迪曼森
Dimensen.com

签名验签服务器
产品白皮书

版本：V1.6

迪曼森科技

版权声明

目　录

签名验签服务器产品白皮书

1 前言

1.1 背景

随着社会信息化的发展，“电子化”时代应运而生。在“电子化”的业务活动中，各参与方通过对应用系统中关键业务信息进行签名，来确保这些业务活动或者业务信息的完整性、不可抵赖性。签名验签服务器不但可以有效的保障业务数据的完整性和不可抵赖性，同时还大大降低应用系统中实现电子签名的复杂度，可广泛应用于电子政务、电子商务、电子金融等各个行业中。

1.2 术语

SM2 算法（SM2 algorithm）

一种椭圆曲线公钥密码算法，其密钥长度为 256 比特。

SM3 算法（SM3 algorithm）

一种杂凑密码算法，其杂凑值长度为 256 比特。

SM4 算法（SM4 algorithm）

一种对称分组密码算法，其密钥长度和分组长度都为 128 比特。

标识密钥集成平台（Identity Key Infrastructure/Integration 简称 IKI 平台）

对可信标识进行全生命周期管理的安全系统，由可信标识管理中心 IMC、注册管理系统 RA 和可信标识认证查询系统 IPA 构成。

实体（Entity）

指现实世界中的客观事物，它是现实世界中任何可区分、可识别的事物。实体可以指人，也可以指物。

实体标识（Entity Identity）

由实体无法否认的信息组成，如实体的可识别名称、电子邮箱、身份证号、电话号码等。

可信标识（Trusted Digital Identity 简称可信标识 TID）

由中心根据实体身份计算出的私钥进行签名的包含实体标识、加密公钥、签名公钥、有效期以及扩展信息的一种数据结构。

2 产品概述

2.1 产品简介

签名验签服务器是一款支持多种算法的商用密码应用设备，该设备主要应用在采用 IKI 技术的电子商务、电子政务和企业信息化系统中，为各类应用系统提供基于可信标识的身份认证、数字签名验签、数据加解密等安全保护功能。

