



Hardware Security Module Comparison

By Features

29 September 2026

Version 2.00

Contact details:	Telephone: +61 2 6140 4494
	Email: sales@cogitogroup.net
© Cogito Group Pty Ltd 2026	
All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorisation of Cogito Group Pty Limited. Reproduction and use of all or portions of this publication is not permitted. No rights or permissions are granted with respect to this work.	

Contents

1	Overview.....	4
2	Description.....	5
2.1	What is a HSM.....	5
2.2	What is a Virtual HSM.....	5
2.3	Why Use a HSM.....	5
2.4	What is FIPS 140.....	6
2.4.1	FIPS 140 Levels.....	6
2.5	Limitations of this Comparison Document.....	6
2.6	Summary of How Each Device Family Operates.....	7
2.6.1	Thales Luna 8.....	7
2.6.2	Thales Luna 7.....	10
2.6.3	Thales Luna PCIe HSM 7.....	13
2.6.4	Thales Luna G7.....	13
2.6.5	Entrust nShield 5c.....	14
2.6.6	Entrust nShield XC.....	16
2.6.7	Entrust nShield 5s.....	18
2.6.8	Entrust nShield Solo.....	19
2.6.9	Entrust nShield Edge.....	20
2.6.10	Utimaco CryptoServer.....	22
2.6.11	Utimaco u.trust GP HSM Se-Series.....	23
2.6.12	Utimaco CryptoServer USB.....	24
2.6.13	YubiHSM 2 FIPS.....	24
2.6.14	Thales ProtectServer 3/3+.....	28
3	Other HSM Types and Providers.....	30
3.1	Other General Purpose HSM Vendors.....	30
3.1.1	Marvell LiquidSecurity (formerly Cavium).....	30
3.1.2	Futurex.....	30
3.1.3	Securosys.....	30
3.1.4	Crypto4A.....	31
3.1.5	Eviden (Atos) Trustway Proteccio.....	31
3.1.6	Fortanix.....	31
3.1.7	Nitrokey NetHSM.....	32
3.1.8	IBM.....	32
3.2	Cloud HSM Services.....	32
3.3	Smaller and Legacy Providers.....	33
3.4	Vendor Acquisitions.....	33
4	Benefits, Limitations and Specification Comparison.....	34
4.1	Benefits Table.....	34
4.2	Specification Matrix.....	38
5	Resources.....	44
5.1.1	Thales.....	44
5.1.2	Entrust.....	44
5.1.3	Utimaco.....	44
5.1.4	Yubi HSM.....	45
5.1.5	Other devices.....	45

1 Overview

This document is intended to assist with the selection of the right HSM for an organisation. The details in the document may change over time as the manufacturers change their product lines.

Thales, Entrust and Utimaco remain the mainstream general purpose HSM vendors. Thales and Entrust have the highest overall costs but have the widest support of all solutions. All three now support PQC algorithms and have FIPS 140-3 Level 3 validated platforms (Luna 7, nShield 5 and the u.trust GP HSM Se-Series) and all three have delivered or are delivering virtual (multi-tenant) HSM capability: the Utimaco Se-Series supports up to 31 isolated containers, Thales released the multi-tenant Luna 8 in October 2026 with limited availability, and Entrust has built the nShield 5 on a container-based architecture intended to support multi-tenancy. Total Cost of Ownership (TCO) is still generally lowest with Utimaco, thanks to no client, partition or ECC licence charges, but they have slightly less third party application support than Thales or Entrust. YubiHSM 2 has the lowest purchase cost and is now available in a FIPS 140-3 validated model, however, it has the lowest features, performance, capacity and support of all, and has no post-quantum algorithm support or means of adding it. The primary use case should be used to drive the best device for the specific requirement.

2 Description

2.1 What is a HSM

A Hardware Security Module (HSM) is specialised hardware that is designed specifically for processing cryptographic operations. HSMs can encrypt and decrypt information and can manage digital keys. They're made specifically to protect sensitive data.

The specialised hardware and software are often thoroughly tested and certified by third-party organisations against schemes such as Common Criteria and FIPS Federal Information Processing Standards, specifically in this case Publication 140-3.

2.2 What is a Virtual HSM

This is where one HSM chassis acts as multiple virtual HSMs. Virtual HSMs is a capability that has been offered for some time in the HSM as a Service market, but is relatively new to the mainstream HSM manufacturers in hardware available to customers. While Cavium (a first mover) released the LiquidSecurity HSM with virtual HSM back on 20 April 2015, and Utimaco had CryptoServer SE, which had a rudimentary form of virtual HSM back in 2014, both Thales and Entrust came later to the party. Utimaco's current u.trust GP HSM Se-Series supports up to 31 isolated containerised HSMs per device. Thales released the Luna 8 in October 2026 with limited availability, which can host up to 15 isolated HSM instances per crypto module (up to 30 per appliance with two crypto modules). As of writing, the Entrust nShield 5c is the hardware designed for virtual HSM (its firmware is container-based), but the availability of Entrust's multi-tenancy feature should be confirmed with Entrust before relying on it.

2.3 Why Use a HSM

There are two main benefits to using a HSM. The first is the security that they provide to digital cryptographic keys and the second is the performance that they can offer

Breaking this down further, some of the benefits of using HSM are:

- Meeting compliance requirements such as PCI DSS (Payment Card Industry Data Security Standard) for instance or Government regulations.
- Critical key protection such as the private key of a Certification Authority or a key used to encrypt or sign critical data. This is protected from:
 - Unauthorised copying of key material
 - Authorised copying in some instances where the key material must not be moved out of the HSM.
 - Physical and logical tamper resistance and showing evidence of tampering
 - Secure backup and High Availability without affecting security.
- Better and more secure key generation by using an certified Random Number Generator (RNG).
- Faster key generation and key operations than would be possible with other non specialised hardware or software.

2.4 What is FIPS 140

The 140 series of Federal Information Processing Standards (FIPS) are U.S. government computer security standards that specify requirements for cryptographic modules, providing four increasing qualitative levels intended to cover a wide range of potential applications and environments.

FIPS 140-3 is the latest iteration for validating the effectiveness of cryptographic hardware, aligns with international [ISO/IEC 19790 standards](#) and introduces new security enhancements (over FIPS 140-2) including:

- Requirement for multifactor authentication at level 4
- Stricter integrity test requirements
- Key zeroization is required for ALL unprotected “Sensitive Security Parameters” (SSP) at all levels, including public keys
- Roles, services, and authentication: must be met by a cryptographic module’s implementation (not through policy, rules, etc.), for example password size restrictions.
- Lifecycle assurance: vendors need to demonstrate adequate internal testing on a module, in addition to the validation lab testing

FIPS 140-2 has been replaced by FIPS 140-3. On 21 September 2026 the NIST Cryptographic Module Validation Program (CMVP) moved all remaining FIPS 140-2 certificates to the Historical list. Modules on the Historical list should not be included in new procurements by U.S. federal agencies, although agencies may continue to use them in existing systems. Any new requirement for “FIPS validated” hardware should therefore be read as FIPS 140-3, and it is important to check that the specific firmware version in use is the validated version.

2.4.1 FIPS 140 Levels

The FIPS certification standard defines four increasing, qualitative levels of security:

- Level 1: Requires production-grade equipment and externally tested algorithms.
- Level 2: Adds requirements for physical tamper-evidence and role-based authentication. Software implementations must run on an Operating System approved to Common Criteria at EAL2 or the equivalent protection profile
- Level 3: Requires physical tamper-resistance and identity-based authentication. There must also be physical or logical separation between the interfaces by which “critical security parameters” enter and leave the module. Private keys can only enter or leave in encrypted form
- Level 4: Makes the physical security requirements more stringent. Requires the ability to be tamper-active, erasing the contents of the device if it detects various forms of environmental attack.

From an operational perspective level 3 is a good compromise between effective security, operational convenience.

2.5 Limitations of this Comparison Document

While there are numerous vendors of HSMs, this document compares a limited number of vendors products. It is limited to a list of devices we actively support and supply to customers for the following reasons:

- Product Support is a key factor linked to market share. Thales, Entrust and Utimaco would make up more than 90% of the market. This high market share drives third parties to integrate first with Thales

and Entrust, then other vendors depending on region. Greater third party product support gives greater flexibility in how they can be used now and in the future. We encourage customers to consider future growth, and as such we highly recommend one of these three products due to the greater possibility of finding support for their product with vendors.

- Accreditations, and history of accreditations, is also an important factor in determining which devices to list. Most of our customers require at least FIPS 140, and all of the listed devices meet this criterion.
- Longevity of the product indicates a tried and true product that hopefully has constant, but an iterative approach to improving the platform. This gives great assurance of long-term support of the product as well as by third party products. It also gives some assurance that the product is less likely to suffer from large scale security issues. Newer device issues are best demonstrated by the revolutionary (at the time) approach of Fortanix using the Intel SGX capability. [Fortanix's use of SGX had a large number of side channel attacks](#) found not long after they started. This shows that new approaches in this space sometimes lead to benefits but sometimes lead to very poor outcomes too.
- Longevity in the market is another consideration, which the Cavium platform and company demonstrates. Cavium as a company is no longer and the product has been purchased by [Marvell](#) with the product now called [Liquid Security](#) they are no longer Cavium and security. This can lead to orphaned product sets. Marvell has since continued the line with LiquidSecurity 2, which now underpins several hyperscale cloud HSM services, so in this case the product survived the change of ownership, but customers were still exposed to the risk.
- To provide the best possible advice, training and support to customers we must know the devices we are evaluating.
- We must know the devices we are comparing intimately. This can only be done with the devices we know well.

2.6 Summary of How Each Device Family Operates

Below is a summary of the how each of the various brands operate at a high level.

2.6.1 Thales Luna 8

Luna 8 is the next generation of the Luna network HSM, announced by Thales on 4 August 2026. It is the first product on the new Thales HSM platform and is built around a custom, Thales designed cryptographic processor. Thales positions it as its fastest HSM to date, with native post-quantum cryptography (PQC) support and a multi-tenant architecture. At launch it is only available as a network appliance; PCIe, USB and Luna Cloud HSM versions are planned for future releases. Luna 7 remains available for existing customers.

A key differentiator from Luna 7 is true multi-tenancy. Each appliance contains one or two independent crypto modules, and each crypto module can host up to 15 isolated Luna 8 HSM instances (secure containers), giving up to 30 HSM instances per appliance, each with guaranteed Quality of Service. Different Luna 8 firmware versions can run in different containers on the same hardware, and new instances can be created on demand.

