险等级为高。 | 1 | 0 | 0 |
| 19 | 建设运行 | 制定密码应用方案：系统建设前未制定密码应用方案。 | TK7 | 未制定密码应用方案，无法明确系统的密码应用需求，违背了同步建设的原则，导致后期投入成本增高，延缓系统上线等风险，结合信息系统密码应用高风险判定指引，判定该问题的风险级别为高。 | 1 | 0 | 0 |
| 20 | 制定密码实施方案：系统建设未制定密码实施方案。 | TK7 | 未制定密码实施方案，无法按照应用方案实施建设，可能延缓系统上线等风险，结合信息系统密码应用高风险判定指引，判定该问题的风险级别为中。 | 0 | 1 | 0 |
| 21 | 投入运行前进行密码应用安全性评估：系统投入运行前未进行密码应用安全性评估 | TK7 | 系统投入运行前未进行密码应用安全性评估，可能延缓系统上线等风险，判定该问题的风险级别为中。 | 0 | 1 | 0 |
| **统计** | | | | 21 | 9 | 11 | 1 |

# **评估结论**

通过对内蒙古自治区卫生健康委员会基于全员人口数据库的计划生育综合服务管理系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行和应急处置等方面的测评，该系统综合得分为27.81分，系统密码应用面临高风险，不符合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[[5]](#footnote-5)。

# **附录A测评结果记录**

## 物理和环境安全

**表A-1物理和环境安全测评结果记录**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **测评单元** | **测评对象** | **结果记录** | **量化指标** | | | | **测评单元得分** |
| **密码使用有效性**  ***D*** | **密码算法/技术合规性**  ***A*** | **密钥管理安全**  ***K*** | **测评对象评分**  ***Si,j,k*** |
| **身份鉴别** | 政务云中心机房 | 经访谈机房管理员，审查电子门禁系统相关技术文档，以及实地检查电子门禁系统后核实：机房访问人员使用电子门禁卡方式实现机房进出的身份鉴别, 进入机房后进入机柜列也需要使用电子门禁卡方式实现机柜列进出的身份鉴别,以上门禁均未使用商用密码技术对访问人员做身份鉴别。图A.1-机房门禁、A.1-机柜列门禁、A.1-门禁系统登录。 |  |  |  | 0 | 0 |
| **电子门禁记录数据存储完整性** | 政务云中心机房 | 访谈机房管理人员并现场查看，未使用商用密码技术保护电子门禁系统进出记录完整性。但电子门禁系统的登录具有身份鉴别机制，登录后才可对访问记录操作。电子门禁系统登录时身份鉴别方式为用户名+口令。A.1-门禁系统版本及事件查询、A.1-门禁系统事件。 |  |  |  | 0 | 0 |
| **视频监控记录数据存储完整性** | 政务云中心机房 | 访谈机房管理人员并现场查看,未使用商用密码技术实现监控记录的完整性保护。视频监控设备被“面对面”放置，确保可以全方位监控机房内动态。图A.1-机房视频监控-1、A.1-机房视频监控-2、A.1-视频监控系统登录、A.1-视频监控系统版本、A.1-视频记录存储A.1-实时监控界面。 |  |  |  | 0 | 0 |



