## ET299 时间授权方案

ET299 是坚石诚信科技有限公司推出的以高性能智能卡硬件为基础,使用简单方便的高质量加密锁。对于受保护的软件,通过它,不仅可以保护软件不被非法复制或使用,同时也可以实现 对软件加密的时间授权和计次授权。

应用需求:对软件加密,并实现时间授权,同时需要远程升级同步用户加密锁的时间授权。 下面对 ET299 的时间授权功能作以如下方案说明。

## 加密锁设置

这里以两支 ET299 加密锁为例,设置成相同 PID,使用种子"123456",产生新的 PID "FFC5EB78"。其中一支作为母锁,开发商保留,用于产生更新时间授权的升级文件;另外一支 作为子锁,用户使用。因为时间授权的设置,需要远程升级功能的支持,所以需要首先在 ET299 加密锁内设置升级密钥对,母锁中保存升级公钥,子锁中保存升级私钥,制作升级文件时使用母 锁公钥产生加密的升级文件,客户端升级时通过子锁私钥在锁内解密,以此来实现安全的远程升 级。ET299 智能卡硬件可以有效保证子锁中私钥的安全,任何人无法获取。运行 GenRemoteKey. exe 工具,如下图所示:

🗄 GenRe	emoteKey		×
硬件PID	ffc5eb78	ī	产生密钥对
USERPIN	*****	1	呆存到 <b>文</b> 件
SOPIN	*****		从文件导入
RSAGenK Close E Find 1 1 now oper Verify 1 写入升级 Close E Find 1 now oper	ey successfully! [299 Success! ET299 a the first ET299 Sopin Success! 【密钥成功! [299 Success! ET299 a the first ET299	<u> </u>	写毋锁 5子锁
写入升组 Close E	Sopin Success: [密钥成功] [299 Success!	<u>~</u>	退出

首先,插上母锁,输入正确的"硬件 PID","USERPIN"和"SOPIN",点击"产生密钥对", 提示"RSAGenKey successfully"后,点击"写母锁"。母锁制作完成。

然后,换上子锁,点击"写子锁",提示"写入升级密钥成功!",子锁制作完成,可发给用 户使用。

注意:此过程可设置多把子锁,只有通过这个步骤设置子锁后,才能完成远程升级。另外, 建议将产生的密钥对保存到文件中,供以后产生相同的子锁和母锁使用。

## 加密软件并设置授权

运行 ET299 加密锁的外壳加密程序 ET299Env. exe, 如下图所示:

PID UserPIN	FFC5EB78 *****	Timing Check	120 117B6F0C181C8000
SC Adl ile Se ource Encry rror M Me Mes	vanced Settings Author dvanced Options U V V V a	ization Settings Enable Authorization Chec Timer Date Con Init: 1 Lue: 2015- 4- 7	k 
Counte	Ok r Expire Message	Cancel	

首先,插上母锁,输入正确的"PID","UserPIN"和"SOPIN",点击"Advanced Settings", 出现时间授权的操作界面。ET299 加密锁共提供 32 个时间授权单元,针对不同的软件,开发商 可以选择不同的授权单元设置时间授权,相互之间不影响。如针对一套软件,可以任选一个单元 设置授权。按图示设置,即在1号单元设置授权,授权模式为截止日期,授权时限到 2015 年 4 月7日,点击"0k"。

然后选择待加密的程序,这里以系统目录下的 Notepad. exe 为例。点击 "Source File"后 边的浏览按钮,选择待加密文件,点击 "Encrypt",执行加密。如下图所示:

Hardware Inf	ormation	n	Encryption Setti	ngs
PID	FFC5EB7	78	Timing Check	120
VserPIN	****	жжжжжж	Bind with HI	11786F0C181C8000
SOPIN	****	****		Advanced Settings
7ile Selecti	on			
Source File	C:\WINI	DOWS\NOTEPAD. EXE		
Encrypted	C:\WINI	DOWS\ET299_NOTEPAD. E	XE	
Irror Messag	e Window	v Settings		
Message	Window Title	ET299 Dongle		
Message	Content	Cannot find correct	t ET299 dongle	
Timer	Expire Message	Counter expired		
	Expire Message	Timer expired		
Counter				

软件解密完成,并设置授权使用到2015年4月7日。这时,子锁还没有办法解密运行加密 后的程序。为了让子锁能够解密程序并获得正确时授权,需要使用母锁制作一个远程升级文件以 实现子锁的时间授权。

## 升级时间授权

运行远程升级编辑器工具 ET299RemoteUpdate.exe,如下图所示:

SOPIN :	rmation *****	Bind	n.	Bind with
User PIN :	****			
PID :	FFC5EB78	UI	Adjust Dongle Time	
lid Until :	2010- 4- 7	<b>V</b>	C:\Documents and Setting	s\HaiBo\桌 Brows
odate memory	Update timer uni	Add Timer		
Edit Timer	Vnits 00 Vp 01 Vp 02 Vp 03 Vp	⊙ Date ○ How 2015- 4- 7 OK	r Days 6 Up 7 Up Cancel 8 Up 9 Up	24 Up 25 Up 26 Up
	04 Up	12 Vp	20 Vp	28 Up
	05 Vp	13 Vp	21 Up	29 Vp
-	06 Vp	14 Vp	22 Vp	30 Vp
	07 Up	15 Vp	23 Vp	31 Up

同样,输入正确的"SOPIN","User PIN"和"PID",在"Update"组中选择"Update timer unit"标签,授权单元选择设置时间授权时同样的单元号,这里即是1号单元。按图示,完成设置,点击"OK",确认升级信息无误,点击"Generate"。升级成功,在目录下会产生一个授权升级文件。

制作远程升级文件时,可以选择"Adjust Dongle Time"。如果勾选此项,则产生的远程升级文件可以校正用户子锁的锁内时钟,且锁内时钟只能向后调整,不能向前调整。特别注意,当选择校正锁内时间时,要保证当前计算机的时间基本准确。

用户运行客户端升级工具 RemoteUpdate.exe,如下图所示:

Update file	path:		
C:\Documents	s and Settings\Hai	Bo\桌面\ET299 V	
1		1.0	
Status			
Update succeed	led!		

选择开发商发来的远程升级文件,点击"Update",提示"Update successed!",升级成功,

至此,用户手中的子锁可以解密加密后的程序,并已获得正确的时间授权。

注意:建议在产生远程升级文件时,应确保系统时间与本地时间基本一致,如果设置校正 锁内时钟时系统时间超前过多,升级后将会造成锁内时钟的超前,而锁内时钟不能再向后调整, 以至于不能设置或者获取正确的时钟授权。