文档类型：

文档编号：V500R005C00SPC820

电子文档安全管理系统

技术白皮书

北京亿赛通科技发展有限责任公司

2021 年 4 月

目录

第一章 产品背景 4

第二章 产品介绍 5

2.1 产品概述 5
2.2 产品组成 5
2.3 设计原则 7
2.3.1 实用性原刚 7
2.3.2 兼容性原则 7
2.3.3 安全性原则 7
2.3.4 可靠性原则 7
2.3.5 成熟和先进行原则 8
2.3.6 规范性原则 8
2.3.7 可管理性原则 8
2.3.8 可扩展性原则 9
2.3.9 法规遵从原则 9

第三章 产品架构 10

第四章 核心功能 12

4.1 透明加密 12
4.1.1 透明加密 12
4.1.2 半透明加密 12
4.1.3 智能加密 12
4.1.4 全盘扫描加解密 13
4.1.5 文件访问控制 13
4.1.6 内容安全控制 13
4.1.7 打印控制 14
4.1.8 打印水印 14
4.1.9 阅读水印 14
4.1.10 邮件白名单 15
4.1.11 文件备份 15
4.1.12 多密钥隔离 15
4.1.13 进程签名 16
4.2 防勒索软件 16
4.3 权限管理 16
4.4 流转工具 16
4.5 外发管理 17
4.6 流程管理 17
4.7 应用安全网关 17
4.8 安全中间件 18
4.9 智能移动终端 18
4.10 全文检索 18
4.11 恶意软件 18

4.12 上传下载加解密服务 18
4.13 数据展板 19
第五章 系统实施与部署 20
5.1 部署环境 20
5.1.1 服务器 20
5.1.2 客户端 21
5.2 部署架构 22
5.3 部署步骤概述 22
第六章 核心技术 24
6.1 文件级智能动态加解密技术 24
6.2 网络级智能动态加解密技术 24
6.3 文件虚拟磁盘技术 25
6.4 设备过滤驱动技术 26
6.5 其他核心技术 26
第七章 产品优势 27
第八章 公司资质 28
第九章 技术支持 29
9.1 售后服务 29
9.2 产品问题处理方式及机制 29
9.2.1 问题级别 29
9.2.2 服务方式 30
9.2.3 服务流程 31
9.2.4 售后人员管理制度 31

第一章　产品背景

随着国内经济的不断发展，信息化已经成为了企业日常办公的重要手段，根据相关部门统计，目前企业的数据 80%以上已经实现了电子化，在某些特定行业如制造业，金融业，通信行业等数据电子化程度更高。数据电子化为企业带来了巨大的效率提升，与以往使用的纸质文件相比，电子文件的流转不再受制于特定的传播途径和传播效率，可以通过内部网络，公网以及多种移动存储介质进行便捷性使用，极大的提高了企业内部及同外部的信息沟通，减少了因信息传递而造成的时间浪费及准确性等问题。

但随着高速网络的普及和终端应用的不断增加，也给制造企业的信息安全带来了较为严重的威胁，近年各企业资料外泄事件，均在一定程度上为制造业相关企业敲响了警钟。网络高速化发展为内部信息外泄提供了便捷的手段，终端应用的不断丰富也为制造企业的内部防控带来了一定难度，传统的安全控制手段如桌面管理，上网行为，网络防火墙等均无法有效的防止内部核心数据的外泄，因此信息安全，必须从信息源头抓起，才能有效的实现信息全生命周期保护。亿赛通作为国内数据泄露防护领域的第一品牌，专注于数据安全研究，为企业提供最优的安全解决方案。

第二章　产品介绍

2.1 产品概述

亿赛通文档安全管理系统是国内最早基于文件过滤驱动技术的文档加解密产品，系统包括透明加密、权限管理、外发管理、应用安全网关、安全中间件、智能移动终端、U 盘客户端七个核心组件。

主要通过对电子文档的加密保护，防止内部员工泄密和外部人员非法窃取企业核心重要数据资产。保护范围涵盖终端电脑（Windows、Mac、Linux 系统平台）、智能终端（Android、IOS）及各类应用系统（OA、知识管理、文档管理、项目管理、PDM 等），根据用户需求可以对电子文档进行自动加密、手动加密、智能加密和文档细粒度权限控制，对文档的全生命周期进行安全管控，做到事前防御、事中控制、事后审计，帮助企业搭建一套完善的文档防泄密体系。

2.2 产品组成



亿赛通电子文档安全管理系统包括透明加密、权限管理、外发管理、应用安全网关、安全中间件、智能移动终端、U 盘客户端七大核心组件，用于对用户电脑终端、移动办公、各类应用系统上的数据，从生产、存储、流程、外发到销毁进行全生命周期保护。

（1） 电脑终端文档数据安全

- **透明加密**

保证用户核心数据文档从产生开始一致处于加密状态，防止由于数据生产者泄密给企业带来的数据安全风险。

透明加密方式包含三类：主动加密、自动加密、智能加密。

- **权限管理**

通过对文档加密授权及角色对应，控制文档在内部受控使用，避免越权使用带来的泄密风险。

- **外发管理**

通过对文档加密、授权及封装，控制文档在外部传播和使用时造成的泄密风险。

（2） 应用系统数据安全

- **应用安全网关**

通过软硬一体化结合的方式为应用系统提供安全保障，应用安全网关可以为应用系统提供安全准入和数据加解密双重防护。

- **安全中间件**

以接口的方式为应用系统提供加解密能力，提升应用系统的保密性，保障数据的安全性。安全中间件基于标准 restful 接口，不受协议和网络环境限制，只要应用系统具备二次开发能力，通过调用接口快速完成与第三方应用系统无缝对接。

（3） 移动办公数据安全

- **移动客户端**

移动客户端即 U 盘客户端，将透明加密客户端植入 U 盘，合法用户可以根据需要将 U 盘插入任意电脑，即可打开和使用加密文档，无需连网加密服务器，无需携带办公电脑，主要适用于员工回家加班、出差等情况。

