



# World's First Converged Crypto Platform for General Purpose and Payment Use Cases



UTIMACO

u.trust Anchor CSAR

# u.trust Anchor CSAR In a Nutshell

## Single platform for multiple use cases

The trend towards digital transformation is forcing cloud service providers and enterprises to enhance their products, services and operations to ensure the most robust security.

Today many business processes require hardware-based security as the foundation of confidentiality and integrity. Hardware Security Modules (HSMs), as the Root of Trust, are playing a key role in keeping the cloud service and enterprises services and systems secured.

Using traditional HSMs for cloud services requires several HSMs for individual use cases, resulting in complicated security architecture. In addition, operating HSMs comes with specific processes and policies based on the use cases and requires expert teams who can manage them.

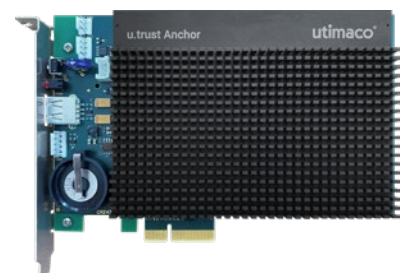
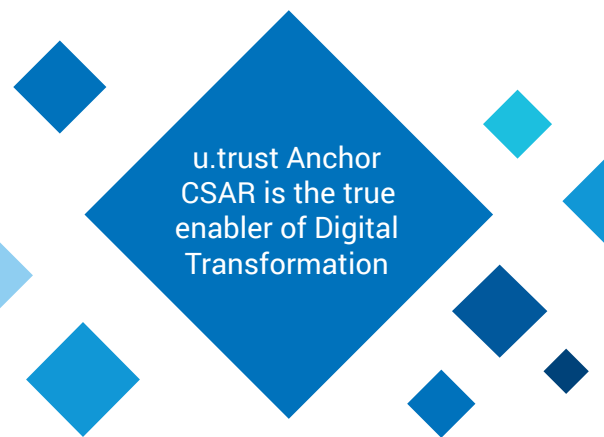
Enterprises are facing increasing challenges using HSMs within both private cloud and on-premises solutions. Having a fleet of HSMs across an enterprise can bring difficulties for centralized HSM management, often leading to HSMs not being used to their full potential. Cloud service providers and enterprises are demanding greater flexibility and scalability, simplicity of management and better value.

UTIMACO is covering all of these market needs with its u.trust Anchor CSAR solution, bringing one single platform for HSMs covering a variety of use cases. This platform can combine certified payment, custom firmware, and general-purpose usages on the same platform providing a crucial building block for future-proofing services.

## u.trust Anchor CSAR: Converged HSMAaaS

**u.trust Anchor CSAR is the world's first multi-tenant and converged cloud HSM platform for general purpose and payment use cases.**

It addresses multiple use cases and compliance mandates, leveraging the same underlying crypto service platform; enabling cloud service providers to offer HSM-as-a-Service or enterprises to use HSM-as-a-Service for internal security requirements. u.trust Anchor CSAR can run multiple containerized HSMs (cHSMs) instances concurrently, each with their own firmware stack, while simultaneously keeping all stacks entirely separated from each other in their respective cHSM ensuring true segregation and multi-tenancy. These firmware stacks can address various use cases and compliance mandates based on the business requirements. For example, PCI-compliant payment transaction processing, FIPS and Common Criteria compliant general purpose use cases, blockchain applications, authentication, key agreement in mobile networks, post-quantum crypto, and more.



## Highlights

### Multi-tenancy



**True Multi-tenancy** with strong separation of tenants

### Converged Platform



**Convergence** of general purpose and payment HSMs

### HSM Utilization



**Aggregation of HSM loads** and **scaling on demand**

### Compliance



**Various compliance requirements** on one platform

### Cost



**Reduce Total Cost Of Ownership**

### Location



**Service Provider-ready**

## Use Cases



Document Signing



Key Injection



Card Personalization



Code Signing



Key Management



DKE



PKI



Payment Transaction Processing



TLS

## Industries



Cloud Service Providers



Manufacturing and IoT



Banking and Financial Services



Government and Public Sector



Retail Industry



Telecommunication



Many more

# u.trust Anchor CSAR Solution

## Key features



### True multi-tenancy

Multi-tenancy with up to 31 truly independent and fully isolated containerized HSM instances with quality of service. Each instance is opaque, i.e., access to the administrative and cryptographic functionality is limited to the respective user only and ensures the required level of confidentiality for their sensitive data and keys.



