

EsafenET 北京亿赛通科技发展有限责任公司
BEIJING E-SAFENET SCIENCE&TECHNOLOGY CO.,LTD.

亿赛通文档安全管理系统
CDG3.0

技术白皮书

二〇〇九年四月

版本历史

版本	日期	备注
1.0	2009 年 4 月 1 日	第 1 版《亿赛通文档安全管理系统 DLP-CDG3.0 技术白皮书》

Copyright © 2009 ESAFENET Corporation BeiJing P. R. China

ESAFENET CONFIDENTIAL: This document contains proprietary information of ESAFENET Corporation and is not to be disclosed or used except in accordance with applicable agreements.

Due to update and improvement of ESAFENET products and technologies , information of the document is subjected to change without notice.

目 录

1. 研发背景	4
2. 设计理念	5
3. 核心优势	7
4. 产品概述	8
5. 产品靓点	19
6. 运行环境	20

亿赛通版权

1. 研发背景

随着计算机和网络技术的飞速发展,越来越多的信息以电子形式存储在个人和商用电脑中,并且通过网络进行广泛地传递,在大量的信息存储和交换中,信息的安全问题越来越引起人们的重视。

企业一般有着完善的书面文档涉密管理制度,并且由单独的文控中心负责制订、监督、审计企业内部重要情报信息使用状况,亦达到了很好的效果。而电子文档却都以明文方式存储在计算机硬盘中,电子格式存储的重要情报信息却由于传播的便利性和快捷性,对分发出去的文档无法控制,极大的增加了管理的复杂程度,这部分的资产极易于受到损害,那就是明文泄密!

按照对电子信息的使用密级程度和传播方式的不同,我们将信息泄密的途径简单归纳为如下几方面:

➤ 由电磁波辐射泄漏泄密(传导辐射、设备辐射等)

这类泄密风险主要是针对国家机要机构、重要科研机构或其他保密级别非常高的企、事业单位或政府、军工、科研场所等,由于这类机构具备有非常严密的硬保密措施,只需要通过健全的管理制度和物理屏蔽手段就可以实现有效的信息保护。

➤ 网络化造成的泄密(网络拦截、黑客攻击、病毒木马等)

网络化造成的泄密成为了目前企业重点关注的问题,常用的防护手段为严格的管理制度加访问控制技术,特殊的环境中采用网络信息加密技术来实现对信息的保护。访问控制技术能一定程度的控制信息的使用和传播范围,但是,当控制的安全性和业务的高效性发生冲突时,信息明文存放的安全隐患就会暴露出来,泄密在所难免。

➤ 存储介质泄密(维修、报废、丢失等)

便携机器、存储介质的丢失、报废、维修、遭窃等常见的事件,同样会给企业带来极大的损失,在监管力量无法到达的场合,泄密无法避免。

➤ 内部工作人员泄密(违反规章制度泄密、无意识泄密、故意泄密等)

目前由于内部人员行为所导致的泄密事故占总泄密事故的70%以上,内部人员的主动泄密是目前各企业普遍关注的问题,通过管理制度规范、访问控制约束

再加上一定的审计手段威慑等防护措施,能很大程度的降低内部泄密风险,但是,对于终端由个人灵活掌控的今天,这种防护手段依然存在很大的缺陷,终端信息一旦脱离企业内部环境,泄密依然存在。

➤ 传统防御手段的不足

对于核心电子信息的防护,传统方法为完善的管理制度和人性感化,同时也采用终端防御类技术配合,如:防水墙、终端安全平台、审计平台、行为管理等,这类技术和方法的主要缺陷在于无法防止内部员工的有意识、主动泄密!如重新安装操作系统、从盘引导、破坏防御平台运行环境等带来的泄密隐患。

信息的安全保护,必须从源头做起,即信息加密;只有对信息进行加密,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。

2. 设计理念

核心信息的加密保护,已经成为企业信息资产保护的一个必要手段。为了配合企业人性化管理的特点,亿赛通公司贯彻先进的设计理念,结合丰富的实施经验,并吸收广大客户建议,设计出符合企业安全现状和发展需要的数据防泄露解决方案-亿赛通文档安全管理系统 V3.0(简称 CDGV3.0)。

