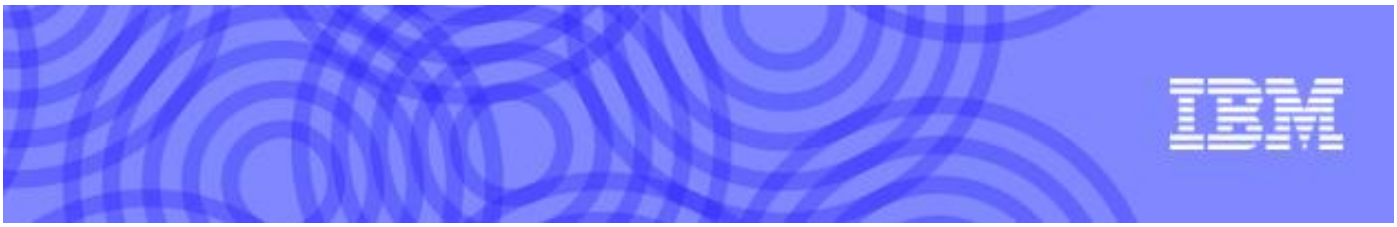
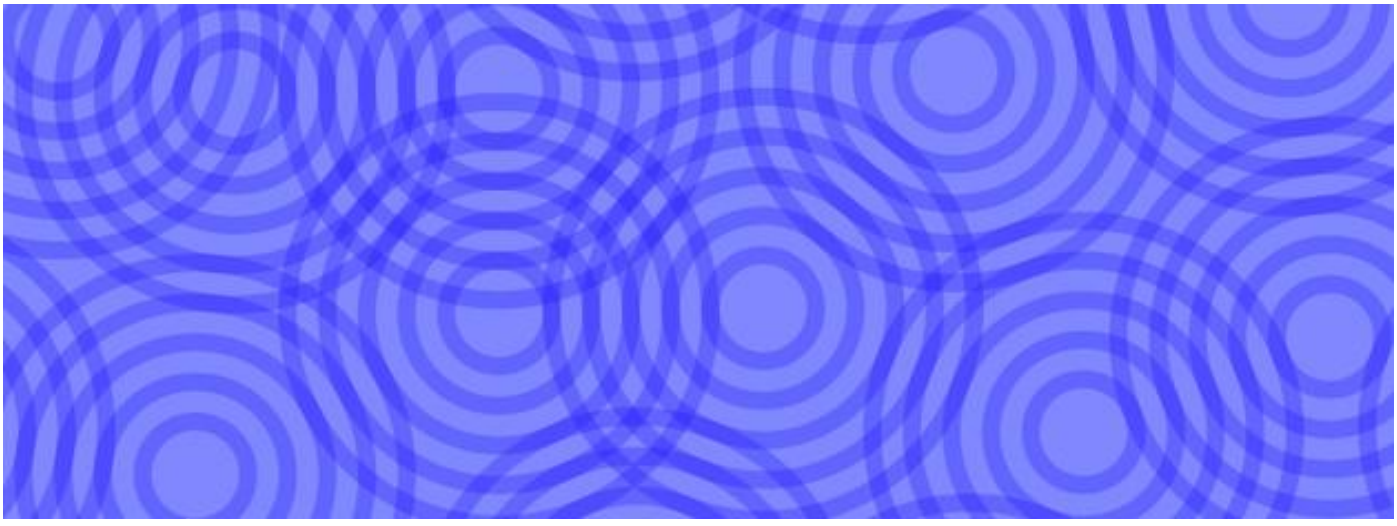


IBM —Joinhand SecurDoc

企业文档保护系统方案建议书



Proposal Insert 文档说明

版本号	方案撰写	方案提供与确认	联系方式	完成日期	计划更新日期	名称
1.0	XuKeJin – GCG PCoE	Zhang Min	Min SH Zhang/China/IBM@IBMCN	2011-5-25	2012-5-25	IBM —JoinHand SecurDoc 企业文档保护系统方案建议书

描述：通过各种途径对自有的知识产权进行严密保护是企业维护自身利益的必然选择。这些需要保护的文档包括：软件设计文档和源代码；设计图纸或资料；产品成分或配方及其他重要的内部资料或机密文档。JoinHand SecurDoc 企业文档保护系统方案是一个基于 IBM Lotus Domino/Notes 和 Windows 2003 Server 的系统集成方案，并将基于 IBM Lotus 的文档管理系统成功的向前推进到企业文档中心、知识中心和文控中心！帮助企业快速建立企业文档中心；对受控文件和敏感文件进行防护；提升 IT 对企业智力资产的保护能力。

目 录

第1章　综述

1.1　我们对您的目标的理解

当前许多大型企业的分支机构、研发机构分散在世界各地，因工作需要而涉及高等级机密文档的人员及环节众多，给知识产权的保护带来了管理上的困难。在以往的商业机密案例中，由于在知识产权损失的取证和赔偿方面的鉴定技术要求较高，以及我国现有知识产权保护法律尚有许多需要完善的地方，企业的损失往往是巨大且无法挽回的。在这种现状下，通过各种途径对自有的知识产权进行严密保护成为企业必然的选择。这些需要保护的涉及知识产权的文档包括：软件设计文档和源代码；设计图纸或资料；产品成分或配方；其他重要的内部资料或机密文档等。

通过制订相关的知识产权保护制度，可以加强对各种文档流转、保密的管理，但是传统的文档管理措施和安全产品仍然存在很多不足：

- 无法杜绝泄漏重要知识产权信息（例如重要产品的部分代码，公司预研方向阶段性成果等）的安全隐患；
- 不可避免因安全原因而导致的工作效率下降以及公司资源的浪费（例如对重要文档进行借阅申请、复印、销毁）；
- 不利于公司内部研发部门之间进行协同工作和沟通。