2.6.1.1 Models

The Luna 8 Network HSM is available in three models based on performance, key capacity and number of supported containers: the Luna 100 (Standard Performance), Luna 150 (Enterprise Performance) and Luna 190 (Maximum Performance), mirroring the Luna 7 A700/A750/A790 range. Each secure container hosts an isolated Luna 8 HSM instance supporting up to 10 partitions. The Luna 8 product brief (July 2026) lists the key storage and container counts below. Thales has not published per-model transaction rates, so performance figures should be obtained from Thales before sizing a deployment.

Luna 8 Network HSM models

	Luna 100 (Standard Performance)	Luna 150 (Enterprise Performance)	Luna 190 (Maximum Performance)
Key storage	128 MB	1,024 MB	4,096 MB
Containers (HSM instances)	1	Up to 6	Up to 15
Maximum partitions	10	Up to 60	Up to 150
Performance	Not published	Not published	Not published

Source: Thales Luna 8 Network HSM Product Brief. Partition totals are derived from the stated limit of 10 partitions per container. Container counts appear to be per crypto module; a dual-module appliance can host up to 30 HSM instances. Unlike Luna 7 there are no separate password (A) and PED (S) series, as quorum (M of N) and multi-factor authentication are standard. Network connectivity is 4 x 10G SFP+ ports plus a 1G BMC management port.

2.6.1.2 Key Storage:

Luna 8 continues the Luna approach of keeping keys inside tamper-resistant hardware, with partitions used to segregate keys and access to them. Keys continue to be backed up in hardware using the Luna Backup HSM. Thales states that migration capabilities are provided for existing Luna 7 key material, and that existing applications continue to work through the Luna HSM Universal Client.

2.6.1.3 Availability

Luna 8 is backwards compatible with the Luna HSM Universal Client, so High Availability is expected to be configured in the same way as Luna 7 (client-managed HA groups), and the same caveats regarding monitoring of HA members apply. Luna 8 HA has not yet been tested by Cogito.

2.6.1.4 Key Backup

Keys are backed up hardware to hardware using the Luna Backup HSM, and Thales describes Luna 8 backup and restore as quantum-safe. As with Luna 7, key material never leaves Luna hardware in plaintext. Thales has not yet stated which Luna Backup HSM models and firmware versions are supported with Luna 8, or how backup works per container, so compatibility with existing Luna Backup HSM 7 units should be confirmed with Thales before deployment. HA group members keep a live copy of keys on other HSMs, but replication is not a substitute for an offline backup, as deletions and corruption are replicated too.

2.6.1.5 Security

At the time of writing Luna 8 is not yet certified. Thales lists FIPS 140-3 Level 3, Common Criteria, QSCD listing for eIDAS 2, Brazil INMETRO, Singapore NITES and NATO SECRET approval as in process. Organisations that must use a FIPS 140-3 validated module today should continue to use Luna 7 (certificate #4684) until the Luna 8 validation appears on the NIST CMVP list or get authorisation to use

Luna 7 firmware within a module of the Luna 8. This does not make the unit FIPS validated, but does bridge some of the gap to that requirement. Security features on the Luna 8 include quorum (M of N) authorisation, multi-factor authentication, multiple roles for separation of duties, side-channel protection for the custom crypto processor, device attestation, secure audit logging, a dual on-board entropy source including a quantum random number generator (QRNG), and support for an external entropy source.

2.6.1.6 Performance

Thales describes Luna 8 as its fastest HSM ever, claiming up to 10 times faster performance for traditional algorithms and up to 100 times faster performance for PQC algorithms (ML-DSA and ML-KEM) than the previous generation, and 20 times better energy efficiency per transaction. These are vendor claims, and independent benchmark figures were not available at the time of writing.

2.6.1.7 Support

Luna 8 inherits the Luna ecosystem, and Thales cites hundreds of existing Luna 7 integrations that support migration. APIs and CLI tools are provided for automation, monitoring and logging integrations, and the Luna Client can run in a container. As a brand new platform, customers should confirm that the specific third party integrations they rely on have been validated against Luna 8, and should expect early firmware releases to mature over time.

2.6.1.8 Costs

Pricing and licensing for Luna 8 had not been published at the time of writing. Given the multi-tenant design, customers should confirm how Thales licenses HSM instances, partitions and clients on Luna 8 compared with the Luna 7 Client Access Licence (CAL) and partition licence model.

2.6.1.9 PQC Support

Yes, natively. PQC is built into the Luna 8 custom crypto processor rather than added through firmware extensions. The product brief lists ML-KEM (FIPS 203) and ML-DSA (FIPS 204), with high throughput optimisation for ML-DSA-65 and ML-KEM-768, plus the stateful hash-based signature schemes LMS and HSS (NIST SP 800-208). The platform also uses quantum-safe mechanisms internally, including quantum-safe firmware updates, HA failover and hardware-to-hardware backup and restore, and it includes a quantum random number generator (QRNG) as one of its entropy sources.

Example uses: issuing ML-DSA certificates from a PQC or hybrid CA, and high volume ML-KEM key establishment. As Luna 8 is not yet FIPS 140-3 validated, its PQC algorithms cannot currently be used in a FIPS validated configuration.

Luna 8 compared to Luna 7

Feature	Luna 8 (Luna 100 / 150 / 190)	Luna 7 (A/S700, 750, 790)
Released	October 2026	2017 (still available, firmware 7.9.x)
Form factors	Network appliance (PCIe, USB and cloud planned)	Network, PCIe, USB (G7) and Backup HSM
Crypto processor	Custom Thales designed processor	Luna K7 cryptographic module
Multi-tenancy	Up to 15 isolated HSM instances per crypto module, up to 30 per appliance, each with up to 10 partitions	Partitions only (5, 20 or 100 depending on model)
Post-quantum	Native, hardware accelerated ML-DSA and ML-KEM	ML-KEM and ML-DSA from firmware 7.9

Feature	Luna 8 (Luna 100 / 150 / 190)	Luna 7 (A/S700, 750, 790)
FIPS 140-3 Level 3	In process	Validated (certificate #4684)
Common Criteria / eIDAS QSCD	In process	Certified
Key storage	Onboard	Onboard, plus Scalable Key Storage (SKS)
Status	Current flagship	Available for existing customers

2.6.2 Thales Luna 7

Thales Luna 7 became a Thales product through Thales' acquisition of Gemalto, which acquired SafeNet, which in turn had acquired Rainbow Technologies which had earlier acquired Chrysalis- ITS.

The Luna 7 A/S series are networked HSMs that supersedes the Luna 6, 5 and older models. These devices are now owned by Thales, but before this the Luna Series was sold under the Gemalto banner and before that under the SafeNet banner. Since October 2026 the Luna 7 has been succeeded by the Luna 8 network HSM, although Luna 7 remains available for existing customers.

2.6.2.1 Models

Historically (up to and including Luna 6) came in SA and SP versions and at two speeds being 1700 and 7000. The SA version did not allow customer code execution whereas the SP allowed for this.

The Luna 7 HSMs come in six (6) models, three of which are the password only versions being the A700, A750 and A790. There are another three versions with the same specification except that they support Multi-Factor Authentication through a Pin Entry Device (PED). Those models are the S700, S750 and S790. All have been validated against FIPS 140-3 Level 3 (NIST certificate #4684, listed as the Luna K7 Cryptographic Module) and were previously validated against FIPS 140-2 Level 3¹. The higher the model number the higher the performance and memory available for keys and partitions.

2.6.2.2 Key Storage:

Luna devices are designed to primarily store keys internally to the device. Previous models such as the Luna 5/6 could only store keys internally, although they could use Thales key management capability to allow for greater volumes of keys to be stored with a master key.

Luna devices have a concept of partitions to logically separate the key storage. This allows Luna devices to entirely segregate keys and access to them from one another.

The various models have differing memory, processing speeds and partition numbers onboard with the smallest having 5 partitions and the largest up to 100 partitions. Due to the different memory installed in the different models there is no ability to upgrade or downgrade a device.

From Luna 7 you can also store keys externally to the device without dedicated key management services. This feature is known as **Scalable Key Storage (SKS)** and addresses a key advantage seen in some other HSM models.

¹ Luna 7 FIPS 140-2, Level 3 validation <https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3205.pdf> Luna 7 FIPS 140-3 Level 3 validation (certificate #4684) <https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/4684>

2.6.2.3 Availability

High Availability (HA) is provided through the universal client and the concept of HA Partitions. HA partitions are effectively virtual partitions and use an underlying physical partition on each device in the HA capability. The universal client managing the HA means that a device can be effectively managed on a per client basis. This has some down sides however. If a client is not set up with HA, keys are created and then HA is enabled, the keys are not replicated between the two physical partitions until a separate command is run. Another issue is that without monitoring on these partitions the first knowledge that one of the HA devices has failed can be the failure of the second device. A solution to this is to use SNMP traps to provide notification of any issues.

2.6.2.4 Key Backup

Because keys are held inside the HSM, backup relies on the Luna cloning protocol, which only copies objects between Luna HSMs that share the same cloning domain, so key material never leaves Luna hardware in plaintext. The standard method is the Luna Backup HSM 7, a separate USB-attached device (FIPS 140-3 Level 3, certificate #4962) that can be connected directly to the appliance, or to a client workstation and used remotely through the Remote Backup Service (RBS). Backups are taken offsite by physically moving the Backup HSM, which is why the benefits table shows Luna as requiring separate backup tokens. Luna Backup HSM 7 firmware 7.9.3 supports quantum-safe backup and restore of both classical and PQC keys. The older Luna Backup HSM G5 reached end of life on 30 September 2026.

The cloning domain is set when a partition is initialised (a domain secret on password-authenticated A series HSMs, or a red PED key on PED-authenticated S series HSMs), and backups can only be restored to partitions in the same domain. The domain secret or red PED keys are therefore critical recovery items and must be protected and stored separately from the Backup HSM. Keys held using Scalable Key Storage (SKS) are stored outside the HSM encrypted under an SKS master key, so they can be covered by normal file backups provided the SKS master key is itself backed up. HA groups keep a synchronised copy on other HSMs but are not a substitute for a backup.

2.6.2.5 Security

The HSM can run in up to FIPS 140-3 Level 3, provided a FIPS 140-3 validated firmware version is installed and the HSM is set to FIPS approved configuration. The Luna HSM ethos of onboard key storage is a foundational component to how they seek to secure keys. This approach also offers a way to provide granular access to key storage as well. The lowest level of authentication is performed at the partition level allowing for the HSM to be treated in essence like a number of virtual HSMs. The Luna 7 can also be specified with strong multifactor authentication in the form of a PED (Pen Entry Device) and PED keys on the S series. It also has the ability to provide M of N (multiple factors) as part of this.

