Encrypt Basic

ICARO Encrypt Basic ist ein Service zur Verschlüsselung eines Wortes (*String*) mit einem Hash-Verfahren. Ein typisches Beispiel für solche *Strings* sind Benutzernamen (*User*) und **Passwörter**.

Umfang von Encrypt Basic

Softwarehersteller erhalten für ihre Anwendungen (*Apps*) von ICARO Software:

- Zugang zu einem Service, mit dem *Strings* verschlüsselt werden. Das Ergebnis (*Secret*) wird der *App* zur Verfügung gestellt
- ein Programm (*Code*), zum Beispiel in der Programmiersprache C, mit dem man durch **ENCRYPT BASIC** erzeugte *Secrets* entschlüsselt

Master Password

Für die Ver- und Entschlüsselung wird ein *Master Password* benötigt, welches von der *App* vorgegeben oder vom *User* bestimmt wird.

Ablauf

Die *App* benötigt beim Start das *Master Password,* zum Beispiel durch die manuelle Eingabe eines *Users* (typischerweise ein Administrator), durch das Einlesen einer Datei (typisch für automatisierte Anmeldevorgänge) oder unter Zuhilfenahme eines Hardware Security Modules. Zur Laufzeit wird das *Secret* gelesen und entschlüsselt, um dann beispielsweise die in der *App* hinterlegten, verschlüsselten Zugangsdaten zu einem System (z.B. SAP) zu ermitteln und einen Anmeldevorgang auszulösen.

Sicherheit

ICARO Encrypt Basic erzeugt die Schlüssel (*Keys)* mit einer standardisierten Schlüsselableitungs-funktionen (*KDF*, Key Derivation Function). Der Rechenaufwand für die Generierung der *Keys* ist hierbei eine wählbare Größe. Hierdurch wird ein Erraten eines *Secrets* durch systematisches Durchprobieren („Brute Force“) auch bei vergleichsweise kurzen *Strings* deutlich erschwert. ICARO wird den erforderlichen Rechenaufwand an gestiegene Rechenleistung, neu bekanntgewordene Angriffe gegen die *KDF* und verfügbare Spezialhardware zum *Secret*-Cracken anpassen, sowie gegebenenfalls den Algorithmus austauschen.

Vorteile für den Softwarehersteller

Wir wissen, dass viele Software-Hersteller hervorragender Apps nur einen eingeschränkten Fokus auf höchste Sicherheitsanforderungen haben oder/und es diesen Herstellern an entsprechendem Know-how mangelt. **ICARO Encrypt Basic** löst dieses Problem durch eine einfach zu installierende und sich aktualisierende Erweiterung für deren Apps.