例程限制：

1、增加了C++的封装

2、增加ECDH的数字信封的支持，但是仅仅支持AES算法

3、CAdES增加CAdES-C、CAdES-X Long、CAdES-X Type 1、CAdES-X Type 2、CAdES-X Long Type 1 or 2和CAdES-A的支持

4、SignedData验证增加同时验证证书的功能

5、增加更多的证书项的获取，主要是补充完整RFC5280里的要求的主体项以及EV证书里的主体项

6、COM版本增加构造国密SM2标准的数字信封和SignedData

7、修正一些OCSP验证的错误

8、SignedData支持SHA-3相关的签名

9、JCE增加对称加解密、MAC运算等的功能

10、JAVA部分，如果不需要私钥操作，可以用纯JAVA实现涉及SM2算法的数字信封的加密和SignedData的验证

11、JAVA部分的简化封装增加JCE的实现

12、CNG增加ECDSA的支持

13、增加一个IIS专用的CNG，可以使用RSA和ECDSA证书来配置SSL

14、提供Android的版本

15、增加企业机构身份标识和个人身份标识等新扩展的支持

16、增加动态加载设备DLL的功能

17、非Windows系统增加设置验证密码回调函数的功能

18、优化了SHA3的速度