CryptoScript SDK

utimaco®

```
and open key
attr = ATTR_SET();
attr.KEY_ALGO = CXI.KEY.ALGO_RSA;
attr.KEY_NAME = "RSA_2048"
key = CXI.openKey( attr, CXI.FLAG.KEY_VOLATILE );

-- hash data
mech = MECH(CXI.MECH.HASH_ALGO_SHA512);
hash = CXI.hash(mech, data_in)

-- sign data
mech = MECH(CXI.MECH.PAD_PKCS1);
signature = CXI.sign( key, mech, hash );

return tostring(signature);
```

Utimaco CryptoScript SDK – Schnell, intuitiv, leistungsstark, sicher

Mit CryptoScript können Sie Ihre Anwendungen innerhalb des sicheren Utimaco CryptoServer HSM ausführen, selbst wenn Sie im FIPS-Modus* arbeiten.

Das Skripten neuer Schlüsselableitungsmechanismen war nie einfacher. Erstellen Sie auf spezifische Anwendungen zugeschnittene Datenverarbeitungsfunktionen und maßgeschneiderte Erweiterungen und entwickeln Sie Ihre Anwendungen mit deutlich reduziertem Aufwand und Unkosten.

- Führen Sie mehrere Anwendungen gleichzeitig in virtuellen HSM aus.
- Firewalls, separate Datenbanken und Benutzerrollen ermöglichen Mandantenfähigkeit.
- Um kundenspezifische Anforderungen, z. B. für Industrie 4.0-Anwendungen, die Automobilindustrie, Versorgungsunternehmen oder Zahlungsanwendungen einfach umzusetzen, ist CryptoScript die Lösung für Sie.

Design benutzerdefinierter Crypto-Anwendungen

Sicher

- Automatische Speicherverwaltung
- Virtuelle Laufzeitumgebungen für Mandantenfähigkeit
- Zwischenergebnisse verbleiben im HSM

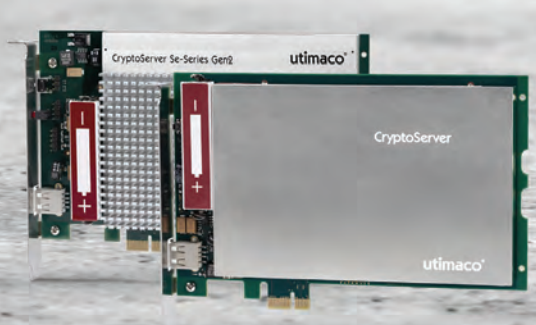
Effizient

- Einfach zu verwenden
- Optimiert für Crypto-Anwendungen
- Automatische und effiziente Speicherverwaltung

Vielseitig

- Kryptografie, Audit-Protokolle und mehr

** Evaluierung in Vorbereitung*



Kontakt
hsm@utimaco.com
hsm.utimaco.com

EMEA
Utimaco IS GmbH – Headquarter
Germanusstraße 4
52080 Aachen, Deutschland
Tel.: +49 241 1696 200

Americas
Utimaco Inc.
910 E Hamilton Ave., Suite 150
Campbell, CA 95008, USA
Tel.: +1 844 UTIMACO

APAC
Utimaco IS GmbH – Office APAC
One Raffles Quay, North Tower, Level 25
Singapore 048583
Tel.: +65 6622 5347

Funktionalität

- Voll ausgestattete Krypto-Bibliothek
- Unterstützung von Langzahlarithmetik
- Interner und externer Schlüsselspeicher
- Optionale Smartcard-basierte Zwei-Faktor-Authentifizierung
- „m aus n“ Authentisierung

Höchste Performance

- Effiziente Laufzeitumgebung
- Optimierte Firmware-Implementierung
- Unterstützung des Hardwarebeschleunigers
- Zwischenergebnisse verbleiben im HSM

Mandantenfähigkeit

- Mehrere virtuelle Laufzeitumgebungen
- Separate Datenbanken (optional)
- Datenbankkontingent
- Trennung von Backup-Daten
- Rollenbasierte Zugriffskontrolle

Bibliotheken

- CXI (Cryptographic eXtended services Interface)
- Langzahlarithmetik
- Strings, Tabellen, Felder, Listen, Datensätze, ...
- Daten packen und entpacken
- Befehlsverwaltung, Protokollierung und Authentifizierung

Sichere Entwicklung

- CryptoScript Compiler wird im HSM ausgeführt
  - Effizienter, fehlerfreier Code
  - Geringer Speicherbedarf
- CryptoScript Host-Tool
  - CryptoScript Signaturschlüssel laden
  - CryptoScript Firmware-Module signieren
  - Module laden, ausführen, stoppen und löschen
  - Sichern und Wiederherstellen privater Datenbanken

Sichere Laufzeitumgebung

- Speicherverwaltung
- Signierter Code
- Private Datenbank (optional)
- Firewall-geschützte virtuelle HSM

Einfach zu verwendende Programmiersprache

- Abgeleitet von Lua
- Umfangreiche Datentypen
- Automatische Speicherverwaltung

Plattformen

- CryptoServer Se-Serie Gen2
- CryptoServer CSe-Serie
- CryptoServer Simulator