### Convergence of general purpose and payment HSMs

The general purpose and payment use cases have varied requirements for firmware stacks to operate. The ability to combine certified payment, custom firmware, and general purpose usage on the same platform is a crucial building block for future-proof attractive service offerings. u.trust Anchor CSAR offer organizations a singular platform for a wide variety of use cases that is flexible, scalable, and simple.



### Scaling on demand

Based on the business requirements, your organization might need to increase or decrease the number of HSMs. u.trust Anchor CSAR enables the organization or cloud service providers to aggregate multiple HSM instances on their HSMs and shift instances based on the necessity of the business.



### Various compliance requirements on one platform

u.trust Anchor CSAR adheres to stringent certification and validation requirements enforced by various industries for general purpose and payment use cases to ensure that the security requirements are fulfilled. Some examples are FIPS 140-2, Common Criteria (CC EAL4+), and PCI HSM.



### Reduces total cost of ownership

Converging various use cases and dedicated interfaces into one service running on the same hardware and administered with the same operator interface reduces the total cost of ownership.



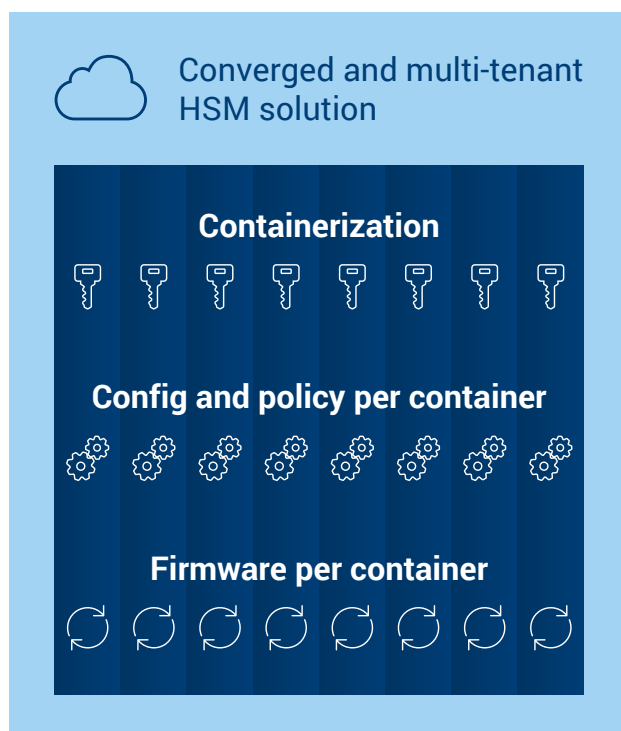
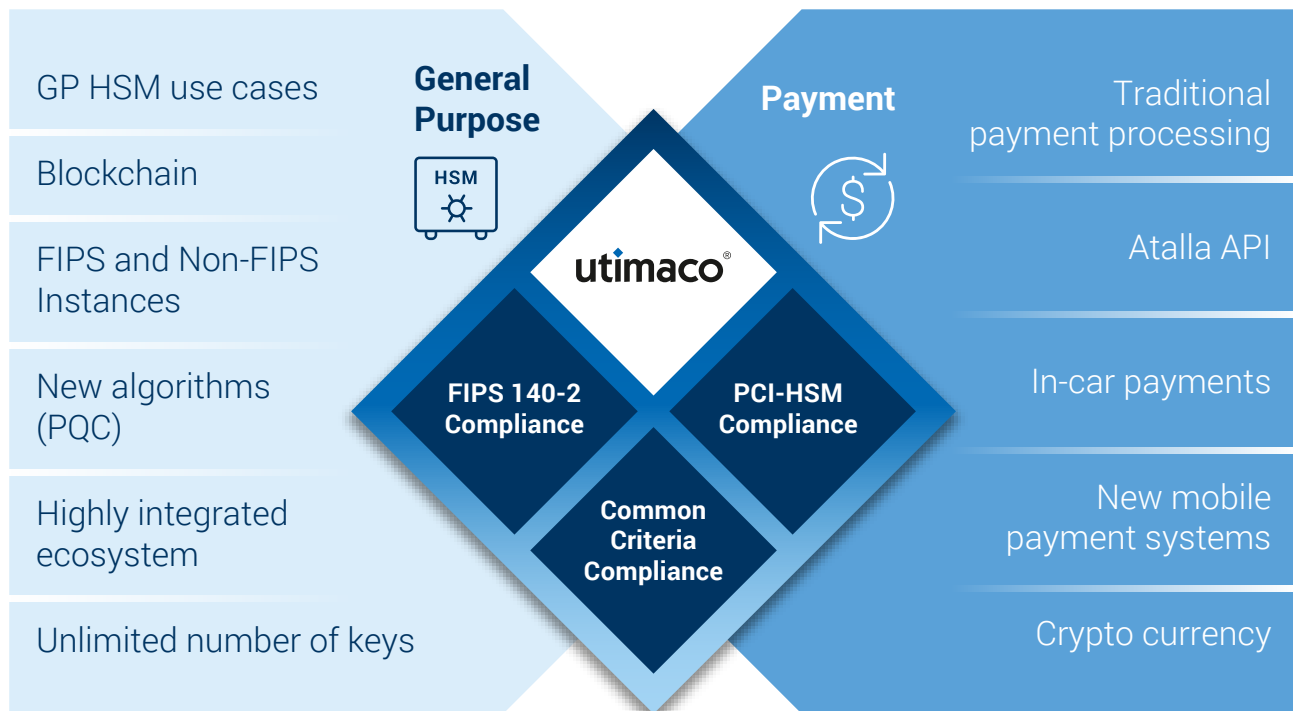
### Service Provider-ready