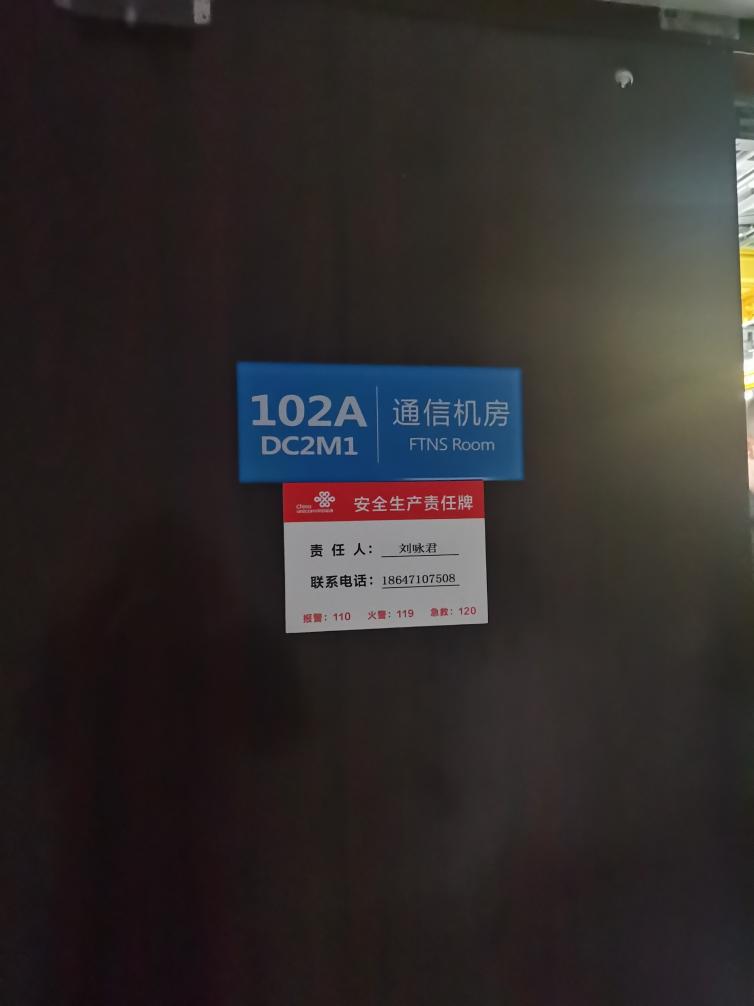
A.1-机房视频监控-1



A.1-机房视频监控-2



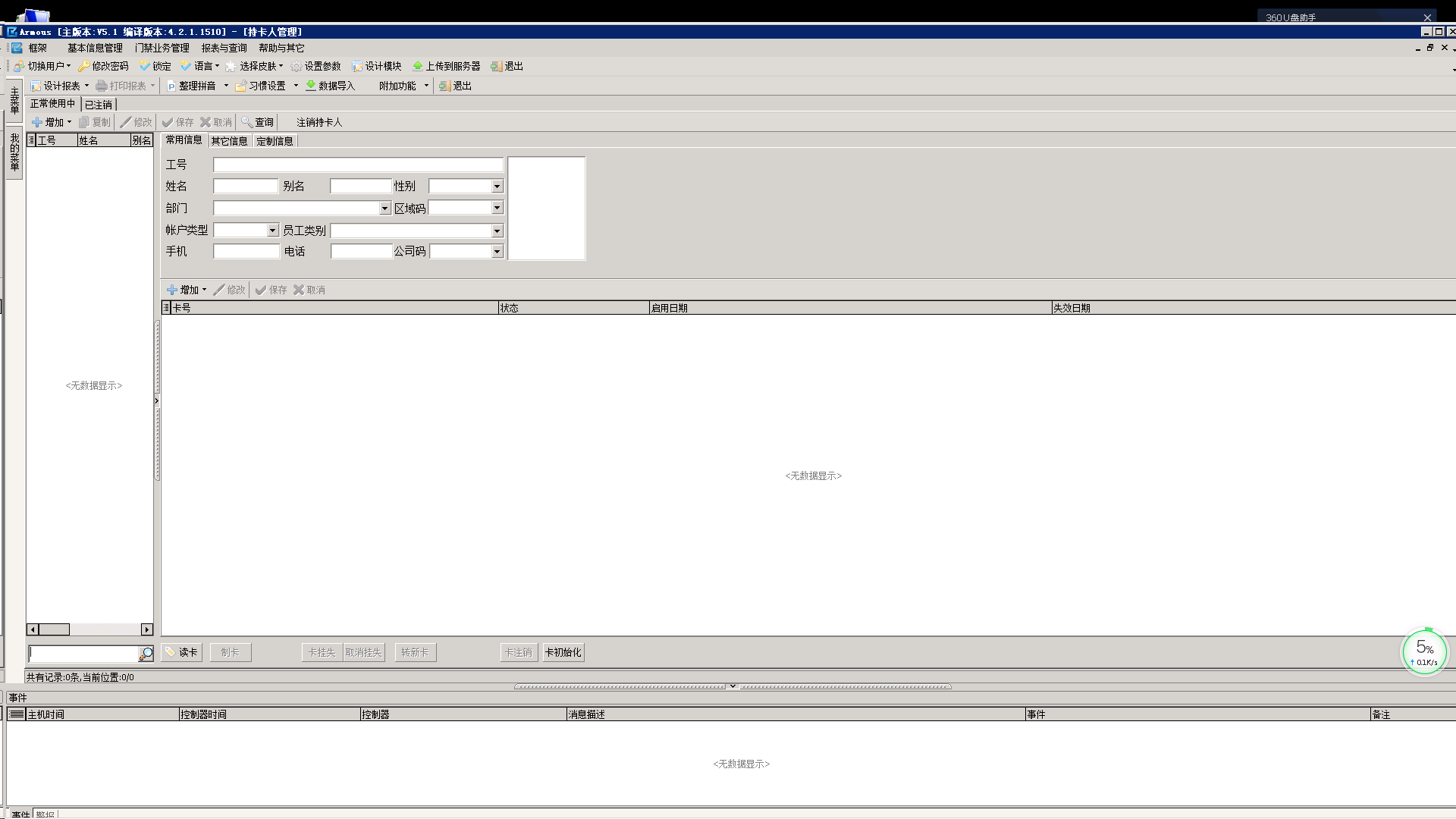
A.1-机柜列门禁



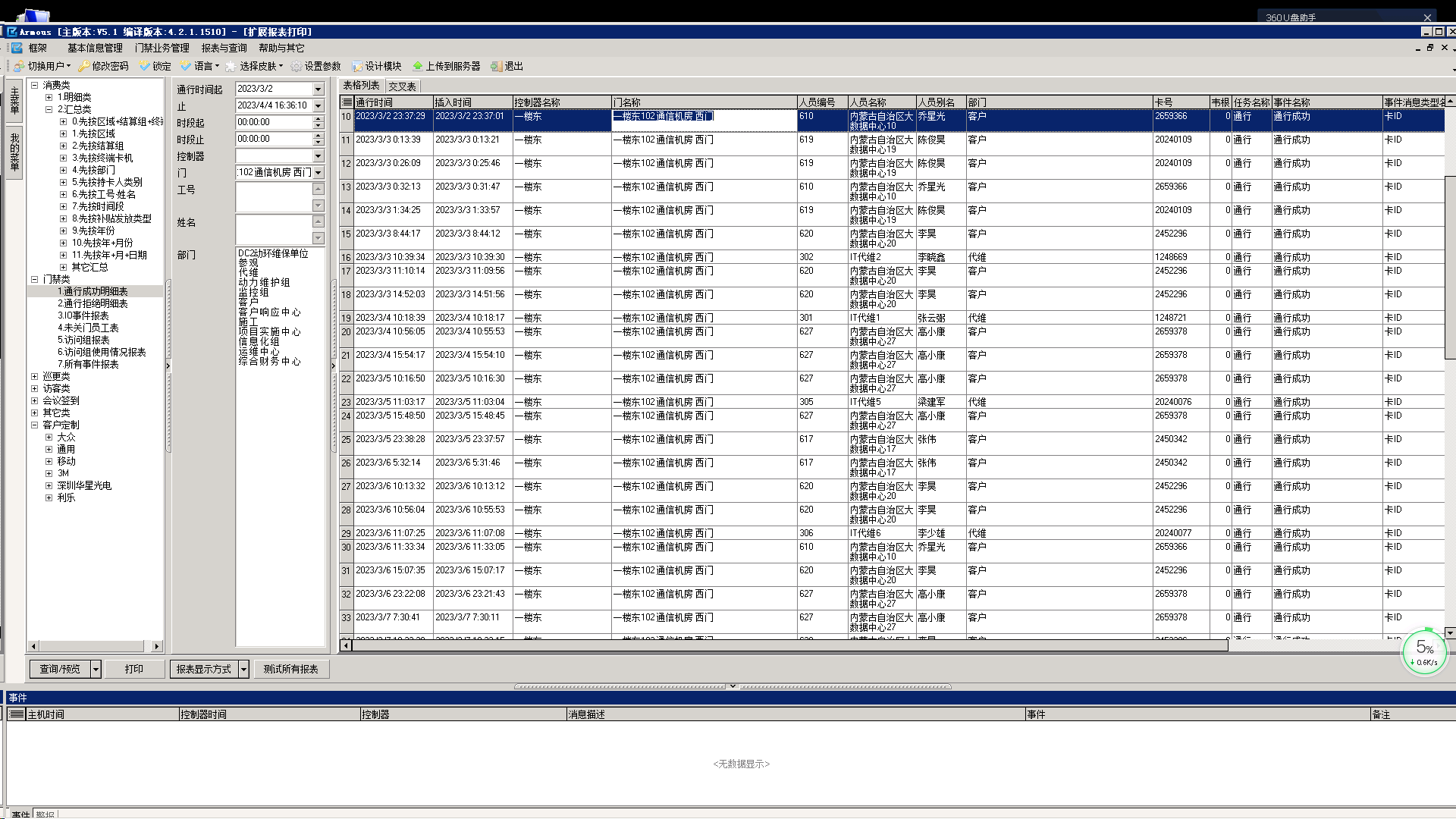
A.1-机房门禁



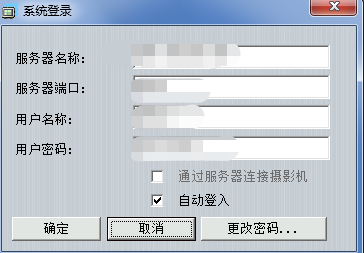
A.1-门禁系统登录



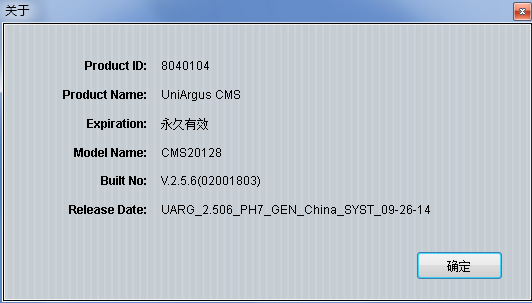
A.1-门禁系统版本及事件查询



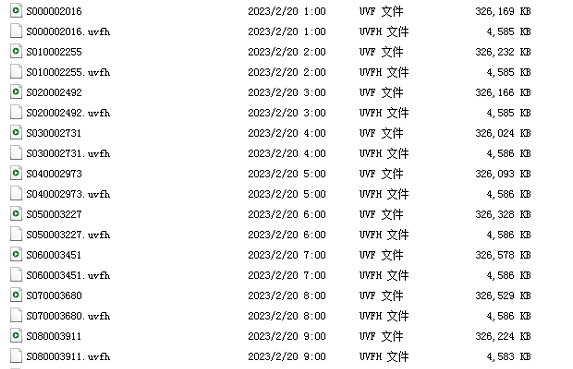
A.1-门禁系统事件



A.1-视频监控系统登录



A.1-视频监控系统版本



A.1-视频记录存储



A.1-实时监控界面

## 网络和通信安全

**表A-2网络和通信安全测评结果记录**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **测评单元** | **测评对象** | **结果记录** | **量化指标** | | | | **测评单元得分** |
| **密码使用有效性**  ***D*** | **密码算法/技术合规性**  ***A*** | **密钥管理安全**  ***K*** | **测评对象评分**  ***Si,j,k*** |
| **身份鉴别** | 政务外网非国密浏览器与应用系统之间的通信信道 | 1．经核查，该信道采用HTTP通信协议，如图：A.1-应用系统身份鉴别，互联网非国密浏览器与应用系统之间建立连接时未使用密码技术对通信实体进行身份鉴别，无法保证通信实体身份的真实性。 |  |  |  | 0 | 0.1250 |
| 互联网VPN客户端与运维SSL VPN之间的运维通信信道 | 1．经核查，该信道采用TLSv1.2通信协议，通过数字证书进行身份认证，使用的签名密码算法为sha256RSA，未采用合规的密码算法保证通信实体身份的真实性。 2. 经核查数字证书为设备自签发，在有效期内，如图: A.2-运维SSL VPN数字证书。 |  |  |  | 0.25 |
| **通信数据完整性** | 政务外网非国密浏览器与应用系统之间的通信信道 | 1．经核查，该信道采用HTTP通信协议，如图：A.1-应用系统通信协议，政务外网非国密浏览器与应用系统之间的通信信道之间建立连接时未采用密码技术保证该信道通信过程中数据的完整性。 |  |  |  | 0 | 0.1250 |
