MarkAny

White Paper

Document Safer Version 1.6

1. 版权管理系统 (DRM)

最近,许多企业、事务所、学校、金融机构、高科技尖端技术研究所等机关都在利用知识管理系统(KMS; Knowledge Management System)或电子文件管理系统(EDMS; Electronic Document Management System)来管理内部文档及信息的共享，从而提高业务效率。

但是电子文档类信息一般都是以非定性的格式保存在数据库中，用户大多不是为了提高业务效率而进行信息共享，而是公然地进行非法的发布，这是实际存在的不可回避的实情。知识管理系统共享的信息资料中有一般的可共享文件，也有研究所及主要部门需要对内外保密文件资料，这些资料可能因为内部人员的失误或为某种目的而有意泄漏，则给企业或机关带来的打击和损失很大。

MarkAny(株)公司的企业信息安全管理系统(以下称 Document Safer)是保护知识管理系统或电子文档管理系统(以下称知识管理系统)的资源文件的；利用美国国家标准技术院认证的密码运算法则，在用户进行下载时根据使用权限政策(Access Control Logic)对用户查阅、保存、复制及打印信息进行限制。从而防止用户之间非法复制、对外发布及光盘拷贝等，达到对信息泄漏及使用进行控制的目的。

防止了IT企业的源程序代码等尖端技术文件、事业计划书、图像数据、财务报表、战略企划书、研究论文等技术资料通过软盘、光盘、电子邮件等形式非法泄漏给竞争企业或机关的行为。

MarkAny开发的企业信息安全管理系统是以版权管理(Digital Rights Management)技术为基础设计开发的。

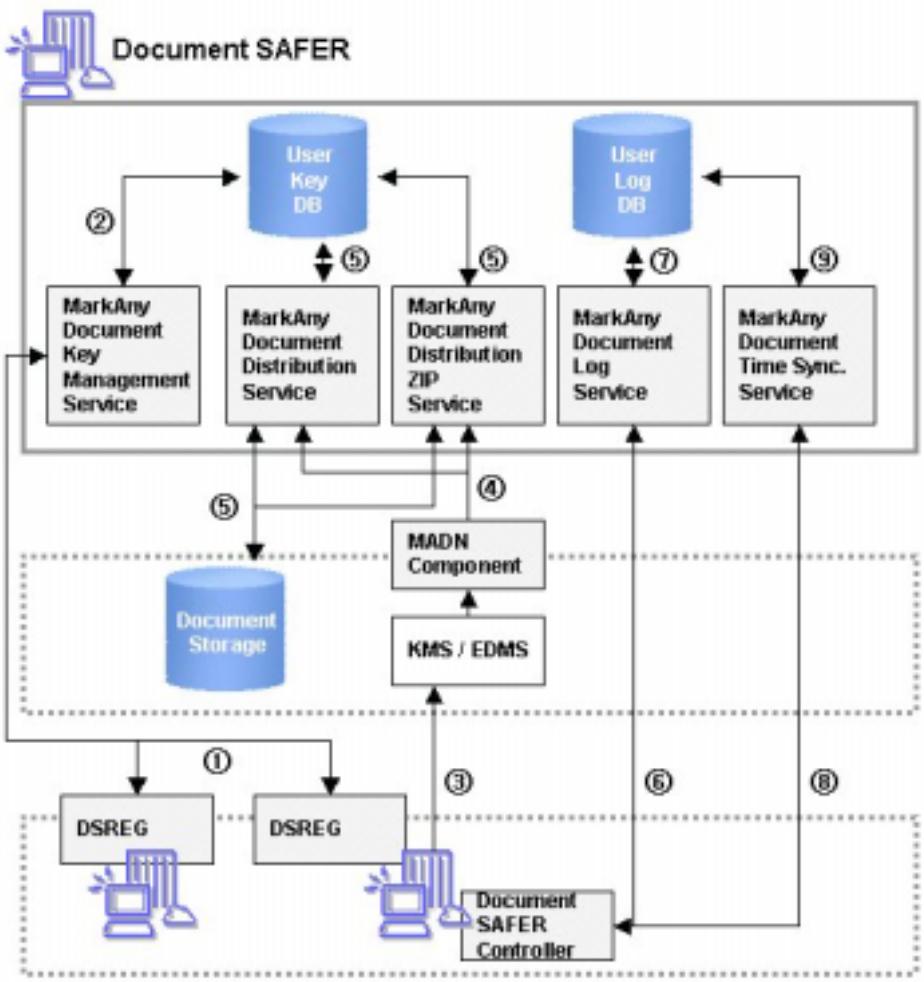
版权管理系统(Digital Right Management,以下简称DRM)是因特网上提供多媒体文件的内容服务商CP(Contents Provider)与利用多媒体服务的客户(Client)之间保证安全传送各种文件,并且防止非法流通的系统管理技术. DRM系统中最重要的是加密技术,加密时利用客户的密码或客户电脑固有的各种序列代码当作加密密匙来加密,所以即使是文件非法传送给第三者也无法解密.除此之外,版权管理系统还需要文件使用协议,如付款/结帐协议等配合.