2.1. 事前主动防御

企业对于信息资产的保护,传统保护模式均为被动式防御:出现泄密事件后才引起信息资产的保护重视,紧急调整管理制度并采用硬屏蔽手段来约束泄密再次发生,无法快速锁定泄密对象和途径来降低泄密损失。亿赛通 CDGV3.0 将打破传统的保护思路,采用对企业信息资产主动设防的理念,一旦设定保护策略,将对核心信息进行全生命周期强制加密保护,有效规避员工由于有意识或无意识导致的信息泄密,让企业变被动为主动;同时,提供用户主动的细粒化权限设置保护,防止核心信息在内部共享、流转、使用时所带来的数据扩散泄密。

2.2. 事中灵活控制

亿赛通 CDGV3.0 拥有强大的策略设定平台和密钥定制平台，能够根据企业各种复杂应用和业务需求定制出个性化的管理策略，并通过管理策略的调整来灵活设定各个终端及用户的保护范围和保护模式，并可动态调整保护对象的安全密级，如企业分公司与分公司间、部门与部门间、部门内部不同分组间、项目组与项目组间以及部门与临时项目组间、人员与人员之间等。可以根据各种不同的业务需求来设定和调整对应安全策略，在保证安全的同时又能支持灵活的业务应用，给企业带来前所未有的安全收益。

2.3. 事后追踪审计

亿赛通 CDGV3.0 提供了强大的日志审计平台，能够为企业提供丰富的日志报表查询，同时根据需要可设定日志存活周期，也可支持无期限记录系统日志；系统管控范围内终端及用户的所有操作日志，均被详细记录，同时根据审计需要可输出各种类型报表。亿赛通 CDGV3.0 结合企业多维审计的需求，在国内率先推出图文并茂的审计功能，在传统报表审计的基础上，融入统计报表功能，通过直观统计图来为企业提供详细的日志审查信息。

2.4. 集中管理

亿赛通 CDGV3.0 采用权限集中化管理、信息可分布存储的特点，为企业提供了强大的集中管控平台。可集成化的身份认证平台、强大的终端管控能力、科学的管控策略、灵活的审批流程等特点，为企业提供高质量的规范管理、高性能的安全管控和低开销的运营成本。

2.5. 管控分级

亿赛通 CDGV3.0 采用权限分离、管控分级的信息安全管理理念，将系统管理维护和日志审计权限有机分离，避免由于管理人员权限过大而导致的泄密隐患；同时为了缓解大中型企业系统管理人员工作压力和强度，亿赛通 CDGV3.0 提供了管控权限分级下放功能，通过各种分级管理权限来分担系统管理职责，同时也可根据企业需要来自设置管理权限组合，方便企业规范管理。

2.6. 人性化应用

亿赛通 CDGV3.0 在面向终端用户时，采用了透明、无感知特性，任意受控

用户基本感觉不到安全系统的存在。不改变用户原有工作习惯、不增加用户工作负担、不限制用户的操作行为，在保证用户原有业务模式的情况下，不影响用户的工作效率，让用户在安全的环境中无感知的处理各种涉密业务。人性化的平台支持让用户舒心、称心。

2.7. 流程化协同

为了保障企业原有的工作效率和业务流程，亿赛通 CDGV3.0 提供了功能强大、操作简单、设计合理的流程化协同 workflow，如在线审批流程、离线审批流程、卸载审批流程、邮件自动化申请发送流程、权限变更审批流程等，结合冒泡提醒、在线短消息、短信通知、邮件通告等特性功能，为企业自动化协同办公提供了保障，也极大的方便了终端用户的使用，更促进了企业的规范化管理。

3. 核心优势

3.1. 完全自主知识产权

亿赛通拥有软件产品著作权，并是国内第一套完全基于 BS7799 信息安全管理标准的内网信息安全管理产品。

3.2. 世界领先技术

亿赛通公司的核心技术“智能动态加解密”，应用于操作系统文件过滤驱动层，是由亿赛通自主研发并在国内外首先提出的文档安全管理理念，该技术安全、高效、稳定、升级维护简单，具有很强的兼容性和延展性，不管应用层为何种文件格式，只需策略设定，即可对所有格式文件进行加密。

3.3. 最有效系统集成

对不同行业特点及技术平台，凭借亿赛通 CDGV3.0 本身具备的兼容性，有效地与不同行业不同客户的系统进行集成，推出了不同行业的文档加密行业解决方案。目前已经广泛应用于政府、军队、电信、制造业、研究院及教育机构。