2.6.2.6 Performance

When released, the Luna 7 was one of the fastest HSMs available, but they have now been superseded by the Luna 8 (October 2026) and are outperformed by a number of other models, with higher transactions per second (tps) measured over RSA 2048 bit key use. Examples include the nShield 5c/s, Marvell LiquidSecurity (formerly Cavium) models (with 30,000 tps vs Luna A/S790 at 10,000 tps) and the most recent Utimaco version (at 40,000 tps vs Luna A/S790 at 10,000 tps). An advantage to some customers is the on-board key storage but from Luna v7 they also offer a [Scalable Key Storage \(SKS\)](#) option. An issue with on-board key storage is that complicates backup. It requires specialist backup units to be used. Onboard storage also sets a hard limit to how many keys can be stored on a device, limiting it to the

onboard memory of the unit. Performance and specifications of the series can be found on the Thales Website [here](#). More information is below.

Table 1 - Luna A/S Series Specifications

Standard Performance A700	Enterprise Performance A750	Maximum Performance A790
2 MB Memory	16 MB Memory	32 MB Memory
Maximum Partitions: 5	Maximum Partitions: 20	Maximum Partitions: 100
Performance: RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	Performance: RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	Performance: RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps
Standard Performance S700	Enterprise Performance S750	Maximum Performance S790
2 MB Memory	16 MB Memory	32 MB Memory
Maximum Partitions: 5	Maximum Partitions: 20	Maximum Partitions: 100
Performance: RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	Performance: RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	Performance: RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps

2.6.2.7 Support

The Luna series (along with the nShield) are the most prolific general purpose HSMs available. This gives them great product support within software and hardware items.

2.6.2.8 Costs

In terms of costs, Thales charge for both Client Access Licences (CALs) and Partition Licences for Luna devices, but do not charge for ECC use. The CAL is also per client not per HSM accessed reducing costs where more than one HSM is provided for HA purposes for example. Accessories are generally quite expensive even compared to other HSMs manufacturers.

2.6.2.9 PQC Support

Yes, through firmware. Luna HSM firmware 7.9 (mid 2025) added native ML-KEM (FIPS 203) and ML-DSA (FIPS 204) to the core firmware, removing the need for separate functionality modules. Firmware 7.9.1 added PQC key wrapping and unwrapping (for key import and export with third party systems), multi-part LMS and HSS signing for large code and firmware signing jobs, and attestation of PQC keys. Luna appliance software 7.9.1 added hybrid ML-KEM key exchange for NTLS, SSH and the REST API, and Universal Client 10.9.4 (September 2026) added ML-DSA to the Luna Key Storage Provider, so Microsoft AD CS can issue quantum-safe certificates.

Note that the current FIPS 140-3 certificate (#4684) covers pre-7.9 firmware. Thales describes firmware 7.9.2 as the next FIPS candidate with PQC, so until that validation is published, using PQC on Luna 7 means running firmware that is not yet in a validated configuration. PQC is not accelerated in hardware on Luna 7, which is one of the main reasons Thales gives for Luna 8.

2.6.3 Thales Luna PCIe HSM 7

These HSMs replicate the models, features and performance of the Luna 7 series differing only in the fact that they are PCIe, rather than network based. The Luna PCIe HSM 7 is FIPS 140-3 Level 3 validated under the same certificate (#4684). A Luna 8 PCIe version is planned but not yet available.

2.6.3.1 Key Backup

Backup works in the same way as the Luna Network HSM 7, by cloning to a Luna Backup HSM 7 connected to the host server, or remotely using the Remote Backup Service.

2.6.3.2 PQC Support

Yes. The Luna PCIe HSM 7 runs the same firmware as the Luna Network HSM 7, so it gains the same ML-KEM, ML-DSA and LMS/HSS support from firmware 7.9, with the same caveat that the PQC capable firmware is not yet FIPS 140-3 validated.

2.6.4 Thales Luna G7

The Luna G7 is a USB HSM that replaces the G5. The older Luna G5 USB and Backup HSMs reached end of life on 30 September 2026, so any remaining G5 units should be replaced. A Luna 8 USB version is planned but not yet available.

A key differentiator from some other HSM models is that key storage on a G7 is only onboard. All Luna devices maintain a concept of partitions to logically separate the key storage.

2.6.4.1 Models

The Luna G7 HSM come in one model only, but they can support Password or Multi-Factor Authentication through a Pin Entry Device (PED).

2.6.4.2 Key Storage:

Luna G7 devices are designed to store keys internally to the device. The Luna device has a concept of partitions to logically separate the key storage. This allows Luna devices to entirely segregate keys and access to them from one another.

2.6.4.3 Availability

There is no HA option although manual backup and replication is possible between devices.

2.6.4.4 Key Backup

The G7 is backed up in the same way as other Luna 7 HSMs, by cloning its partition to a Luna Backup HSM 7 (or another G7) in the same cloning domain. This is a common arrangement for an offline root CA, with both the G7 and the Backup HSM locked away when not in use, ideally in separate locations. Luna Backup HSM 7 firmware 7.9.3 supports quantum-safe backup and restore of both classical and PQC keys.

2.6.4.5 Security

The HSM can run in up to FIPS 140-3 Level 3 (NIST certificate #4962, listed as the Luna G7 Cryptographic Module, which also covers the Luna Backup HSM 7). The Luna HSM ethos of onboard key storage is a foundational component to how they seek to secure keys. This approach also offers a way to provide granular access to key storage as well. The lowest level of authentication is performed at the partition level. The Luna G7 can also be specified with strong multifactor authentication in the form of a PED (Pen Entry Device) and PED keys on the S series. It also has the ability to provide M of N (multiple factors) as part of this.

2.6.4.6 Performance

This device is a low powered unit designed for offline or test capability.

2.6.4.7 Support

The Luna series (along with the nShield) are the most prolific general purpose HSMs available. Unlike the G5, the G7 successor USB HSM does support the ESXi virtualised platform with HSM pass through, but not other hypervisors.

2.6.4.8 Costs

Luna G7 units are relatively expensive compared to the competition but can be purchased in a bundle of 2 units to reduce the cost.

2.6.4.9 PQC Support

Yes. Luna USB HSM 7 firmware 7.9.2 supports ML-KEM and ML-DSA, including PQC key wrapping, PQC cloning cipher suites and PQC key attestation, and Luna Backup HSM 7 firmware 7.9.3 (September 2026) adds hybrid quantum-safe backup and restore of both classical and PQC keys. With these releases Thales states it is the first vendor to support PQC across network, PCIe and USB form factors, which makes the G7 a practical option for an offline PQC root CA.

2.6.5 Entrust nShield 5c

The nShield 5 series is the latest networked HSM that replaces XC series HSMs. The Edge is a USB HSM and the Solo is a PCI HSM. The nShield 5 HSM operates with three (3) models of differing performance being the Base, Mid and High. A 10 Gigabit variant, the nShield 5c 10G, is also available with four SFP+ ports.

A key differentiator for this HSM model is cloud support (where) there is a concept through their security world capability to treat the HSM as multiple virtual HSMs. Another is that they are one of the first devices to have released a PQC capable HSM that is FIPS certified.

2.6.5.1 Models

The Entrust HSMs come in three (3) models. These are Base, Mid and High. All have been validated against FIPS 140-3 Level 3 and Common Criteria EAL4+. The higher the model number the higher the performance of the device. FIPS 140-3 Level 3 validation was announced in August 2024.

2.6.5.2 Key Storage:

The on-client key storage allows a greater number of keys to be stored than a HSM storing keys on board. Due to the on-client storage model the backups of keys, HSM configurations, and authentication components (Cardsets and Softcards) can be handled by existing backup and recovery procedures and often requires minimal modification to a Business Continuity Plan or Disaster Recovery procedure. The on-client model provides a clear separation of the keys accessible by a client machine.

2.6.5.3 Availability

High Availability (HA) is yet to be tested by Cogito, but a major disadvantage in their HSM has been resolved now since the previous series, according to the Entrust team. This is where, on a device going offline and coming back online, the client accessing it would require the service to be restarted before the return of the device would be recognised.

2.6.5.4 Key Backup

nShield backup is based on the Security World. Application keys are stored on the client as encrypted key blobs in the Key Management Data (kmdata) directory, protected by the Security World key and by the Operator Card Set or softcard associated with each key. These files can be backed up with existing file backup tools and copied to other hosts; they are useless without an HSM enrolled in the same Security World. To recover from an HSM failure, a new or replacement HSM is enrolled into the Security World using a quorum of the Administrator Card Set (ACS), so no separate backup HSM is required.

The ACS is the critical recovery item: if a quorum of ACS cards (or their passphrases) is lost, the Security World cannot be restored onto new hardware and the keys are effectively lost. ACS cards, their passphrases and at least one current copy of the kmdata directory should be kept in separate secure locations. Keys using module-only protection can be loaded by any HSM in the Security World without operator cards, which is convenient but provides weaker protection.

2.6.5.5 Security

The on client key storage allows the use of existing backup mechanisms. It does however mean that the keys are not stored in the device itself, but rather on the client in an encrypted form.

2.6.5.6 Performance

The 5c model is new to the market. This is reflected in performance of the highest 5c model, which exceeds Luna 7 performance and most of the Utimaco range, with the exception of the Utimaco u.trust GP HSM Se15k and Se40k models. How it compares with the new Luna 8 is not yet known. A key benefit over the Luna in terms of performance however is that the devices can be upgraded in the field, as unlike the Luna the hardware is the same and only a licence file is required to unlock extra performance. More performance information on old and new models can be found on the Entrust website².

nShield 5c models	Base	Mid	High
RSA signing performance (tps) for NIST recommended key lengths			
2048 bit	580	3,460	11,680
4096 bit	110	680	2,050
ECC prime curve signing performance (tps) for NIST recommended key lengths			
256 bit	2,070	7,530	23,890
Key generation (keys/sec)			
RSA 2048 bit	10	50	70
ECDSA P-256 bit	2,060	3,700	3,790
ECDSA P-521	860	3,040	3,090
Client licenses			
Included	3	3	3
Maximum	10	20	1,000

Figures above are from the current Entrust nShield 5c data sheet (firmware 13.8.3 in hybrid hardware accelerated mode, lab conditions). The same data sheet lists ML-DSA-65 signing at 270, 620 and 2,160 tps for the Base, Mid and High models respectively. From Security World v13.6 onwards client licences are counted as simultaneous active connections.

