Notes on WinCryptoAPI

adriamassanet@gmail.com

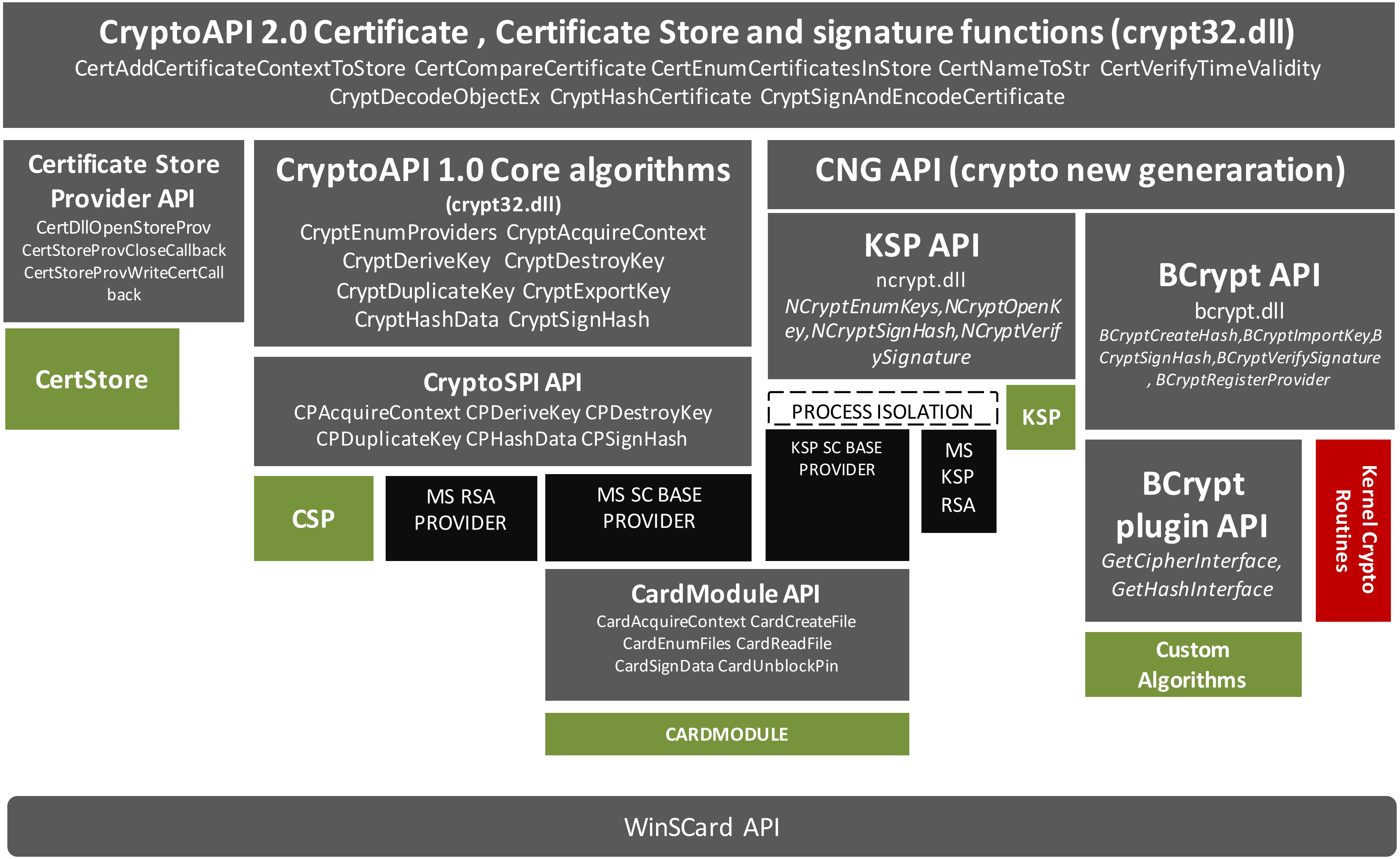
Long term, Windows XP based CSP signing should be retired completely. If the entire country of Spain is using this technology for ID cards, a **breach** in the very old **XP CSP** security would be a **very high risk**. There are much more secure and easier to use cryptographic services built into windows. **I strongly advise** the use of more modern Windows CryptoAPI. http://msdn.microsoft.com/en-us/library/aa380255(v=vs.85)

As I said to Santiago, regarding Windows XP CSP signing, continuing XP support is not high on the list of priorities for the company in general, and I don't foresee any new resources being put on supporting the XP OS.

Thanks-Andrew Lan, CISSP

API | Custom | UserSpace Module | Kernel Module

Windows Crypto APIs



CryptoAPI 2.0 Certificate , Certificate Store and signature functions (crypt32.dll)

CertAddCertificateContextToStore CertCompareCertificate CertEnumCertificatesInStore CertNameToStr CertVerifyTimeValidity CryptDecodeObjectEx CryptHashCertificate CryptSignAndEncodeCertificate

Certificate Store Provider API

CertDllOpenStoreProv CertStoreProvCloseCallback CertStoreProvWriteCertCallback

CertStore

CryptoAPI 1.0 Core algorithms (crypt32.dll)

CryptEnumProviders CryptAcquireContext CryptDeriveKey CryptDestroyKey CryptDuplicateKey CryptExportKey CryptHashData CryptSignHash

CryptoSPI API

CPAcquireContext CPDeriveKey CPDestroyKey CPDuplicateKey CPHashData CPSignHash

CSP

MS RSA PROVIDER

MS SC BASE PROVIDER

CardModule API

CardAcquireContext CardCreateFile CardEnumFiles CardReadFile CardSignData CardUnblockPin

CARDMODULE

CNG API (crypto new generaration)

KSP API

ncrypt.dll

NCryptEnumKeys,NCryptOpenKey,NCryptSignHash,NCryptVerifySignature

PROCESS ISOLATION

KSP SC BASE PROVIDER

MS KSP RSA

KSP

BCrypt API

bcrypt.dll

BCryptCreateHash,BCryptImportKey,BCryptSignHash,BCryptVerifySignature, BCryptRegisterProvider

BCrypt plugin API

GetCipherInterface, GetHashInterface

Kernel Crypto Routines

Custom Algorithms

WinSCard API

- CertStore is OK
- No CryptoAPI: obsolete => No CSP
- No KSP SmartCard Module: are linked to predefined ATR retrieved via SCardChannel by Windows core
- KSP using CNG API