4. 产品概述

4.1. 产品架构

亿赛通 CDGV3.0 系统由服务器端和客户端两大部分组成，同时支持 C/S 和 B/S 两种组织结构，如图 1 所示：

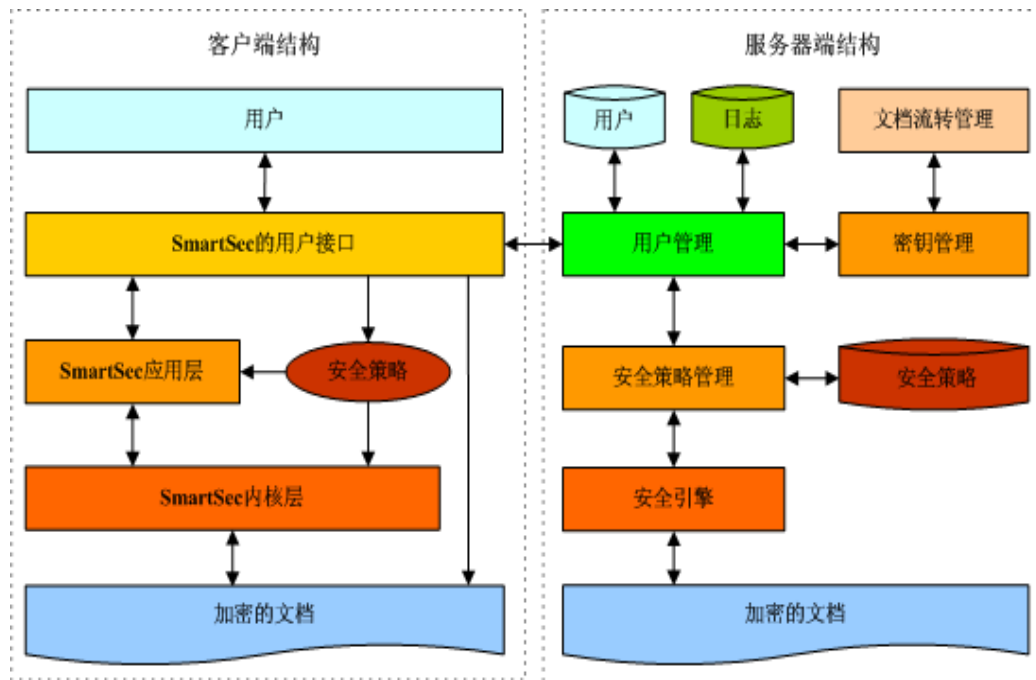


图 1 CDGV3.0 文档安全系统的架构

服务端主要由用户管理、密钥管理、文档流转管理、安全引擎等组成。其中用户管理主要负责用户身份的验证，权限的分配和管理等；文档流转管理的主要功能是负责文档在单位内部不同部门之间的流转和单位内部与外部之间的流转工作，在保证文档不影响用户交流的情况下，为文档提供安全保障。如控制文档的浏览次数、使用时间，拥有的权限等。密钥管理用于实现不同部门之间的密钥分配和交换等功能；安全策略管理用于设置和管理系统的安全策略以及为每个用户分配相应的安全策略等；安全引擎主要为服务器系统提供安全保障，如验证安全系统模块的运行权限和条件等，并提供对服务器端存储的文档进行加密/解密等多种安全相关的功能。

图 2 给出了亿赛通 CDGV3.0 客户端的实现原理，从中可以看出，CDG 的动态加解密是以文件过滤驱动程序的方式进行实现的，同时在应用层和内核层均提

供访问控制功能，除此之外，还提供了日志和程序行为控制等功能，这种通过应用层和内核层相互配合的实现方式，不仅能提供更高的安全性，而且有助于降低安全系统对系统性能的影响。