² Entrust nShield Tech Specs <https://www.entrust.com/sites/default/files/documentation/datasheets/dps-entrust-nshield-5c-ds.pdf>

2.6.5.7 Support

The nShield series (along with the Luna) are the most prolific general purpose HSMs available. This gives them great product support. Another benefit in the support arena is the aforementioned ability to field upgrade their performance. Remote management is another feature that Entrust believes separates their product from other products on the market.

2.6.5.8 Costs

The nShield 5c series charge for Client Access Licences (CALs). The CAL is charged per client and per HSM accessed increasing costs where more than one HSM is provided for HA purposes for example. All nShield variants charge for ECC support. Both CALs and ECC licences also attract ongoing maintenance fees. This arrangement makes the nShield one of the most expensive options where a large number of clients are using the HSMs.

Accessories are also expensive. The standard smartcards provided with the units are not able to be used remotely and specialist remote smartcards must be used; remote smartcards may also be used locally.

2.6.5.9 PQC Support

Yes. Entrust first offered draft PQC algorithms in 2022 through the Post-Quantum Option Pack, which runs inside the HSM using the CodeSafe secure execution environment. ML-DSA was then released in firmware in 2025, and Security World v13.9 exposes ML-DSA-44, ML-DSA-65 and ML-DSA-87 through PKCS#11 (firmware 13.8 or later with the PostQuantum feature enabled), and adds ML-KEM (FIPS 203) and SLH-DSA (FIPS 205) through the nCore API. The nShield 5c has a field-programmable crypto accelerator that supports PQC in hardware; the current data sheet quotes ML-DSA-65 signing at 270, 620 and 2,160 tps for the Base, Mid and High models. Stateful schemes such as LMS remain available through the Post-Quantum Option Pack.

Example uses: ML-DSA certificate issuance and code signing via PKCS#11. Customers should check whether the PQC mechanisms they intend to use are within the scope of the FIPS 140-3 validated firmware.

2.6.6 Entrust nShield XC

When the nShield XC was the newest HSM from Thales, the hardware company nCipher was spun out of Thales as part of an Entrust purchase. This means that Thales had recently owned both the largest and 2nd largest HSM manufacturers, but not at the same time. The Entrust purchase of nCipher from Thales was after Thales purchased UK based nCipher back in 2008. The nCipher name was retired by Thales in favour of their own only to return so that the business unit could be sold to enable them to buy Gemalto without falling foul of anti-competition organisations in numerous countries.

The nShield XC series is a networked HSM that replaces the Connect 1500 and 6000 series HSMs. The Edge is a USB HSM and the Solo is a PCI HSM. The nShield XC HSM operates with three (3) models of differing performance being the Base, Mid and High. Entrust ended sale of the nShield Connect XC and Solo XC (excluding Common Criteria specific versions) on 31 October 2025, and mainstream support, including firmware updates, ends on 31 December 2027. The nShield 5c and 5s are the direct replacements, and XC units can operate in a mixed Security World with nShield 5 units to ease migration.

A key differentiator from some other HSM models is the concept of a security world for key storage. The actual key storage occurs encrypted on the server that will utilise the keys and they are passed into the HSM for unwrapping and use when they are needed.

2.6.6.1 Models

The Entrust HSMs come in three (3) models. These are Base, Mid and High. All have been validated against FIPS 140-2 Level 3. The higher the model number the higher the performance of the device. These FIPS 140-2 certificates moved to the NIST Historical list on 21 September 2026, so the XC is not suitable for new deployments that require FIPS validation.

2.6.6.2 Key Storage:

The on-client key storage allows a greater number of keys to be stored than a HSM storing keys on board. Due to the on-client storage model the backups of keys, HSM configurations, and authentication components (Cardsets and Softcards) can be handled by existing backup and recovery procedures and often requires minimal modification to a Business Continuity Plan or Disaster Recovery procedure. The on-client model provides a clear separation of the keys accessible by a client machine.

2.6.6.3 Availability

High Availability (HA) until the XC (6000 series) was poor. While HA was said to be available, on a device going offline and coming back online, the client accessing it would require the service to be restarted before the return of the device would be recognised. This has now been resolved in later versions of the firmware/software that can be applied to both XC and 6000 models.

2.6.6.4 Key Backup

Backup works in the same Security World based way as the nShield 5c (kmdata files plus the Administrator Card Set). As XC and nShield 5 HSMs can operate in a mixed Security World, subject to Security World version requirements, the existing Security World and its backups are the main mechanism for migrating keys from the XC to nShield 5.

2.6.6.5 Security

The on client key storage allows the use of existing backup mechanisms. It does however mean that the keys are not stored in the device itself, but rather on the client in an encrypted form.

2.6.6.6 Performance

The signing performance of the highest XC model is better than the highest Utimaco CyrptoServer model, however, is not as good as the Luna or the higher performance Utimaco u.trust Anchor models. A key benefit over the Luna in terms of performance however is that the devices can be upgraded in the field, as unlike the Luna the hardware is the same and only a licence file is required to unlock extra performance. More performance information on old and new models can be found on the Entrust website³. Performance specifications can be found [here](#).

nShield Connect models	XC Base	XC Mid	XC High
RSA signing performance (tps) for NIST recommended key lengths			
2048 bit	430	3,500	8,600
4096 bit	100	850	2,025
ECC prime curve signing performance (tps) for NIST recommended key lengths			
256 bit	680	7,5152	14,4002
Symmetric encryption (KB/sec) 1024 byte plain text			

³ Entrust nShield Tech Specs <https://www.entrust.com/digital-security/hsm/products/nshield-hsms/nshield-connect>

nShield Connect models	XC Base	XC Mid	XC High
AES 128 bit	825	7,700	11,300
AES 256 bit	795	7,700	9,700
Key generation with ECC activation (keys/sec)			
RSA 2048 bit	6.0	6.2	7.3
ECDSA P-192 bit	110	650	1,050
ECDSA P-256 bit	100	630	1,050
ECDSA P-521	65	480	710
Client licenses			
Included	3	3	3
Maximum	10	20	Unlimited but requires enterprise licence.

2.6.6.7 Support

The nShield series (along with the Luna) are the most prolific general purpose HSMs available. This gives them great product support.

2.6.6.8 Costs

The nShield XC series charge for Client Access Licences (CALs). The CAL is charged per client and per HSM accessed increasing costs where more than one HSM is provided for HA purposes for example. All nShield variants charge for ECC support. Both CALs and ECC licences also attract ongoing maintenance fees. This arrangement makes the nShield one of the most expensive options where a large number of clients are using the HSMs.

Accessories are also expensive. The standard smartcards provided with the units are not able to be used remotely and specialist remote smartcards must be used; remote smartcards may also be used locally.

2.6.6.9 PQC Support

Partial. Entrust released ML-DSA in firmware for the nShield XC in 2025, and the Post-Quantum Option Pack (CodeSafe) supports the XC for LMS and other algorithms. However, the XC has no PQC hardware acceleration, it is past end of sale, it only holds FIPS 140-2 (historical) certificates, and firmware updates end on 31 December 2027, so it should not be selected for a PQC migration.

2.6.7 Entrust nShield 5s

These HSMs replicate the models, features and performance of the Entrust nShield 5c series differing only in the fact that they are PCIe, rather than network based.

2.6.7.1 Models

The Entrust nShield 5s HSM comes in Base, Mid and High models and has the same certifications as the 5c.

2.6.7.2 Key Storage:

Keys are stored in exactly the same way as the Entrust nShield 5c series of HSMs.

2.6.7.3 Availability

No High Availability (HA) is provided by this device, but the key storage on the client means that any edge in the security world can be used with the correct cards to perform key operations.

2.6.7.4 Key Backup

Backup works in exactly the same way as the nShield 5c, with key blobs stored on the host server and backed up with it, and recovery relying on the Administrator Card Set.

2.6.7.5 Security

As the 5s works in exactly the same way as the 5c, except it is PCIe rather than networked, the security considerations are exactly the same.

2.6.7.6 Performance

The 5s has the same performance as the 5c.

2.6.7.7 Support

The nShield series (along with the Luna) are the most prolific general purpose HSMs available. This gives them great product support.

2.6.7.8 Costs

The HSM has similar costs as the 5c it is based on.

2.6.7.9 PQC Support

Yes. The nShield 5s has the same PQC support as the nShield 5c (ML-DSA in firmware and PKCS#11, ML-KEM and SLH-DSA via nCore in Security World v13.9, and the Post-Quantum Option Pack via CodeSafe 5).

2.6.8 Entrust nShield Solo

These HSMs replicate the models, features and performance of the Entrust nShield XC series differing only in the fact that they are PCIe, rather than network based. As with the Connect XC, the Solo XC reached end of sale on 31 October 2025 and its end of maintenance date is 31 December 2027.

2.6.8.1 Models

The Entrust nShield Solo HSM comes in Base, Mid and High models. The HSM has been validated against FIPS 140-2 Level 3⁴. This FIPS 140-2 certificate is now on the NIST Historical list.

2.6.8.2 Key Storage:

Keys are stored in exactly the same way as the Entrust nShield XC series of HSMs.

2.6.8.3 Availability

No High Availability (HA) is provided by this device, but the key storage on the client means that any edge in the security world can be used with the correct cards to perform key operations.

2.6.8.4 Key Backup

Backup works in the same way as the nShield XC, using the Security World (kmdata files plus the Administrator Card Set).

⁴ Entrust FIPS 140-2, Level 3 validation <https://www.entrust.com/digital-security/hsm/solutions/compliance/certifications/fips-140-2>

2.6.8.5 Security

As the Solo works in exactly the same way as the XC, except it is PCIe rather than networked, the security considerations are exactly the same.

2.6.8.6 Performance

The Solo has the same performance as the XC.

2.6.8.7 Support

The nShield series (along with the Luna) are the most prolific general purpose HSMs available. This gives them great product support.

2.6.8.8 Costs

The HSM has similar costs as the XC it is based on.

2.6.8.9 PQC Support

Partial. As with the Connect XC, ML-DSA is available in Solo XC firmware and the Post-Quantum SDK can build CodeSafe machines for the Solo XC, but the product is past end of sale and is not suitable for a PQC migration.

2.6.9 Entrust nShield Edge

The nShield Edge is a portable, USB-connected desktop HSM with an integrated smart card reader. It is the lowest cost HSM in the nShield family and is aimed at low volume uses such as offline key generation for certificate authorities, development and test, and Bring Your Own Key (BYOK) environments where keys are generated before being securely exported to a cloud provider. It is the Entrust equivalent of the Thales Luna G7 and a direct alternative to the YubiHSM 2 for offline root CA use.