| 互联网VPN客户端与运维SSL VPN之间的运维通信信道 | 1.经核查，该信道采用TLSv1.2通信协议，协商的密码套件为 TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 ，未采用合规的密码算法保证该信道通信过程中数据的完整性。如图A.2-互联网VPN客户端与运维SSL VPN之间的运维通信信道协商密码套件。 |  |  |  | 0.25 |
| **通信过程中重要数据的机密性** | 政务外网非国密浏览器与应用系统之间的通信信道 | 1．经核查，该信道采用HTTP通信协议，如图：A.1-应用系统通信协议，政务外网非国密浏览器与应用系统之间的通信信道之间建立连接时未采用密码技术保证该信道通信过程中数据的机密性。 |  |  |  | 0 | 0.1250 |
| 互联网VPN客户端与运维SSL VPN之间的运维通信信道 | 1.经核查，该信道采用TLSv1.2通信协议，协商的密码套件为 TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384，未采用合规的密码算法保证该信道通信过程中数据的机密性。如图A.2-互联网VPN客户端与运维SSL VPN之间的运维通信信道协商密码套件。 |  |  |  | 0.25 |
| **网络边界访问控制信息的完整性** | 政务外网非国密浏览器与应用系统之间的通信信道 | 1.经核查，系统网络边界处的网络安全设备均为通用型产品，没有使用密码技术保护访问控制信息完整性。 |  |  |  | 0 | 0 |
| 互联网VPN客户端与运维SSL VPN之间的运维通信信道 | 1.经核查，系统网络边界处的网络安全设备均为通用型产品，没有使用密码技术保护访问控制信息完整性。 |  |  |  | 0 |
| **安全接入认证** | 政务外网非国密浏览器与应用系统之间的通信信道 | 1.经访谈系统管理人员，该系统不涉及从外部设备连接到内部网络进行的工作场景。 | / | / | / | 不适用 | 不适用 |
| 互联网VPN客户端与运维SSL VPN之间的运维通信信道 | 1.经访谈系统管理人员，该系统不涉及从外部设备连接到内部网络进行的工作场景。 | / | / | / | 不适用 |