1.2　我们如何帮您实现目标

针对上述需求，我们开发了 SecurDoc 企业文档保护系统，以帮助您更有效的对企业敏感文件和受控文件进行安全防护。本方案将基于 IBM Lotus 的文档管理系统成功的向前推进到企业文档中心、知识中心和文控中心。

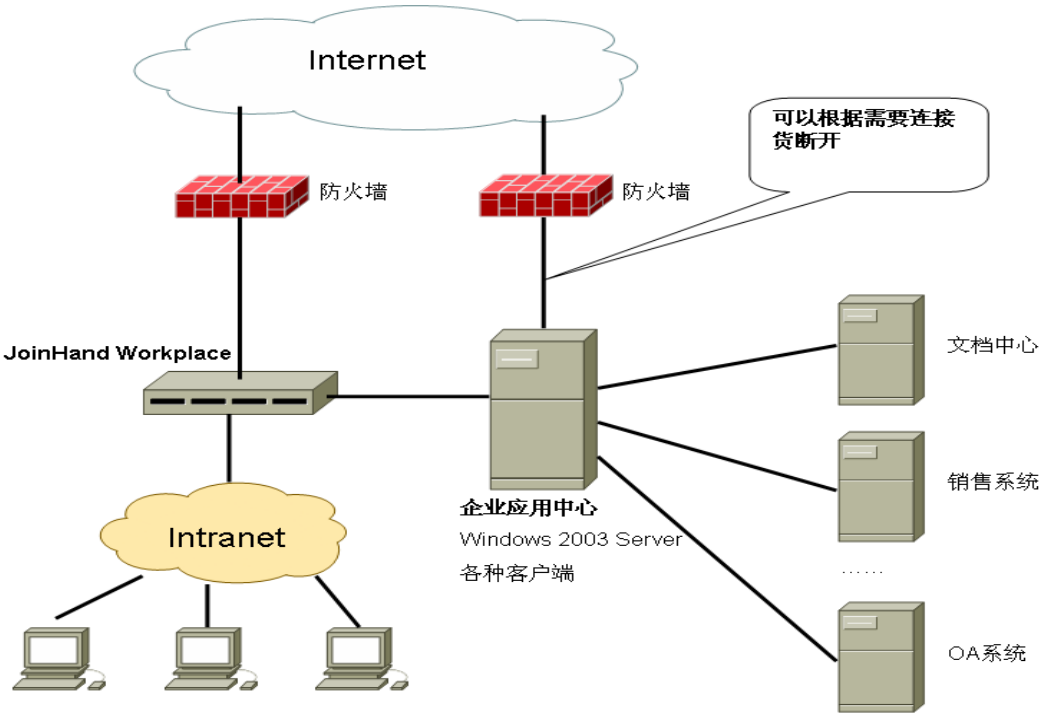
在本方案中，所有的应用（包括开发工具、文档阅读和管理工具、其他需要集中的应用）和机密文档全部集中在数据中心，应用程序集中于“企业应用中心”，机密文档保存于文档服务器；所有用户无需安装任何客户端的软件，仅需要支持 Java 的 Web 浏览器，通过 JoinHand SecurDoc 企业应用中心，即可方便地使用权限范围内的各种开发和项目工具、文档阅读和管理工具以及其他应用，根据授权浏览或修改机密文档，所有的存取操作都在服务器端，客户端任何对文档的输出操作均可被管理和禁止，用户的操作流程和习惯与原来一致，以达到兼顾高安全性同时又不妨碍公司员工进行正常的工作。客户端可以被管理和禁止的操作包括：

- 可以管理或禁止客户端对保密文档的各种存储操作，包括硬盘存储、软盘存储、光盘存储、优盘存储和其他客户端存储设备；

- 可以管理或禁止客户端对保密文档的其他输出操作，包括打印、文档编辑中的复制/粘贴操作、email 操作；

JoinHand SecurDoc 企业应用中心的后台服务器身份认证可以和 JoinHand SecurDoc 所在的 Domino 服务器认证做用户映射，可以为同一用户在不同区域实现不同的权限管理。通过用户映射，可以将一组 JoinHand SecurDoc 用户(Domino 用户)的企业应用权限映射给后台服务器上的某个特定的用户上。

被授权用户可在内网方便的使用服务器端的授权软件或查阅授权资料。整体方案架构如下：



JoinHand SecurDoc 和企业应用中心使用标准的 RDP 协议进行通信，并通过内置的安全认证策略和用户映射保证每个 JoinHand SecurDoc 用户对企业应用中心上的各类软件具有受控的访问权限。

通过部署和实施 JoinHand SecurDoc 企业应用中心，用户将可以降低在客户机的维护成本，并有效划分客户机权限。

1.3 方案价值

- **快速建立企业文档中心；**
- **对受控文件和敏感文件进行防护；**
- **提升 IT 对企业智力资产的保护能力；**

1.4 成功案例

- 上海先进半导体制造有限公司
- 无锡华润微电子有限公司
- 上海宏力半导体

第2章　JoinHand SecurDoc 企业文档保护方案介绍

2.1　实现文档安全的主流技术

从目前实现文档安全的主流技术来看，主要有三种可行方案：**文档加密、控件技术和远程访问保护**。三种方案的优缺点对比如下表所示：

	文档加密	控件技术	远程访问保护
优点	● 文档安全性高，可以离线访问 ● 可以设置文档的访问周期、时限等	● 可以集成在大多数的文档管理系统中 ● 可以防止在客户端直接访问文件 ● 可以具有签名、批注等功能	● 具有双重保护机制：一个是保护设备的验证，一个是被远程访问的系统的验证。 ● 本地不留任何访问痕迹 ● 所有操作全部虚拟化，用户仅得到操作的“演示” ● 支持瘦客户机
缺点	● 文档必须经过文档加密软件处理以后才具有安全性保障 ● 会破坏文件的原有结构 ● 支持的文档格式有限 ● 文档打开时是一个脱壳解密过程，会留下本地痕迹。 ● 认证服务器一旦发生问题，将导致加密的文件无法解密 ● 用户大多需要保留不加密的原始文件	● 支持文件格式有限 ● 无法控制用户获得文档的真实存储位置 ● 有时候需要安装客户端插件，维护比较困难	● 对硬件要求很高，以便支持并发用户的访问 ● 软件安装和实施比较复杂