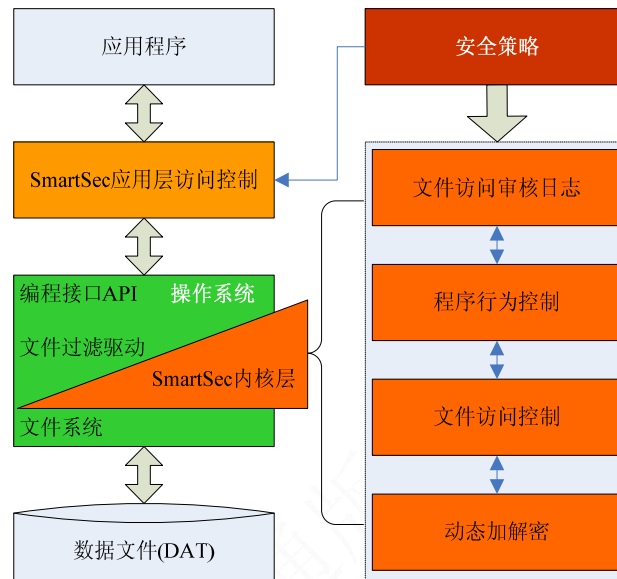


图 2 亿赛通 CDGV3.0 动态加解密的实现

4.2. 连接支持

亿赛通 CDGV3.0 系统服务器端与客户端间采用 IP 可达的连接原则，可以适用于各种网络环境，在确保不改变企业内部网络构造的基础上，满足企业的不同的连接需求。亿赛通 CDGV3.0 能够在包括域结构、内部专线、VPN、拨号连接、Internet、VLAN 以及各种内部隔离网络间进行部署和正常连接，如图 3 所示：

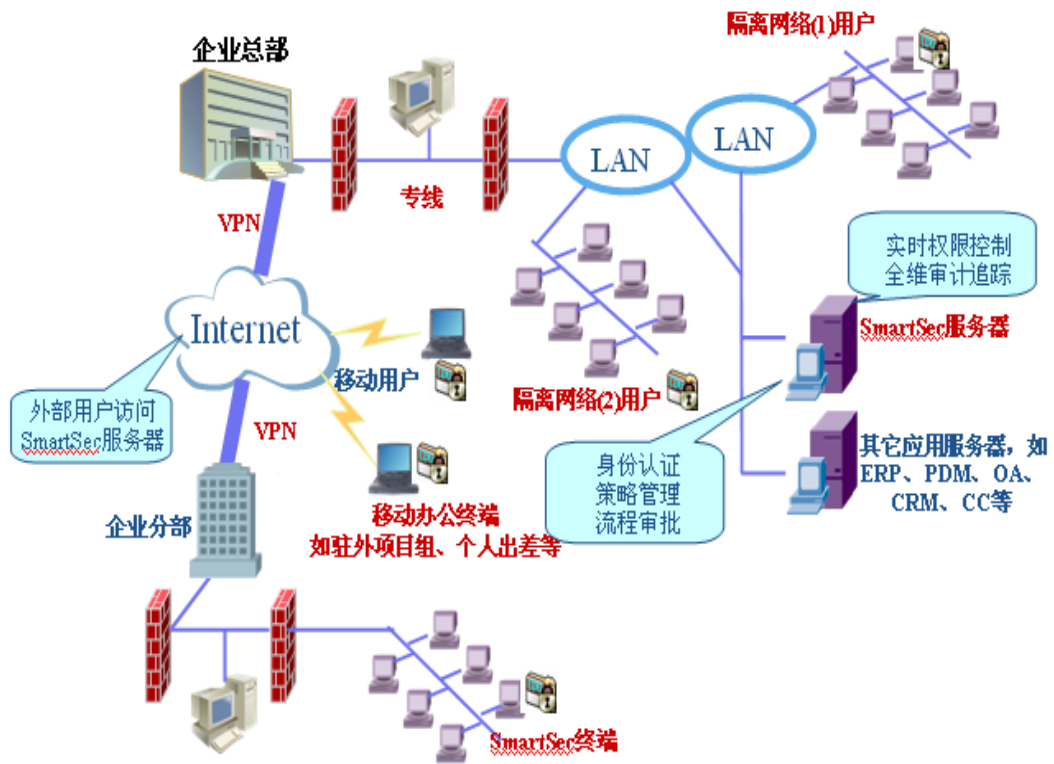


图 3 亿赛通 CDGV3.0 网络连接支持

4.3. 功能详情

CDGV3.0 服务器端			
功能模块	功能说明	备注	
组织人员管理	用户认证	支持本地认证机制	支持企业自主创建用户及组织结构、支持批量录入用户及组织结构
		支持统一认证机制	支持与 AD、ED、CA 等统一身份认证平台无缝集成，并支持基于 Ldap 标准协议的其他第三方认证平台集成
		帐户生命周期管控	可以设置用户的生命周期，可设定正式用户(无期限限制)、临时用户(启用周期限制)等属性
		帐户安全等级设定	可以设定帐户的密级等级(A 级、B 级、C 级、D 级或企业自定义密级)，对账号进行不同级别的安全保护，并提供冻结、密码重置等管理功能
		统一初始化密码	系统支持对所有用户设置统一初始化密码，用户在使用加密系统时，必须强制修改初始化密码，

