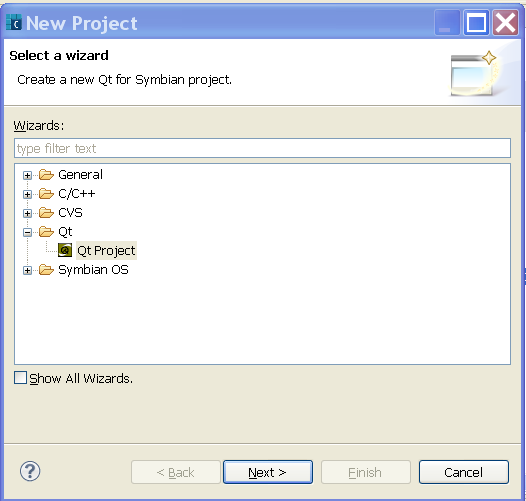
Network configure in Qt

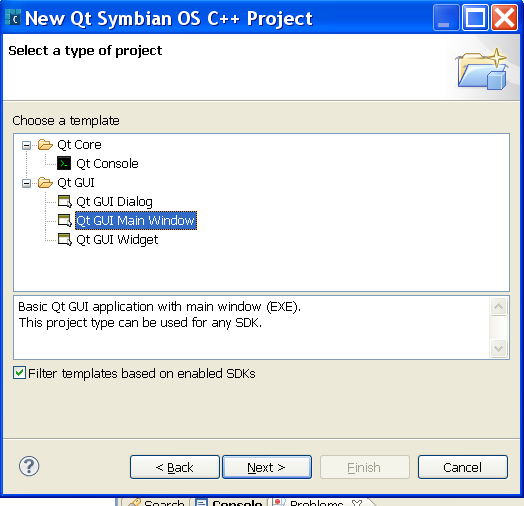
Date: 2010-07-06 version: 0.1

Author: William

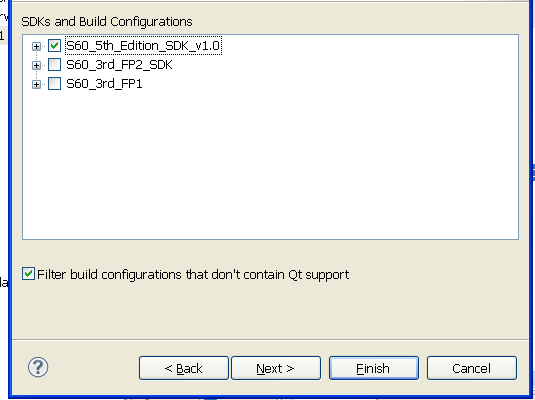
1. 创建Qt需要使用TCP/UDP的工程
   1. 使用Carbide创建



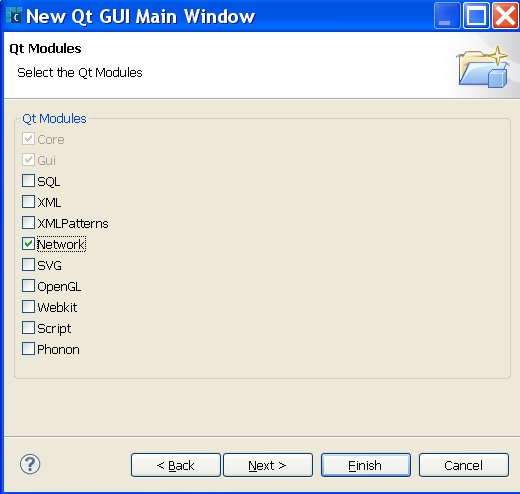
新建Qt工程，选择Qt Project



选择Symbian SDK版本



选择工程需要Qt SDK的lib

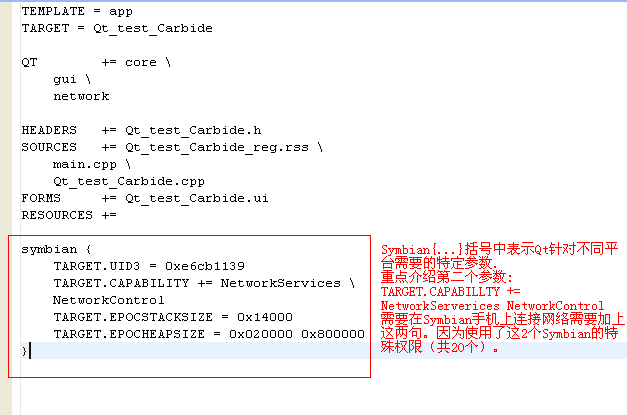


实例TCP/UDP ，只用选Network。

* 1. 在Carbide中配置\*.Pro文件。

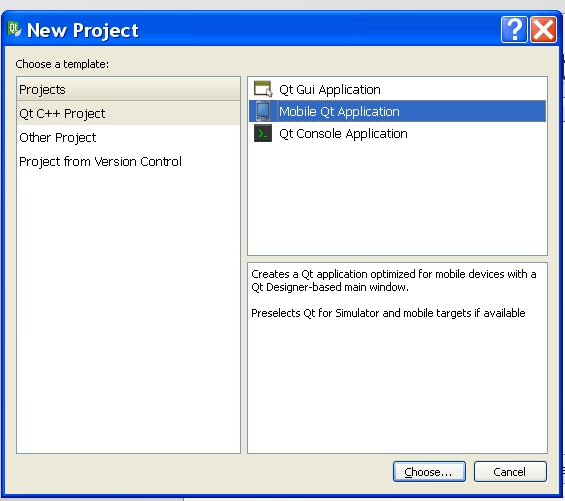