2.2 JoinHand SecurDoc 企业文档保护方案的功能和特点

JoinHand SecurDoc 企业文档保护方案是一个基于 IBM Lotus Domino/Notes 和 Windows 2003 Server 的系统集成方案。

本方案结合了 Sun J2EE 技术(类似于上述的控件技术)和远程访问保护两种方案，即：用户通过远程访问保护机制以后，再使用控件技术去访问文件。这样，即使用户获得了文档的实际存储位置，也无法将其获取到本地，文档只能保留在被访问的远程计算机上。

JOINHAND SECURDOC 企业文档保护中心要求用户首先通过 IBM Lotus Domino/Notes 的用户认证，然后 JOINHAND SECURDOC 企业文档保护中心会自动将此认证转到企业应用中心上的 Windows 2003 Server 进行第二次认证。只有两次认证都成功以后才能进入企业应用中心然后去访问受保护的企业文档中心。

对于已经部署和实施了 IBM Lotus Domino/Notes 的企业，JoinHand 企业文档保护中心(JOINHAND SECURDOC 企业文档保护中心)可以方便地被整合到企业现有 IT 架构中。

1. JOINHAND SECURDOC 企业文档保护中心使用了 IBM Lotus Domino 的用户认证机制，不会影响用户现有的 Lotus Domino 应用系统的认证方式。
2. JOINHAND SECURDOC 企业文档保护中心非常适合那些已经使用了企业级文档管理系统的用户使用，因为 JOINHAND SECURDOC 企业文档保护中心可以通过文档管理系统的分布式部署来实现与文档管理系统的无缝集成（见架构设计）。
3. JOINHAND SECURDOC 企业文档保护中心方案中，所有访问文档的工具软件仅需要一套，并且只要安装在企业应用中心服务器上。
4. JOINHAND SECURDOC 企业文档保护中心方案保护的是企业智力成果，一般不会保护处于草稿、审核中的文档。除非用户愿意将文档的起草和审核的应用系统放置到 JOINHAND SECURDOC 企业文档保护中心所保护的企业文档中心上。
5. JOINHAND SECURDOC 企业文档保护中心不是一个文档管理系统，而是一个用来保护企业文档中心的解决方案。即使用户找到了一个具有文档保护机制的文档管理系统，也必须要考虑引进一个系统对企业 IT 架构的影响。
6. JOINHAND SECURDOC 企业文档保护中心保护的是企业的文档中心，这意味着凡是放置在企业文档中心中的文件都将被保护起来。与传统的基于 Java Applet/ActiveX 的 B/S 架构的文档管理系统相比，它的安全性更高，因为传统的基于控件技术的文档管理系统仅仅是通过控件屏蔽了用户对文件的下载访问。如果用户获得了文档的实际存储位置，这些文件就会变得不安全。

7. JOINHAND SECURDOC 企业文档保护中心不限制用户采用何种方式来管理企业文档中心上的数据，用户可以采用磁盘目录的方式，也可以采用文档管理系统。JOINHAND SECURDOC 企业文档保护中心只要能够有方法访问到这些文件即可。

8. JOINHAND SECURDOC 企业文档保护中心方案对企业文档中心的保护还体现在企业文档中心是专人管理的。有权限管理企业文档中心的人员不一定是计算机系统管理人员。我们建议由计算机软件系统实时管理或者企业文档控制中心集中管理。与传统的文档管理系统相比，系统管理员的权限在 JOINHAND SECURDOC 企业文档保护中心方案中体现的并不明显。

9. JOINHAND SECURDOC 企业文档保护中心内置了世界最著名的 CAD 浏览软件——AutoVue，可以浏览 500 多种 2D/3D/PDM 等文件格式。与其它内置文件阅读器的文档管理系统相比，AutoVue 支持的文件类型更加广泛。

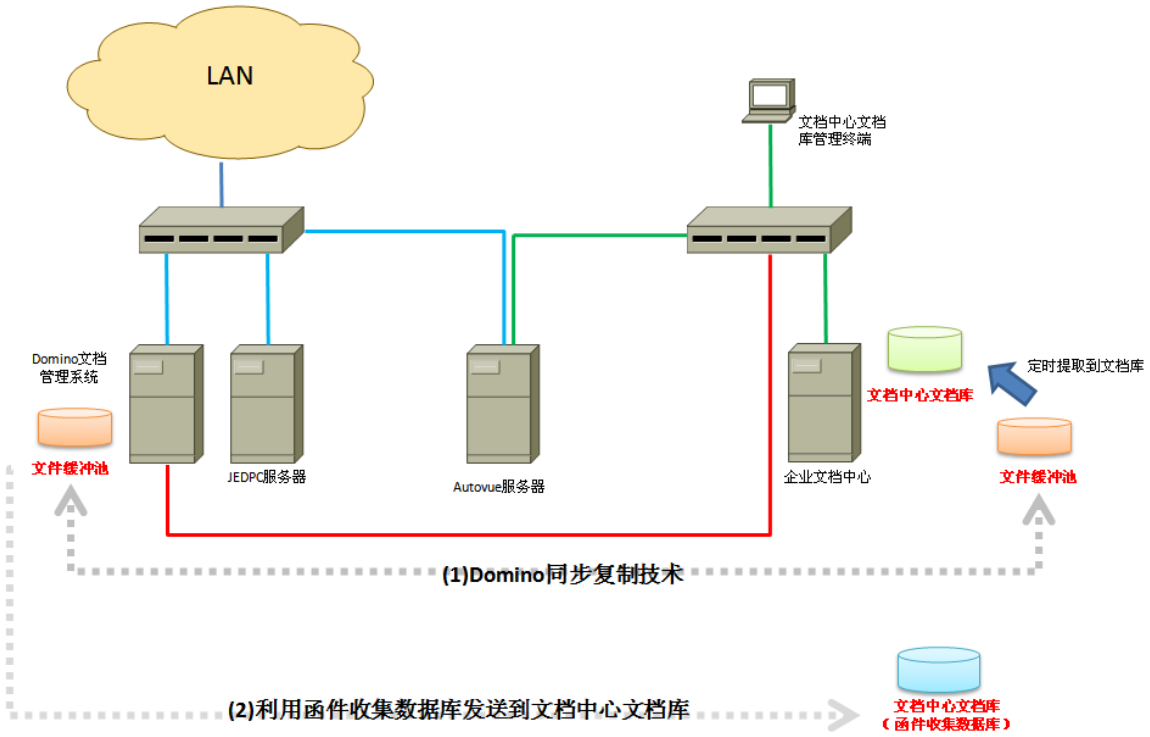
10. JOINHAND SECURDOC 企业文档保护中心不仅仅可以保护企业文档中心，还可以保护企业其它软件系统，不论是 C/S 还是 B/S 的软件系统，都可以通过集中部署实现远程访问的保护。

