**XXX智慧系统**

安全保证措施

拟制：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

审核：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

会签：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**XXXXX科技有限公司**

**目录**

**[一、 身份鉴别 3](#_Toc6092)**

**[二、 访问控制 3](#_Toc23057)**

**[三、 通信完整性、保密性 5](#_Toc1575)**

**[四、 抗抵赖 5](#_Toc21928)**

**[五、 数据完整性 6](#_Toc9161)**

**[六、 数据保密性 6](#_Toc13675)**

**[七、 应用安全支撑系统设计 7](#_Toc13989)**

# 身份鉴别

* 基本要求

1、应提供专用的登录控制模块对登录用户进行身份标识和鉴别；

2、应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

3、应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

4、应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；

5、应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；

* 实现方式

通过部署PKI/CA与应用系统相结合实现该项技术要求。

# 访问控制

* 基本要求

1、应提供访问控制功能控制用户组/用户对系统功能和用户数据的访问；

2、应由授权主体配置访问控制策略，并严格限制默认用户的访问权限。

3、应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；

4、访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；

5、应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

6、应具有对重要信息资源设置敏感标记的功能；

7、应依据安全策略严格控制用户对有敏感标记重要信息资源的操作；

* 实现方式

通过部署PKI/CA与应用系统相结合实现该项技术要求。

* 基本要求

1、应提供访问控制功能控制用户组/用户对系统功能和用户数据的访问；

2、应由授权主体配置访问控制策略，并严格限制默认用户的访问权限。

3、应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；

4、访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；

5、应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

6、应具有对重要信息资源设置敏感标记的功能；

7、应依据安全策略严格控制用户对有敏感标记重要信息资源的操作；

* 实现方式

通过部署PKI/CA与应用系统相结合实现该项技术要求。

# 通信完整性、保密性

* 基本要求

1、应采用约定通信会话方式的方法保证通信过程中数据的完整性。

2、应采用密码技术保证通信过程中数据的完整性。

3、在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；

4、应对通信过程中的整个报文或会话过程进行加密。

* 实现方式

应通过应用数据加密实现对于数据的完整性和保密性安全。

# 抗抵赖

* 基本要求

1、应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；

2、应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

# 数据完整性

* 基本要求

1、应能够检测到重要用户数据在传输过程中完整性受到破坏。

2、应能够检测到鉴别信息和重要业务数据在传输过程中完整性受到破坏；

3、应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；

4、应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；

* 实现方式

通过使用Hash校验的方法确保数据的完整性。传输过程的完整性受到损坏则采取数据重传的机制；

对于存储的数据则应采取多个备份的方式，防止单一数据损坏造成的损失。

* 部署方式

1、针对应用数据的其他完整性保护可以采用Hash校验，在进行安全编程时采用；

2、针对应用存储数据进行完整性保护时，应当采用多种备份机制进行恢复。

# 数据保密性

* 基本要求

1、应采用加密或其他保护措施实现鉴别信息的存储保密性；

1、应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性；

2、应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性；

* 实现方式

无论在身份验证阶段还是数据传输阶段都使用加密的形式传输数据，通常的方法可以使用SSL或TLS等方式，也可以使用VPN或专用协议传输。

对存储的重要数据需要采取加密手段进行保存。对于本身就是加密方式存储和使用的数据，在传输过程中可以适当降低对传输过程中加密的要求。

# 应用安全支撑系统设计

应用安全支撑平台是面向电子政务应用，构建在网络基础设施、系统平台以及安全保障体系基础之上，为电子政务系统提供一体化的政务应用安全支撑。

* 应用安全支撑系统整体结构

应用安全支撑系统基于数字证书构建安全认证、加密传输、加密存储系统，并为政务应用系统、网络提供安全支撑服务，如可信网站、远程应用访问、网上业务安全服务、数据保护、安全电子邮件应用等。

图示

描述已自动生成应用安全支撑系统设计以安全认证网关、安全存储控制服务器、签名验证模块接口等组成，其组成逻辑结构如下图所示：

* 应用远程访问（B/S、C/S）安全设计

基于安全认证网关的应用远程访问，实现安全的身份认证及数据安全传输。

对于B/S应用系统，浏览器自带SSL模块，因此只需要在服务端部署安全认证网关，而对于C/S应用系统，则必须在客户端与服务端同时部署安全认证网关及相应的客户端安全接口，为了使C/S应用也能够真正获取用户证书信息，客户端还需要部署签名模块，服务端部署签名验证模块。对应用系统进行防护后的系统结构如下：

图片包含 图示

描述已自动生成

经过安全防护的B/S应用访问流程如下：

用户使用浏览器访问应用系统。

安全认证网关要求用户提交用户数字证书。

用户登录USBKEY提交个人证书。

安全认证网关验证用户证书，包括证书自身有效性，信任证书链，黑名单。

验证通过后，安全认证网关将请求发送给真正应用服务器，并将用户证书信息添加到HTTP请求中。

应用服务器从HTTP请求中获取用户的身份，进行访问控制并为用户提供服务。