天融信文档安全管理系统TDSM-DSM

www.topsec.com.cn

产品概述

天融信文档安全管理系统（以下简称TDSM-DSM产品）以文档透明加解密技术为核心，通过技术平台与管理体系有效结合，实现对客户核心资产的全方位保护。通过网络安全边界的建立，降低核心信息资产如源代码、技术文档、设计图纸、财务数据、经营分析以及其他任意信息资产的有意或无意泄密风险。

产品支持对电子文档进行细粒度的权限控制如：只读、打印、修改的权限控制，同时也为客户提供了灵活的协同管理功能，比如可以允许用户是否在授权等功能，结合文档的使用次数、使用时间、文档生命周期、打印自定义水印等控制功能，可满足客户细粒度的权限控制需求。同时采用安全的密文控制技术，对授权敏感文档进行安全保护，防止客户通过复制、另存为、拖拽等方式泄密。

产品特点

高效稳定的透明加解密技术

使用微软推荐的透明加解密驱动及时，技术成熟有很高的稳定性及兼容性。同时系统可支持国产加密算法。

系统自身安全性高

系统采用“驱动级终端保护技术”，防止用户或恶意程序破坏终端运维服务和配置环境。客户端的卸载举报阉割的认证机制，防止通过非法手段强制移除或终止客户端，当客户端被轻质终止运行时，加密驱动讲自动转入安全保护模式，系统进入只加密、不解密的安全保护状态，有效确保所有加密文档的存储和使用安全。

适用范围广

系统默认已经支持近百种应用的加解密支持，如设计类的Prc/E、UC、CATIA、AutoCAD、SolidWorks等，办公类Office系列等，编程类VC.VB系列等可以产生文件的程序，并且可以与业务系统进行完美的集成，如果需要快速添加新的应用支持加解密，无需修改程序代码即可完成。

支持多级分布式环境

系统支持服务器的多级分布部署，对拥有多个分公司且分布在不同区域的大型企业而言，该功能可充分满足其使用需求，服务器分布后，所有子服务器的用户列表，用户权限，系统操作日志等均可与主服务器保持同步。

客户价值

防止非结构化数据泄密

为了应对当前非结构化数据面临的外部窃取和内部窃取的双重威胁，通过文档透明加解密技术后，可保障文档不管是在用户无意还是恶意泄密的情况下，数据的安全可控，可保证文档在安全范围内可根据权限使用，脱离安全范围的文档将是加密状态，任何未授权单位和个人均无法直接查询。

防止对文档的越权使用

系统通过细粒度的权限控制功能，可以根据用户、部门、密级、角色等多种角度进行文档权限细粒度分配、可控制文档在传输过程中感动阅读、编辑、打印、二次授权等权限、从而可以防止无权限人员对文档的查询、窃取和篡改。

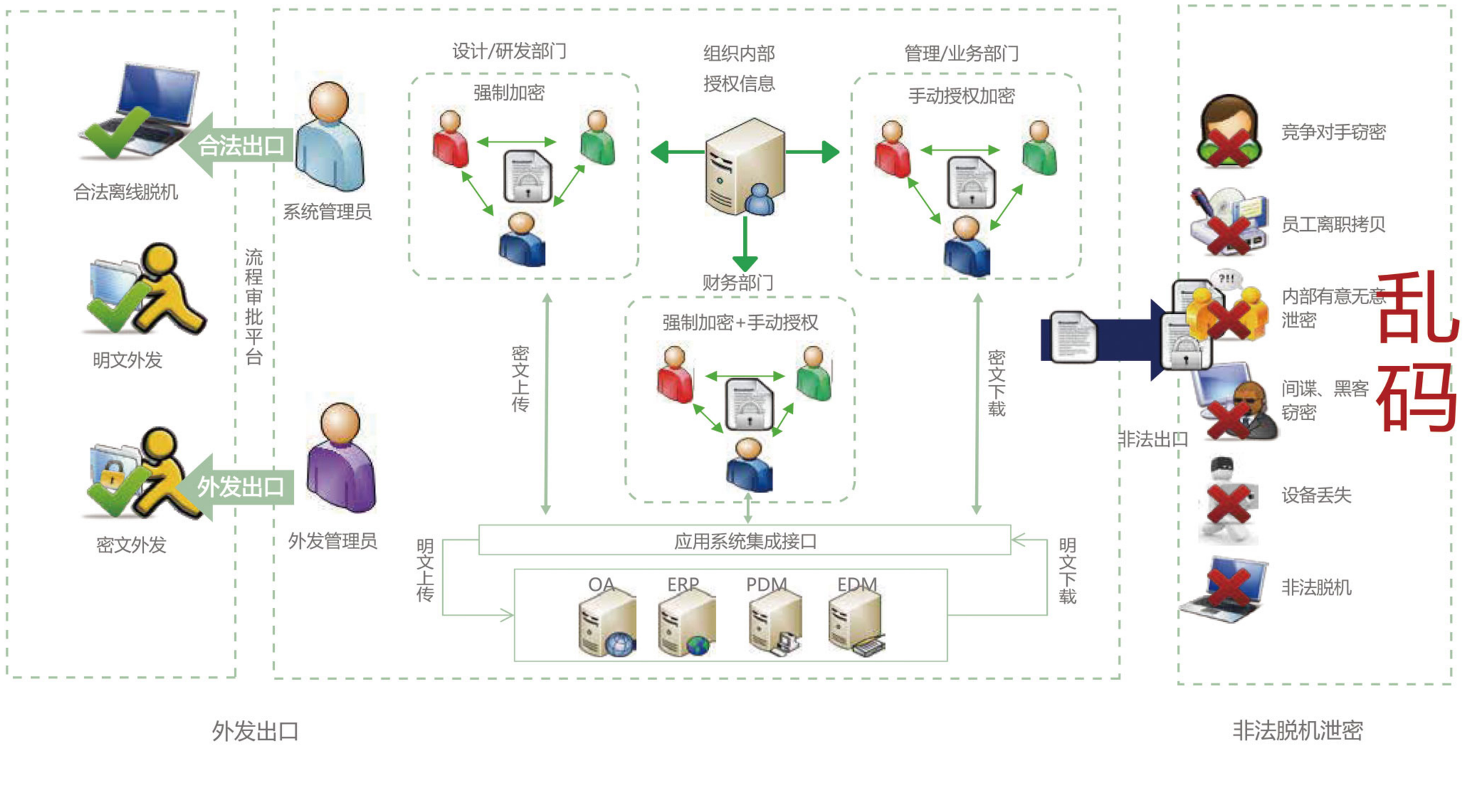
文档外带安全可控

通过系统对文档加密，可防止企业文档在员工出差，外部交流过程中可能存在的泄密风险，并且系统通过离线策略以及文档外发策略，即可控制文档泄密风险，又不影响员工正常工作。

文档操作详细审计

对文档的阅读、编辑、删除、打印、外发、授权等动作，系统具备详细日志审计功能，详细记录操作人、时间等信息，满足客户对文档操作的事后审计要求。

示意图


文档安全管理-解决方案
设计/研发部门
组织内部
授权信息
管理/业务部门
强制加密
手动授权加密
合法出口
合法离线脱机
系统管理员
流程审批平台
明文外发
财务部门
强制加密+手动授权
密文上传
密文下载
外发出口
密文外发
外发管理员
明文上传
应用系统集成接口
明文下载
OA
ERP
PDM
EDM
竞争对手窃密
员工离职拷贝
内部有意无意泄密
间谍、黑客窃密
设备丢失
非法脱机
非法出口
乱码
外发出口
非法脱机泄密