2.3 架构设计——基于 Lotus Domino

JOINHAND SECURDOC 企业文档保护中心方案不会要求用户对现有的 Lotus Domino 系统进行彻底改造，也不会影响现有的基于 Lotus Domino 的应用系统。

实施 JOINHAND SECURDOC 企业文档保护中心时，用户需要安装 Lotus Domino Server 或者在现有的 Lotus Domino 网络域中注册一个服务器，因为 JOINHAND SECURDOC 企业文档保护中心需要运行于 Domino 之上并采用 Domino 安全控制策略。

系统整体架构如下图所示：



架构说明：

- 蓝色网路用于 Domino 文档管理系统和 JOINHAND SECURDOC 企业文档保护中心服务器通信以及用户远程访问企业应用中心服务器。
- 红色网路用于文件缓冲池的 Domino 同步复制；如果使用函件收集数据库的方法来传递文档，该网路将用于传输函件。
- 绿色网路用于受保护的计算机之间的通信。
- JOINHAND SECURDOC 企业文档保护中心服务器、企业应用中心、受保护的企业文档中心服务器和文档控制中心客户端需要使用单独的交换机（JOINHAND SECURDOC 企业文档保护中心交换机）连接在一起。该 JOINHAND SECURDOC 企业文档保护中心交换机与企业其它交换机没有级联关系。
- 如果用户使用 JOINHAND SECURDOC 企业文档保护中心文件缓冲池，那么企业文档管理系统服务器需要连接到 JOINHAND SECURDOC 企业文档保护中心交换机上，即企业文档管理系统服务器需要有两个网络地址，一个是用于 LAN 通信，一个用于与受保护的企业文档中心通信。

- Domino 企业文档管理系统服务器上的文件缓冲池（一个 Domino 应用数据库）通过 Domino 同步复制技术来实现将受保护的文档自动上传到受保护的企业文档中心。

- 文档中心文档库管理终端的使用权要严格进行控制。该终端主要对受保护的文档进行管理和维护。

在上述架构中，我们采用了物理网段隔离的方式来保证 JOINHAND SECURDOC 企业文档保护中心的安全，并且事先考虑到了企业中可能已经实施了基于 Domino 的文档管理系统。

如果企业已经实施了基于 Domino 的文档管理系统，需要对该系统进行一个简单的改造：

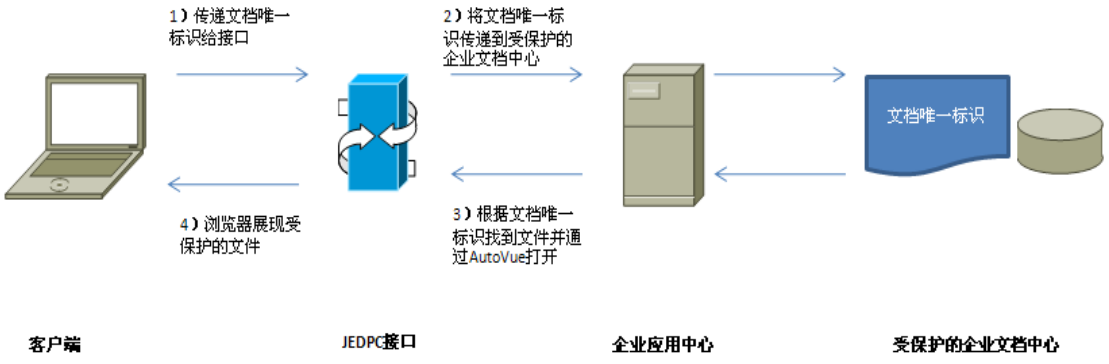
1. 文档管理系统中需要受到保护的文件需要通过计算机程序保存到 JOINHAND SECURDOC 企业文档保护中心的“文件缓冲池”（一个 Domino 应用数据库）中。建议将文档管理系统中的文件做删除或者其它处理以防止用户直接访问。
2. JOINHAND SECURDOC 企业文档保护中心的“文件缓冲池”有开发接口，用户需参照开发接口将文档保存到文件缓冲池中。放到缓冲池中的文档应该根据其在文档管理系统中的权限控制做好了权限控制。
3. 用户也可以使用函件收集数据库的方法将文件传输到受保护的企业文档中心。