图 A.2-应用系统身份鉴别

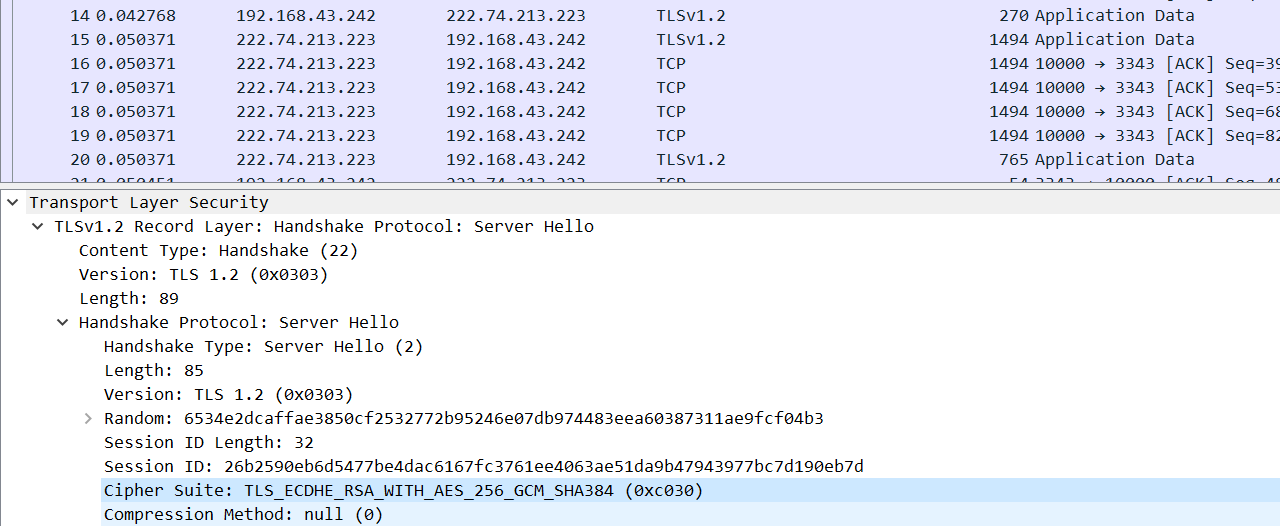


图 A.2-互联网VPN客户端与运维SSL VPN之间的运维通信信道协商密码套件

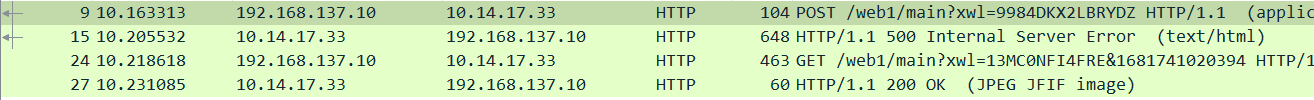


图 A.2-应用系统通信协议

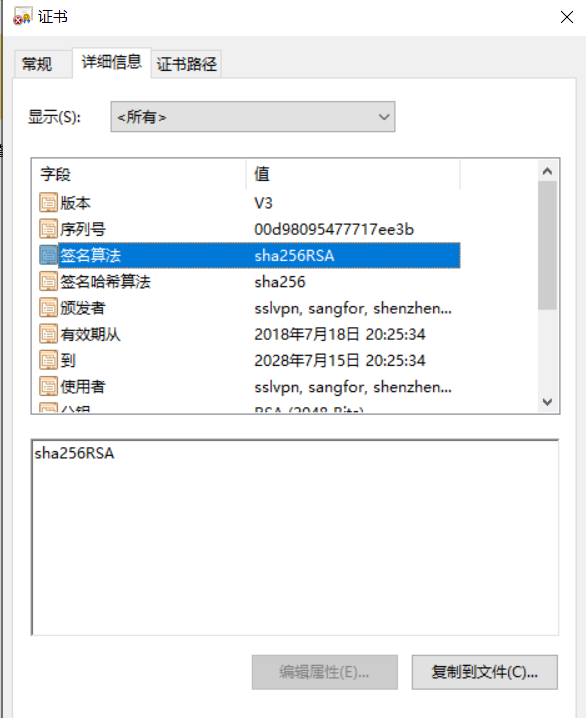


图 A.2-运维SSL VPN数字证书

## 设备和计算安全

**表A-3设备和计算安全测评结果记录**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **测评单元** | **测评对象** | **结果记录** | **量化指标** | | | | **测评单元得分** |
| **密码使用有效性**  ***D*** | **密码算法/技术合规性**  ***A*** | **密钥管理安全**  ***K*** | **测评对象评分**  ***Si,j,k*** |
| **身份鉴别** | 应用服务器（虚拟机-Windows Server 2012） | 1．经核查，登录服务器使用“用户名+静态口令”的方式，未使用密码技术无法保证用户身份真实性，如图 A.3-应用服务器身份鉴别。 |  |  |  | 0 | 0 |
| 数据库服务器（虚拟机-Windows Server 2012） | 1．经核查，登录服务器使用“用户名+静态口令”的方式，未使用密码技术无法保证用户身份真实性，如图 A.3-数据库服务器身份鉴别。 |  |  |  | 0 |
| 系统数据库（Oracle 11g） | 1．经核查，登录数据库使用“用户名+静态口令”的方式，未使用密码技术无法保证用户身份真实性，如图 A.3-数据库身份鉴别。 |  |  |  | 0 |
| 运维SSL VPN | 1．经核查，登录服务器使用“用户名+静态口令”的方式，未使用密码技术无法保证用户身份真实性，如图 A.3-运维SSL VPN身份鉴别。 |  |  |  | 0 |
| **远程管理通道安全** | 应用服务器（虚拟机-Windows Server 2012） | 1.经核查，管理员远程管理使用TLSv1.2协议连接服务器，协商使用密码算法套件: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 ,如图A.3-应用服务器远程管理，未使用核准的的密码技术。 |  |  |  | 0.25 | 0.1875 |
| 数据库服务器（虚拟机-Windows Server 2012） | 1.经核查，管理员远程管理使用TLSv1.2协议连接服务器，协商使用密码算法套件: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 ,如图A.3-数据库服务器远程管理，未使用核准的的密码技术。 |  |  |  | 0.25 |
| 系统数据库（Oracle 11g） | 1.经核查，远程管理数据库使用默认TNS协议进行明文通信远程管理，未使用密码技术。 |  |  |  | 0 |
| 运维SSL VPN | 1.经核查，远程管理运维SSL VPN采用TLSv1.2协议，TLSv1.2协议建立连接时协商的密码套件为： TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 ，未使用核准的密码技术和密码算法，如图A.3-运维SSL VPN远程管理通道。 |  |  |  | 0.25 |
| **系统资源访问控制信息完整性** | 应用服务器（虚拟机-Windows Server 2012） | 1.经核查，应用服务器未使用密码技术保证系统资源访问控制信息的完整性。 |  |  |  | 0 | 0 |
| 数据库服务器（虚拟机-Windows Server 2012） | 1.经核查，数据库服务器未使用密码技术保证系统资源访问控制信息的完整性。 |  |  |  | 0 |
| 系统数据库（Oracle 11g） | 1.经核查，系统数据库未使用密码技术保证系统资源访问控制信息的完整性。 |  |  |  | 0 |
| 运维SSL VPN | 1.经核查，运维SSL VPN未使用密码技术保证系统资源访问控制信息的完整性。 |  |  |  | 0 |
| **重要信息资源安全标记完整性** | 应用服务器（虚拟机-Windows Server 2012） | 访谈系统管理员，被测信息系统不涉及安全标记数据，本项不适用。 | / | / | / | 不适用 | 不适用 |
| 数据库服务器（虚拟机-Windows Server 2012） | 访谈系统管理员，被测信息系统不涉及安全标记数据，本项不适用。 | / | / | / | 不适用 |
| 系统数据库（Oracle 11g） | 访谈系统管理员，被测信息系统不涉及安全标记数据，本项不适用。 | / | / | / | 不适用 |
| 运维SSL VPN | 访谈系统管理员，被测信息系统不涉及安全标记数据，本项不适用。 | / | / | / | 不适用 |
| **日志记录完整性** | 应用服务器（虚拟机-Windows Server 2012） | 1.经核查，应用服务器未使用密码技术保证日志记录存储的完整性。 |  |  |  | 0 | 0 |
| 数据库服务器（虚拟机-Windows Server 2012） | 1.经核查，数据库服务器未使用密码技术保证日志记录存储的完整性。 |  |  |  | 0 |
| 系统数据库（Oracle 11g） | 1.经核查，系统数据库未使用密码技术保证日志记录存储的完整性。 |  |  |  | 0 |
| 运维SSL VPN | 1.经核查，运维SSL VPN不具有商用密码产品认证证书，无法保证自身重要可执行程序完整性、重要可执行程序来源真实性。 |  |  |  | 0 |
| **重要可执行程序完整性、重要可执行程序来源真实性** | 应用服务器（虚拟机-Windows Server 2012） | 1.经核查，应用服务器未使用密码技术保证重要可执行程序的完整性。 |  |  |  | 0 | 0 |
| 数据库服务器（虚拟机-Windows Server 2012） | 1.经核查，数据库服务器未使用密码技术保证重要可执行程序的完整性。 |  |  |  | 0 |
| 系统数据库（Oracle 11g） | 1.经核查，系统数据库未使用密码技术保证重要可执行程序的完整性。 |  |  |  | 0 |
| 运维SSL VPN | 1.经核查，运维SSL VPN不具有商用密码产品认证证书，无法保证自身重要可执行程序完整性、重要可执行程序来源真实性。 |  |  |  | 0 |