2. Document Safer

Document Safe是Markany公司为防止企业信息的泄漏，利用自己独自研究出的技术来开发的防止企业信息泄漏方案。

2.1 Document Safer 系统拓扑图

[图 1]是Document Safer系统拓扑图。用版权管理系统防止KMS，EDMS上保存着的内部机密文件的泄露.



[图 1] Document SAFER Architecture

① 用户利用DSREG模块向MADKMS传送用户Key信息。此模块为了也能在Web上使用，由ActiveX CAB文件形式构成

② 传送的用户Key信息与用户的ID等固定信息一同保存于数据库中。

③ 用户可以利用Web浏览器或客户/服务器(Client/Server)结构的终端客户程序来选择或要求需要下载的文件。

④ 在知识管理系统(或文档管理系统)上，对该文件的信息和用户信息、文件的使用权限进行设置后，通过MADN模块与Document SAFER进行通信。

⑤ 该服务利用权限、物理文件、用户Key信息，生成只能在文件访问者的电脑上浏览及使用的密码化的文件，并将此处理结果传送到知识管理系统。

⑥ 知识管理系统分析从Document Safer接收的结果值，并判断为经过正常处理的文件后，向提出要求的用户传送该文件.

⑦ Document Safer Controller根据用户文件使用权限执行复制、输出及保存时，将该源文件保存于用户的数据库中，并传送于MADLS。

⑧ 传送的登录信息记录于登录数据库中.

⑨ 如果用户为了防止文件使用时间结束造成的使用限制而故意改变时间或因失误而改变了系统时间时，利用MADTSS可自动执行时间同步操作。此时，系统必须处于在线状态下。

2.2 Document Safer的主要技术

Document Safer提供防止企业机密泄漏方案应具备的核心功能(如，加密技术，键码管理技术，用户级别权限设置及控制技术)之外，还根据客户的安全性及方便性需求开发其他所需功能.

提供多种加密算法及安全管理用户键码的功能

Document Safer 系统已装有 NIST 公认的加密算法(AES).还可以替换使用国际标准化机构认可的 DES、3-DES、BLOWFISH、IDEA、 CRYPTON 等其他加密算法。可以选择性适用多种加密算法(如韩国政府承认的 SEED 算法，其他国家承认的特定 XXX 加密算法)。

一般的 DRM 系统中用户的键码通常保存于系统特定的文件夹中，例如用户键码记录在登记处(Registry)，在这种结构上用户可以拷贝或变更自己的键码；Document Safer 的方式与其不同，它把引出用户键码的模块内插到 Document Safer Controller 里，用户登录时键码一次性传送给服务器管理，故用户不能拷贝或变更自己的键码，也不能传给第三者。

安全解密文件

Document Safer 是以微软公司的 DCOM 模型为基础设计的。它位于应用程序与操作系统之间，用中途拦截(Interception)技术来控制使用权限。

Document Safer不是采用加密文件解密成特定临时文件(Temp)后再用应用程序打开的模式，所以不需要中间临时文件的生成及解密过程；Document Safer可以直接使用应用程序打开适用安全措施的文件，故在用户端上保存着的文件始终保持着加密状态。

打印文件的追查功能(Watermarking(Fingerprinting))

数字水印技术是以电子内容(Contents)的版权保护为目的研究开发的技术，是一种在电子内容里嵌入版权信息的技术。如果某一电子内容有版权纠纷时，可以用此技术确认电子内容的所有权。数字水印技术可分为两种，一种是可视水印(Visible Watermarking)另一种是不可视水印(Invisible Watermarking)。

数字水印技术的应用范围很广，根据要嵌入的信息可区别为两种；若嵌入的信息是电子内容的制作者信息则称为数字水印，若嵌入的信息是用户相关的信息则称为fingerprinting（”指纹”识别）技术。打印文件时用”指纹”识别技

术把用户的信息嵌入在打印文件的某一部分中，若有泄漏机密，则用它可以追查泄漏机密的当事者．最简单的方式是打印文件的下端用可视水印技术嵌入打印时间及打印者的一些信息，这种方式能让用户提高警惕，但是用户用一些手段删除可视信息的可能性比较高，所以也提供用不可视水印技术隐藏信息的功能(打印者用肉眼不能识别隐藏信息与否)．

适用TRS(Tamper Resistance Software) 技术

对软件最近常出现一些非法攻击，如通过软件的逆分析方法攻击解密文件、变更使用权限或迂回攻击、解密密钥以及个人密钥的攻击、许可证(license)及相关软件的拷贝攻击等等．

Document Safer防止认证键码(KEY)及解密密钥的泄漏，而且在限制权限的程序代码中使用控制流(Control flow)和数据流(Data flow)的混合迷惑(obfuscation)、代码加密术(Code Encryption) 、安全键码隐藏技术(Security key hiding)等TRS技术。所以Document Safer是任何逆分析程序(反向破解可执行程序的方式)技术也不易破解的安全的解决方案．