本方案充分考虑到了用户所使用的文档的格式，Autovue 服务器提供的文档阅读功能目前支持近 500 种常见的 2D/3D/PDM 文件格式。

2.4 与 Domino 企业文档管理系统/Domino OA 系统的对接

JOINHAND SECURDOC 企业文档保护中心可以与企业文档管理系统从如下两个方面进行对接：

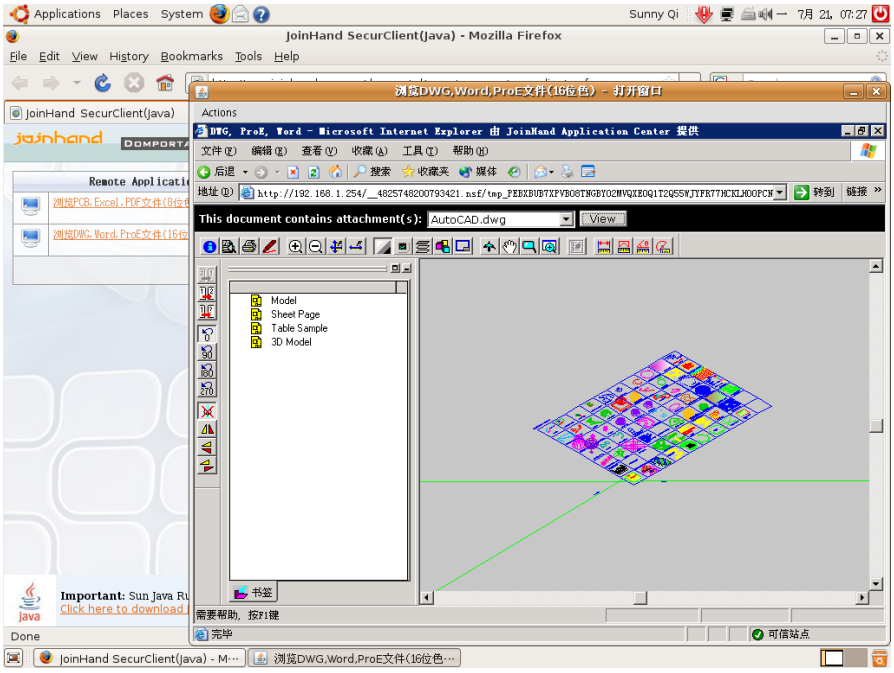
- 将企业文档管理系统中的文档附件通过文件缓冲池或者函件收集数据库传输到受保护的企业文档中心
- 用户需要浏览文件附件时，可以通过编程来打开受保护的企业文档中心上的某个文件。



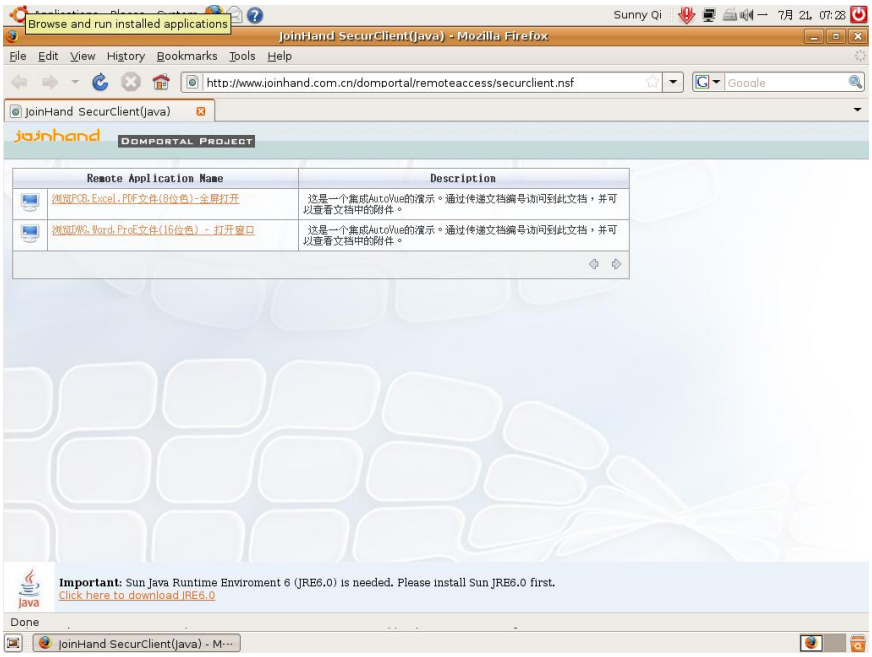
上图中，用户需要提供文档唯一标识（一个唯一的关键字）来启动 JOINHAND SECURDOC 企业文档保护中心的控制机制。我们可以将唯一标识传入到 JOINHAND SECURDOC 企业文档保护中心架

构中的企业应用中心，然后通过在受保护的企业文档中心中利用文档唯一标识查找该文件并显示的方式来访问指定要的单个文件。

JoinHand 文档管理解决方案支持各类操作系统和 Web 浏览器。我们仅仅要求您的操作系统支持 Java 1.6，使用支持 Java1.6 的 Web 浏览器。