			防止账号盗用或设置简单口令所带来的泄密隐患
		树型视图显示	可以按照企业实际组织结构动态树型视图显示，管理和维护更简单
		自动同步机制	可以自动定期同步统一身份管理平台的组织结构信息，无需管理人员参与，保障信息的安全运行
		实时状态显示	可以实时显示用户连接状态，如在线、异常离线、正常离线、卸载等状态
	群管理	创建群组	创建群组，并可以设置为“公开”（所有人可见）或“私有”（仅自己可见）属性，并且可以将用户添加到相应的群组中
	角色管理	定义角色的具体权限	自定义某种角色的相应权限，并且可以将某种角色赋予用户
	用户管理	用户管控	可以创建、修改、查询、删除组织架构；添加删除用户，对用户添加删除安全策略，对账户进行冻结和启用，对每个安全组进行添加删除策略，对用户进行密码的重置初始化，显示用户的状态是否在线，给指定用户授予相应的角色，使之享有相应的权限等。
	用户高级	功能权限设置	设置用户是否拥有使用外发工具，是否允许使用流转工具，是否允许使用加密工具，是否允许使用解密工具，是否允许制作 CDG 文档，是否允许管理公共文档的权限
	流转控制	给具体到单个用户授予流转控制的权限。	
	加密控制	给具体到单个用户授予加密文件的权限，批量删除具有加密文件的用户的加密权限（流转工具中的手动加密）。	
	解密控制	给具体到单个用户授予解密文件的权限，批量删除具有解密文件的用户的解密权限（流转工具中的手动加密）。	

	外发控制	给具体到单个用户授予外发文件的权限，批量删除具有外发文件的用户的外发权限（客户端中的外发工具）。	
角色管理	模块化的角色功能	系统所有管理功能均由独立模块组成，每一个独立模块均可完成特定的功能，用户可以根据所分配的管理模块的不同定制出不同权限的角色	
	基于角色的管理权限	用户具备的访问及管理权限，均通过该用户所具备的角色来体现，可以通过变更用户的角色或调整角色所具备的管理模块来灵活控制用户权限	
文档管理	私人文档	个人文件夹	用户可以管理个人文件夹，包括新建目录、上传文件、单个或批量 CDG 安全文档制作、删除和下载文件。
		CDG 审批箱	可以审批（只有该文档作者，或拥有该文档再授权权限的用户才可以审批）用户对 CDG 文件权限的变更申请，并且可以察看审批的记录。
		CDG 收件箱	CDG 收件箱可以接收所有当前用户拥有使用权限的 CDG 安全文档。
		CDG 发件箱	CDG 发件箱会保存所有当前用户制作的 CDG 文档的记录，并且可以对这些文档进行详细的设置：1. “再授权” 对该文档进行权限的再次设定 2. 可以下载该文档 3. “生命周期” 规定该文档的使用起止时间 3. “权限缓存” 当用户离线时，可以设置该文档的离线使用时长、次数
	公共文档	被授权用户可以访问和管理公共文档，包括创建目录以及上传文件，以及对已上传文件的下载和删除操作。	
	CDG 管控	可以管控系统内用户对于文档的使用权限，详细功能操作：1.可以进入用户的发件箱，可以进行“归档”(将该文件的所有权限信息清空)、“冻结”(暂时将该文件的所有权限信息清空)、“解冻”(恢复该文件解冻前的权限信息)“下载”等操作 2.可以进入用户的发件箱，并可以管控	

