身份鉴别系统密码应用解决方案

1. 密码应用方案概述

身份鉴别系统是面向业务网各应用系统平台提供身份鉴别服务的系统，可对各类业务网中应用系统的用户身份进行集中管理并实现身份鉴别和授权。身份鉴别系统的密码应用主要解决用户身份真实性、单点登录场景下鉴别协议的安全性、鉴别和授权过程中敏感数据（如凭证信息和用户信息）传输和存储的安全性等问题。

身份鉴别系统密码应用安全性方案设计的重点包括：①利用密码技术实现身份鉴别的安全性及可靠性；②利用密码技术保证单点登录场景下鉴别协议的安全性及可靠性；③利用密码技术对凭证信息的完整性和用户信息的保密性进行保护。

身份鉴别系统密码应用安全性评估的重点包括：①身份鉴别系统和各应用系统之间的通信是否采用密码技术，保证了通信过程的安全性；②身份鉴别协议执行过 程中密码技术应用的正确性和有效性；③身份鉴别过程中是否正确使用密码技术保 护敏感信息的保密性和完整性。

2. 密码应用需求

身份鉴别系统在日常运行和管理过程中，密码应用需求主要包括：

1. 身份鉴别需求。对登录系统的用户以及使用身份鉴别系统获取用户登录状态的应用系统进行身份鉴别，保证用户和应用系统身份的真实性。
2. 关键数据的安全存储需求。保证用户信息、应用系统信息等关键数据在存储过程中的保密性和完整性。
3. 关键数据的安全传输需求。保证用户信息、访问令牌（Access Token）等关键数据在传输过程中的保密性或完整性。

3. 密码应用架构

身份鉴别系统包括身份鉴别服务器、数据库服务器、服务器密码机和 SSL VPN 等。业务网终端用户（包括普通用户和系统管理员用户）在访问应用系统前，身份鉴别系统需要对其进行身份鉴别；身份鉴别后获取授权来访问应用系统。身份鉴别系统密码应用部署如图 1 所示。具体说明如下：

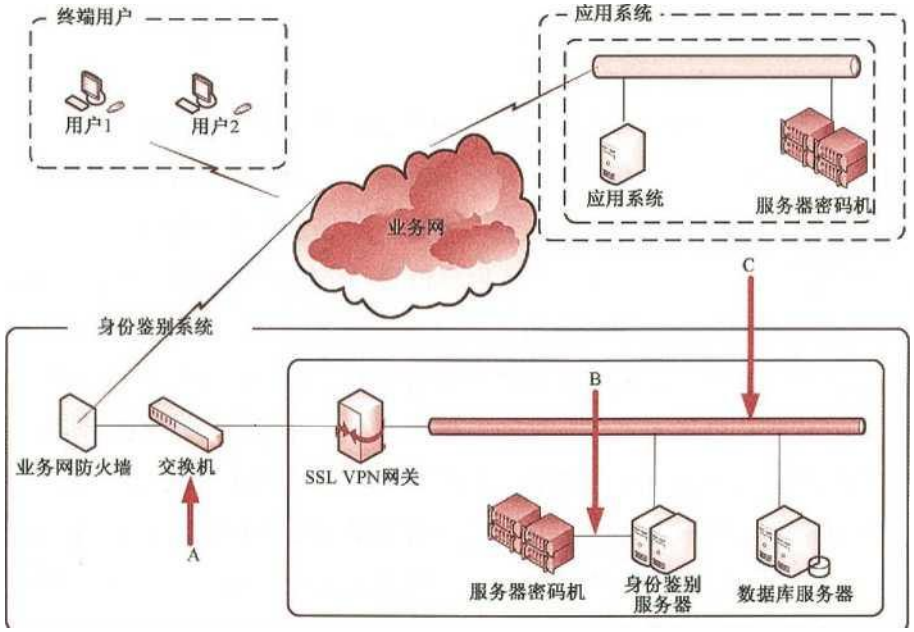

图 1 身份鉴别系统密码应用部署图

在机房部署 SSL VPN 网关，用于安全通信链路的构建。SSL VPN 网关是身份鉴别服务器的外部访问出口，确保通信安全。

在机房部署身份鉴别服务器，调用服务器密码机，完成身份鉴别协议逻辑的实现。

在机房部署服务器密码机，为身份鉴别服务器提供数字签名、验证签名和数据加解密等密钥管理和密码运算服务。

4. 重要设备和关键数据

本系统包括的密码产品、通用服务器、关键业务应用和关键数据分别如表 1—表 4 所示。

表 1 身份鉴别系统部署的密码产品列表

序号	密码产品名称	涉及的密码算法	主要功能
1	服务器密码机	SM2、SM3、SM4	用于支撑身份鉴别服务器的相关密钥管理 和密码运算
2	智能密码钥匙	SM2、SM3、SM4	用于存储用户私钥和数字证书
3	SSLVPN 网关	SM2、SM3、SM4	用于与用户和应用系统建立 SSL 安全通信 链路