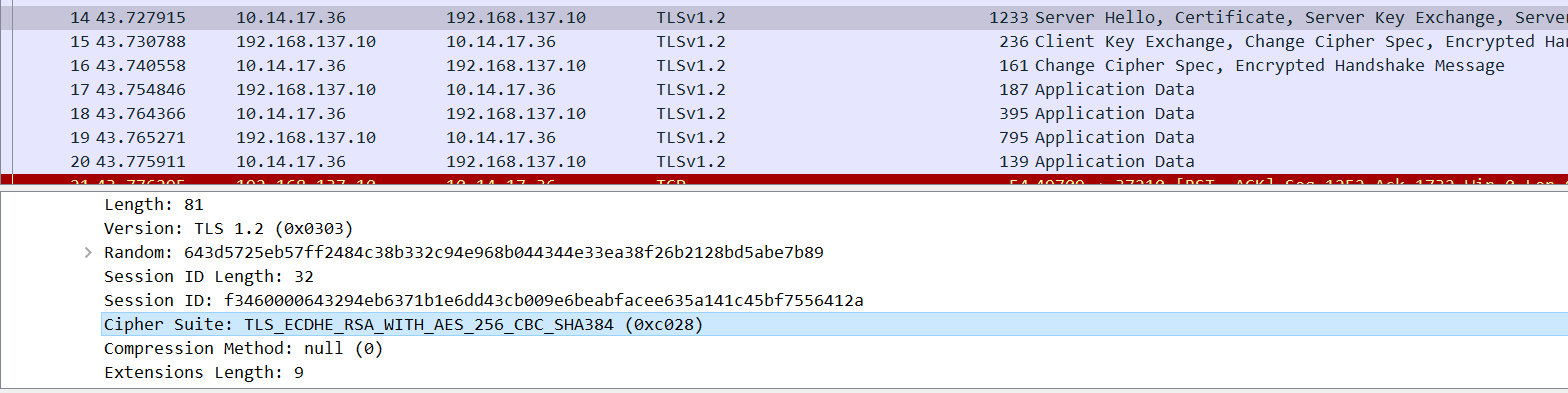


图 A.3-数据库服务器远程管理

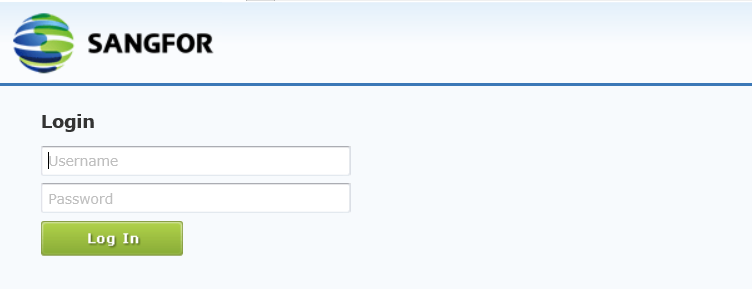


图 A.3-运维SSL VPN身份鉴别

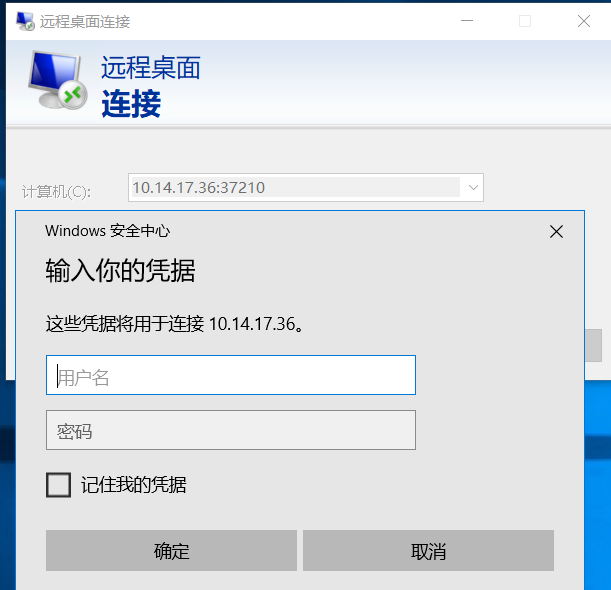


图 A.3-数据库服务器身份鉴别

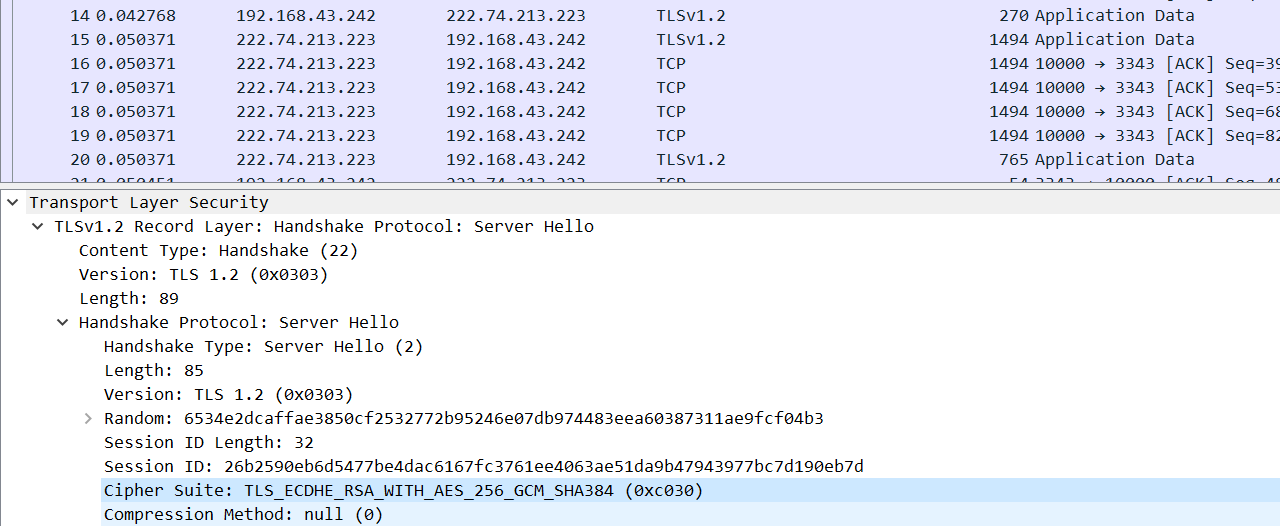


图 A.3-运维SSL VPN远程管理通道

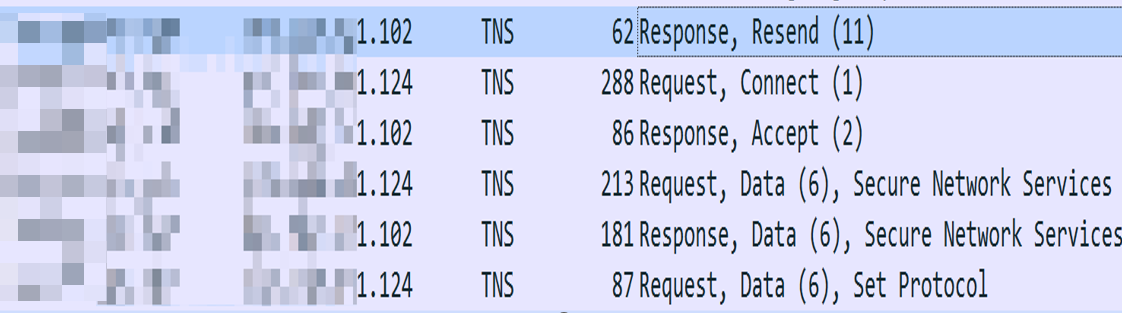


图 A.3-数据库远程管理

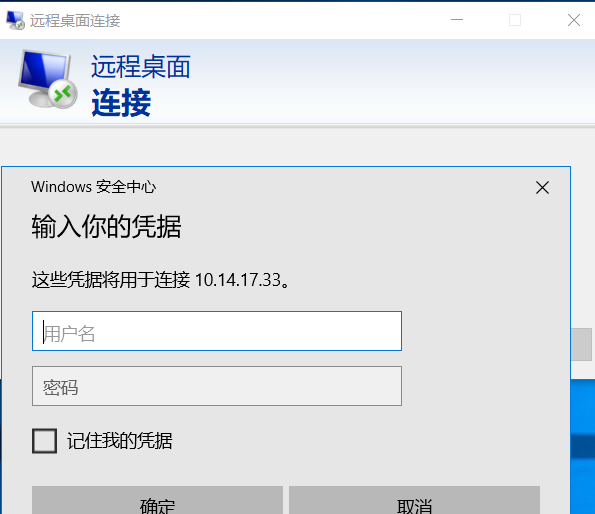


图 A.3-应用服务器身份鉴别

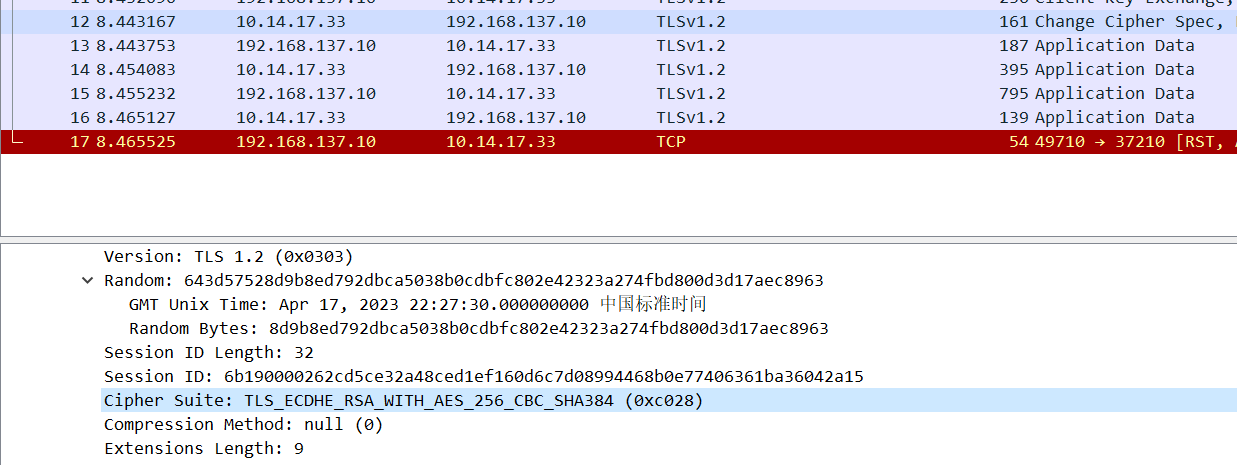


图 A.3-应用服务器远程管理



图 A.3-数据库身份鉴别

## 应用和数据安全

**表A-4应用和数据安全测评结果记录**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **测评单元** | **测评对象** | **结果记录** | **量化指标** | | | | **测评单元得分** |
| **密码使用有效性**  ***D*** | **密码算法/技术合规性**  ***A*** | **密钥管理安全**  ***K*** | **测评对象评分**  ***Si,j,k*** |
| **身份鉴别** | 系统用户 | 1.经核查，系统管理用户登录采用“用户名+口令”进行身份认证，未使用密码技术保证用户身份真实性。如图A.4-应用系统身份鉴别。 |  |  |  | 0 | 0 |
| **访问控制信息完整性** | 基于全员人口数据库的计划生育综合服务管理系统 | 1.应用系统访问控制信息保存在数据库中，如图A.4-用户权限表，没有使用密码技术保护业务应用系统访问控制信息的完整性。 |  |  |  | 0 | 0 |
| **重要信息资源安全标记完整性** | 基于全员人口数据库的计划生育综合服务管理系统 | 经访谈并核查，该系统没有重要信息资源的安全标记数据，无需保证重要信息资源安全标记的完整性。本项不适用。 | / | / | / | 不适用 | 不适用 |