u.trust Anchor CSAR has been designed with the needs of Service Providers in mind. In addition to its container architecture, it features redundant system components and supports various network interfaces including modern fiber channel technology.



## Convergence and Multi-tenancy for general purpose and payment use cases

u.trust Anchor is the first converged and multi-tenant platform that enables service providers and enterprises to offer HSM as a Service (HSMaaS) for general purpose and payment use cases such as PKI, Code Signing and Payment Transaction Processing.



# Technical Specifications



UTIMACO  
u.trust Anchor



## Network Appliance



### Physical Dimensions

- ♦ **Form factor:** 19" 1U
- ♦ **Weight:** 22.05 lb (10 kg)
- ♦ **Width:** 17.56 in (446 mm) excluding brackets
- ♦ **Depth:** 21.79 in (533.4 mm) excluding handles
- ♦ **Height:** 1.73 in (44 mm)



### Connectivity

- ♦ **Interfaces:** 2 RJ45, 1 Gb/s
- ♦ 2 SFP+ 10Gb/s or 2 RJ45 1Gb/s network interfaces as optional extension



### Electrical Characteristics

- ♦ **Power Supply:** Redundant field-replaceable, 2 x 100 ~ 240 V AC, 50 ~ 60 Hertz, 300 W
- ♦ **Power Consumption:** typically 55 W / 78 VA, max. 65 W / 90 VA
- ♦ **Heat dissipation:** max. 222 BTU/h



### Operating Environment

- ♦ **Operating temperature:** +50°F to +122°F (+10°C to +50°C)
- ♦ **Operating relative humidity:** 10% to 95%, non-considering
- ♦ **Storage temperature:** +14°F to +131°F (-10°C to +55°C)
- ♦ **MTBF:** 134,250 hours, in acc. With Telcordia Issue 3, temperature 30°C, environment Ground Benign