- **智能移动终端**

为智能移动设备提供亿赛通专属 APP 安全服务，保证通过移动设备下载到客户端的加密数据可以正常查看，脱离受控范围无法使用。此模块一般与透明加密、应用安全网关或安全中间件等配合使用。

2.3 设计原则

2.3.1 实用性原刚

系统采用先进的体系架构，充分与信息安全管理体系理论进行结合，对体系建设过程提供完整的安全规划方法，有效提高安全规划的合理性和实用性。

在进行安全保密性设计的同时，以解决企业现有的安全隐患为基础，重点考虑系统的方便性、合理性以及适应企业未来发展的需要，在加密算法、加密技术、网络安全基础架构和安全产品方面均采用成熟先进的技术。系统已经支持市面上绝大部分的主流操作系统、应用软件。而且可以自由配置需要支持的文件类型，完全满足公司未来发展的需要。

2.3.2 兼容性原则

系统兼容主流的杀毒软件，如：360 安全卫士、麦咖啡、卡巴斯基、赛门铁克(诺顿、SEP)、趋势、瑞星、江民等单机和网络版本杀毒软件和防火墙。

支持市面上绝大部分的主流操作系统、应用软件。具备良好的兼容性，在提高企业数据安全防护性的同时，不会对公司现有的开发生产业务造成影响。

在与应用系统兼容方面，安全网关可实现与现有的 OA、代码配置管理平台以及其它应用系统的兼容，并可与公司未来部署的大部分应用系统实现兼容。如有特殊需求，亦可通过提供文档加密系统的二次开发接口实现与公司内各种应用系统的无缝集成。

2.3.3 安全性原则

系统采用先进的安全防护技术，对软件本身提供高强度保护功能，必须有卸载口令才能对软件进行卸载操作。可以防止用户采用非常规手段对软件进行修改、卸载、停止、删除或破解等行为，同时可以对试图对软件进行的非法操作行为产生日志记录。方便管理人员进行审计。

2.3.4 可靠性原则

本系统作为公司业务运营系统的重要组成部分，系统的可靠性和安全性和准确性同等重要。采用计算机技术是为了提高业务处理能力，改善客户服务的水平，如果系统的可靠性无法保证，就大大降低了该系统的可用性。因此，系统提供较强的容错、容灾能力、完善的系统安全机制、

可靠的纠错恢复能力。服务端可以采用双机备份方式部署，避免单点故障，客户端采用先进的内核级加密技术，稳定性强，同时支持文件备份功能，最大限度上避免无故报错的情况产生，不会对数据、代码的完整性产生影响和破坏。系统采用灵活的部署方式，确保不会对现有的网络环境和系统环境造成影响。

根据公司的实际需要，先建立基本稳定的安全体系，保证基本的、必须的安全性。随着今后随着业务规模的扩大及应用的增加，网络应用和复杂程度的变化，网络脆弱性也会不断增加，调整或增强安全防护力度，保证整个业务网络最根本的安全需求。

2.3.5 成熟和先进行原则

系统在架构设计、系统配置、系统管理、加密技术等方面均采用成熟、实用和先进的技术。系统架构采用最适合企业现状的 C/S 与 B/S 相结合的架构设计，保证企业数据安全性的同时，在系统配置与管理上提供简单方便而又灵活管理配置平台，方便管理人员进行维护。加密技术采用目前最先进的第三代内核驱动层（虚拟文件系统：LayerFSD）智能动态加解密技术，完全适应企业现状以及未来的发展。

2.3.6 规范性原则

系统在采用成熟先进的技术，采用符合国际信息安全行业的标准和规范；具有良好的护展性，可以提供二次开发接口和灵活的技术方案，为系统的扩展升级、与其它系统的集成互联提供良好的基础。

2.3.7 可管理性原则

系统采用了众多人性化的设计，界面友好、设计合理，管理操作简单，具备如下特点：

- ◆ 不影响各应用系统的正常使用；
- ◆ 不影响各应用系统检索功能等；
- ◆ 不改变用户对应用系统的操作习惯；

并可以进行远程管理和故障诊断，极大的降低了用户的工作量。系统提供运维管理、策略安全管理、文档权限管理、日志审计管理及流程审核管理等核心功能，在数据安全级别设置和解密审批流程上，操作十分简单，完全可以适合企业领导操作的同时进行监视和控制。

2.3.8 可扩展性原则

系统在产品的软件架构和硬件架构方面，都重复考虑了其平滑扩展功能，可以在不影响使用的前提下可以自由扩展所需要使用的 License 和功能，不影响公司各种应用系统的使用，如果有特殊的需求时，可通过提供加密系统的二次开发接口实现与公司内各种应用系统的接口无缝集成。在整个集成过程中，不会影响应用系统的使用。

2.3.9 法规遵从原则

信息安全技术 电子文档安全管理产品安全技术要求 GA/T 989 -2012

第三章　产品架构



- **服务器端**

整个加密软件的核心是集中管理服务器，用以支持整体系统的用户管理、系统配置、终端管理、策略管理、密钥管理以及系统日志和审计管理等。

针对不同类型的终端文档通过终端加密和具体应用权限管理来统一实现支持和管控，通过与终端部署的客户端控制软件进行交互配合完成终端使用用户身份识别，以及对不同类型的终端电子文档的加解密控制、用户权限控制、文件外发、离网终端（暂时不能够连接到服务器的终端电脑）控制和终端加密文档操作记录日志回收等功能。

对于加密软件的使用操作者身份认证是通过成员认证体系接口管理来完成的。在没有其它认证体系的情况下，本系统将提供自建的用户认证支持体系，用于管理使用用户的身份注册、系统角色、组织机构、安全策略分组等与用户身份相关的信息并提供运行状态下的动态认证支持服务；同时成员认证体系接口管理还面向 MS-AD 域、LDAP 等标准准统一认证体系提供集成手段，以完成使用用户身份识别能力；从而满足系统使用用户身份识别能力的要求。