| **重要数据传输机密性** | 系统用户鉴别数据 | 1.经核查，应用层面系统用户鉴别数据明文传输，没有采用密码技术保护鉴别数据的传输机密性，如图A4-鉴别信息传输。 |  |  |  | 0 | 0 |
| 人口信息数据 | 1.经访谈，应用系统采用HTTP协议传输，人口信息数据明文传输，没有采用密码技术保护人口信息数据的传输机密性。 |  |  |  | 0 |
| **重要数据存储机密性** | 系统用户鉴别数据 | 1.经访谈核查，系统管理用户鉴别数据口令采用MD5算法存储在数据库，没有采用核准的密码技术保护鉴别数据的存储机密性，且MD5算法为高风险算法，如图A.4-用户口令存储。 |  |  |  | 0 | 0 |
| 人口信息数据 | 1.经核查，人口信息数据在系统数据库中明文存储，如图 A.4-人口信息数据存储。没有使用密码技术保护重要业务数据的存储机密性。 |  |  |  | 0 |
| **重要数据传输完整性** | 系统用户鉴别数据 | 1.经核查，应用层面系统管理用户鉴别数据明文传输，没有采用密码技术保护鉴别数据的传输完整性，如图A4-鉴别信息传输。 |  |  |  | 0 | 0 |
| 人口信息数据 | 1.经访谈，应用层面证照文件数据明文传输，没有采用密码技术保护鉴别数据的传输机密性。 |  |  |  | 0 |
| **重要数据存储完整性** | 系统用户鉴别数据 | 1.经访谈核查，系统用户鉴别数据口令采用MD5算法存储在数据库，没有采用核准的密码技术保护鉴别数据的存储完整性，且MD5算法为高风险算法，如图A.4-用户口令存储。 |  |  |  | 0 | 0 |
| 人口信息数据 | 1.经核查，人口信息数据在系统数据库中没有使用密码技术保护重要业务数据的存储完整性，如图 A.4-人口信息数据存储。 |  |  |  | 0 |
| 系统操作日志数据 | 1.经核查，系统操作日志数据在数据库存储，没有使用密码技术保护系统操作日志数据的存储完整性。如图A.4-操作日志数据存储。 |  |  |  | 0 |
| **不可否认性** | 不适用 | 经访谈并核查，系统不涉及需要法律认定的重要操作的不可否认性，本项不适用。 | / | / | / | 不适用 | 不适用 |