### Certification / Compliance

- ♦ **Safety and Electromagnetic Compliance:** IEC/EN 60950-1, IEC/EN 62368-1, UL, CB Certificate, CE, FCC Class B
- ♦ **Environmental:** RoHS II, REACH
- ♦ **Security:** FIPS 140-2 Level 3



### Time Source

- ♦ DCF-77 or GPS receiver as optional extension



## PCIe Card



### Physical Dimensions

- ♦ **Form factor:** Half – length, full-height 4 lane, PCI Express Card
- ♦ **Compatibility:** PCIe 1.1, PCIe 2.0 and PCIe 3.0 slots
- ♦ **Height:** 0.74 in (18.6 mm)
- ♦ **Width:** 4.38 in (111.15 mm)
- ♦ **Depth:** 6.60 in (167.65 mm) excluding brackets
- ♦ **Weight:** 0.88 lb (0.4 kg)



### Connectivity

- ♦ **Interface:** PCIe x4



### Electrical Characteristics

- ♦ **Power Supply:** 3.3 V supplied by PCIe connector
- ♦ **Power consumption:** max. 25 W
- ♦ **Backup battery:** 3 V lithium battery, type CR2447



### Operating Environment

- ♦ **Operating temperature:** +50°F to +113°F (+10°C to +50°C)
- ♦ **Operating relative humidity:** 10% to 95%, non-considering
- ♦ **Storage temperature:** +14°F to +131°F (-10°C to +55°C)
- ♦ **MTBF:** 389,797 hours, in acc. with Telcordia Issue 3, temperature 30°C, environment Ground Fixed, temperature 50°C for parts in potting material



### Certification / Compliance

- ♦ **Safety and Electromagnetic Compliance:** IEC/EN 60950-1, IEC/EN 62368-1, UL, CB Certificate, CE, FCC Class B
- ♦ **Environmental:** RoHS II, REACH
- ♦ **Security:** FIPS 140-2 Level 3

# About UTIMACO

**UTIMACO is a global platform provider of trusted Cybersecurity and Compliance solutions and services with headquarters in Aachen (Germany) and Campbell, CA (USA).**

UTIMACO develops on-premises and cloud-based hardware security modules, solutions for key management, data protection and identity management as well as data intelligence solutions for regulated critical infrastructures and Public Warning Systems. UTIMACO is one of the world's leading manufacturers in its key market segments.

500+ employees around the globe create innovative solutions and services to protect data, identities and communication networks with responsibility for global customers and citizens. Customers and partners in many different industries value the reliability and long-term investment security of UTIMACO's high-security products and solutions.

Find out more on [utimaco.com](https://utimaco.com)



Headquarters Aachen, Germany



Headquarters Campbell, USA



# Contact us



## EMEA

### UTIMACO IS GmbH

📍 Germanusstrasse 4  
52080 Aachen,  
Germany

☎ +49 241 1696 200

✉ [hsm@utimaco.com](mailto:hsm@utimaco.com)

## Americas

### UTIMACO Inc.

📍 900 E Hamilton Ave., Suite 400  
Campbell, CA 95008,  
USA

☎ +1 844 UTIMACO

✉ [hsm@utimaco.com](mailto:hsm@utimaco.com)

## APAC

### UTIMACO IS Pte Limited

📍 6 Temasek Boulevard, #23-04  
Suntec Tower Four  
Singapore 038986

☎ +65 6631 2758

✉ [hsm@utimaco.com](mailto:hsm@utimaco.com)

For more information about UTIMACO® HSM products, please visit:

[utimaco.com](http://utimaco.com)

© UTIMACO IS GmbH 08/22 – Version 1.0

UTIMACO® is a trademark of UTIMACO GmbH. All other named trademarks are trademarks of the particular copyright holder. All rights reserved. Specifications are subject to change without notice.

Creating Trust in  
the Digital Society

**utimaco**®