Hinweis:

Die Seite wurde ausschließlich zu SEO-Zwecken erstellt.

Sollten Sie Fragen bezüglich der genannten Themen haben oder Unterstützung benötigen, sprechen Sie uns an: 02366-305330.

Signierung mittels X-509-v3-Zertifikat:

Digitale Signaturen sind asymmetrische Krypto-Systeme und verwenden folglich ein Schlüsselpaar, das aus einem geheimen Signaturschlüssel und einem öffentlichen Verifikationsschlüssel besteht: Private Key <-----> Public Key

Die Struktur eines X-509-v3-Zertifikats setzt sich aus folgenden Punkten zusammen: Zertifikat, Version, Seriennummer, Algorithmen-ID, Aussteller, Land/Region, Bundesland/Kanton, Ort, Organisationseinheit, Organisation, gemeinsamer Name, Gültigkeit, Zertifikatinhaber, Zertifikatinhaber-Schlüsselinformationen, Public-Key-Algorithmus, Public Key des Zertifikatinhabers, Eindeutige ID des Ausstellers (optional), Eindeutige ID des Inhabers (optional), Erweiterungen, Zertifikat-Signaturalgorithmus und Zertifikat-Signatur.

Herausgeber- und Inhaber-ID wurden in Version 2 eingeführt, Erweiterungen in Version 3.

Das Zertifikat wird gebraucht um das Programm vertrauenswürdig zu machen. Soweit der öffentliche Schlüssel mittels eines elektronischen Zertifikats einer Person zugeordnet wurde, kann auf Grund dessen, dass es nur einen zum öffentlichen Schlüssel korrespondierenden privaten Schlüssel gibt, über das öffentliche Verzeichnis des Zertifizierungsdiensteanbieters (ZDA) die Identität des Signaturerstellers ermittelt bzw. überprüft werden.

Eine weitere wichtige Eigenschaft eines Signaturverfahrens ist die Nichtabstreitbarkeit der Signatur (engl. Non-repudiation). Wenn eine Signatur mit einem öffentlichen Schlüssel verifiziert wurde, sollte damit auch bewiesen sein, dass die Signatur mit dem zugehörigen privaten Schlüssel erzeugt wurde.

Wenn das Zertifikat und die pvk Datei vorhanden sind, kann das Zertifikat einfach mit signtool.exe oder signwizard (nur älter als Vista) in der Visual Studio CMD in das Programm eingebunden werden (.exe)