系统自我管理功能是通过系统配置管理来支持的，主要面向系统控制台、一部分系统内部信息报表查询、部分系统预警功能配置等方面提供管理通道；同时如果需要由其他系统对于本系统的管理功能进行无人值守配置，还可以通过本系统的配置接口管理和配置扩展管理来实现，这也是基于系统配置管理完成的。

- 应用安全网关/安全中间件

应用安全网关和安全中间件主要与第三方应用系统进行无缝集成，实现应用系统数据安全防护。

应用安全网关可以为应用系统提供应用安全准入控制、数据加解密能力，支持旁路部署、串联部署（桥连接），应用安全准入支持标准 TCP/IP 协议，数据加解密支持标准 HTTP 协议、FTP 协议。

安全中间件，可以为应用系统提供加解密能力、流程审批能力，不受协议和网络环境限制，只要应用系统具备二次开发能力，通过调用接口快速完成与第三方应用系统无缝对接。

- 客户端

客户端控制软件是文件加密系统执行系统功能的必备模块组，其主要承担文件加解密的执行，终端应用程序的控制（另存、剪贴板、打印、截屏等等）、终端安全策略的控制（用户签入/签出，用户对应策略获取和执行等等）以及跟踪和预警控制（什么用户在什么时间对什么文件做了什么，哪些属于风险动作需要进行系统预警报告）。

客户端通过网络数据交换管理与策略集中管理服务器进行沟通，完成策略获取、日志上报以及加解密关键信息接换等等功能操作，该操作是以终端“心跳”模式唤醒通讯及数据交换服务的，“心跳”频率是可配置的。

在终端离网状态下，客户端与服务器的沟通失败，将自行转向离网服务支持缓存，保证相关业务功能的执行，当缓存过期系统解密功能将全面失效，离线使用期限可配置且可以通过多种方式实现延时；当终端能够连接到服务器时网络数据交换恢复，离网日志会自行上报。

对于终端上需要进行加密管理的文件，客户端控制软件将主要从两个维度的结合进行管理控制，其一是文件格式，本方案采用的是驱动层加密技术（参见技术基础章节中的加解密技术描述）可以支持任意格式文件的加解密，文件格式约束主要是实现加密和解密动作本身的执行，其二是特定文件格式对应的操作程序进程（例如：*.DOC 由 WinWord 来操作），这主要是为了实现加密文档在容许被解密打开的情况下进行应用控制（诸如：另存、打印、剪贴板等等）。

第四章　核心功能

4.1 透明加密

4.1.1 透明加密

透明加密是一种自动加密技术（强制性），所谓透明是指文档加密、解密过程对使用者来说是无感知的。主要用于解决用户核心数据文档在生产过程中，由于明文存储面临的众多泄密风险，如离职人员拷贝、移动存储设备丢失、网络传输拦截等情况。

用户通过服务器平台下发透明加密策略（关联的应用软件进程及其产生的文件类型）后，客户端根据策略实时监控应用程序对指定类型文件的读写操作（读解密、写加密），实现文档的实时动态加解密，文档加密后，在受控范围（安装客户端的合法用户）内透明使用，脱离受控环境无法使用，从而有效解决用户核心数据文档在生产过程中面临的数据泄密风险。

4.1.2 半透明加密

半透明加密是一种主动加密技术，主要用于解决用户文档非强制性的加密需求，半透明加密作为一种加密策略，可以独立使用，也可以根据客户需求与透明加密策略组合使用，实现不同部门按需进行加密，在保障用户核心数据安全情况下，兼容文档交互效率。

用户通过服务器平台下发半透明加密策略（关联的应用软件进程及其产生的文件类型）后，客户端根据策略实时监控应用程序对指定类型文件的读写操作（读解密、写加密），智能区分加密文档和普通文档，对于加密文档进行全面控制，可以设置是否允许另存、拷贝粘贴、截屏、对象插入、拖拽、网络发送等，对于普通文档（明文）可以随意使用，不受加密控制的影响。

4.1.3 智能加密

智能加密是一种全新的加密技术，它融合了透明加密和内容智能识别技术，用户打开文档时，客户端根据服务器下发的安全策略，对文档内容进行检测，如果检测到敏感文档中包含有机密信息，则会自动加密，整个过程对使用者来说是无感知的。

4.1.4 全盘扫描加解密

全盘扫描加解密是一种批量加密或解密方式，主要用于用户对电脑终端历史资料一次性处理（加密），或者用户更换电脑、终端数据不需加密保护情况对终端数据批量解密。

全盘扫描加解密根据设置的文档类型进行全盘扫描，用户通过服务器下发全盘扫描策略后，客户端根据策略中设置的文档类型，自动完成全盘文档的批量加密或解密。设置策略时支持对文件类型设置通配符，全盘初始化解密支持*或*.*，支持设置例外路径，支持压缩包（压缩包范围：RAR、ZIP、7Z）穿透加解密。

4.1.5 文件访问控制

文件访问控制是一种文档安全增强策略，主要用于防护用户重要数据被恶意删除。

文件访问控制策略可以实现防止非法删除目录、文档及更改文档后缀名，用户通过服务器管理平台设置要保护的文档目录及文档类型，客户端根据策略对指定目录进行保护，从而防止用户核心数据恶意被删除或更改文档后缀名绕过文档加密保护。

4.1.6 内容安全控制

内容安全控制是一种文档内容安全保护策略，主要用于对用户核心数据文档基于内容上安全保护，防止数据使用者在使用文档内容过程中，通过复制、拖拽、另存、插入、连接（网络）、截屏，造成的文件内容泄密风险。

内容安全控制策略包括复制、拖拽、另存、插入、连接（网络）、截屏控制，各项控制支持自定义黑白名单，用户通过管理平台灵活配置内容安全控制策略，客户根据安全策略进行文档内容安全防护，可以实现：