1.2.1 Carbide中 \*.pro简介

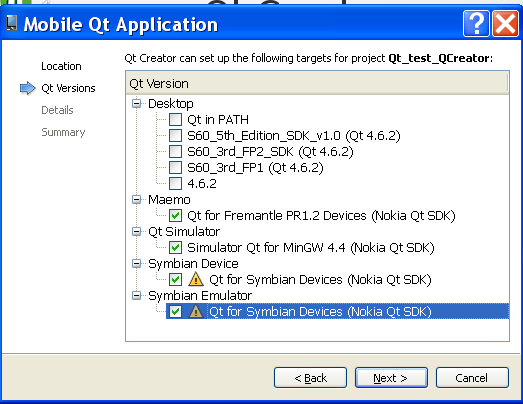


1.2.2 增加CAPABILITY。TCP/UDP需要网络连接，要增加NetworkServerices 和NetworkControl 

2. QCreator创建TCP/UDP工程

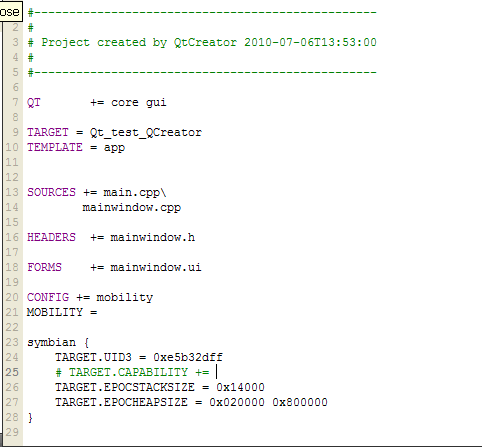
首先选择Qt工程类型。这里选Moblie Qt Application





再次选择对应的SDK。 QCreator中区分出了编译生成程序运行环境。有Desktop，Meamo，Qt Simulator，Symbian Device和 Symbian Emulator。

最有一步也是增加CAPABILITY。同Carbide一样。



为什么需要手动添加CAPABILITY？

我的理解：Symbian特有的签名机制以前就有，据说Qt普及后也会一直存在。程序在使用某种硬件/软件功能时需要被签了名的软件才能生效——签名=授予“权限”（CAPABILITY）。