图：在 Ubuntu Linux 上使用本产品浏览 AutoCAD 图档



图：基于 IBM Lotus Domino/Notes 的权限控制的完全受保护的文档中心

2.5 常见需求和开发任务一览表

根据用户提供的一些功能需求，我们整理了下面的表格。

用户需求	本方案如何实现	工作着力点
实现单个具体文档的授权管理，能够确保文档在浏览过程中不能被用户随意的打印、下载、编辑及抓屏等。	由于使用了 JoinHand SecurClient 访问受保护的文档或附件，已经可以屏蔽用户的下载、编辑、打印和抓屏。 备注：抓屏软件无法屏蔽；屏幕拷贝可以屏蔽。	JoinHand SecurClient
文档的授权能够进行分级管理，即设计部门副总能够具备借阅、下载、新建目录等授权，设计室总监具有借阅、新建目录的授权。	需要在 OA 系统中加入这些功能。	OA 系统
1） 文件的借阅可实现单个文件的借阅、下载。 2） 文档的下载和查阅必须经过相关的流程的审核，方可由系统管理员授权。 3） 文档的借阅授权应能够对借阅时间进行限制，超过借阅时间后，文档的浏览权限自动失效。	经过 OA 系统审核以后，需要 DCC 开放文档附件访问权限。同时可以设置访问时间限制等。 最简单的实现办法是 DCC 收到审批认可的申请，将文档作为附件存入数据库中，并设置访问权限和时限。系统每天检查超过期限的文件并予以删除。	OA 系统 DCC 工作规范
文档下载授权应与用户 IP 地址绑定，任何用户所申请的文档下载仅能下载一次，且仅能使用 IT 部门配给的 IP 地址下载。	在文件下载访问时，需要通过 CGI 变量得到访问机器的 IP 地址并进行控制。 实现方式类似于上面的需求。	OA 系统 DCC 工作规范
地址栏中的文档地址应进行加密，不允许用户复制地址后，通过地址栏粘贴继续能打开此份文档。	JoinHand SecurClient URL 接口文件（JNLP）是一个加密的文本文件，无法得到确切的可阅读信息。进入受保护的服务器以后，用户即使下载也无法保存到本地，只能保存在“桥接服务器”上。	JoinHand SecurClient

文档的安全管理不能改变原来文档的格式，不改变现有 file Server 文档存放的方式	我们采用了 Autovue 浏览器用于浏览近 500 种 2D、3D 和 PDM 等软件的文档。用户将文件服务器放置到“桥接服务器”后面进行保护。	Autovue Desktop Edition
无权限查看的目录或者文件在用户查看的目录树里面看不到该份文档	我们采用惯了虚拟目录的存放方式。虚拟目录是存储在 Domino 数据库中，可以设置用户的读者权限。 如果采用文件服务器方式，如果用户进入共享文件夹，就可以看到目录结构或目录下的文件。	暂时没有有效的解决办法 建议用户将文件服务器存放的方式转变为基于 Domino 数据库的存储方式。
文档的借阅和下载系统应记录其访问日志，以便于事后进行追溯，同时应该能够出相关的报表，以便于进行安全分析管理	提供借阅记录 提供下载记录	OA 系统
文档的目录维护应具有便利性，用户部门或 DCC（文档管理员）新建目录后或者有了新的文档时，文档目录树应该能够自动更新	由 DCC 或者用户部门自己维护“虚拟目录”。该目录树存储在 Domino 数据库中。每个用户根据读者权限，将看到不同的目录树，因为每个人对于目录树中的“目录”的读者权限不一样。	OA 系统
用户在 Domino OA 中上传附件，同时应能选择该文件在文件服务器存放的目录，文档目录，管理员应该可维护	“虚拟目录”功能 “虚拟目录”对应文件服务器上的实际文件夹	OA 系统
文档审核流程结束后，文档进行自动拆分，并自动放入用户提交文档所设置文档的目录地址	OA 中的文件审核结束以后，发送“拆离指令”到后台受保护的文件服务器，由 Domino 代理进行拆离。	JoinHand 将扩展后台受保护的系统
对于用户提交的大附件（5M 以上）或者三个以上附件时，用户可通过发送带附件的邮件到固定的邮箱触发新的申请流程，同时附件的地址信息直接加载到申请表单上	OA 系统中使用函件收集数据库。收到邮件以后触发工作流程序进入审批。	OA 系统

根据上述需求，基于本方案的开发计划如下：

阶段	工作描述	周期
需求调研	● 了解用户需求 ● 调研 OA 系统实现模式 ● 确定 OA 系统改造范围和方式	15 日
OA 系统改造	● 改造 OA 系统 ● 完成借阅、下载等文档权限控制流程	
JoinHand SecurClient 二次开发	● 后台服务器数据接口开发 ● 函件收集数据库开发 ● OA 服务器和文档中心数据传输功能实现	15 日
系统测试和联调		10 日
上线试运行和用户培训	● OA 用户培训 ● DCC 培训 ● 系统管理员培训	10 日

硬件和软件需求一览表：

设备名称	硬件和软件需求
JoinHand SecurDoc 服务器 **备注：可以运行在现有的 Domino 系统平台上**	硬件需求 ● CPU - 2.0GHz 或者更高 ● RAM - 2GB 或者更高 ● HDD - 至少 20GB

	软件需求 ● Lotus Domino Enterprise Server
桥接服务器/通道服务器	硬件需求 ● CPU – 2.0GHz 或者更高,1 颗或者更多 ● RAM – 最低 4GB（支持 50 用户并发） ● HDD – 至少 20GB ● 2 个 1000Mbps 网络适配器
	软件需求 ● Windows 2003 Server 企业版或者标准版
客户端	操作系统支持： Windows XP / Windows Vista / Windows 2000 专业版 Ubuntu Linux 8.0.4 Mac OS X 10.5 浏览器支持： Microsoft IE 6 / IE7 Mozilla Firefox Apple Safari Opera 客户端需要安装：Sun JRE 1.6 版本

第3章　IBM 和 JoinHand 公司简介

3.1　JoinHand 公司简介

JoinHand 成立于 2003 年。是一家以软件开发、技术服务、系统集成和软件分销为主营业务的高科技企业。公司自成立之初就定位于 IBM 平台的软件开发业务为主导，结合自有知识产权的软件产品销售，并为客户提供 IBM 软件的技术服务。公司现有 Lotus 技术人员 30 人，其中工作年限超过 3 年的占到 80%。这是一支技术实力强，项目经验丰富的团队，无论在规模还是在能力上在华东地区都属于一流。

JoinHand 现已成为 IBM 公司华东地区最重要的合作伙伴之一，公司有多项软件解决方案入选 IBM 解决方案集锦。从 2006 年开始，JoinHand 与 IBM IGS 合作，向 IBM 输出技术人员，为客户提供外包服务。

JoinHand 的软件产品设计部门从 2005 年开始研发自有知识产权的软件产品：JoinHand SecurDoc。经过 3 年的努力，该系统上已经实现协同办公、工作流、文档管理、文档保护、企业门户等诸多功能，使用该系统的最终用户已经超过 30 家。