		该用户是否可以访问收件箱内文件 3.“权限转移” 该作者制作的所有 CDG 文件的权限将被收回，并取消作者权限，同时可再以某种权限赋予可见密级人员。 4.“生成离线权限文件” 为用户脱机浏览 CDG 文件的一种功能设置，并且可以设置脱机时长。
终端管理	终端信息管理	可以对终端进行维护和管理,如自动卸载、删除、自动升级、补丁分发等
	部署方式	可手动安装、下载安装、域推送。
流程审批	自动解密审批流程	解密审批管理人员可以在线对待审批申请进行处理,系统将自动反馈相应处理结果，并对通过审批的信息自动完成解密，无需手动参与
	离线脱机审批流程	离线审批管理人员可以在线对待审批申请进行处理，系统将自动反馈相应处理结果，并对通过审批的用户自动完成离线设定，无需手动参与
	自动卸载审批流程	卸载审批管理人员可以在线对待审批申请进行处理，系统将自动反馈相应处理结果，并对通过审批的终端自动完成卸载，无需手动参与
	邮件自动化审批解密流程	终端用户提交邮件解密申请单，根据系统设置的审批流程，管理员审批通过后将自动集成企业邮件服务器进行自动明文发送，无需手动参与
	审批分级功能	可以根据企业的需要，设置分级审批功能，实现指定人员审批指定部门或组织需求
	审批员设置	对用户设置可否审批解密，可否审批卸载，可否审批非接触性解密的权限，可否审批子组，以及审批员的终端通知功能。
策略管理	智能动态加解密策略管理	系统提供强大的策略定制平台，并提供可复用策略库。多达 10 多种策略类型可以组合出企业各种复杂的应用需求，而不限应用格式的特性为企业的发展提供了安全保障
	打印策略管理	可以设置打印黑白名单，同时支持定制化水印，

		用户可以自主设置水印内容、背景颜色深浅度，同时也支持用户自定义上传图片水印等
	脱机策略管理	可以设置脱机时长，并提供补时机制，方便用户出差并在超出预定期限后通过补时策略来支持出差使用
	终端安全强度管理策略	可以对终端的保护强度进行设置，并可以实时调整终端的保护强度，如是否控制拷屏、打印、复制粘贴等，并支持设置特定签名白名单来满足特殊业务需要
	磁盘初始化策略	可以对终端磁盘历史资料进行自动初始化处理，通过策略的下放，对不同密级的历史资料进行安全转换，同时也支持对磁盘数据进行自动解密还原
	文件自动备份策略	为了保证核心数据的安全存储，可以对核心信息提供自动备份功能，科学的滚动备份机制，在不占用过多存储空间的同时，规避由于病毒破坏、误删除、终端故障等带来的数据丢失、损坏的风险
	邮件白名单自动解密策略	为了提高用户工作效率，保证资料外发的安全，安全系统提供了灵活、安全的邮件白名单自动解密功能，通过设定邮件白名单，实现邮件发送自动解密
日志管理	日志报表在线审计功能	提供内容丰富的日志审计平台，用户可以自定义审计组合条件对系统行为进行审计
	日志报表自动导出功能	支持审计报表导出功能，并提供多种导出格式
	日志图形化在线审计功能	提供日志统计图报表审计功能
	日志图形化打印功能	支持日志统计图报表打印功能

	能	
	服务器日志	记录服务器端的“用户类日志”“客户端类日志” “审批类日志”“系统类日志”“策略类日志”
	客户端日志	记录客户端上的针对文件的操作记录,可以根据 “用户 ID”“文件名称”等查询条件来查询具体的 CDG 权限文件的操作日志
系统消息	实时冒泡提醒业务	系统实时对审批管理员进行审批业务冒泡提醒, 同时实时对审批申请用户冒泡通告审批结果
	系统在线短消息业务	所有审批提醒和通告均会通过服务器短消息进 行滚动显示
	短信通知业务	可以结合短信平台,对审批管理员进行审批业务 短信通知,同时实时对审批申请用户短信通告审 批结果
	邮件通知业务	可以结合企业内部邮件系统,对审批管理员进行 审批业务邮件通知,同时实时对审批申请用户邮 件通告审批结果
密钥管理	高强度密钥设置机制	支持用户自定义 512 字节以内高强度密钥
	多密钥支持机制	系统支持多密钥,不同的部门、不同的策略可以 采用不同的密钥管控
	安全的密钥备份及 导入导出机制	支持对密钥硬件 USB-KEY 备份和还原
	安全的密钥合并技 术	根据企业要求,提供密钥合并技术,通过自动合 并不同管理人员设定的密钥段来强化企业密钥
系统管理	数字签名技术	采用安全的程序数字签名技术,可以有效防止用 户通过程序欺骗泄密
	补丁管理	提供补丁管理功能,对不同部门或用户进行定制 化补丁服务,方便企业进行系统管理
细化文档权限设置	权限控制	支持对需加密文档或代码包提供细化权限加

