CryptWatch

CryptWatch ermöglicht hochsichere Verarbeitung mobiler sensibler Daten außerhalb gesicherter Umgebungen unter vordefinierten Auflagen und Nutzungsszenarien.

Alle bekannten Angriffsmuster, wie z.B. USB-Dumper auf unsicheren Drittrechnern, wird durch diese hardwaregebundene Lösung mit hoher Mechanismusstärke entgegen getreten. Es ergeben sich viele Mehrwerte sowohl im Enterprise-Umfeld als auch in den mobilen Umgebungen. Global Player profitieren von dieser Lösung genauso wie öffentliche Auftraggeber, KMU und private Nutzer. Die Managementfunktionen erlauben es in einfacher Weise die Mehrwerte und Kostenoptimierungen in allen Bereichen zu heben.

CryptWatch besteht aus seiner gekapselten Hardware in Form eines Smart Card basierten CodeMeter-USB-Stick, genannt CmStick, mit folgender technischen Ausstattung:

1. Eigene technisch geschützte und selbstverteidigende Kryptoinfrastruktur
   - Schlüsselspeicher
   - Implementierung der Verschlüsselungsalgorithmen in Hardware
2. Integritätsgeschützer Applikationsspeicher
3. Kryptographisch geschützter Datenspeicher, welcher folgendes sicherstellt:
   - Daten können nur mit den Schlüsseln und den Kryptoalgorithmen unter 1 ausgelesen werden
   - Daten können nur mit den Applikationen im Applikationsspeicher unter 2 entschlüsselt werden. Die Entschlüsselung findet in der Hardware statt

Die Nutzungsszenarien:

Mobility

Der Stick enthält integritätsgeschützte Anwendungen im „Secure Application Store", alle Schlüsselalgorithmen und Daten in drei unterschiedlichen Hardwaresegmenten.

- Kein unberechtigter Zugriff durch Wirtsystem (von außen) möglich
- Entschlüsselung ausschließlich durch die sichere Applikation PDWatch im Secure Application Store
- Arbeitet Unabhängig von einer itWatch Enterprise Security Suite und ohne Installation in jeder Umgebung – integriert aber mit vielen Mehrwerten in Enterprise Umgebungen.
- Verschlüsselungsapplikation gegen Veränderungen geschützt
- Schutz vor unberechtigter Datenweitergabe, da die Entschlüsselung nur im Kryptosytem des CmStick möglich ist.
- Ver- und Entschlüsselung erfolgt ausschließlich in der Hardware auf dem CmStick.
- Keine Installation nötig

Enterprise

Die Nutzung kann an den für den Anwender personalisierten CmStick gebunden werden und die Daten sind nur auf diesem Stick nach korrekter Authentisierung des Benutzers gegenüber dem CmStick entschlüsselbar; das heißt die Weitergabe der Daten ist an die konkrete Hardware gebunden

Starke Zwei- und Mehr-Faktor-Authentisierung

Prinzip Wissen und Besitz wirkt mehrfach:

- Besitz:

  Personalisierter CryptWatch-Datenträger CmStick
- Wissen:
  - Standardlogin am Arbeitsplatz
  - PIN / Passphrase für Datenträger optional
  - Höchste Sicherheit

Als Voraussetzung muss die itWESS installiert sein.

Es sind keine PKI, keine zusätzlichen Server oder Hardware nötig.

Personalisierte Datenträger CmStick für hochsicheren Datentransport innerhalb und außerhalb des Unternehmens

Krypto erfolgt in Hardware. Das Unternehmen entscheidet zwischen:

- Schlüsseln zur Weitergabe an Dritte
- Und Unternehmensschlüsseln (Company Key), welche sicherstellen, dass die Information in vordefinierter Infrastruktur bleibt (Kein Datenklau, kein Data Loss)

Company Key Verschlüsselung ist an den Cm-Stick UND an die vorhandene itWESS Installation gebunden

Verschlüsselung in der Cloud unabhängig vom Arbeitsplatz (Heimarbeitsplätze, Partnerkommunikation ...)

itWatch GmbH

WIBU SYSTEMS