

# 密文卫士 —— 基于内容的电子文档防泄密系统

上海谷巨软件有限公司

2007-7-14

**摘要:** 在保护企业电子文档时, 用户经常需要根据内容来决定一个文档是否需要保密。但是现有的某些防泄密软件产品只能通过文件的后缀来设定要保护的文件, 这会导致加密了大量不该加密的文件和一些事先没有设定为加密类型的文件不能加密。密文卫士采用全新的涉密态概念, 允许用户自己随时决定要保密的文件。

**关键词:** 电子文档防泄密 文件后缀 文件内容 涉密态 密文卫士

## 1 基于后缀加密存在的问题

现有的某些防泄密软件产品是根据文件的后缀来设定要保密的电子文档, 通常称之为“透明的强制动态加解密系统”。这种类型的产品能满足一些特定的行业客户的保密需求。

但是, 随着电脑应用的普及和应用软件的层出不穷, 导致文件类型越来越多, 各种应用软件交叉阅读编辑各种文件类型也越来越普遍。在一个企业内部, 任何一个应用程序, 只要它在使用, 就有可能生产出一个需要加密的文件。这样, 最终的结果是几乎所有后缀的文件都需要加密, 即防泄密软件的加密策略需要不停地增长。而且对于每一种软件, 都要仔细检查是否存在泄密的功能, 逐个设置策略。

因此, 软件厂商采用文件后缀方式加密的防泄密软件产品面临的服务压力和技术挑战太大了。对用户而言, 也需要时刻清楚地了解该产品目前使用的策略, 否则会给他们的工作带来许多不便。

这些都不是问题的本质, 最根本的问题是: 文件是否重要, 是否需要保密不是由文件的后缀决定的, 是由它的内容来决定的。

## 2 基于内容加密的需求

用户事实上已经意识到防泄密软件应该具有这种由内容决定的选择性加密功能。在一些公开的个人论坛上, 可以看到下述案例:

“某企业在选择电子文档防泄密产品的时候, 会提出这样的要求: 对于同一种类型的文档, 如 doc 文档, 我希望能由我们来选择哪些文档是需要加密的, 哪些文档是不需要加密的。这样不会给员工带来使用上的麻烦。”

看看我们的一些软件厂商的业务人员是如何分析这个需求的:

“这个需求看似合理, 但其实这个需求和企业文档防泄密的初衷是相违背的。如果允许用户选择性加密, 那么可能导致文档原作者的泄密, 因为只要公司内部保留了一份明文状态机密文档, 谁能保证这份明文的文档不会传播开去。”

看来, 他应该就是这样向用户进行了误导和技术讹诈, 将自己产品没有实现的功能向客户貌似负责地辩解该功能会导致泄密。

事实上, 企业用户的这个需求不仅仅是看似合理, 实际上也是很迫切、很实际的需求。

从我个人在涉密单位的工作经历来看, 企业的确是根据涉密的内容, 而不是文档的类型来进行保密的。如企业在实施涉密单位的涉密项目时, 会要求所有和该项目相关的资料都保密, 从需求、合同、设计, 一直到最后的测试和验收, 各个环节的所有电子文档和纸质文档都要保密。

如果要这样根据项目来保密，那么我们在事先是很难确定这个项目到底会产生哪些文件类型，会需要哪些软件。如果使用基于文件后缀的防泄密软件，基本上无法实现根据项目或者说内容来选择性加密的需求。

### 3 涉密态概述

为解决基于内容的选择性加密而又不会导致文档作者泄密的难题，谷亘软件创新地提出了电脑的涉密态概念。

为理解涉密态概念，可以设想为处理涉密和非涉密操作，企业需要组建两个电脑网络，一个是非涉密网络，一个是涉密网络。两个网络的关系是涉密网络可以访问非涉密网络读取文件，但是不能向非涉密网络传输文件，非涉密网络不能访问涉密网络。非涉密网络内的电脑可以任意使用，而涉密网络里的电脑限制了不能上 Internet，不能发送文件，不能使用 U 盘等等。

为创建这样的两个网络，企业需要花费大量的成本，而且单纯从网络设备上也难以完全实现这个需求。

谷亘软件为解决这个难题，创新地提出了电脑的涉密态概念，即一个电脑即可以工作在普通的状态，也可以工作在涉密态。这样，在原来的电脑网络上，通过软件的方式构建一个涉密网络。

为实现这个概念，谷亘软件研发了密文卫士软件。密文卫士软件能够在我们通常的电脑网络上搭建出一个安全的、隔离的涉密网络，既满足我们的涉密工作需要又满足非涉密操作需要。

### 4 基于内容加密功能的实现

密文卫士软件是一个电子文档防泄密系统。所谓防泄密就是保护企业的涉密电子文档，限制涉密电子文档只能在企业内部使用，不让它们流传到企业的外部。形象地说，就是为每一个涉密电子文档拴上一个铁链，锁在企业内部的一个铁柱上。它自己跑不了，别人也偷不去。

因此，密文卫士软件也可以说是企业的涉密电子文档的一个安全防护边界。

有了这个安全防护边界，基于内容的加密问题迎刃而解。把需要保密的文件放在边界内，不需要的保密的放在边界外。而任何人，如果想要访问边界内的涉密文件，只有进入边界内，即进入涉密态后才能访问，所有边界内的涉密文件“只进不出”。

这样，一个涉密项目开始时，将需求等初始文档放在边界内保护起来，其后所有参与该项目的人使用密文卫士进入涉密态后开始工作，产生的新文件自动保存在边界内。当开始非涉密项目工作时，退出密文卫士就可以了。退出密文卫士后，边界内的文件都被加密保护，无法查阅。

### 5 结束语

密文卫士通过为电脑增加涉密态功能，使得一台电脑既能处理普通操作，又能处理涉密操作。通过为电脑增加一个涉密态，密文卫士软件完美地解决了基于内容的选择性加密问题。在涉密态内创建、编辑电子文档时，产生的电子文档自动受到保护，在非涉密态不能访问到涉密态内保存的文件。

用户在日常工作中，如果要访问涉密电子文档，只能进入涉密态工作。如果要把一个非涉密的文档保存为涉密文档，进入涉密态后复制该文档就可以了。

当然，对于企业而言，最需要保护的是企业员工集体创作的智慧结晶，即在协作环境下，共同编辑制作的电子文档。密文卫士提供了点对点的通讯工具，支持在涉密态的文件安全交换。

使用密文卫士软件，能将涉密电子文档牢牢锁在企业内部，无论威胁来自内部还是外部，都能够保护它们，避免它们流失到外部。