深入WINDOWS2003的加密文件系统EFS PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/140/2021_2022__E6_B7_B1_E5_85_A5WIND_c100_140438.htm 首先说明一下，这篇文章是一篇普及性文章，不是一篇对EFS深入剖析的技术性分析文章。 1、没有DRA策略不等于没有恢复代理，因为DRA策略里可以定义成没有恢复代理的，这也是策略。但在XP里确实可以没有恢复代理，但是没有恢复代理的情况下使用加密系统，是相当危险的。 2、至于你说的那位能解密EFS的DXKo Sung Hoon(▲▲)，很遗憾，我在你给出的链接里没有看到具体的描述，不能确定其真实性，我只能从通常情况下给你分析，EFS依赖于用户证书，但用户证书的产生是和用户的SID以及用户密码有关的，但在实际情况下，有时用户密码是空白的，这时系统将使用SYSKEY来做主密钥的加密。
而SYSKEY是有一定的安全漏洞的，可以通过某种手段破解。因此EFS的安全性和用户密码的安全性相同，如果用户使用了复杂的密码，则EFS的安全性就很高了。当你丢失了证书后，可以从用户配置文件里通过某种手段得到，在MS的PSS里，有这样的一个工具。但如果完全丢失了证书和用户配置文件，想恢复EFS就很难了。至于NTBACKUP里有解密这一功能，我还没发现。 3、EFS加密的文件在移动或复制时，都必须先解密，因此没有解密证书是不能移动和复制EFS文件的。如果要是能移动的话，就麻烦了，我就可以把文件转移到一个新的不具备加密书信的文件夹或FAT分区，这样就可以破解文件了。显然这不可能。 4、组策略中确有禁止EFS的地方，和我提供的注册表一样。 补记：实际上EFS在国外很多大的

企业都在广泛应用，如果按你说的那么不安全的话，那可能没人敢用了哦。另外，在WIN2003里，EFS证书可以由系统CA来颁发，这更加使EFS证书的安全性得到了有效保障。以下是一个EFS的内部结构图500)this.width=500" border=0>