联网算一种能力。需要增加对应的能力，最后在通过签名，权限才能最后生效。

CAPABILITY总结：

共有20个权限，分三层：

       第一层：五项基本权限。这一层的权限，软件使用自签名证书就可以获取，而由用户来核准。我们安装软件时，有时弹出窗口，说该软件需要接入网络、使用什么什么设备等，问是否同意，就是这个过程。

　　LocalServices  
　　获取例如蓝牙或者红外的近距离远程服务，其对像位置是已知的。  
　　它并没有授权访问网络或者拨打电话（那需要NetworkServices）。   
　　UserEnvironment  
　　访问用户的个人数据和一般性环境信息的服务。  
　　此项权限可以让应程序访问个人记录的声音、图片、健康数据等。它并不需要确定用户的位置，如果要　确定用户的位置，需要Location。   
　　NetworkServices  
　　使用不受位置限制的远程服务。   
　　具体说来，就是语音呼叫，短信，上网。  
　　ReadUserData  
　　对用户敏感数据的读取访问   
　　比如短信，名片，日历。  
　　请注意，读取用户信息和写入用户信息并不是同步的，并不是选择了其中一项能力的话就必须选择另外一项。   
　　WriteUserData  
　　对于用户敏感信息的写入访问

我们需要NetworkServerices

    第二层：扩展权限，需要由symbian授权的签名来得到。

　　Location  
　　获取手机设备当前的位置   
　　手机的位置信息可以由内部或者外部的GPS模块提供，也可以是运营商的网络定位或者其他外部设备。注　　意，如果使用外部的蓝牙GPS设备而不是通过位置API获取位置的话，那么应用程序需要使用的就不是此项权限，而是 LocalServices。   
　　SwEvent  
　　产生按键和手写笔事件，并在任何情况下捕获事件的权利   
　　注意，在获得焦点的时候，一般程序并不需要这个权限来分配到按键事件。  
　　SurroundingsDD  
　　授权访问外围逻辑设备驱动，以获得一些输入信息。  
　　典型的例子是GPS程序。  
　　ProServ   
　　授权注册一个拥有受保护命名的服务器，目前，这类命名是以“！”开头的。系统核心拒绝没有此项权限的服务注册此类命名，这样，就使拥有者不会没有被别的程序仿冒。  
　　PowerMgmt   
　　允许关闭进程，转换情景格式，唤醒或关闭系统。  
　　注意，这一权限并不使程序有能力管理电池。  
　　ReadDeviceData  
　　读取设备信息，诸如当前网络运营商、手机型号（包括串号IMEI）、以及手机设备的设置信息（安装软件列表）、PIN码等。    
　　WriteDeviceData   
　　写入控制系统行为的一些设备信息，比如设置手机锁码、系统时间、时区、闹钟等。  
　　TrustedUI   
　　授权产生受信UI进程，这类进程很少使用，常见的例子是密码对话框。  
　　NetworkControl   
　　允许访问甚至修改网络协议控制。  
　　比如强行中断连接，改变一个通话的优先级等。  
　　MultimediaDD   
　　直接访问多媒体设备驱动。  
　　除非需要特别的优先级，普通的播放、录制行为并不需要这一权限。  
　　CommDD   
　　允许直接访问一切通讯设备驱动，比如 EComm，Ethernet，USB等。  
　　DiskAdmin   
　　磁盘管理，比如格式化（有点吓人，是吗？）

    第三层：只发放给生产厂商的权限。正常情况下，第三方程序是无法获得的。

　　AllFiles  
　　访问整个的手机文件系统。注意这一权限是能够进行写操作的，要特别小心。   
　　DRM   
　　数字版权管理(Digital Rights Managment)   
　　TCB   
　　最核心的一项权限，允许对可执行文件及其权限进行写操作，同时授权了对/sys或/resource之类的敏感目录的访问。这可是阻止恶意程序的最后一道门槛，获得此项授权的程序，基本上想干什么就能干什么。