互联网远程升级系统解决方案
（ET199）

北京坚石诚信科技股份有限公司

2008-3-28

随着互联网的广泛普及和迅猛发展，生活中越来越多的应用都在网上完成，带给人们更多更好的便捷服务。那么软件升级是否也可以在互联网完成呢？回答是肯定的，软件开发商可以通过互联网，完成软件功能升级、延长使用时间、增加使用次数等操作。当然，通过互联网进行升级，除了功能需求外，最主要的还是安全需求，即要在一种即方便快捷，又安全的过程中完成软件升级。下面我们就详细的介绍一下使用 ET199 在互联网上如何实现远程升级功能。

首先我们可以将整个系统分为三个模块：登录验证模块、产生升级文件模块、升级文件下载升级模块。完成远程升级前，ET199 锁内要先预制用于升级的 C51 可执行文件和一个 RSA 私钥。

登录验证模块：

（1）页面通过 ActiveX 控件取得用户插在计算机上的 ET199 的硬件序列号（以下简称 SN），并将序列号传给服务器，服务器通过这个序列号查看该用户是否已经交纳升级费。如果已经交费，进入下面的第二步。

（2）服务器端产生一个随机数，发给客户端，客户端通过 ET199 内的 RSA 私钥把这个随机数加密后传给服务器端，服务器端通过与存在 ET199 中的 RSA 私钥对应的 RSA 公钥解密，然后将解密后的结果与产生的随机数进行比对，一致允许进入升级页面，否则返回错误页面。