图 A.4-应用系统身份鉴别



图 A.4-用户权限表

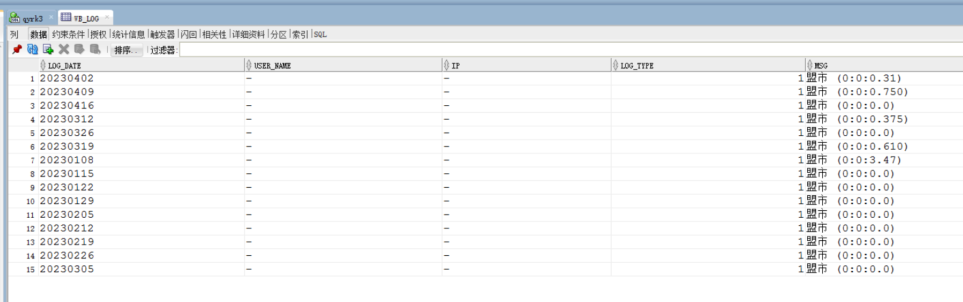


图 A.4-操作日志数据存储

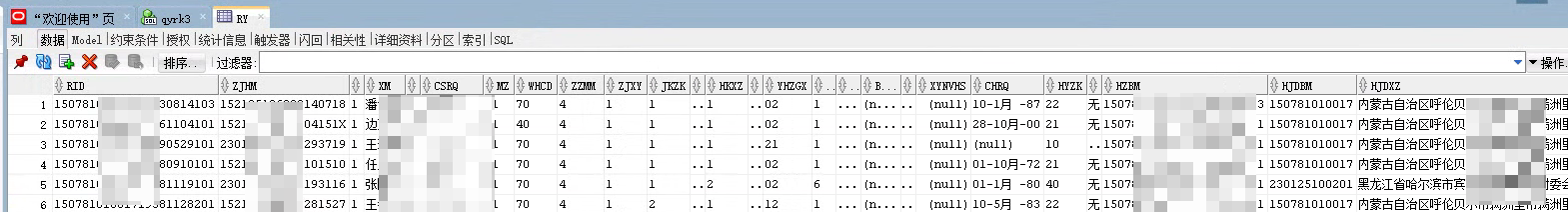


图 A.4-人口信息数据存储

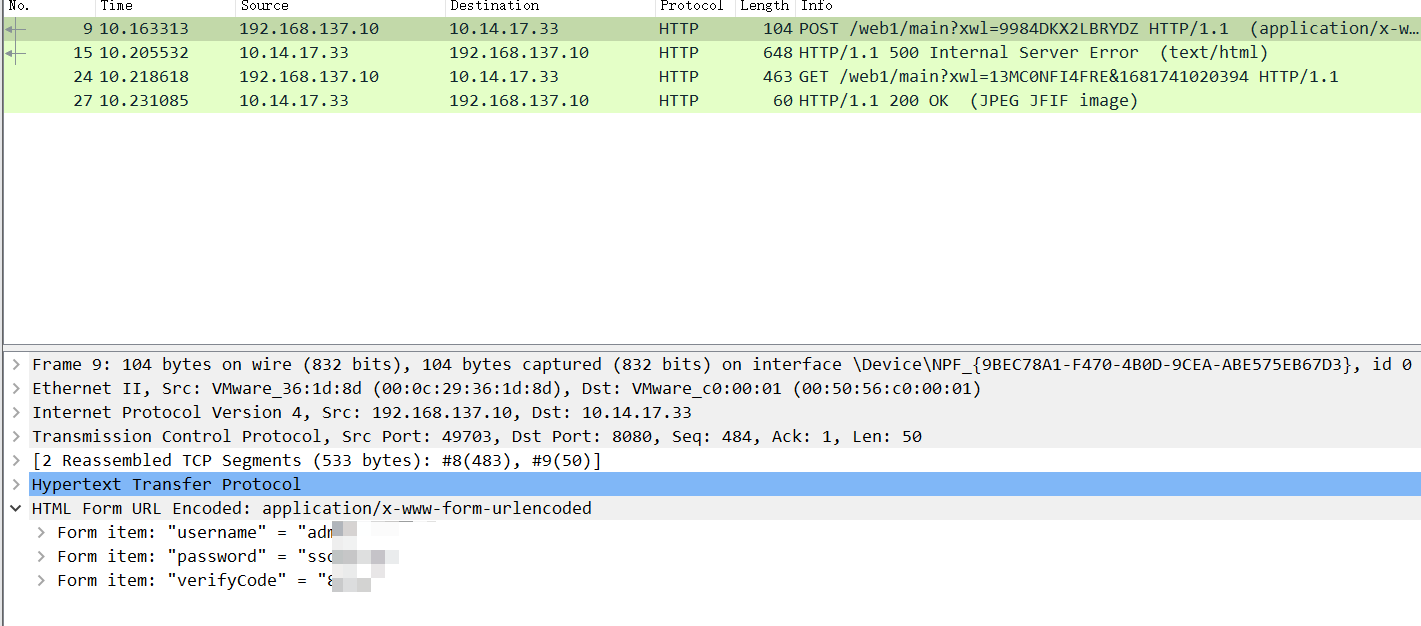


图 A.4-鉴别信息传输

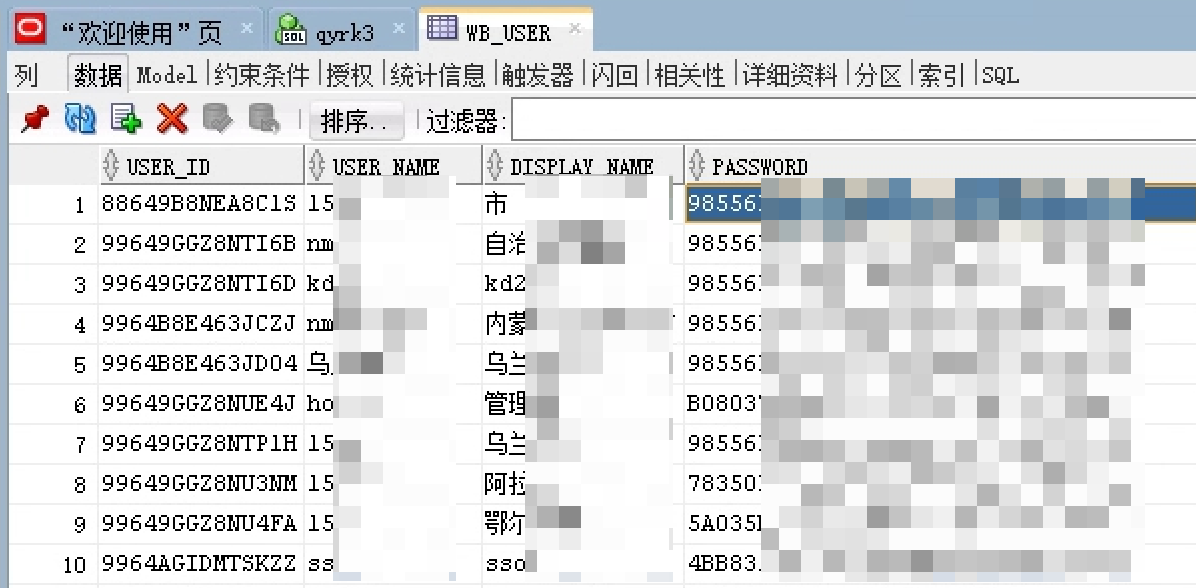


图 A.4-用户口令存储

## 管理制度

**表A- 5管理制度测评结果记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **测评单元** | **测评对象** | **结果记录** | **测评指标符合情况（符合/部分符合/不符合/不适用）** | **测评单元得分** |
| **具备密码应用安全管理制度** | 管理体系（包括安全管理制度类文档、密码应用方案、密钥管理制度及策略类文档、操作规程类文档、记录表单类文档、系统相关人员） | 1.访谈管理员说明，具有密码应用安全相关的管理制度。 2.现场查看现有管理制度，在《商用密码应用安全性评估管理制度汇编》中具有密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理方面制度。 | 符合 | 1 |
| **密钥管理规则** | 1．访谈管理员说明，建立了密钥管理规则。 2．现场查看现有管理制度，在《商用密码应用安全性评估管理制度汇编》第二章节中说明了密钥管理的规则。 | 符合 | 1 |
| **建立操作规程** | 1.访谈管理员说明，建立了密码产品操作规程。 2.现场查看现有管理制度，在《商用密码应用安全性评估管理制度汇编》第六章节针对密码产品建立了操作规程。 | 符合 | 1 |
| **定期修订安全管理制度** | 1.访谈管理员说明，具有定期修订安全管理制度的规定； 2.现场查看管理制度，在《商用密码应用安全性评估管理制度汇编 》第七章节明确了管理制度的修订流程。 | 符合 | 1 |
| **明确管理制度发布流程** | 1.访谈管理员说明，建立了安全管理制度的发布流程。 2.现场查看管理制度，在《商用密码应用安全性评估管理制度汇编 》第七章节明确了管理制度的发布流程。 | 符合 | 1 |
| **制度执行过程记录留存** | 1.访谈管理员说明，单位指定制度执行过程记录文档记录密码相关操作记录。 | 符合 | 1 |

## 人员管理

**表A-6人员管理测评结果记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **测评单元** | **测评对象** | **结果记录** | **测评指标符合情况（符合/部分符合/不符合/不适用）** | **测评单元得分** |
| **了解并遵守密码相关法律法规和密码管理制度** | 管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员） | 1.访谈管理员说明，具有了解并遵守密码相关法律法规和密码管理制度的相关规定。 2.现场查看管理制度，在《商用密码应用安全性评估管理制度汇编》第一章节中明确了相关人员应了解并遵守相关法律法规、密码应用安全管理制度的规定。 | 符合 | 1 |
| **建立密码应用岗位责任制度** | 1.访谈管理员说明，设置了密钥管理员、密码审计员、密码操作员等岗位并定义岗位职责。 2.现场查看管理制度，在《商用密码应用安全性评估管理制度汇编》第一章节中明确了密码应用相关岗位职责。 | 符合 | 1 |
| **建立上岗人员培训制度** | 1.访谈管理员说明，具有上岗人员培训制度及培训计划。 2.现场查看管理制度，在《商用密码应用安全性评估管理制度汇编》第一章节中明确了人员上岗时需要进行专业培训。 3.访谈管理员说明，目前为止还未进行人员培训，未形成相关培训记录。 | 符合 | 1 |
| **定期进行安全岗位人员考核** | 1.访谈管理员说明，具有进行安全岗位人员考核的规定。 2.现场查看管理制度，在《商用密码应用安全性评估管理制度汇编》第一章节中明确了要定期进行岗位人员考核。 3.访谈管理员说明，目前为止还未进行过人员考核。 | 符合 | 1 |
| **建立关键岗位人员保密制度和调离制度** | 1.访谈管理员说明，具有关于对关键岗位人员保密制度和调离制度。 2.现场查看管理制度，在《商用密码应用安全性评估管理制度汇编》第一章节中明确了关键岗位人员保密制度和调离制度的规定。 3.访谈管理员说明，目前为止还没有人员调离。 | 符合 | 1 |

## 建设运行

**表A-7建设运行测评结果记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **测评单元** | **测评对象** | **结果记录** | **测评指标符合情况（符合/部分符合/不符合/不适用）** | **测评单元得分** |
| **制定密码应用方案** | 密码应用方案、密钥管理制度及策略类文档、密码实施方案、商用密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告、整改文档 | 1.访谈管理员说明，在信息系统规划阶段，未依据密码相关标准和信息系统密码应用需求制定密码应用方案。 | 不符合 | 0 |
| 管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员） | 1.访谈管理员说明，具有密码应用安全相关的管理制度。 2.现场查看现有管理制度，在《商用密码应用安全性评估管理制度汇编》中具有密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理方面制度。 |
| **制定密钥安全管理策略** | 密码应用方案、密钥管理制度及策略类文档、密码实施方案、商用密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告、整改文档 | 1.经核查，制定有《密钥安全管理制度》明确密钥管理办法。 | 符合 | 1 |
| 管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员） | 1.经核查，具有密码应用安全相关的管理制度《密码管理制度总则》明确系统密钥管理体系。 |
| **制定实施方案** | 密码应用方案、密钥管理制度及策略类文档、密码实施方案、商用密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告、整改文档 | 1．访谈管理员说明，未依据密码相关标准和信息系统密码应用需求制定密码应用方案，未制定有密码实施方案。 | 不符合 | 0 |
| 管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员） | 1.访谈管理员说明，未依据密码相关标准和信息系统密码应用需求制定密码应用方案，未制定有密码实施方案。 |
| **投入运行前进行密码应用安全性评估** | 密码应用方案、密钥管理制度及策略类文档、密码实施方案、商用密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告、整改文档 | 1.访谈管理员说明，该系统在投入运行前未进行密码应用安全性评估，且经过本次评估，系统存在高风险项，结论不符合。 | 不符合 | 1 |
| 管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员） | 1.访谈管理员说明，未提供密码应用安全相关的管理制度。 |
| **定期开展密码应用安全性评估及攻防对抗演习** | 密码应用方案、密钥管理制度及策略类文档、密码实施方案、商用密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告、整改文档 | 1.经核查，该单位已制定计划每年开展攻防对抗演习，本系统首次进行密码应用安全性评估。 | 符合 | 1 |
| 管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员） | 1.访谈管理员说明，具有密码应用安全相关的管理制度。 2.现场查看现有管理制度，在《商用密码应用安全性评估管理制度汇编》中具有密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理方面制度。 |