（1） 明文内容可以复制到密文，密文内容无法复制到明文，密文直接复制到密文不受影响。

（2） 密文另存为任何文件类型都加密。

（3） 明文无法插入密文对象。

（4） 应用软件读取加密文档时，禁止网络传输密文文档内容。

（5） 禁止通过 QQ、截屏键等应用软件进行截屏、录屏（显示黑屏）。

4.1.7 打印控制

打印控制是一种文档打印控制策略，主要用于防止用户核心数据文档（加密文档）通过打印方式引发的数据泄密风险。

打印控制策略支持虚拟打印机和物理打印机控制，用户通过服务器管理平台设置打印控制策略，开启后，指定部门或用户则无法打印加密文档，物理打印控制支持自定义黑白名单，可实现可信应用程序可以打印加密文档。支持禁止密文打印，明文文档不受影响，可以在客户端操作明文打印。

4.1.8 打印水印

用于用户打印加密文档时，根据需要添加文档浮水印，主要便于打印文档泄密事件追溯和警示（文档保护用户名、用户姓名、IP 等信息）。

水印显示位置包括文档中央、左上角、左下角、右上角、右下角，打印在文档中央的水印支持按宫格进行显示设置，宫格支持选择：1、4、9，水印内容支持图片或文字信息，文字信息包括计算机名、IP&MAC、打印日期、用户信息，可自定义水印显示位置（全部显示或部分显示）、水印内容、水印深浅度、文字大小。

4.1.9 阅读水印

用于用户打开加密文档使用过程中，根据需要添加文档浮水印，主要便于通过手机拍照引发的泄密事件追溯和警示。

支持屏幕和文档两种水印格式，水印内容包括计算机名、IP&MAC、打印日期、用户名、用户姓名，水印内容和显示位置支持自定义。屏幕水印包含：显水印及盲水印（矢量图）。

（1）屏幕水印

水印显示位置包括文档中央、左上角、左下角、右上角、右下角，水印内容支持图片或文字信息，文字信息包括计算机名、IP&MAC、当前日期、用户名、用户姓名，可自定义水印显示位置（全部显示或部分显示）、水印内容、水印深浅度、文字大小。

显水印以附着于应用窗口的形式进行显示，盲水印以矢量图形形式显示在屏幕上。

支持根据打开文档（明、密文）、业务系统、应用进程设置是否显示阅读显水印或阅读盲水印。

（2）文档水印

文档水印显示在文档中央，水印信息包括公司名称、当前日期、用户名、用户姓名，可自定义水印信息、显示样式（斜式、水平）、字体大小和颜色。

4.1.10 邮件白名单

邮件白名单属于一种文档解密方式，主要用于安装客户端用户与未安装客户端用户之间文件交互，实现用户通过邮件客户端（OUTLOOK、Foxmail）发送加密附件给指定用户自动解密，提供用户文档交互效率。

用户通过服务器管理平台设置白名单邮箱地址，客户端根据下发的邮件白名单策略，自动识别收件人是否是白名单用户，从而实现白名单收件人附件解密后发送，普通用户以密文附件进行发送。

邮件白名单支持目的地址白名单和源地址白名单。

（1）目的地址白名单

用户通过邮件客户端，发送加密附件到指定邮箱地址时，附件自动解密。

（2）源地址白名单

指定用户邮箱地址，通过邮件客户端发送加密附件时，自动解密后再进行发送。

4.1.11 文件备份

文件备份是系统提供的一种容灾保护机制，主要用于一些不可抗因素（如病毒破坏、意外断电、保存死机、人为操作等）情况下可能导致数据出现异常或损坏，保障核心数据文档的完整性。

用户通过管理平台设置文件备份策略（根据文档类型进行备份），客户端根据文件备份策略自动完成对指定类型文档进行备份。

系统支持本地备份和远程备份，远程备份首次完整备份后续增量备份，支持自定义备份周期（天、周月），本地备份采用循环滚动式备份，支持备份预警，硬盘小于指定空间后进行提示。

4.1.12 多密钥隔离

基于密钥的一种权限控制策略，主要用于解决用户不同部门数据隔离管控需求，如：

（1）某一部门数据只允许指定部门查看，其他部门无法查看。

（2）指定部门数据可以相互查看，其他部门无法查看。

通过灵活配置密钥，可实现部门间数据单向隔离、双向隔离，

系统提供智能密钥和主动密钥两种模式。

智能密钥模式情况下，用户打开文档时，客户端根据策略自动识别用户密钥权限，拥有权限用户可以正常使用加密文档，没有权限则无法使用。

主动密钥模式，用户打开文档时，需要根据文档所属部门，自主选择对应密钥，才能正常使用加密文档。

4.1.13 进程签名

用于对系统进程进行合法性校验，系统根据应用进程特征和属性，按照特有算法生成进程的唯一标识，从而防止仿冒进程窃取加密文档内容或非法篡改合法进程逃脱加密保护。

系统支持手动签名和自动签名，用户启用签名后，客户端根据安全策略，对进程合法性进行校验，当合法应用软件启动时，对进程进行合法性校验（完整校验只需一次，后续校验通过缓存进行，保证安全性的情况下兼容效率），实现合法进程可以打开加密文档。

4.2 防勒索软件

采用应用实体可信计算技术，通过对应用软件进程进行合法性检测与识别，实现合法应用软件可以访问指定文件类型，非法应用软件无法访问，从而防止勒索软件、病毒等恶意应用软件对用户文件的恶意破坏。

4.3 权限管理

通过对文档加密授权及角色对应，控制文档在内部受控使用，避免越权使用带来的泄密风险。数据作者可以根据需要设定数据的传播范围（用户、部门、项目组等）和查看权限（只读、打印、修改、阅读次数、阅读时长），也可以根据企业需要建立权限模版，对文档批量授权。

4.4 流转工具

流转工具是 CDG 客户端特有的功能，用户可以使用流转工具批量制作加解密文件，以及更改密文的密钥，支持按文件加解密；支持按目录批量加解密；支持穿透压缩文件进行加解密。同时，为了防止制作时文件意外破坏，流转工具特提供了备份功能，采用异步机制，本地先进行加解密，