JoinHand 的客户群体遍布各行各业，在制造、服务、研发、金融和教育行业都有成功案例。其中知名的集团型企业有：统一集团（中国）股份有限公司、香格里拉（中国）有限公司、欧莱雅（中国）有限公司、先进半导体股份有限公司等。

3.2　IBM 公司简介

IBM，即国际商业机器公司，1911 年创立于美国，是全球最大的信息技术和业务解决方案公司，业务遍及 170 多个国家和地区。2008 年，IBM 公司的全球营业收入达到 1036 亿美元。

在过去的九十多年里，世界经济不断发展，现代科学日新月异，IBM 始终以超前的技术、出色的管理和独树一帜的产品领导着全球信息工业的发展，保证了世界范围内几乎所有行业用户对信息处理的全方位需求。

IBM 与中国的业务关系源远流长。早在 1934 年，IBM 公司就为北京协和医院安装了第一台商用处理机。80 年代中后期，IBM 先后在北京、上海设立了办事处。1992 年 IBM 在北京正式宣布成立国际商业机器中国有限公司。到目前为止，IBM 在中国的办事机构进一步扩展至 26 个城市。伴随着 IBM 在中国的发展，IBM 中国员工队伍不断壮大，目前已达到 14000 人。除此之外，IBM 还成立了 10 家合资和独资公司，分别负责制造、软件开发、服务和租赁的业务。

IBM 非常注重对技术研发的投入。1995 年，IBM 在中国成立了中国研究中心（2006 年更名为 IBM 中国研究院），是 IBM 全球八大研究中心之一，现有 200 多位中国的计算机专家。随后在 1999 年又率先在中国成立了软件开发中心，现有 3000 多位中国软件工程师。

二十多年来，IBM 的各类信息系统已成为中国金融、电信、冶金、石化、交通、商品流通、政府和教育等许多重要业务领域中最可靠的信息技术手段。IBM 的客户遍及中国经济的各条战线。 与此同时，IBM 在多个重要领域占据着领先的市场份额，包括：服务器、存储、服务、软件等。

对于 IBM 在中国的出色表现和突出贡献，媒体给予了 IBM 十分的肯定。IBM 先后被评为“中国最受尊敬企业”、“中国最受尊敬的外商投资企业”、“中国最具有价值的品牌”、“中国最佳雇主”等。2004 年，IBM 中国公司被《财富》杂志中文版评选为“中国最受赞赏的公司”，并荣居榜首。2005 至 2007 年，IBM 连续三次被中国社会工作协会企业公民工作委员会授予“中国优秀企业公民”荣誉称号。

2010 年，IBM 提出“智慧的地球”理念，倡导以智慧引领转变，从容应对金融危机、气候变暖、恐怖主义、能源紧张、环境污染等全球问题；同时，针对当今国际经济形势，分析中国企业的机遇与挑战。IBM 从新锐洞察、智慧运作、动态架构、绿色未来等几个方面，分享建设“智慧的地球”的具体经验和方案，帮助您的企业抓住机遇，开启新的里程。我们相信以科技为助力，一定可以转危为″机″，共建智慧的企业，更有智慧的国家，甚至更有智慧的地球。

附录：用户常见问题解答

- **JoinHand SecurClient（JoinHand 企业应用中心 3.1）如何与企业现有的基于 Domino 的 OA 系统整合？**

首先，请将 JoinHand SecurClient 安装在与 OA 同属于一个 Domino 网络域的附加的服务器上。这样，访问 JoinHand SecurClient 的认证就可以与现在的 OA 系统保持一致。

如果 OA 中存在有需要受控访问的文档附件，请按照下面的需求修改 OA 系统。

1. OA 需要将现在的 Notes 数据库中的 Notes 文档的附件进行处理：不论采用何种方式，附件必须转移到某个另外的 Notes 文档中，并从现在的 Notes 文档中删除掉。
2. 按照 JoinHand SecurClient 的规则，在现在的 Notes 文档中提供一个访问 JoinHand SecurClient 的链接（即 SecurClient URL，一个存在于 JoinHand SecurClient 数据库中的文档）。用户点击该链接时，将启动 JoinHand SecurClient。

为了保证文档附件的安全性，SecurClient URL 的访问权限必须在后台根据 OA 权限进行更新。SecurClient URL 中有两个很重要的域：PublishTo（读者域，多值）和 DocAuthors（作者域，多值）。用户可以根据 OA 权限更新这两个域的值。

综上所述，OA 系统与 JoinHand SecurClient 的整合主要是完成以下工作：

- 在 JoinHand SecurClient 数据库中根据 OA 权限创建一个 SecurClient URL 文档。
- 在现有 OA 中提供一个 URL 链接，该链接将自动启动 JoinHand SecurClient，并访问后台受保护的文档附件。

Application name:	浏览DWG,Word,ProE文件(16位色) - 打开窗口
Description:	这是一个集成AutoVue的演示。通过传递文档编号访问到此文档，并可以查看文档中的附件。
Server:	www.joinhand.com.cn
Port:	3456
Login user:	JoinHandWorkplace
Password:	••••••••••
Domain:	
Desktop geometry:	Full Screen
Desktop width:	800
Desktop height:	600
Color deepth:	8bit 16bit
Window Title:	("_" means blank space)
Program (Shell):	c:\program files\internet explorer\iexplore.exe http://192.168.1.254/domportal/av.nsf/viewbysn?openagent&sn=SN20080710N001
Work Directory:	

上图显示的是一个 SecurClient URL 文档的范例。该范例通过 AutoVue 服务器（一个 JoinHand 企业应用中心）来访问位于 192.168.1.254 服务器上的 Domino 的 Notes 文档中的附件。

OA 系统中提供的文档链接范例如下：

<a href=”
/__48257487001455EF.nsf/JavaWebStart?openagent&unid=5247CABCD4493BFD4825748600
4A91A8