表 2 身份鉴别系统部署的通用服务器列表

序号	通用服务器名称	主要功能
1	身份鉴别服务器	完成身份鉴别协议的业务逻辑
2	数据库服务器	完成用户信息等敏感数据的安全存储

表 3 身份鉴别系统的关键业务应用列表

序号	应用名称	主要功能
1	身份鉴别服务	主要面向业务网终端用户，提供身份鉴别、单点登录、访 问令牌同步、访问接入等服务

表 4 身份鉴别系统的关键数据列表

序号	关键数据	关键数据描述	安全需求
1	Access Token	作为授权凭据	完整性
2	用户信息	用户的账号、头像等授权信息	保密性、完整性
3	鉴别信息	用于用户的身份鉴别，如口令	保密性、完整性
4	日志信息	设备和应用产生的日志信息	完整性

5. 密钥体系

身份鉴别系统“应用和数据安全”层面的密钥主要分为对称和非对称两类密钥体系。

1）对称密钥体系

身份鉴别系统的对称密钥及其功能如表 5 所示。

表 5 身份鉴别系统的对称密钥列表

序号	密钥名称	功能
1	Access Token 完整性保护密	用于身份鉴别系统对 Access Token 的完整性保护

2）非对称密钥体系

本系统涉及的非对称密钥体系基于 PKI 技术实现，包括两层密钥，如表 6 所示。需要指出的是，在双证书体系下，证书还包括了加密证书，但由于本系统的应用并不涉及其使用，因此本节涉及的证书指签名证书。

表 6 身份鉴别系统的非对称密钥列表

层次	密钥名称	功能
1	CA 公钥	CA 证书是非对称密钥体系的信任源，用于验证用户证书和应用系统证书
2	用户签名密钥对	用于身份鉴别系统对用户的身份鉴别，公钥由 CA 签发后形成用户证书，私钥存放在智能密码钥匙内部
	应用系统签名密钥对	用于身份鉴别系统对应用系统的身份鉴别，公钥由 CA 签发后形成应用系统证书，私钥存放在应用系统服务器密码机内

6. 密码应用工作流程

身份鉴别服务对登录应用系统的用户进行身份鉴别和授权，所涉及的三方包括用户、身份鉴别服务器、应用系统。为了保护传输用户名/口令、用户信息的保密性,身份鉴别服务器端部署了 SSL VPN 网关以支持数据的安全传输。身份鉴别系统的工作流程如图 2 所示。

身份鉴别系统的密码应用工作流程如下：

1. 用户身份鉴别。用户通过用户名/口令和智能密码钥匙登录身份鉴别系统；身份鉴别系统对用户的身份进行鉴别，以确保用户身份的真实性。
2. 生成 Access Token 身份鉴别服务器根据应用系统的 redirect uri(回调地址)和用户信息生成 Access Token,并采用 HMAC-SM3 算法对其进行完整性保护。

3. 应用系统签名。应用系统使用自己的签名私钥对 Access Token 进行签名。
4. Access Token 合法性检查。首先，身份鉴别服务器使用应用系统证书对应 用系统签名进行验证，以鉴别应用系统的身份；然后，身份鉴别服务器对 Access Token 进行 HMAC-SM3 验证，以确认 Access Token 的合法性；最后，检查 Access Token 与应用系统是否匹配。
5. 应用系统关联用户账户。身份鉴别服务器通过 SSL 安全通信链路将请求的用户信息返回给应用系统，应用系统根据用户信息进行账号关联。