A key differentiator is that the Edge uses the same Security World architecture as the rest of the nShield range, so it can be part of a mixed Security World with nShield 5 and XC HSMs. For example, a root CA key can be generated and used offline on an Edge while subordinate CA keys in the same Security World are used on networked nShield 5c appliances, with a single set of administrative procedures.

Another benefit of the model is that you can start an Edge up with different security worlds, allowing it to have an infinite number of different configurations and keys supported, but it can only have one of these loaded and running at a time.

Another key differentiator as compared to the Thales G5 is support for Virtual Machines with USB pass through. Supported platforms are Microsoft Hyper-V Server 2016, 2019 and 2022, VMware ESXi 7.0 and 8.0 and Citrix XenServer 8.2. However the G7 has now added this support, but only for ESXi.

2.6.9.1 Models

The nShield Edge is available in FIPS 140-2 Level 2 and Level 3 variants, plus a non-FIPS developer edition. There is a single performance level; unlike the Connect and Solo ranges it cannot be upgraded in the field.

2.6.9.2 Key Storage:

Keys are stored in the same way as other nShield HSMs: as encrypted key blobs in the Security World Key Management Data (kmdata) directory on the host computer, protected by the Security World key and by an Operator Card Set or softcard. Key storage is therefore not limited by the capacity of the device.

2.6.9.3 Availability

There is no High Availability for the Edge itself, as it is a single USB device attached to one host. However, because keys are held in the Security World rather than on the device, any other HSM enrolled in the same Security World (including another Edge) can load the keys with the correct cards, which provides a practical form of redundancy for offline use.

2.6.9.4 Key Backup

Backup works in the same Security World based way as the other nShield HSMs: the kmdata files are backed up with normal file backup tools, and a replacement HSM is enrolled into the Security World using a quorum of the Administrator Card Set (ACS). No separate backup HSM is needed. For an offline root CA, the host's kmdata directory, the ACS and the Operator Card Set should each be backed up or stored in separate secure locations, as losing a quorum of the ACS makes the Security World unrecoverable on new hardware.

2.6.9.5 Security

The nShield Edge is validated to FIPS 140-2 Level 2 or Level 3 (depending on variant) with firmware 12.72, and Entrust's published certification information lists the Edge only as FIPS 140-2 certified. As all FIPS 140-2 certificates moved to the NIST Historical list on 21 September 2026, and we could not find any FIPS 140-3 validation for the Edge, it is not suitable for new deployments that require a current FIPS validation. Authentication uses the same smart card based Administrator and Operator Card Sets (with M of N quorum) as the other nShield HSMs, using the built-in card reader, and the device provides secure audit logging.

2.6.9.6 Performance

The nShield Edge is designed for low volume use and is rated at only 2 RSA 2048 bit signatures per second and 0.2 RSA 4096 bit signatures per second. It can in practice however, on some platforms, take up to 30 minutes to generate a single RSA 4096 key pair. This is slower than the Luna G7 but still well suited to an offline root CA that signs only a handful of certificates and CRLs each year.

2.6.9.7 Support

As it uses the same Security World software and APIs (PKCS#11, OpenSSL, Java JCE, Microsoft CAPI and CNG, and nCore) as the rest of the nShield range, the Edge benefits from the same wide third party application support. It is powered from the USB port and connects via USB 1.x/2.x to Windows and Linux hosts, including laptops. The USB connection can be passed through to virtual machines, as noted in the benefits table.

2.6.9.8 Costs

The Edge is the most economical HSM in the nShield range. As it is a locally attached device, the client licences that apply to networked nShield Connect and 5c appliances are not relevant. Smart cards for the Administrator and Operator Card Sets are additional consumables.

2.6.9.9 PQC Support

No. Entrust has released ML-DSA in firmware for the nShield 5 and XC ranges, but the Edge remains on firmware 12.72, and the PQC capabilities added in Security World v13.8 and v13.9 require nShield 5 or XC firmware. The Edge therefore cannot be used for PQC keys; an organisation planning a PQC root CA on nShield would need an nShield 5s or 5c.

2.6.9.10 Lifecycle

We could not find an end of sale notice for the nShield Edge. However, with no FIPS 140-3 validation, no PQC support and no firmware updates beyond 12.72, it appears to be at the end of its development. Customers should confirm its roadmap and support dates with Entrust before buying new units, particularly for a root CA that is expected to remain in service for many years.

2.6.10 Utimaco CryptoServer

The Utimaco CryptoServer LAN V5 series is a networked HSM and the CryptoServer Se and CSe Series are PCI HSM models. There is also a full featured HSM simulator and newly arrived u.trust Anchor which is a containerised HSM. The CryptoServer LAN HSM operates with four (4) models of differing performance being the Se12, Se52, Se500 and Se1500. Utimaco's current mainstream general purpose line is the u.trust GP HSM Se-Series (covered below). The CryptoServer GP HSM remains available, mainly for eIDAS (Common Criteria) and German VS-NfD classified use cases, and the CSe-Series is the high physical security option.

A key differentiator from some other HSM models is the concept of being able to choose either on board or off board key storage.

2.6.10.1 Models

The CryptoServer HSMs come in number of models, All have been validated against FIPS 140-2 Level 3⁵. The higher the model number the higher the performance of the device. These FIPS 140-2 certificates are now historical; Utimaco states that its current HSM portfolio is FIPS 140-3 Level 3 certified.

Upgrade path is dependant on the starting model as a common hardware platform is not used by all variants.

Starting Model	Can	Can't
Se12	Se52	Se500, Se1500
Se500	Se1500	CSe1500, Se4000
Se1500	CSe4000	CSe1500, Se4000

2.6.10.2 Key Storage:

Utimaco CryptoServer offers either onboard or offboard storage making it one of the most flexible HSMs available. The offboard key storage allows a greater number of keys to be stored than a HSM storing keys onboard. Backup of those keys is also far easier as it occurs simply by backing up the client that has an encrypted key on it.

2.6.10.3 Availability

High Availability (HA) is provided.

2.6.10.4 Key Backup

Utimaco backups are protected by the Master Backup Key (MBK), an AES-256 key generated when the HSM is initialised and split into shares on smart cards or key files using XOR or m of n (Shamir) secret sharing. Internal key databases and external key stores can be backed up to files encrypted under the MBK, using tools such as the CryptoServer Administration Tool (CAT), P11CAT or p11tool2, and restored onto any HSM into which the same MBK has been imported. The MBK is also used to synchronise HSM

⁵ Utimaco FIPS 140 certifications <https://utimaco.com/use-cases/fips-140-3>

clusters. Keys held in external key storage are already stored encrypted on the host, so they are covered by normal database or file backups. No separate backup HSM is required.

As with the nShield Administrator Card Set, the MBK shares are the critical recovery item: without a quorum of MBK shares, backups cannot be restored onto new hardware.

2.6.10.5 Security

The CryptoServer CSe is one of the few HSMs that can be purchased with FIPS 140-2 Level 4 hardware certification. It also has electronic certification to FIPS 140-2 Level 3 like its competitors. Utimaco states that the CSe-Series physical security meets FIPS 140-3 Level 4; this should be checked against the current CMVP listing for the specific model.

2.6.10.6 Performance

The performance of the CryptoServer models is exceeded by both the Thales and Entrust models.

2.6.10.7 Support

The Utimaco CryptoServer series are less prolific general purpose HSMs than Entrust and Thales models. This means while application support is good, it is not as widely supported by third party vendors as Entrust and Thales models.

2.6.10.8 Costs

Utimaco do not charge for Client Access Licences (CALs), partitions or ECC use. This reduces overall costs even where HA is desired for example. The cost of its accessories is also one of the lowest for a HSM provider. One key versatility benefit with this series of HSM is that it offers a virtual or software version of itself that is useful for test environments.

Accessories are some of the most inexpensive in the industry of the main players

2.6.10.9 PQC Support

Limited. Utimaco's Quantum Protect PQC firmware extension is offered for the u.trust GP HSM Se-Series and CSe-Series, but it is not listed among the application packages for the older CryptoServer GP HSM, so customers who need PQC should plan to move to the Se-Series or confirm model support with Utimaco.

2.6.11 Utimaco u.trust GP HSM Se-Series

The u.trust General Purpose HSM Se-Series, built on the platform previously marketed as u.trust Anchor, is Utimaco's next generation high performance, multi-tenant HSM, supporting up to 40,000 RSA 2048 signatures per second on the top model. It is designed to have unlimited key storage (both internal and external key storage are supported), to be scalable and flexible and to have remote management and monitoring. It is effectively a platform for multiple virtual HSMs, with up to 31 fully isolated containerised HSMs (cHSMs), each supporting multiple PKCS#11 partitions. All models are available as a LAN appliance or a PCIe card.

The models are the Se100 (up to 101 RSA 2048 signatures per second, 1 container), Se2k (up to 2,050, 4 containers), Se5k (up to 5,100, with 8, 16 or 31 containers), Se15k (up to 15,000, 4 containers) and Se40k (up to 40,000, with 8, 16 or 31 containers). In-field performance upgrades are available from Se100 to Se2k to Se5k, and from Se15k to Se40k.

All Se-Series models were validated to FIPS 140-3 Level 3 in May 2026 (NIST certificate #5223), and existing units can be brought to the validated firmware by an on-site upgrade with no hardware

replacement. The platform is also Common Criteria and PCI PTS HSM v3 certified. Post-quantum algorithms (ML-DSA, ML-KEM, XMSS/XMSS-MT and LMS/HSS) are available through the Quantum Protect firmware extension, and a free simulator is available for testing. Utimaco does not charge for CALs, partitions or ECC use on this platform, which keeps its licensing simple.

2.6.11.1 Key Backup

Backup uses the same MBK based approach as the CryptoServer, with internal and external key stores backed up to files encrypted under the MBK and restored to any HSM holding the same MBK. On multi-tenant models each container is an independent HSM, so customers should confirm with Utimaco how MBKs and backups are managed for each container.

2.6.11.2 PQC Support

Yes. The Quantum Protect firmware extension adds ML-DSA, ML-KEM, XMSS/XMSS-MT and LMS/HSS, and Utimaco has also obtained NIST algorithm (CAVP) certification for ML-KEM, ML-DSA and SLH-DSA. A Quantum Protect simulator is available for testing. A public example is NXP, which uses the Se-Series with Quantum Protect to sign firmware updates with ML-DSA.

2.6.12 Utimaco CryptoServer USB

Utimaco do not produce a USB variant of their HSMs.