将文件备份到本地目录（注意备份路径请勿备份在 C 盘，需备份在当前当前操作文件的根目录。），然后再异步处理上传到服务器进行审计。

流转工具还集成了明文打印入口，当打印控制策略禁止密文打印时，用户可以方便地通过明文打印功能打印明文。

4.5 外发管理

通过对文档加密、授权及封装，控制文档在外部传播和使用时造成的泄密风险。

外发文档支持四种认证方式，分别为 【直接阅览】、【机器绑定】、【密码验证】、【机器绑定+密码验证】：直接阅览指的是用户打开外发文档时，无需身份认证，直接打开使用外发文档；机器绑定指的是外发文档绑定指定用户电脑终端，只允许在指定电脑终端上打开使用外发文档；密码验证指的是用户打开文档时需首先输入密码并通过密码验证后才能正常打开文档。

用户可以根据实际需要精细化设定外发文档使用权限，包括：只读、打印、修改、阅读次数、阅读时长、阅读水印、打印水印等。

制作生成外发文档时，系统会将文档封装成 EOD 文件，只可通过专用 EOD 阅读器才可打开文档，更好地保障文档安全。并且，系统详情地记录了外发文档的操作日志，实现文档外发事后安全审计。

4.6 流程管理

为更安全、高效地管理文档日常使用，系统内置了【文档解密】、【文档还原】、【文档外发】、【文件流转】、【权限申请】、【离线申请】、【邮件解密】等流程。用户可以使用客户端工具或者直接右键点击文档发起申请流程，通过进入我的工作台链接到服务器页面查看申请流程情况，【我的申请】中可以查看已申请的流程表单；【我的待办】中可以查看需要我审批的流程表单信息；【我的已办】中可以查看已经审批过的流程表单。另外，通过邮件控制策略，可以设置邮件白名单实现邮件发送附件自动解密；支持邮件审批设置。

4.7 应用安全网关

通过软硬一体化结合的方式为应用系统提供安全保障，应用安全网关可以为应用体统提供安全准入和数据加解密双重防护，安全准入通过终端身份识别、应用系统仿冒、传输隧道加密、终端访问日志等多方面进行应用数据安全访问控制，数据加密通过对应用系统核心数据进行上传解

密、下载加密，解决企业核心数据离线安全使用。

4.8 安全中间件

安全中间件提供了统一、标准的 API 接口，可以为第三方应用系统提供加解密能力。

应用系统可以调用中间件解密接口解密文件，例如将密文上传至应用系统时自动进行解密处理，方便应用系统合法用户正常使用；应用系统也可以调用中间件的加密接口加密文件，例如用户从应用系统下载文件时自动进行加密处理，防止文件发生泄密，切实保障文件安全；应用系统还可以调用中间件的流程审批接口，获取待审批等表单信息，通过与应用系统之间的联合开发将表单审批结果回传，实现与应用系统的流程审批无缝衔接。

中间件的接口是基于通用标准的 rest 接口，不受协议和网络环境限制，只要应用系统具备二次开发能力，通过调用接口即可快速、高效地完成与第三方应用系统无缝对接。

4.9 智能移动终端

为智能移动设备提供亿赛通专属 APP 安全服务，保证通过移动设备下载到客户端的加密数据可以正常查看，脱离受控范围无法使用。此模块一般与透明加密、应用安全网关或安全中间件等配合使用。

4.10 全文检索

全文检索系统，通过对流程审批（解密流程、外发流程）的文档进行内容解析，建立文档数据索引，日志管理员通过输入文档关键字内容，即可快速查询出包含相关内容的流程及文档，实现文档附件与流程的动态关联与查询。

4.11 恶意软件

将提取的恶意软件特征值导入服务器中，再下发到终端，用于检测终端用户是否运行恶意软件（如：破解软件），检测到非法运行后则以邮件方式向管理员进行告警。恶意软件特征支持更新。

4.12 上传下载加解密服务

基于浏览器访问业务系统，实现本地密文上传业务系统解密、从业务系统下载数据加密。支持 http/https 协议和域名、IP 解析。通过 CDG 客户端应用层实现，解决 NDIS 网络控制策略因为进

程 PID 管控导致浏览器新开页面无法访问的问题，保护业务系统数据安全。

4.13数据展板

为管理用户提供统一的数据安全态势感知平台，支持对资产数量、泄密风险、异常行为等进行统计分析，对风险预警事件实时披露，以柱状图、饼图和趋势图等多种形式展现。包括文件传播大数据、累计保护终端和保护天数、异常预警统计、预警仪表盘、文件外发周排名、特权解密行为统计、违规行为披露、流程审批状态分析等展示模块。