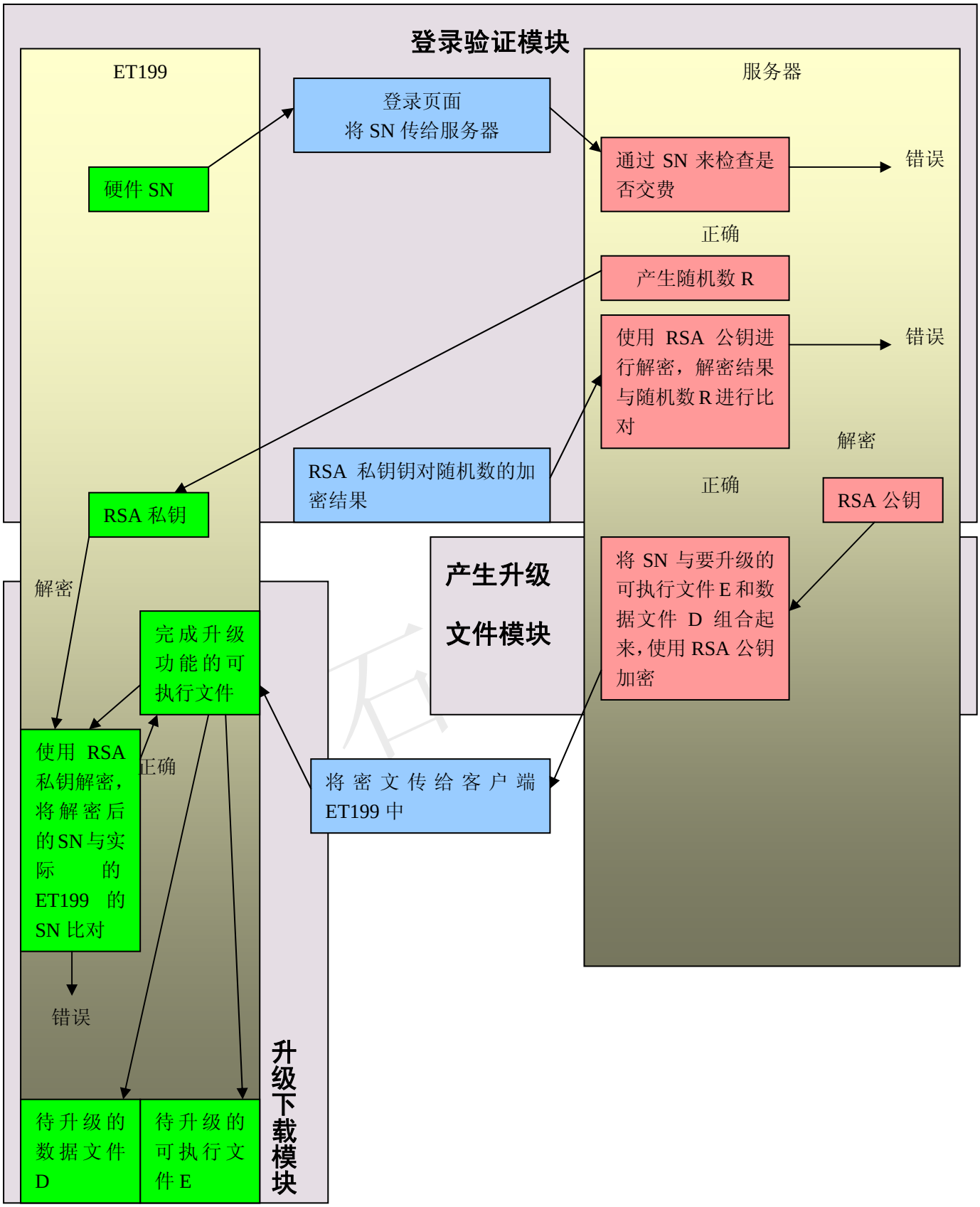
产生升级文件模块：

服务器端将客户端传来的 SN、新的锁内的 BIN 文件和数据文件使用 RSA 公钥加密，将密文结果产给客户端，或者产生一个升级密文文件供升级用户下载。

升级下载模块:

客户端得到升级的密文后，可以通过网页或者专有工具将密文下载到锁内，在锁内由预先内置好的，专门用来完成升级功能的 C51 可执行文件进行升级。该文件使用锁内 RSA 私钥将密文解密，比较解密结果中的 SN 与 ET199 实际的 SN 是否一致，不一致则退出升级过程。然后升级文件将解密后的数据写入到锁内，替换要升级的可执行文件或者数据文件。

如下面的原理图所示。


登录验证模块
ET199
服务器
登录页面
将 SN 传给服务器
硬件 SN
通过 SN 来检查是否交费
错误
正确
产生随机数 R
使用 RSA 公钥进行解密，解密结果与随机数 R 进行比对
错误
解密
RSA 私钥钥对随机数的加密结果
正确
RSA 公钥
RSA 私钥
解密
产生升级文件模块
将 SN 与要升级的可执行文件 E 和数据文件 D 组合起来，使用 RSA 公钥加密
完成升级功能的可执行文件
使用 RSA 私钥解密，将解密后的 SN 与实际的 ET199 的 SN 比对
正确
将密文传给客户端 ET199 中
错误
升级下载模块
待升级的数据文件 D
待升级的可执行文件 E

特点一：升级前验证身份

用户在升级前，需要将硬件的 SN 传给服务器端，由服务器端从数据库信息中查看该用户是否交费。如果有交费记录，服务器与客户端进行了一个身份认证的过程。这个过程通过 RSA 加解密来完成，由于只有 ET199 内才有 RSA 私钥，且锁内的私钥不可导出，那么只有锁内有这个 RSA 私钥的 ET199 的用户才能登录到升级系统中，没有这个私钥的用户，即不是这个软件的用户是无法登录到系统中的。

特点二：安全远程升级

整个升级过程中，是将要升级的数据通过 RSA 公钥加密后在互联网上传输，只有对应的 RSA 私钥才可以解密，而 RSA 私钥只能在 ET199 硬件中，且不能导出，那么只有拥有正确的 RSA 私钥的 ET199 用户才能升级。同时，升级密文的解密过程也是在 ET199 硬件内部完成，不存在任何安全隐患。

特点三：升级文件针对特定的用户

ET199 的硬件序列号 SN 每把锁都是不同的，根据这个特性，为每把锁产生不同的升级包，这个升级包这能针对相同 SN 的 ET199。

特点四：防止没有交费的用户进行升级

升级包在 ET199 内部解密后，完成升级功能的 C51 可执行程序将解密后的 SN 与通过锁内接口得到的实际的 ET199 的 SN 进行对比，来判断这个包是不是给这个 ET199 使用的。只有 SN 验证正确才能继续升级，防止升级包被用来共享。这个设计的安全在于，升级包是密文，即使泄漏出去或者被修改，那么将导致升级失败，其次验证 SN 是在锁内进行，与外界隔离，不受任何安全攻击的影响。

特点五：升级包只能升级一次

当客户交纳费用，在网上正确升级后，ET199 锁内记录版本信息的文件内容已经更新为新的版本号，如果用户再次使用升级包进行升级，负责升级的 C51 可执行文件会去比对升级包解密结果中的软件版本是不是比锁内的软件版本高，这时由于已经升级过，那么只能是相同或者是更低，从而不能继续升级。