2.2 产品组成

签名验签服务器包含签名验签服务器硬件设备、应用集成 SDK 和管理服务客户端。

签名验签服务器硬件设备：提供数据的签名、验证签名、数字信封等密码运算功能。

应用集成 SDK：应用系统通过集成签名验签服务器 SDK，调用其密码运算服务，进行数据的签名、验证签名、数字信封等密码运算。

管理服务客户端：管理员通过安装管理服务客户端，对签名验签服务器可信标识及相关参数进行配置，以提高服务管理效率。

签名验签服务器产品组成如图 1 所示。

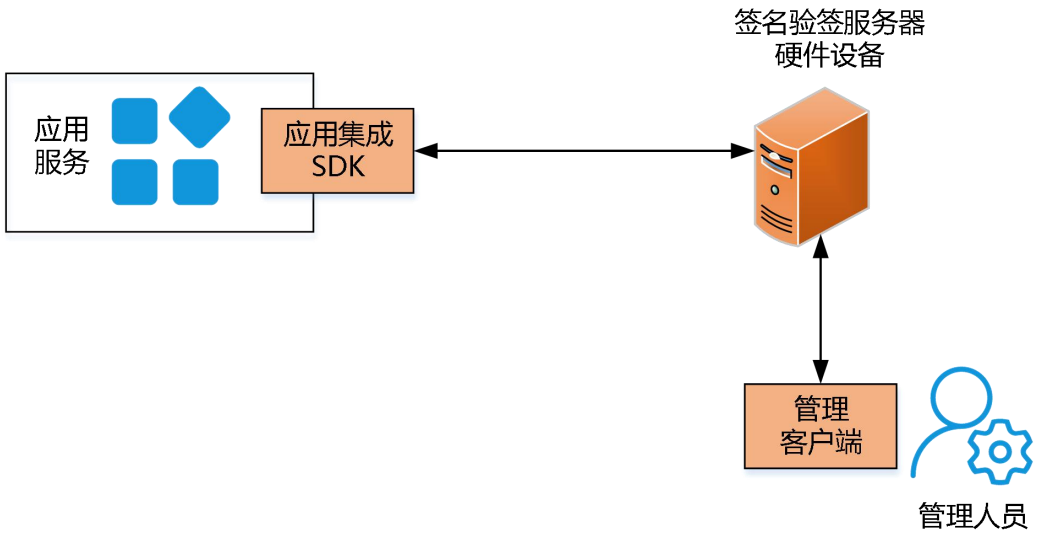

图 1 签名验签服务器产品组成

3 产品功能

3.1 数字签名和验签

提供 GM/T 0009 数字签名验签功能，提供 GM/T 0010 消息签名验签功能。

3.2 数字信封加密和解密

提供数字信封加密、解密功能，信封结构符合 GM/T 0010 标准。

3.3 可信标识管理

提供颁发机构公钥矩阵、可信标识导入功能。支持同时配置多个颁发机构公钥矩阵，验证多机构颁发的可信标识。

3.4 权限管理

对管理人员采用基于角色的权限管理，分为管理员与审计员两种角色，管理员负责签名验签服务器可信标识及相关参数的配置，审计员负责对管理员操作日志进行审计。

3.5 日志管理

系统记录完整的操作日志和业务日志，提供日志查询、审计功能。

3.6 系统备份恢复

系统可以备份当前配置，保证系统瘫痪时能快速恢复。

3.7 性能监测

提供可视化的系统资源使用情况管理界面，通过管理界面监测系统性能。

3.8 系统自检

提供上电时自检和接收自检指令时自检的功能，检测硬件设备是否正常启动以及密码算法正确性、存储公钥矩阵、密钥和数据的完整性等。

4 产品特点

4.1 完全采用国产算法

系统采用的 SM2、SM3、SM4 密码算法是我国自主产权的国产密码算法，安全强度远高于 DES、AES、RSA 等国际通用密码算法。

4.2 支持多种操作系统

应用服务器与签名验签服务器之间采用 TCP/IP 协议进行通信，可支持多种主流的操作系统，如 Windows 系列、Linux 系列。

4.3 标准化

签名验签服务器严格遵循以下标准设计研发：

- 《GM/T 0009-2012 SM2 密码算法使用规范》
- 《GM/T 0010-2012 SM2 密码算法加密签名消息语法规范》
- 《GM/T 0014-2012 数字证书认证系统密码协议规范》
- 《GM/T 0015-2012 基于 SM2 密码算法的数字证书格式规范》
- 《GM/T 0029-2014 签名验签服务器技术规范》

4.4 安全性强

管理人员采用基于可信标识的高强度身份认证和鉴权，确保管理人员的合法身份及其操作权限。

操作系统封闭管理端口和业务端口以外的所有端口，加强了产品的抗攻击性。

4.5 简单易用

签名验签服务器提供详细的用户手册便于使用者学习使用，系统操作可视化，用户界面友好，操作简单、易于使用。

5 产品部署

在产品的实际使用中，签名验签服务器与业务系统并行部署，为用户提供高强度的身份认证、数据私密性保护以及业务的抗抵赖、防篡改的综合解决方案，产品典型部署网络拓扑如图 2 所示：

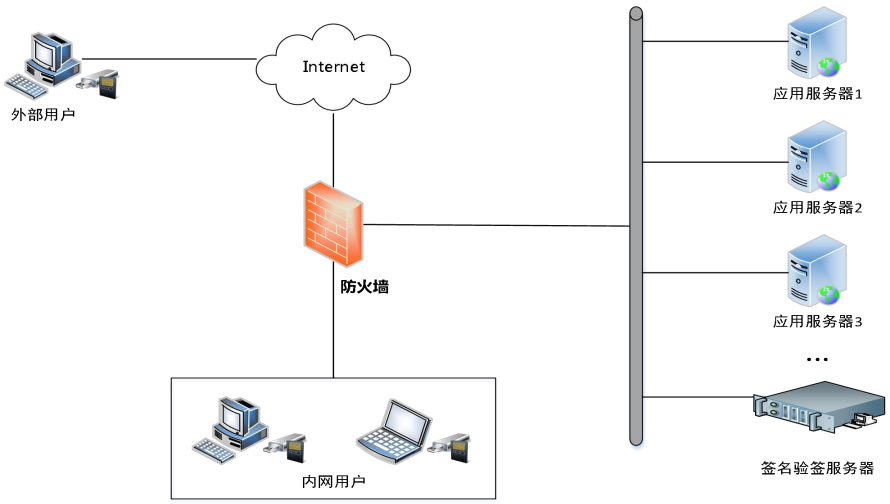

图 2 典型部署结构