第五章　系统实施与部署

5.1　部署环境

5.1.1 服务器

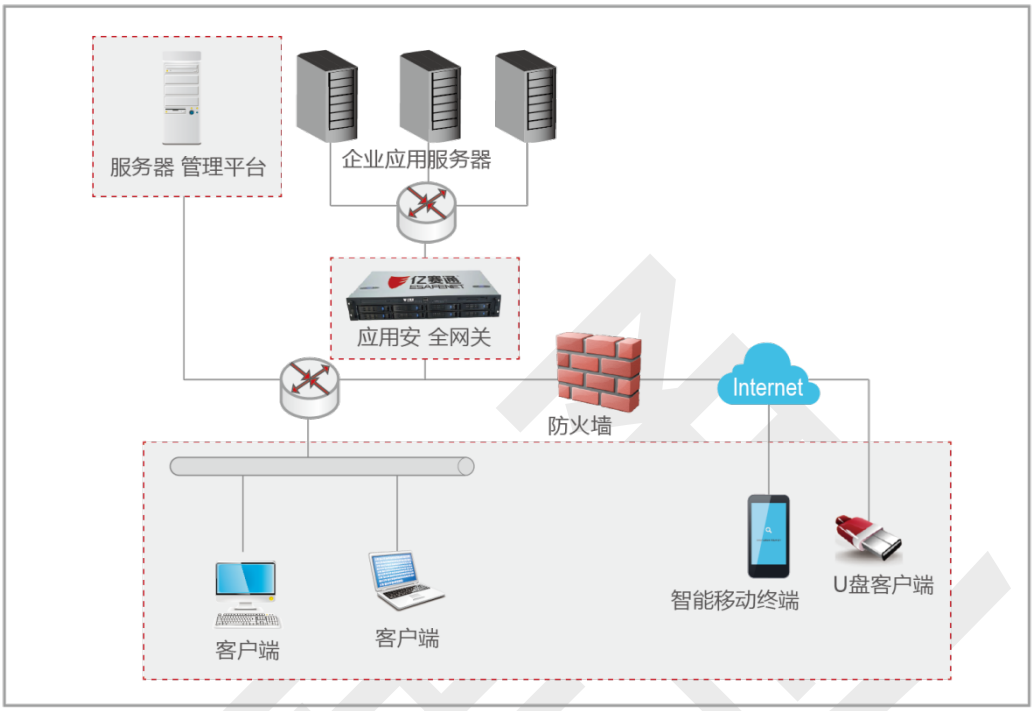
设备名称	配置建议及要求	数量	功能及备注
硬件服务器（建议配置）	CPU:2*Intel 至强四核 E5-2407 内存：4*4G DDR3 ECC 内存 外型：1U/2U 不限	1	用于搭建 CDG 安全管控平台，为避免平台单点故障，建议后期配合第三方热备软件实现冗余备份方案
操作系统	Windows Server2003 SP2　32/64 位、Windows Server2008 SP2 32/64 位 操作系统语言：中文、英文	-	
磁盘存储	存储容量：1*2TB，RAID-5（3/5 年存储规划）	-	用来为 CDG 安全管控平台提供数据存储支撑，包含系统环境存储、数据库存储、文件存储、日志存储等。
数据库服务	Microsoft SQL Server 2008 数据库支持及配套服务	1	用来为 CDG 安全管控平台提供数据库服务支撑，为避免单点故障，建议后期采用双机冗余备份
配套设备	提供 CDG 管控服务器至机房内以太网交换机端口的通信电缆及接头；	-	

	提供管控服务器电源模块至安装机房电源分配设备的电力线引接及机柜电源分配模块的空气开关； 提供所有线缆的标签。		

5.1.2 客户端

设备名称	配置建议及要求
操作系统	客户端部署操作系统支持：Windows XP SP3 32 位、Windows 7 32/64 位、Windows 10 64 位 操作系统语言支持：简体中文、英文
杀毒软件	360 杀毒、360 安全卫士、瑞星杀毒、金山毒霸、趋势杀毒、赛门铁克 SEP、卡巴斯基（部分杀毒软件及最新病毒库版本需确认支持能力）
部署权限要求	非 Administrator 权限（User、PowerUser）安装部署时，需设置当前用户对 drivers 驱动目录、客户端安装目录%\Program Files\ESafeNet\%的读写权限； Windows Vista、Windows 7 需开放 UAC 用户安全权限。 备注：客户端仅支持标准桌面操作系统或虚拟机桌面操作系统部署，不支持 Windows 服务器远程桌面多用户共享和瘦客户机、无盘工作站以及虚拟化桌面发布模式部署。

5.2 部署架构



产品采用 B/S（管理）和 C/S 相结合架构，从实施角度分为服务器管理平台、客户端、应用安全网关/中间件（需二次开发）三大部分：

服务器管理平台：产品集中管理平台，用于系统管理及运维，建议双机热备。

应用安全网关：用于保护应用系统数据。

中间件：以接口方式为应用系统提供加解密能力，需二次开发。

客户端：用于对电脑终端（Windows、Mac、Linux）、智能移动终端（Android、iOS）数据进行安全防护。

5.3 部署步骤概述

1) 服务器配置

- 安装服务器操作系统 WindowsServer2008
- 安装数据库 SQL2008
- 安装文档安全服务端
- 安装 FTP 服务、完成 FTP 服务配置

- 导入亿赛通正式授权文件
- 建立系统组织架构（公司部门及用户信息录入）
- 系统策略制定、策略调试、策略下发

  针对用户级建立策略组

  用户管理角色建立

  解密流程、密文外发流程建立

  透明加解密策略、权限管理策略、外发策略下发

  容灾策略、备份策略下发
- 系统维护设置（数据库及密钥备份）

2）网关基本配置

- 设备上架（机柜位置选取、网关上架、线缆连接、设备加电）
- 通过笔记本电脑直连网关调试
- 登录网关设置通讯口的 IP 地址、子网掩码、默认网关及 DNS 网络信息
- 使用网关的网络工具测试网关和业务服务器的网络连通性
- 网关策略配置 （逻辑拓扑设置、密钥同步、业务系统集成策略设置）

3）CDG 客户端配置

- 登陆客户端本地系统管理员
- 安装客户端软件
- 用户登陆亿赛通软件
- 加解密策略应用
- 文档授权、解密、密文外发流程应用
- 电子文档备份、离线容灾应用

第六章　核心技术

6.1　文件级智能动态加解密技术

是一种文件级过滤驱动编程技术，其发展历经三个阶段：单缓存过滤驱动技术、双缓存过滤驱动技术和虚拟文件系统技术（LayerFSD）。目前商业市场上大多数内核级加密厂商均采用单缓存过滤驱动技术，少量厂商已发展到双缓存过滤驱动技术，而发展到虚拟文件系统技术（LayerFSD）并实现产品化的厂商则屈指可数，亿赛通公司早在 2009 年就实现 LayerFSD 技术。

亿赛通电子文档安全管理系统采用文件过滤驱动技术，通过实时拦截文件系统的读/写请求，对文件进行动态跟踪和透明加/解密处理。其主要优点：文件加/解密动态、透明，不改变使用者的操作习惯；性能影响小，系统运行效率高；不改变原始文件的格式和状态，同时，部署和内部使用非常方便。