” target=_BLANK>访问文档附件

其中：

1. 48257487001455EF 是 Java SecurClient 数据库的数据库复本标识；
2. 5247CABCD4493BFD48257486004A91A8 是 SecurClient URL 文档的 Universal ID。

- **如何实现将 OA 中的文档附件上传到 JoinHand 企业应用中心保护的后台服务器上？如何控制文档附件的权限？如何有效管理后台服务器上存储文档附件的 Notes 数据库？**

  我们采用下图所示的服务器架构来完成一个基于 Domino 系统的文档保护方案。

  在本方案中，从左向右的服务器依次可以被定义为：

  - OA 服务器（图示中是两台，其实可以设置为一台，即 OA 和 JoinHand SecurClient 安装在一台 Domino 服务器上）

- JoinHand 企业应用中心服务器，如果是针对文档保护，可以称之为 AutoVue 服务器。
- 企业文档中心（受保护的文档服务器，基于 Domino）

上述三台服务器中，请确保 OA 服务器和企业文档中心属于一个 Domino 网络域，这样这两台 Domino 服务器即可使用统一的 Domino 验证机制。

如果 OA 系统需要将受保护的文档附件传输到后台受保护的企业文档中心，可以按照下面的步骤进行：

1. OA 系统将文档附件以邮件的方式发送到“函件收集数据库”（该函件收集数据库位于企业文档中心服务器上）
2. OA 系统在 JoinHand SecurClient 数据库中创建 SecurClient URL 文档

例如：

OA 系统中，在 XX 项目审批过程中有一个待审核的文档附件。可以通过下述代码实现将此文档附件传输到文档中心服务器上的 Notes 数据库中。

……

‘doc 是待审核的文档，包含附件。tmpDB 是一个临时的 Notes 数据库

Set tmp = doc.CopyToDatabase(tmpDB)

tmp.Form = “avDocument”

tmp.SN = “20080710N001” **‘该 SN 需要唯一！！！**

tmp.UKEY = tmp.UniversalID

tmp.Subject = doc.XXXXXX(0)

tmp.AllowSendToMailBoxUsers = YYYYYYYY **‘允许将此文档附件发送到个人邮箱里面的存取控制列表，在该存取列表中的人员都可以将此文档发送到自己的邮箱**

tmp.SendTo = “XXX 审批函件收集数据库” **‘每个审批建立一个函件收集数据库以降低 Notes 数据库负载。另外如何划分函件收集数据库可以根据实际的需要。**

call tmp.Send(True) **‘将附件文档发送到函件收集数据库**

%REM

‘XXX 函件收集数据库(Notes 数据库)在受保护的企业文档中心（一台 Domino Server）上。

%END REM

……

MailInDB = ……‘得到“XXX 审批函件收集数据库”的 FilePath，在 Domino 目录（names.nsf）中。

……

set url = SecurClientDB.CreateDocument() 或者是找到已经存在的 URL 文档

url.Form = “AppletClient”

……设置 SecurClient URL 的中各个数值

url.Shell = | c:\program files\internet explorer\iexplore.exe http://192.168.1.254/+MailInDB +|/viewbysn?openagent&sn= |+tmp.SN(0)

Set item = url.GetFirstDocument(“DocAuthors”)

Call item.AppendToTextList(XXXXXX) ‘XXXXXX 是审批者的 Notes ID

item.IsAuthors = True

Set item = url.GetFirstDocument(“PublishTo”)

Call item.AppendToTextList(XXXXXX) ‘XXXXXX 是审批者的 Notes ID

item.IsReaders = True

Call url.Save(True,True)

……

doc.DocLink = |<a href=”
/__48257487001455EF.nsf/JavaWebStart?openagent&unid=|+url.UniversalID+|

” target=_BLANK>访问文档附件| **‘DocLink 是显示 SecurClient URL 的地方，用户可以点击此链接访问受保护的文档附件。**

……

为了降低受保护的企业文档中心上的 Notes 数据库的负载，可以根据不同的 OA 应用创建不同的函件收集数据库。例如：

XXX 项目审批流程可以对应两个函件收集数据库：

- XXX 项目流转中函件收集数据库：用于存放流转中的文档附件
- XXX 项目文档附件库：用于存放流转结束以后，正式成文的文档附件

- **有权限的用户如何将受保护的文档附件保存到本地？**

在实施企业文档保护系统时，确实应该考虑有权限的用户在其用户端本地使用文件的可行性。

目前，有两种有效的受控手段来实现可控的文档本地访问：

第一种方式需要用户制定《受控文件管理规定》，所有需要本地使用的文件必须经过审核以后由 DCC 发放给相关人员。这是一种企业管理手段。

第二种方式是系统提供自动分发功能。该功能允许有权限的用户通过邮件将文档附件发送到自己的个人邮箱中，同时系统记录发送日志。

上面的代码范例中，“tmp.AllowSendToMailBoxUsers = YYYYYYYY”就是记录了有权限进行此项操作的用户列表。凡是在此列表中的用户，均可以通过点击“发送到我的邮箱”这个按钮将文档附件发送到自己的邮箱，同时系统会自动记录发送日志。

- **Notes 数据库中的文件如何拆离到 FileServer？**

有时候用户需要将受保护的文档附件交还给其它软件系统使用。这就需要将受保护的企业文档中心上的 Notes 数据库中的附件拆离到磁盘目录中。

实现方法如下：

1. 将 FileServer 的共享目录映射为受保护的企业文档中心的服务器上的网络驱动器，并提供相关写权限。
2. 使用 Notes 定时代理，将受保护的企业文档中心上的 Notes 数据库中的文档附件根据相应的规则通过程序拆离到这些网络驱动器上。

……

```
fileList = Evaluate(|@AttachmentNames|,doc)
on error resume next
forall v in fileList
   set obj = doc.GetAttachment(v)
   if not obj is nothing then
      Call obj.ExtractFile("G:\MES\XXX 项目\"+v)
   end if
end forall
```

……