		密控制，如：只读、打印、修改、复制、二次授权等权限控制
	打印水印	支持对授权文档设置打印浮水印，水印内容管理员可以自主设置，根据用户需求，还可定制实现阅读文档浮水印
	权限认证	用户在使用任意授权加密文档时，系统将根据当前用户提交的用户信息(用户名/密码)并结合待使用文档的唯一 ID 号，实时与服务器进行权限认证，并回馈权限信息，系统将根据真实权限信息打开授权文档或给出无权操作提示
	在线使用	标准情况下所有授权文档必须在联机情况下在线使用，根据业务需要，用户可以办理离线申请后，实现授权文档的离网安全使用
	内容安全	用户无法将授权文档内容通过复制粘贴、拖拽、截屏等手段移植到其他非授权文档中；用户无法将授权文档通过另存为、输出、发送等手段再版为其他非授权文档
	阅读控制	不具备阅读权限时，用户无法打开权限文档
	打印控制	不具备打印权限时，用户无法将授权文档打印成纸质或虚拟打印为其他电子文档；具备打印权限的用户，无论是打印成纸质文档还是虚拟打印为电子文档，根据策略设置，均可以加载浮水印
	修改控制	不具备修改权限时，用户无法修改保存授权文档
	复制控制	具备复制权限的用户，可以将授权文档内容复制、拖拽到其他授权文档中，保证原始授权文档安全前提下，方便用户对于历史资源的复用
	时效控制	管理员可设置任意用户对授权文档的使用时效，如阅读时限、阅读次数等
	版本管理	具备修改权限的用户，修改授权文档后，均可以

		将最新文档版本上传服务器端存储,系统支持对授权文档的多版本管理,根据需要用户可以下载和使用同一个文档的不同版本
	离线安全	用户办理离线申请后,可实现授权文档的离网安全使用;根据用户安全需要,可以结合离线USB-KEY双认证方式实现离网文档安全;离线控制时,将采用独立计时器进行控制,与用户系统时间无关,防止用户通过修改系统时间所带来的安全隐患
	离线补时	管理员可以根据业务需要,对离线授权文档发布离线补时策略,离线用户通过导入补时策略来实现安全续期
权限管控	权限归档	文档管理员可以将任意用户的权限文档进行权限归档,将文档权限回收服务器控制
	权限冻结	文档管理员可以将任意用户的权限文档进行权限冻结
	权限删除	文档管理员可以将任意用户的权限文档进行权限删除
	权限转移	文档管理员可以将任意用户的权限文档进行权限转移,方便用户离职或其他情况下工作延续
	文档还原	文档管理员可以设置将指定文档进行明文还原
	权限恢复	文档管理员可以将普通用户删除的权限文档进行权限恢复
CDGV3.0 客户端		
安全防护	智能动态加解密技术	采用驱动级智能动态加解密技术,具备有强制、透明、无感知等特点
	另存为控制技术	根据安全策略,对被保护文档*.另存为强制加密保护,防止泄密
	打印控制技术	根据安全策略,对被保护文档进行打印控制及水

		印装填
	拷屏控制技术	根据安全策略,对被保护文件实行禁止拷屏控制
	剪切板控制技术	根据安全策略,对被保护文档内容的复制粘贴进行安全控制,禁止将保护内容粘贴至其他非受控文档或粘贴为乱码
	剪切板加密技术	为了进一步对剪切板内容进行保护,采用了剪切板加密技术,防止用户暴力破解剪切板泄密
	宏安全控制技术	根据安全策略,对被保护文档进行宏安全控制,在保证支持宏功能的同时,防止用户通过宏泄密
	拖拽控制技术	根据安全策略,对被保护文档内容的拖拽进行安全控制,禁止将保护内容拖拽至其他非受控文档或拖拽为乱码
流程申请	解密申请	用户可以对指定文件、文件夹、目录发起自动解密申请,审批通过后将自动完成解密,并实时通告用户审批结果
	脱机申请	用户可以发起出差脱机申请,审批通过后系统将自动完成允许脱机策略设置,并实时通告用户审批结果
	卸载申请	用户可以发起终端卸载申请,审批通过后系统将自动完成终端卸载,并实时通告用户审批结果
	冒泡提醒	对于所有审批反馈和在线短消息通信,终端均提供在线冒泡提醒业务,让用户体验办公自动化
	权限申请	用户可以发起权限变更申请,作者审批通过后系统将自动完成最新权限设置
用户安全	用户登陆	提供强制登陆和自动登陆功能,对终端信息进行强制保护
	用户注销	用户注销可以保障在无用户登陆下,终端存储信息的安全
	修改密码	支持 C/S、B/S 方式修改用户密码