显著特征为：加密强制性、使用透明性、保密彻底性、应用无关性、灵活拓展性。

该技术原理实现如下图所示：

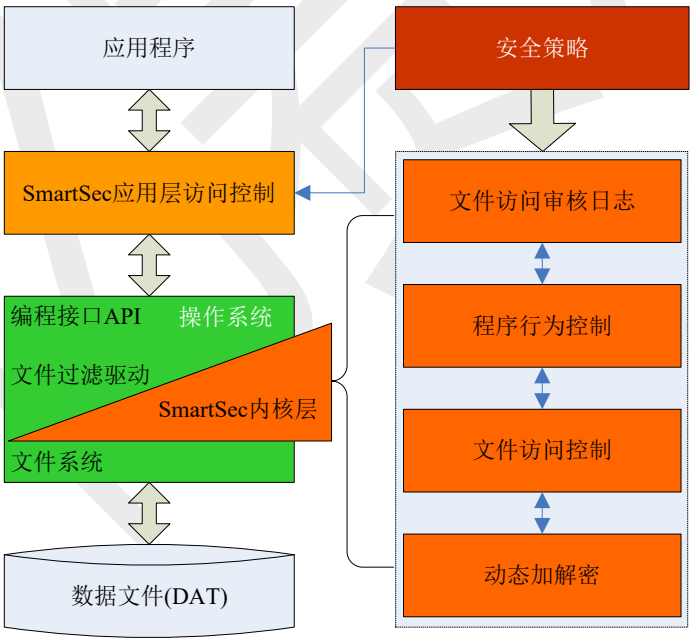


图 3　文件级智能动态加解密技术实现

6.2　网络级智能动态加解密技术

是一种网络过滤驱动编程技术，俗称 NDIS 和 TDI 技术，可实现对网络传输协议及网络应用

协议数据的过滤和控制。亿赛通公司于 2009 年成功研发并完善该技术，产品化为应用安全网关 FNS9000、应用安全准入网关 APS-SAG60/80。目前该类技术主要应用于防火墙、VPN、网络准接入等相关领域，亿赛通公司率先应用于数据安全领域并成功推广。

该技术原理实现如下图所示：

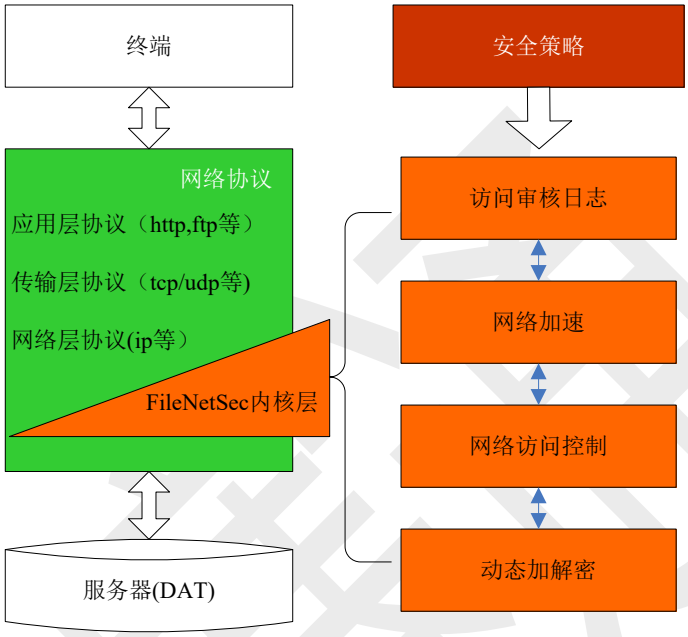


图 4　网络级智能动态加解密技术实现

6.3 文件虚拟磁盘技术

是一种基于映像文件的虚拟磁盘技术，是使用一个映像文件来模拟物理磁盘存储数据，可以通过加载虚拟盘操作，把映像文件虚拟成一个本地磁盘分区，像正常的物理分区一样进行读写操作。卸载虚拟磁盘之后，该虚拟磁盘分区消失，唯一留下的就是映像文件。虚拟盘消失之后，系统无法访问其中的文件，也不能对虚拟盘内存储的文件进行任何操作，因此可以达到保护数据安全的目的。文档外发管理 EOD 模块，其技术实现如下图所示：