2.6.13 YubiHSM 2 FIPS

The Yubico YubiHSM 2 is a USB "nano" form factor HSM that has been on the market since 2017. It is a low-cost, low performance HSM that plugs into a USB-A port on a host and can be shared over a network through that host (using the yubihsm-connector), with a limit of 16 concurrent sessions. There are three current models: the non-FIPS YubiHSM 2 (firmware v2.4), the YubiHSM 2 FIPS 140-2 (firmware v2.2) and the YubiHSM 2 FIPS 140-3 (firmware v2.4). The FIPS 140-3 model was validated at Level 3 under NIST certificate #5302, valid from 3 June 2026.

A key differentiator from some other HSM models is the very low cost.

2.6.13.1 Models

Yubico lists the YubiHSM 2 v2.4 at USD 650, and both the YubiHSM 2 FIPS 140-2 v2.2 and the YubiHSM 2 FIPS 140-3 v2.4 at USD 950. All models share the same form factor and similar performance. The FIPS 140-3 model is validated at FIPS 140-3 Level 3⁶. As the FIPS 140-2 certificate is now on the NIST Historical list, only the FIPS 140-3 v2.4 model should be considered for new deployments that require FIPS validation.

2.6.13.2 Key Storage:

Keys are stored inside the unit, not on the client. All data is stored as objects in 256 object slots with a maximum of 128 KB in total, which equates to at most 127 RSA 2048 bit keys, 93 RSA 3072 bit keys, 68 RSA 4096 bit keys or 255 elliptic curve keys (assuming only one authentication key is present). Unlike Luna SKS, nShield Security Worlds or Utimaco external key storage, there is no way to transparently use keys held outside the device.

2.6.13.3 Availability

High Availability (HA) is not provided for; there is no clustering, load balancing or automatic failover. Keys can be backed up by exporting them under a wrap key (with optional M of N control of the wrap key) and

⁶ YubiHSM 2 FIPS 140-3 Level 3 validation (certificate #5302) <https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5302>

importing them into a second YubiHSM 2, and firmware v2.4 adds backup using asymmetric wrapping. Redundancy therefore has to be achieved manually with multiple devices and application-level failover.

2.6.13.4 Key Backup

Backup is possible, but with significant restrictions. Keys are exported encrypted under a wrap key (AES-CCM) to files, which can be stored offline, and imported into a second YubiHSM 2 that holds the same wrap key. The wrap key can be split into shares held by custodians (M of N) using the YubiHSM Setup tool, and firmware v2.4 adds asymmetric (RSA) wrapping. The YubiHSM Setup and YubiHSM Manager tools can back up and restore all exportable objects on a device, and the Windows KSP supports backup of AD CS keys. The main limitations are:

- Only objects created with the exportable-under-wrap capability can be backed up, and it cannot be added after the object is created. A key created without it can never be backed up and is lost permanently if the device fails or is reset. Yubico's AD CS setup adds this capability to CA keys by default, but keys created with other tools may not have it.
- Backup relies on key export, so a YubiHSM 2 cannot be configured to both back up its keys and prevent those keys from ever leaving the device (see Security below).
- For a full device backup the wrap key must be accessible in all the domains of the objects being backed up and must delegate all of their capabilities; objects that do not meet these conditions are not exported.
- There is no dedicated backup device, replication or HA. The backup target is a second YubiHSM 2 and restoration is a manual process.
- In Yubico's documented procedure the wrap key starts as a plaintext file on the host before being loaded, so the process should be performed on an air-gapped machine and the file securely destroyed.

Backups should be tested by restoring them to a second device at commissioning time, because a key that turns out not to be exportable cannot be recovered later.

2.6.13.5 Security

The YubiHSM 2 is sold as a non-FIPS unit, a FIPS 140-2 Level 3 validated unit (v2.2, now historical) and, since June 2026, a FIPS 140-3 Level 3 validated unit (v2.4, certificate #5302).

There are three main issues with the YubiHSM2 when used with a PKI solution. The main issue, which in our opinion makes them unsuitable in a security PKI is that keys are exportable⁷. While this is through wrapping, it is still possible which is generally considered something that should never be allowed or supported within a PKI.

The second major issue is that YubiHSM2 and all Yubikeys it appears do not allow for firmware updates. Yubico's own site say they do this as a security best practice. Interestingly perhaps this message is on the same part of the site where they indicate a recent compromise of the Infineon chip, that due to their best practice processes, makes it unpatchable⁸. It is impossible to understand Yubico's rationale that states that the best practice is not to patch known vulnerabilities to avoid the possibility of introducing new vulnerabilities. In practice this means that the ECDSA side-channel vulnerability in the Infineon cryptographic library (YSA-2024-03, disclosed in September 2024) can never be fixed on YubiHSM 2

⁷ YubiHSM2 <https://docs.yubico.com/hardware/yubihsm-2/hsm-2-user-guide/webdocs.pdf> YubiHSM2 Crypto Module
<https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3916.pdf>

⁸ Security Advisory YSA-2024-03 with a CVSS Severity Score of 4.9 on YubHSM2 and advice that it is best practice to not update devices.
<https://www.yubico.com/support/security-advisories/ysa-2024-03/>

devices with firmware earlier than 2.4.0; the only remediation is to replace the device. It also means that new algorithms, including post-quantum algorithms, can never be added to a deployed unit.

Logging is also an issue on the devices. Very low logging space presents a challenge. It is possible to configure the device to prevent log rotation (Force Audit mode), however with only 62 entries that can be locally stored, it is extremely easy to overflow the logs and this then requires manual intervention to extract and clear the logs. This presents a major hurdle for deployment in any environment with strict audit logging requirements and regular use as it becomes relatively simple to hide unapproved actions. In firmware 2.4 and later all command logging is disabled by default, so audit logging (and ideally Force Audit mode) must be deliberately enabled during commissioning, otherwise no audit trail is kept at all.

2.6.13.6 Performance

The YubiHSM 2 has low performance. Yubico's published figures for the YubiHSM 2 FIPS 140-3 are an average of about 139 ms for an RSA 2048 PKCS#1 SHA-256 signature (roughly 7 signatures per second), 504 ms for RSA 3072, 852 ms for RSA 4096 and 73 ms for ECDSA P-256 (roughly 13 signatures per second). It also has the lowest key capacity at 127 RSA 2048 bit keys. The on-device logging space is limited to 62 entries at a time making log shipping very important. When logging is enabled the device will, by default, rotate logs, making it possible to overflow the logs to hide activity unless Force Audit mode is set.

2.6.13.7 Support

Although it has been available since 2017, the YubiHSM 2 still has the lowest third party support of the HSMs in this document. Microsoft AD CS (via the Yubico Key Storage Provider) and PKCS#11 applications are supported, but few vendors formally list it as a supported HSM. There is no dedicated network appliance or PCIe version of the product available.

2.6.13.8 Costs

The YubiHSM is one of the lowest cost options available. Yubico do not charge for Client Access Licences (CALs), but is limited to 16 concurrent connections. It also does not charge for partitions or ECC use. This reduces overall costs of an already low-cost option. There are no accessories available or required for the YubiHSM 2 right now. At USD 950 for the FIPS 140-3 model it is a small fraction of the cost of any other device in this document.

2.6.13.9 PQC Support

No. The YubiHSM 2 (all models, including the FIPS 140-3 v2.4 model) supports only RSA, ECC, EdDSA, HMAC and AES key wrap, with no ML-DSA, ML-KEM, SLH-DSA or LMS support. Because its firmware cannot be updated, PQC can never be added to a deployed unit; moving to PQC requires replacing the device with a different product.

2.6.13.10 Limitations Compared to Other Vendors

The YubiHSM 2 is often considered because of its price, so it is worth being explicit about where it falls short of the Thales, Entrust and Utimaco devices in this document. It is best suited to low volume, offline or lab use cases, such as an offline root CA with very few signing events, or development and test, rather than as the HSM behind an issuing CA, TLS, code signing or any other high volume or high availability service. The main issue however is that only keys generated with the "exportable-under-wrap" permission can be exported, and that can't be added later. This says nothing of the fact that the only way (if it was enabled) to backup the key is to export keys, which is something that is not recommended by Cogito. It is something that other vendors recommend against if you require the best possible security. Added to this

is that the key is actually exposed during the key wrap setup as the key starts as a plaintext file and there is no dedicated backup device either.

YubiHSM 2 limitations compared to mainstream HSMs

Area	YubiHSM 2 FIPS 140-3 (v2.4)	Typical Thales / Entrust / Utimaco device
Performance	About 7 RSA 2048 and 13 ECDSA P-256 signatures per second	Hundreds to tens of thousands per second (e.g. nShield 5c High 11,680 RSA 2048 tps; Utimaco Se40k up to 40,000)
Key capacity	256 objects / 128 KB; at most 127 RSA 2048 keys	Megabytes of onboard storage, or effectively unlimited external key storage (Luna SKS, nShield Security World, Utimaco external storage)
Concurrency	16 concurrent sessions	Hundreds to over 1,000 client connections (e.g. nShield 5c High up to 1,000 client licences)
High availability	None; manual duplicate devices only	Clustering, load balancing and automatic failover
Form factor	USB-A nano only; network access depends on the host running yubihsm-connector	Network appliances with redundant power and network bonding, plus PCIe and USB options
Post-quantum	None (no ML-DSA, ML-KEM, SLH-DSA or LMS) and it cannot be added	ML-DSA and ML-KEM available now through firmware (Luna 7.9+, nShield 5, Utimaco Quantum Protect) or natively (Luna 8)
Firmware updates	Not possible; vulnerabilities such as YSA-2024-03 can only be fixed by replacing the device	Signed field firmware updates, including security fixes and new algorithms
Key export	Keys can be exported under wrap by design (controlled by capabilities)	Can be configured so that private keys are never exportable
Authentication	Authentication keys (password derived or ECP256); M of N only applies to wrap key backup and restore	Smart cards, PED keys and quorum (M of N) for administration and key use
Audit logging	62 entries on device, logging off by default in v2.4, no syslog	Large secure audit logs with syslog and SNMP export
Certifications	FIPS 140-3 Level 3 only (no Common Criteria or eIDAS QSCD)	FIPS 140-3 Level 3 plus Common Criteria EAL4+ and eIDAS QSCD on most models
Integration support	Limited formal third party support	Hundreds of documented third party integrations
Cost	About USD 950	Tens of thousands of dollars per device plus licences and support

The lack of post-quantum support, combined with the inability to update firmware, is the most significant long term limitation. With Australian (ASD ISM) and U.S. (CNSA 2.0) guidance setting post-quantum transition timelines in the 2030 to 2035 timeframe, a YubiHSM 2 purchased today will need to be replaced to adopt ML-DSA or ML-KEM, whereas the mainstream vendors are delivering PQC through firmware updates to existing hardware.