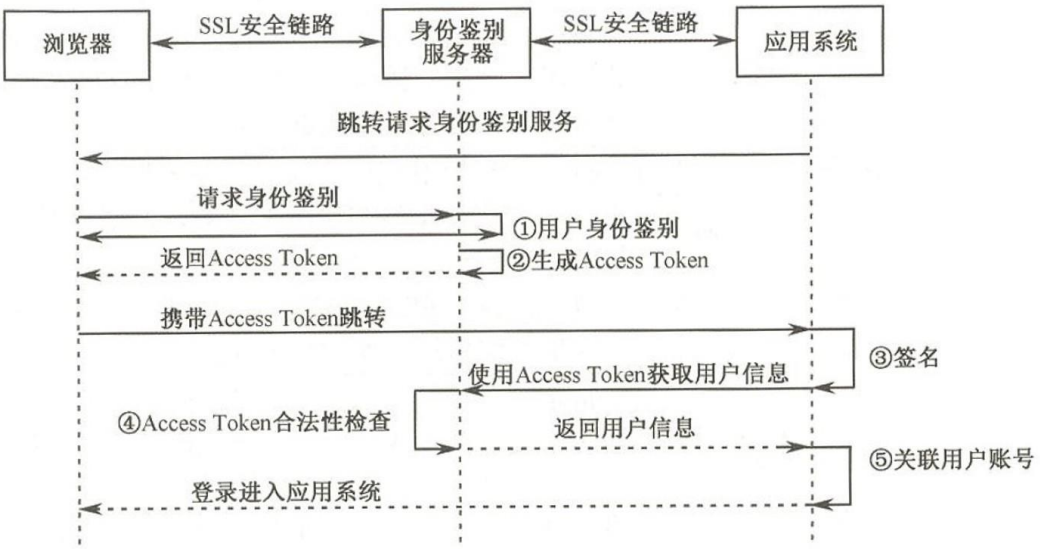

图 2 身份鉴别系统的工作流程

7. 密码技术应用要求标准符合性自查情况

身份鉴别系统的密码技术应用要求标准符合性自查情况如表 7 所示。

表 7 身份鉴别系统标准符合性自查情况（密码技术应用要求部分）

指标要求		标准符合性自查情况
物理和环境安全	身份鉴别	符合。身份鉴别系统所在的机房按照合规的“物理和环境安全”的实现要点进行建设
	电子门禁记录数据完整性	
	视频记录数据完整性	
网络和通信安全	身份鉴别	符合。身份鉴别系统在系统部署边界处配备 SSL VPN 安全网关，完成通信双方的身份鉴别，以及关键数据保密性和完整性的保护。设备管理员通过 SSL VPN 网关对身份鉴别系统内的各个通用服务器进行集中管理
	访问控制信息完整性	
	通信数据完整性	
	通信数据保密性	
	集中管理通道安全	
设备和计算安全	身份鉴别	符合。设备管理员使用用户名/口令和智能密码钥匙（用于产生“挑战一响应”中的 SM2 数字签名）登录身份鉴别服务器和数据库服务器
	访问控制信息完整性	符合。身份鉴别服务器和数据库服务器调用服务

	日志记录完整性	器 密码机，利用 HMAC-SM3 对其访问控制信息、日志记录进行完整性保护
	远程管理身份鉴别信息保密性	符合。通过 SSL VPN 建立的安全通信链路对远程管理身份鉴别信息的保密性进行保护
	重要程序或文件完整性	符合。身份鉴别服务器和数据库服务器中所有重要 程序或文件在生成时利用 SM2 数字签名技术进行完整 性保护，使用或读取这些程序和文件时，进行验签以确认其完整性；公钥存放在服务器密码机中，由服务器密码机进行验签操作
	敏感标记的完整性	不适用。本系统不涉及重要信息的敏感标记
应用和数据安全	身份鉴别	符合。身份鉴别服务包括对以下角色的身份鉴别： •对用户的身份鉴别：身份鉴别服务根据用户的用户名/口令和所持有的智能密码钥匙（用于产生“挑战一响应”中的 SM2 数字签名）进行身份鉴别。 •对应用系统的身份鉴别：应用系统对 Access Token 进行 SM2 数字签名，身份鉴别服务通过验证该签名，以完成对应用系统的身份鉴别。 •对身份鉴别服务管理员的身份鉴别：身份鉴别服务
	访问控制信息和敏感标记完整性	符合。身份鉴别服务调用服务器密码机采用 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
	数据传输安全	符合。身份鉴别服务调用服务器密码机采用 HMAC-SM3 对传输的 Access Token 进行完整性保护，防止用户和应用系统篡改。用户信息的传输安全保护在“网络和通信安全”层面完成
	数据存储安全	符合。身份鉴别服务调用服务器密码机对用户信息 等关键敏感数据进行加密存储，并利用 HMAC-SM3 对其进行完整性保护，保证数据保密性和完整
	日志记录完整性	符合。身份鉴别服务调用服务器密码机采用 HMAC- SM3 对其日志记录进行完整性保护
	重要应用程序的加载和卸载	符合。仅有设备管理员可以进行重要应用程序的加 载和卸载，而设备管理员的身份鉴别在“设备和计算安全”层面完成