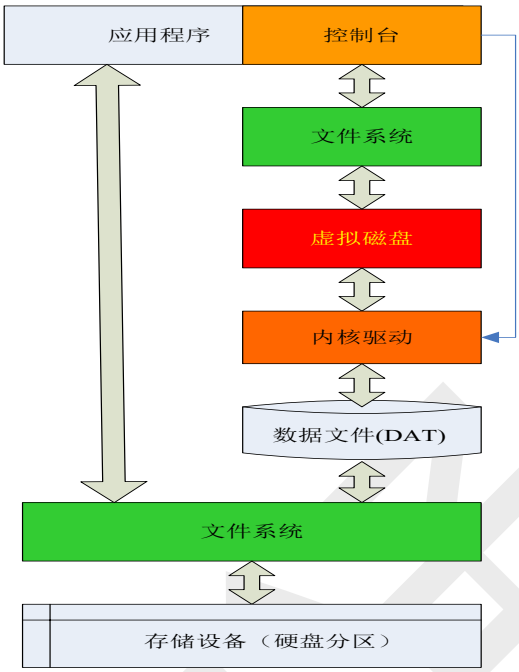


图 6 文件虚拟磁盘技术实现

6.4 设备过滤驱动技术

端口管控是一种设备过滤驱动编程技术，可实现对终端任意设备(USB 端口、打印机、光驱、软驱、红外、蓝牙以及网卡等)的安全保护及控制。

6.5 其他核心技术

(1) 是一种数字版权保护方法和系统 专利号：201110070536.7

(2) 是一种手机程序防破解方法及系统 专利号：201110076337.7

(3) 是一种 SAN 存储加密系统及系统 专利号：201110092437.9

第七章　产品优势

（1） 安全性好

- 有效防护进程查杀，文件信息及注册表删除，确保客户端文档运行。
- 采用进程签名、内存防护等多种数据安全防护手段，防止数据非法破解，安全模式仍可正常运行

（2） 效率高

基于操作系统内核级加密技术，文档加密过程不产生临时明文文件，不增加 I/O 负担，性能损耗低，支持超大型数据应用。

（3） 跨平台支持

支持 Windows、Linux、Android、IOS 多系统平台，任意平台加密文档可透明使用。

（4） 部署方式

服务器支持云部署（如：阿里云）。

服务器支持分级部署。

第八章　公司资质



软件企业认定证书



软件产品登记证书



商用密码产品型号证书



商用密码产品销售许可证



商用密码生产定点单位证书



公安部销售许可证



计算机著作权登记证书



北京市自主创新产品证书



高新技术企业证书



质量管理体系认证证书



军用信息安全产品认证证书



涉密信息系统产品检测证书

第九章　技术支持

9.1 售后服务

对于软件版本升级及性能增强，亿赛通公司将对软件改进的性能予以详细说明，升级方式可以采用下载/自行安装、远程指导安装或现场指导安装进行。功能发生重大变化的版本升级，除予以详细说明外，在必要的时候亿赛通公司还将采取现场指导升级的方式为客户服务，并提供系统的培训服务，以保证用户应用系统的正常运行。具体服务内容如下：

（1）主要设备（见附件清单）提供一年原厂的免费维保服务（含主要设备的易损件的免费更换、定期巡检、现场故障排查维修等），需提供原厂维保服务证明材料；

（2）对项目各个系统提供一年的免费维保服务（含易损件的免费更换、定期巡检、现场故障排查维修等）；

（3）7*8 小时热线电话、传真技术支持（提供热线电话号码）；

（4）7*8 小时网络支持服务。电子邮件、即时通讯工具等。

（5）7*8 小时现场支持服务（提供紧急联系人及联系方式）；

（6）2 小时内响应用户提出问题；

（7）如远程无法解决故障，则故障发生后 48 小时内到达用户现场解决问题；

（8）如 5 小时内无法解决故障，则故障发生后 8 小时内提供同档次及以上备机备件服务支持；

（9）免费维护期内提供短期内的驻现场技术人员及时解决问题；

（10）其他个性化售后服务。

9.2 产品问题处理方式及机制

提供全方位、周到的售后服务，对所服务的问题级别、服务方式和所执行的服务流程、售后人员管理制度都有着明晰的说明。

9.2.1 问题级别

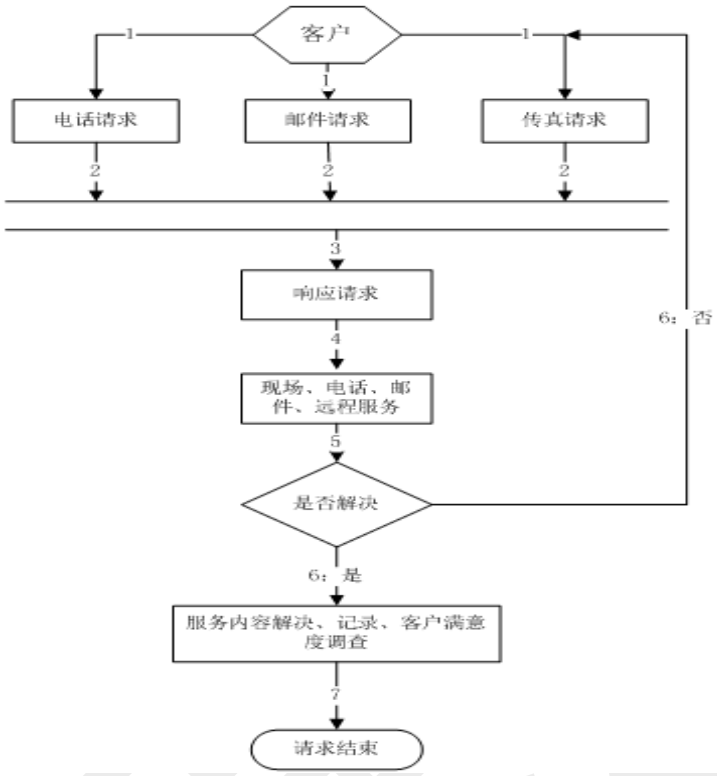
问题级别	问题描述	响应时间

一级	关键设备故障、服务宕机、重大设计缺陷和不可预测的紧急性兼容问题等，对最终用户的业务运作有严重影响或直接导致业务中断的。	1小时内
二级	系统及设备性能或稳定性问题，对最终用户的业务运作有重要影响或直接导致部分非关 键业务中断的。	2小时内
三级	系统兼容性或功能性缺陷问题，对大部分用户日常工作的开展存在一定影响，但不影响关键业务的执行。	8小时内
四级	其他问题，对小部分用户的使用习惯、体验或日常工作存在一定影响，但用户可暂时采取规避措施的。	24小时内
五级	用户体验建议、需求沟通、咨询答疑、产品培训及产品细节问题修正要求等。	48小时内

9.2.2 服务方式

服务方式	服务内容
常驻服务	有偿服务。公司与客户签订服务协议，派遣资深技术工程师常驻客户现场，为客户提供系统升级、技术处理、问题咨询和日常运维等协助。
现场服务	有偿服务。公司与客户签订服务协议，为客户提供短期现场服务，如设备维护、问题处理、功能升级及系统培训等。
远程服务	为客户提供电话咨询、网络协助、传真、远程调试等服务。
开发服务	有偿服务。公司与客户签订服务协议，为用户提供个性化产品开发服务。

9.2.3 服务流程



售后服务流程示意图

9.2.4 售后人员管理制度

为加强本公司的售后管理，更好的配合公司市场人员达成销售目标，提升客户服务质量，对售后人员管理制定了相关制度，具体如下：

- 考勤管理制度
- 工作职责明确制度
- 工作移交管理制度
- 工作计划管理制度
- 工作报表及工作总结管理制度
- 客户管理制度
- 出差规定制度