2.6.14 Thales ProtectServer 3/3+

ProtectServer became a Thales product through Thales acquisition of Gemalto, which acquired Safenet, which in turn had acquired Eracom Inc.

The Thales ProtectServer series is less prolific than Thales's other general purpose HSM offering (Luna 7/G7 and Luna 8 family) but provides a very high level of functionality at a much lower price point. Protect server has few accessories and they are reasonably well priced by HSM standards. The trade-off for the lower price point is the significant performance reduction compared to those offered by other vendors. One key versatility benefit with this series of HSM is that it offers a virtual or software version of itself that is useful for test environments.

2.6.14.1 Models

The Thales ProtectServer 3/3+ is a line network and PCIe based HSM's available in 3 performance tiers PL25, PL220, PL3500. The ProtectServer 3+ is equipped with dual power supplies and only available in the PL3500 variant.

2.6.14.2 Key Storage:

Keys are stored internally to the unit.

2.6.14.3 Availability

High Availability (HA) is provided for if multiple units are used, however only one of the units can be specified with redundant power supplies.

2.6.14.4 Key Backup

Keys can be backed up to encrypted disk files or to smart cards using the ProtectToolkit ctkmu command line tool or the KMU GUI, and restored to another ProtectServer; the ProtectServer 3 External is supplied with a smart card reader for this purpose. Only keys whose attributes allow export can be backed up this way. Keys marked non-exportable cannot be backed up to file or smart card and can only be copied by token replication directly between ProtectServer HSMs.

When ProtectToolkit-M is used (for example with Microsoft AD CS), keysets are backed up individually, each encrypted with a Triple-DES backup key derived from the keyset's password and name, so these backups are only as strong as the keyset passwords used.

2.6.14.5 Security

The ProtectServer is only available with PIN/password-based authentication, but may optionally implement OTP with the use of a SafeNet 110 OTP token. An external PIN pad may be used to further ensure security during credential entry. The ProtectServer 3 was FIPS 140-2 Level 3 validated (certificate #4110, now historical). Firmware 7.03.00 and later is designed to conform with FIPS 140-3 Level 3, but at the time of writing Thales still listed FIPS 140-3 validation (firmware 7.03.02) as pending, so this should be checked before selecting it for a FIPS 140-3 requirement.

2.6.14.6 Performance

The trade-off for the lower price point is the significant performance reduction compared to those offered by other vendors.

2.6.14.7 Support

The ProtectServer supports the common cryptographic interfaces such as PKCS#11, JCA/JCS, and CNG/CAPI which allows for integration with most third-party applications. Unfortunately, due the lower popularity of the platform there is less official integration documentation for these products.

The ProtectServer is very highly configurable and allows a developer to implement additional functionality such as commands and algorithms within the HSM. Developers may expand the standard feature set of the ProtectServer HSM through the use of functionality modules (FM). Functionality Modules are custom commands, algorithms, and mechanisms which are executed within the secure confines of the HSM allowing further customisation or expansion of the feature set.

Thales provide a fully featured and compatible emulator of the ProtectServer software. This allows for rapid development, testing, and proof of concept deployments without the hardware requirements mandated by other vendors.

There is no USB variant available

2.6.14.8 Costs

ProtectServer are capable, relatively well priced units with reasonably priced accessories. Protect server also does not charge for Client Access Licenses and even has a free software version of their product for test environments. This makes them good value for month products.

2.6.14.9 PQC Support

Not natively. We could not find any Thales announcement of native PQC support for ProtectServer 3. Its Functionality Module (FM) capability means custom PQC algorithms could be implemented inside the HSM, but these would be customer or partner developed code outside the FIPS validated configuration. Thales is focusing its PQC delivery on the Luna range.

3 Other HSM Types and Providers

There are many other HSM providers, some of which have large customers. Providers include Crypto4A, Eviden (Atos) Trustway, Fortanix, Futurex, IBM, Marvell (formerly Cavium), Nitrokey, Securosys and Ultra, as well as the HSM services offered by the major cloud providers. Atalla, EKSM and MyHSM are now part of Utimaco. The more relevant of these are summarised below. They are not compared in detail in the rest of this document for the reasons given in the Limitations section.

3.1 Other General Purpose HSM Vendors

3.1.1 Marvell LiquidSecurity (formerly Cavium)

Marvell acquired Cavium in 2018 and continues the LiquidSecurity line. LiquidSecurity HSMs are PCIe adapters designed for cloud and hyperscale deployments rather than enterprise appliances, and they sit behind a number of cloud services; LiquidSecurity has underpinned AWS CloudHSM since its launch, and Marvell states they power Microsoft Azure Key Vault, Azure Key Vault Managed HSM and, since 2025, Azure Cloud HSM. The current LiquidSecurity 2 (LS2) adapter is FIPS 140-3 Level 3 certified, supports up to 45 isolated partitions and up to around one million keys per adapter, and supports both general purpose and payment (PCI PTS HSM) functions on the same hardware. Performance per dollar is excellent, but direct third party application support outside the cloud providers is limited and it is mainly purchased by cloud providers and OEMs rather than end customers. The cloud providers can use these HSMs because they can do custom integrations to the devices. If you are looking to support a number of different applications, it is advisable to check what you intend to support now and in the future to see if native integrations are available and supported by the manufacturer. PQC: Marvell has NIST algorithm (CAVP) certification for ML-KEM, ML-DSA and SLH-DSA and states that LS2 can be field updated to support PQC, so availability depends on the cloud provider or OEM using it.

3.1.2 Futurex

Futurex (USA) is a long established vendor with a strong payments background. Its general purpose HSMs are the Vectera Plus and the CryptoHub platform, which combines general purpose and payment HSM, key management, PKI and tokenisation functions, and it also offers the VirtuCrypt cloud HSM service. The Vectera Plus supports HSM virtualisation (multiple logically separated virtual HSMs, each with their own firmware, security policy and configuration) and a Secure Code Environment for custom applications. Futurex's published general purpose HSM material still references FIPS 140-2 Level 3 validation, so current FIPS 140-3 status should be confirmed before selection. Futurex is well supported in payments but has less general purpose third party integration than Thales, Entrust or Utimaco. PQC: yes, Futurex states its current Excrypt HSMs natively support ML-KEM and ML-DSA, with the CryptoHub PKCS#11 module exposing both through PKCS#11 v3.2.

3.1.3 Securosys

Securosys (Switzerland) produces the Primus HSM range (E-Series and X-Series appliances, including the newer X2 and E2 series) and a CloudHSM service. The X-Series supports up to 120 partitions and around 30 GB of storage, and the top X1000 model is rated at 1,000 RSA 4096 operations per second. Primus HSMs are Common Criteria EAL4+ (EN 419 221-5, eIDAS QSCD) certified and are popular in banking, digital asset custody and European sovereign use cases. Their FIPS 140-2 Level 3 certificates are now historical

and FIPS 140-3 Level 3 validation of firmware 3.1 was still in progress at the time of writing, so they may not currently meet a FIPS 140-3 requirement. PQC: yes, the Primus CyberVault series launched in March 2025 supports ML-KEM, ML-DSA, SLH-DSA, HSS-LMS and XMSS, including in its CloudHSM service.

3.1.4 Crypto4A

Crypto4A (Canada) builds the QxHSM and QxEDGE on a crypto-agile, FPGA based architecture designed from the outset to be quantum-safe, including quantum-safe firmware update and root of trust mechanisms. In August 2026 its QASM cryptographic module was validated to FIPS 140-3 Level 3 with support for all NIST standardised PQC algorithms (ML-KEM, ML-DSA, SLH-DSA and stateful hash-based signatures). Industry analysts regard it as the leading example of an HSM re-architected for PQC rather than having PQC added to an existing design. It is a comparatively small vendor with limited third party integration, so support arrangements should be checked carefully. PQC: yes, it is the most complete PQC implementation of the vendors in this document, and the first to include the NIST PQC algorithms in a FIPS 140-3 Level 3 validation.

3.1.5 Eviden (Atos) Trustway Proteccio

Eviden, the Atos Group cyber security business, produces the Trustway Proteccio NetHSM in France. It is heavily certified for European government use, holding Common Criteria EAL4+, eIDAS, SOG-IS, NATO SECRET and EU RESTRICTED approvals, and Eviden states it is the only HSM with the French ANSSI 'reinforced qualification'. It is a strong option where European sovereignty is a requirement, but FIPS validation has not historically been its focus and third party support outside Europe is limited. PQC: Eviden's product literature listed post-quantum algorithms as due in 2024, but we could not confirm which algorithms are currently available, so this should be checked with Eviden.

3.1.6 Fortanix

Fortanix (USA) takes a software-defined approach, using Intel SGX secure enclaves in its Data Security Manager (DSM) platform, which is offered as a SaaS service and on appliances. It is primarily a key management and HSM as a service platform rather than a traditional HSM, and its reliance on SGX is the main concern. PQC: yes, Fortanix DSM supports LMS, ML-DSA and ML-KEM.

Since 2018 SGX has been subject to a long series of published attacks, several of which stem from the design of the Intel processor itself rather than from software bugs that Fortanix could patch:

- Foreshadow (2018) used speculative execution to extract SGX sealing and attestation keys. Intel had to revoke the exposed attestation keys and rely on microcode updates and later processor designs.
- Plundervolt (2019) used the CPU's software voltage control to corrupt enclave computations and recover keys. The fix was a microcode and BIOS update that disables undervolting, requiring enclaves to re-establish trust.
- SGAXe and CrossTalk (2020) showed that SGX attestation keys could still be extracted, and random numbers leaked, from a machine with all of the previous countermeasures and microcode updates applied at the time.
- ÆPIC Leak (2022) leaked enclave data through an architectural CPU bug. Researchers later found that Intel had not performed a trusted computing base (TCB) recovery for it for an extended period, so vulnerable machines were still reported as trusted.
- Battering RAM and WireTap (October 2025) used low-cost interposers (about USD 50 and under USD 1,000 respectively) on the DDR4 memory bus to read or tamper with enclave memory and extract the

SGX attestation signing key. These exploit SGX's deterministic memory encryption and are physical attacks outside SGX's threat model, so they cannot be fixed by a microcode update and can only be mitigated by physical security of the server.

