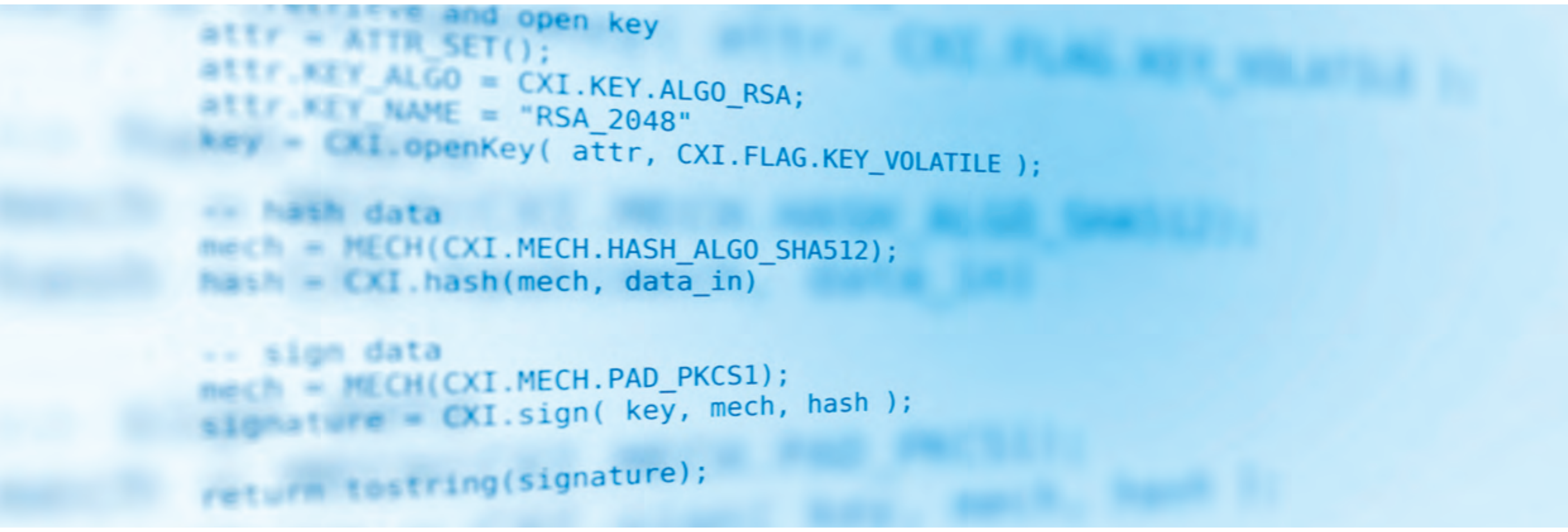
CryptoScript SDK

utimaco®



```
-- retrieve 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);
```

Fast, **I**ntuitive, **P**owerful, **S**ecure – CryptoScript SDK

CryptoScript lets you run your applications inside the secure perimeter of a Utimaco CryptoServer HSM even when operating in FIPS mode.*

Script new key derivation mechanisms, use-case-specific data processing functions and custom extensions, and develop applications with massively reduced effort and overhead.

- Run multiple applications in virtual HSMs.
- Firewalling, separate databases and roles allow for multi-tenancy.
- When easy-to-use customization options are required, such as e. g. for Industrial IoT, Automotive, Utilities or Payment applications, CryptoScript is your readily available solution.

Custom Crypto Application Design

Secure

- Managed language, security monitor
- Intermediate results remain in HSM

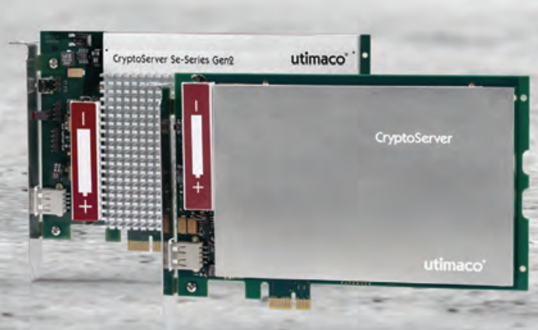
Efficient

- Great performance, memory-efficient
- Virtual HSMs for multi-tenancy
- Easy to use
- Optimized for crypto applications
- Automatic garbage collection

Versatile

- Cryptography, audit logs, and more
- Internal and external key storage

* *Evaluation in preparation*



Contact

hsm@utimaco.com
hsm.utimaco.com

EMEA

Utimaco IS GmbH – Headquarters
Germanusstraße 4
52080 Aachen, Germany
Phone +49 241 1696 200

Americas

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

APAC

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

Functionality

- Full-featured crypto library
- Support for long-number arithmetic
- Internal and external key storage
- Optional smartcard-based two-factor authentication
- M-of-N quorum authentication

High Performance

- Efficient runtime environment
- Optimized firmware implementation
- Support for onboard HW accelerator
- Intermediate results remain in HSM

Multi-Tenancy

- Multiple virtual HSMs
- Separate databases (optional)
- Database quota
- Separation of backup data
- Role-based access control

Libraries

- CXI (Cryptographic eXtended services Interface)
- Long-number arithmetic
- Strings, tables, arrays, lists, records, …
- Data packing and unpacking
- Command handling, logging, and authentication

Secure Development

- CryptoScript compiler runs inside HSM
  - Efficient, untainted code
  - Low memory footprint
- CryptoScript host tool
  - Load CryptoScript signature key
  - Sign CryptoScript firmware modules
  - Load, run, stop, and delete modules
  - Backup and restore private database

Secure Runtime Environment

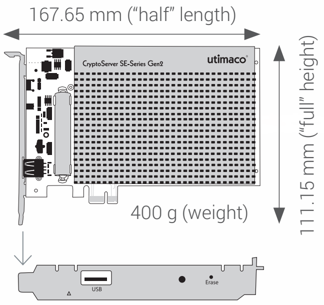
- Secure managed memory
- Signed code
- Private database (optional)
- Firewalled virtual HSMs

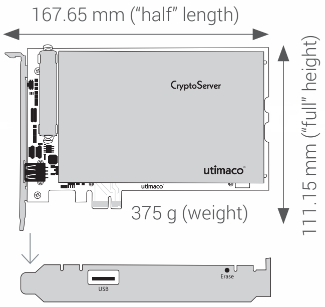
Easy-to-Use Programming Language

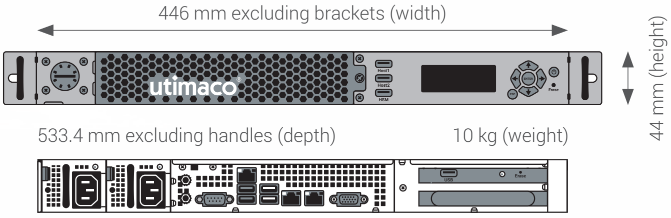
- Derived from Lua
- Rich set of data types
- Automatic garbage collection

Execution Platforms

- CryptoServer Se-Series Gen2
- CryptoServer CSe-Series
- CryptoServer Simulator


167.65 mm (“half” length)
CryptoServer SE-Series Gen2
utimaco
111.15 mm (“full” height)
400 g (weight)
USB
Erase




446 mm excluding brackets (width)
utimaco
44 mm (height)
533.4 mm excluding handles (depth)
10 kg (weight)