5. 产品观点

5.1. 动态图标显示功能

亿赛通 CDGV3.0 可以根据企业需求，对加密文档进行动态图标区分显示，在原有图标的基础上，动态显示企业特有的 Logo 信息，既能够让用户清晰区分文档保密状态，同时也可以打造企业个性化数据防泄露平台。

5.2. 数据完整性保护功能

亿赛通 CDGV3.0 核心技术为数据加密，任何受控数据一旦加密，原则上会改变该数据的原有结构，即使在前端对用户完全透明；数据内部结构一旦发生改变，就会带来数据使用的安全性问题，即数据完整性保障。数据完整性风险主要有：病毒破坏、意外断电、保存死机、人为破坏等。为了能保障受控信息的存储和使用安全，安全终端提供了数据自动备份机制，用户在使用任意受控文档时，文档安全管理系统将自动备份当前操作文档，该备份信息可滚动存储在本地，也可根据设定自动备份存储到指定服务器中。当由于不可抗拒因素导致数据出现异常时，CDGV3.0 安全终端可立即给用户提供备份数据恢复，为企业提供零风险的数据防泄露平台。

5.3. 策略自主定制化功能

亿赛通 CDGV3.0 采用通用化设计路线，其技术特点为不过多依赖上层应用，也就是说和上层应用无关，这样的技术理念为企业后续的安全新需求和新应用打开了方便之门，企业应用的升级和拓展基本无需改动 CDG 的任何环节，只需要在服务器上自主设置一组或多组安全策略，就可以实现企业全部应用需要；同时 CDG 的灵活策略组合技术和简单明了的操作步骤，为企业的安全个性需求提供了有力保障。

5.4. 自动化流程审批功能

亿赛通 CDGV3.0 提供了灵活的流程审批功能，在满足企业安全需求的同时，为用户提供办公自动化环境，让企业在数据安全保护和人性化建设上出现双赢。

5.5. 邮件白名单自动解密功能

亿赛通 CDGV3.0 为企业提供了邮件白名单自动解密功能，即提高了用户工作效率，同时也规避了由于误发送、非法抄送等途径所带来的邮件泄密风险。

5.6. 信息化系统紧密集成功能

亿赛通 CDGV3.0 可以与企业内部信息化信息无缝集成，如 PDM、OA、ERP、CRM，实现服务器明文存储、终端密文下载的无缝集成，而亿赛通 CDGV3.0 独有的访问控制技术，可以有效规避企业信息化系统由于账号复用、盗用所带来的泄密隐患，提供安全的系统准入和准出控制。

6. 运行环境

安装 CDGV3.0 Client 计算机的基本要求：

- 操作系统:WINDOWS 2000/XP/2003/VISTA及SERVER
- 最低配置:Pentium /Cleron/128MB 内存/10G 可用硬盘空间
- 建议配置:Pentium III 500/256MB 内存/20GMB 以上

安装 CDGV3.0 Server 计算机的基本要求：

- 操作系统:WINDOWS 2000/XP/2003/VISTA及SERVER/LINUX
- 最低配置:Pentium 4 500/256MB 内存/10GB 可用硬盘空间
- 建议配置:Pentium 4 3.0/1000MB 内存/50GB 以上

注：建议服务器端和数据库装在同一个机器上，确保最高运行效率。

根据客户端数量规模建议服务器端计算机配置：

客户端规模	服务器建议配置
50 台以下	1G 内存, CPU 2.0, 中高档 PC
50-100 台	1G 内存, CPU 2.0 以上, 高档 PC
100-200 台	1G 内存, CPU 3.0 以上, 高档 PC
200-500 台	2G 内存, CPU 3.0 以上, PC 服务器
500-1000 台	4G 内存, 双 CPU, CPU 3.0 以上, PC 服务器
1000 台以上	4G 内存, 双 CPU, CPU 3.0 以上, 高档 PC 服务器

注:

- 1、 以上仅为参考值，具体应用会有相应调整。
- 2、 对要求 7x24 小时系统运行要求，可采用双机热备方式部署服务器。

亿赛通版权