## 应急处置

**表A-8应急处置测评结果记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **测评单元** | **测评对象** | **结果记录** | **测评指标符合情况（符合/部分符合/不符合/不适用）** | **测评单元得分** |
| **应急策略** | 管理体系（包括密码应用应急处置方案、应急处置记录类文档、安全事件发生情况及处置情况报告、系统相关人员） | 1.访谈管理员说明，制定了密码应用应急策略。 2.现场查看管理制度，在《商用密码应用安全性评估管理制度汇编》第四章节中明确了应急处置管理的规定。 3.访谈管理员说明，目前为止还未进行过应急演练。 | 符合 | 1 |
| **事件处置** | 1.访谈管理员说明，制定了事件处置流程。 2.现场查看管理制度，在《商用密码应用安全性评估管理制度汇编》第六章节中明确了事件处置流程。 3.访谈管理员说明，目前为止未发生过安全事件。 | 符合 | 1 |
| **向有关主管部门上报处置情况** | 1.访谈管理员说明，发生安全事件后具有向有关主管部门上报处置情况的规定。 2.现场查看管理制度，在《商用密码应用安全性评估管理制度汇编》第六章节中明确了发生安全事件后具有向有关主管部门上报处置情况的规定。 3.访谈管理员说明，目前为止未发生过安全事件。 | 符合 | 1 |

# **附录B密评活动有效性证明记录[[6]](#footnote-6)**

## 密评委托证明[[7]](#footnote-7)

**表B-1委托证明文件**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **文件类型** | 合同 | | **签订时间** | 2022年12月18日 | |
| **委托单位** | 内蒙古自治区大数据中心 | | | | |
| **委托金额** | 2,990,000.00元 | | **系统密评单价** | 83,000.00元 | |
|  | |  | | |  |

## 密评活动证明[[8]](#footnote-8)

**表B-2旅住宿等票证[[9]](#footnote-9)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **入场时间** | 2023年02月08日 | | **离场时间** | 2023年02月27日 |
| **责任单位** | 内蒙古信元网络安全技术股份有限公司 | | | |
| **现场测评人员** | 李世昌、蔡子航、冶占猛 | | | |
| 本项目为本地开展，不涉及差旅票证和住宿票证。 | | | | |
| 住宿账单： | | 住宿费发票： | | |

**表B-3进场记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **入场时间** | 2023年01月13日 | **离场时间** | | 2023年03月10日 |
| **信息系统责任单位** | 内蒙古自治区卫生健康委员会 | **现场测评实施地点** | | 内蒙古自治区卫生健康委员会项目组会议室 |
| **现场测评人员** | 李世昌、蔡子航、冶占猛 | | | |
| **现场测评过程记录（现场测评签到表、现场照片、对接记录、机房出入记录等）** | | | | |
| 现场测评签到表： | | | 现场照片： | |

## 密评活动质量文件[[10]](#footnote-10)

**表B-4现场测评授权及风险告知**

|  |
| --- |
| **现场测评授权书** |
|  |
| **风险告知书** |
|  |

**表B-5测评方案评审**

|  |  |  |  |
| --- | --- | --- | --- |
| **方案名称** | 基于全员人口数据库的计划生育综合服务管理系统系统商用密码应用安全性评估方案 | **评审时间** | 2023年02月13日 |
| 测评方案评审记录： | | 测评方案确认记录： | |

**表B-6密评报告评审**

|  |  |
| --- | --- |
| **评审时间** | 2023年03月30日 |
|  | |

## 密评人员资格证明[[11]](#footnote-11)

**表B-7密评人员资格情况**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **姓名** | **角色** | **密评人员考试通过时间** |
| 1 | 蔡子航 | 组长、密评报告编制人 | 2022年07月 |
| 2 | 李世昌 | 组员 | 2022年07月 |
| 3 | 冶占猛 | 组员 | 未通过考试 |
| 4 | 赵文礼 | 密评报告审核人 | 2020年01月 |
| 5 | 李德波 | 密评报告批准人 | 2022年07月 |

**表B-8密评人员考核成绩证明**

|  |  |  |
| --- | --- | --- |
| {*成绩证明扫描件/照片*} | {*成绩证明扫描件/照片*} | {*成绩证明扫描件/照片*} |

## 系统定级匹配证明

**表B-9系统定级备案证明**

|  |  |
| --- | --- |
| **系统等保定级备案名称** | 基于全员人口数据库的计划生育综合服务管理系统 |
| **系统等保定级备案时间** | 2020年08月18日 |
|  | |

1. “身份鉴别”单元测评结果得出过程详见表4‑5。 [↑](#footnote-ref-1)
2. “重要数据传输机密性”“重要数据存储机密性”“重要数据传输完整性”“重要数据存储完整性”单元测评结果得出过程详见表4‑6。 [↑](#footnote-ref-2)
3. “不可否认性”单元测评结果得出过程详见表4‑7。 [↑](#footnote-ref-3)
4. 若测评对象A弥补了测评对象B的不足，测评对象A的分值为*PA*，测评对象B的弥补前分值为*PB*，则测评对象B弥补后的分值为MAX(0.5×*PA*, *PB*)，即0.5×*PA*和*PB*之间的较大值。 [↑](#footnote-ref-4)
5. 评估结论判定规则如下：

   综合得分100分，结论为符合；

   综合得分小于100分、不低于60分，且系统密码应用无高风险，结论为基本符合；

   否则，结论为不符合。 [↑](#footnote-ref-5)
6. 相关证明材料请提供盖章、签字版本的扫描件或照片。 [↑](#footnote-ref-6)
7. 主要指合同、任务书或其他委托证明文件扫描件，文件内容、页数过多的，只需提供服务内容、收费金额、签字盖章等关键页。运营者自行开展密评的，无须提供。 [↑](#footnote-ref-7)
8. **主要指密评人员差旅票证和住宿票证（或订单、支付记录等体现具体人员测评活动的其他证明文件）、进场记录、对接记录、现场照片等实地测评证明依据，根据本报告1.3描述的实际测评情况提供，并用文字分别注明。相关材料应提尽提，不涉及的，可不提供，如在本地开展的测评活动，可以不提供差旅票证、住宿票证。** [↑](#footnote-ref-8)
9. 机票需提供航空运输电子客票行程单扫描件/照片，火车票需提供纸质车票扫描件/照片。 [↑](#footnote-ref-9)
10. 包括测评方案评审记录和密评报告评审记录的扫描件，密评机构与被测单位进行测评方案确认的记录，现场测评授权书、风险告知书扫描件等。运营者自行开展密评的，无须提供测评方案确认记录、现场测评授权书、风险告知书。 [↑](#footnote-ref-10)
11. 本报告1.3.1节中表1-1中列出的实施密评活动人员中至少2名通过密评人员考试的成绩证明扫描件；同时提供密评报告编制人、审核人、批准人（授权签字人）通过密评人员考试的成绩证明扫描件。 [↑](#footnote-ref-11)