Each software-fixable issue also depended on Intel releasing microcode and the platform owner applying it. By contrast, a traditional HSM keeps keys inside a tamper-responsive boundary designed to detect physical attack and zeroise keys. Customers considering Fortanix should confirm its current hardware platform, the FIPS 140-3 status of that platform, and the physical security controls around it. Given the number of compromises related to SGX and the fact that some of them were unable to be fixed, we do not recommend the use of this platform.

3.1.7 Nitrokey NetHSM

Nitrokey (Germany) released the NetHSM in December 2023 as a fully open source network HSM, priced from about EUR 9,999 plus VAT and service contracts. Its software uses a formally verified microkernel and memory-safe code, it exposes a modern REST API as well as a PKCS#11 module, and it is also available as a Docker container for development and testing. Nitrokey quotes around 1,700 RSA 2048 operations per second for the NetHSM 2, far above the YubiHSM 2. Industry analysts noted that it had no NIST or Common Criteria certification after launch, which rules it out for most regulated use cases, but it is an interesting low cost alternative to the YubiHSM 2 where certification is not required. Nitrokey also sells the very low cost USB Nitrokey HSM 2, which is closer to a smart card than a server HSM. PQC: no, the published NetHSM 2 specification lists only RSA, ECC and AES algorithms.

3.1.8 IBM

IBM produces PCIe cryptographic coprocessors (the Crypto Express / 4769 family) primarily for IBM Z and LinuxONE mainframes, as well as the Hyper Protect Crypto Services cloud offering. These are among the few HSMs that have been certified at FIPS 140 Level 4, but they are only relevant where IBM mainframe platforms are in use. PQC: yes, the Crypto Express 8S adapters for IBM z16 and later added quantum-safe CRYSTALS-Dilithium (now ML-DSA) and CRYSTALS-Kyber (now ML-KEM) capabilities.

3.2 Cloud HSM Services

Where an organisation does not want to own and operate HSM hardware, the major cloud providers and several HSM vendors offer dedicated HSMs as a service. These remove the hardware, data centre and HA overheads, but they tie keys to the provider's platform and can make migration of existing keys between vendors difficult.

- AWS CloudHSM provides single-tenant HSM clusters in the customer's VPC. The hsm2m.medium type, launched in August 2024, supports FIPS 140-3 Level 3 clusters and offers greater key capacity and elliptic curve performance than the older hsm1.medium type. The service has been built on Cavium (now Marvell) LiquidSecurity HSMs, and industry sources indicate the hsm2m.medium type is also Marvell based.
- Microsoft Azure Cloud HSM is the successor to Azure Dedicated HSM (which was based on Thales Luna, no longer accepts new customers, and is supported for existing customers until 31 July 2028). Azure Cloud HSM is a single-tenant, FIPS 140-3 Level 3 service built on Marvell LiquidSecurity HSMs. Keys cannot be migrated from Azure Dedicated HSM, so new keys must be generated.
- Google Cloud HSM provides HSM protected keys managed through Google Cloud KMS, without direct access to the device.

- Vendor services, such as Thales Luna Cloud HSM (Data Protection on Demand), Entrust nShield as a Service, Utimaco GP HSM as a Service, Securosys CloudHSM and Futurex VirtuCrypt, provide the vendor's own HSMs as a service, which makes hybrid deployments with on-premises devices of the same brand easier.
- Cogito Group offers HSM as a Service (HSMaaS) and Key Management as a Service (KMaaS).

3.3 Smaller and Legacy Providers

- Blackbox produce inexpensive low powered HSMs.
- Cavium, now part of Marvell, is covered above. Cavium (now Marvell) LiquidSecurity HSMs have been the hardware behind AWS CloudHSM since it moved away from SafeNet Luna devices. AWS does not publicly name the hardware for the current hsm2m.medium type, but industry sources indicate it is still Marvell based, so Marvell HSMs should be considered as still in use by AWS.
- Ultra Keyper HSMs were originally known as AEP Keyper HSMs and have FIPS 140-2 Level 4 certification. They have good legacy software support but have not changed much in many years. The product line has since been discontinued, so existing units should be planned for replacement.

3.4 Vendor Acquisitions

Some of the vendors or product lines that have been acquired include:

- Chrysalis acquired by Rainbow technologies in September 2003
- Rainbow Technologies was acquired by Safenet in Mar 2004
- nCipher acquired by Thales in July of 2008
- Safenet was acquired by Gemalto in August 2014 and Safenet Assured Technologies is born to spin off certain items that must be kept separate from Gemalto.
- Atalla was acquired by Utimaco in May of 2018
- EKSM was acquired by Utimaco in May of 2018
- Cavium was acquired by Marvell in July 2018
- nCipher purchased by Entrust from Thales in June 2019
- Gemalto was acquired by Thales in February 2020.
- MyHSM was acquired by Utimaco in January of 2021

4 Benefits, Limitations and Specification Comparison

4.1 Benefits Table

The below table lays out the benefits of each model. Luna 8 is now shown in its own column, based on the Thales Luna 8 product brief; entries marked "Not stated" or "Not published" should be confirmed with Thales. The FIPS 140-2 rows are retained for reference only, as those certificates are now historical.

Category	Feature	Thales Luna 7 / G7	Thales Luna 8	Entrust nShield 5c/5s/Edge	Utimaco Se / CSe	YubiHSM 2 (FIPS)	Protect Server 3/3+
Operating System	Windows	Y	Y	Y	Y	Y	Y
	Linux	Y	Y	Y	Y	Y	Y
	Other	Y AIX, Solaris, HP-UX	N (Windows and Linux only)	Y AIX, Solaris, HP-UX	N	Y macOS	N
Security	Can prevent key export	Y	Y	Y	Y	N	Y
	Firmware updates supported	Y	Y	Y	Y	N	Y
Availability	Offers High Availability	Y	Y	Y	Y	N	Y
	No requirement for separate management server for HA	Y	Y	Y	Y	N/A	Y
	HA configured on and maintained by client	Y	Y	Y	Y	N/A	Y
	Redundant Power Supplies	Y	Y	Y	Y	N/A	P ProtectServer 3+ Only
Backup	Does not require separate tokens	N	N	Y	N	N	N
	Manual Offsite Storage Possible	Y Through dedicated backup appliance	Y (via Luna Backup HSM)	Y	Y	Y	Y
	Automatic Offsite Storage Possible	P Through HA only	P (through HA only)	Y	P Through HA only	N	N
Flexibility	Field upgradable	N	Not stated	Y	P Limited to select models with specific upgradesa	N/A	Y
	Supports both onboard and offboard keys	N	N	Y (Limited onboard)	Y	N	N

Hardware Security Module Comparison

Category	Feature	Thales Luna 7 / G7	Thales Luna 8	Entrust nShield 5c/5s/Edge	Utimaco Se / CSe	YubiHSM 2 (FIPS)	Protect Server 3/3+
				support)			
	Key storage not limited to onboard memory	N	N	Y	Y	N	N
	Multiple Authentication Mechanisms	Y Token, Password	Y (quorum M of N, MFA)	Y SmartCard, Softcard, Module	Y SmartCard, Password	N Password Only	Y Password, Password + OTP
	Cloud support for client partial separation	Y	Y	N	Y	N	N
	Cloud support for full separation of components (i.e. virtual HSM)	Y (Luna 8)	Y (up to 30 HSM instances)	Coming	Y	N	N
	Wide formal support by vendors	Y	Y (Luna 7 compatible)	Y	Y	N	N
	Widest support by vendors in class	Y	Y	Y	N	N	N
	Key management software available from manufacturer	Y	Y	Y	Y	N	Y
	Logging available	Y Syslog	Y (rsyslog)	Y Secure audit/Syslog	Y	Y	Y Syslog
	Logging to standard external sources	Y	Y	Y	Y	N	Y
	Remote Monitoring	Y SNMP	Y (BMC, metrics)	Y SNMP	Y SNMP	N	Y SNMP
	Hardware agnostic within vendor product line	Y	Y	Y	Y	N/A	Y
Software	Command Line Interface (CLI)	Y	Y	Y	Y	Y	Y
	Graphical User Interface (GUI)	N	Not stated	Y	Y	N	Y
Compatibility	USB Appliance Variant	Y	N (planned)	Y	N	Y	N
	USB Appliance Variant Supports Virtual Machines	N	N/A	Y	N/A	Y Via network connection	N
	PCI version	Y	N (planned)	Y	Y	N	Y
	Network version	Y	Y	Y	Y	N Network Accessible though connected host	Y
	Supports ECC	Y	Y	Y	Y	Y	Y

Hardware Security Module Comparison

Category	Feature	Thales Luna 7 / G7	Thales Luna 8	Entrust nShield 5c/5s/Edge	Utimaco Se / CSe	YubiHSM 2 (FIPS)	Protect Server 3/3+
Security	PKCS#11 Support	Y	Y	Y	Y	Y	Y
	KMIP Support	Y	Not stated	Y	Y	N	N
	FIPS-140-2 Level 2 support	N	N/A	Y	Y	Y	Y
	FIPS-140-2 Level 3 support	Y	N/A	Y	Y	Y	Y
	FIPS-140-2 Level 3 certified with password protection	Y	N/A	N	N	Y	Y
	FIPS-140-2 Level 4 support	N	N/A	N	Y CSe series Physical Only	N	N
	FIPS140-3	Y – Luna 7 K7 (#4684) and G7 (#4962); Luna 8 in process	In process	Y – nShield 5c/5s	Y – u.trust Se-Series (#5223)	Y – FIPS 140-3 model v2.4 (#5302)	ProtectServer 3 – in progress (validation still pending)
	PQC algorithm support	Luna HSM v7.9 • ML-KEM, • ML-DSA, •	Y (native ML-KEM, ML-DSA, LMS/HSS)	5c (with firmware upgrade) • ML-DSA • (other PQ algorithms available via nShield post-quantum option pack)	Se-Series • Available via application package	N (no PQC support; firmware cannot be updated to add it)	N
	Common Criteria Certified	Y	In process	Y	Y	N	N
	M of N support	Y	Y	Y	Y	N	N
Costs	Low Cost Solution	N	N	N	N	Y	N
	No CALs required	N	Not published	N	Y	Y 16 included, no option to purchase additional	Y
	CAL not required for each client access where the HSMs are in a HA cluster	Y	Not published	N	N/A	N/A	Y
	No partition licences required	N	Not published	Y	Y	Y	Y

Hardware Security Module Comparison

Category	Feature	Thales Luna 7 / G7	Thales Luna 8	Entrust nShield 5c/5s/Edge	Utimaco Se / CSe	YubiHSM 2 (FIPS)	Protect Server 3/3+
	No additional cost for ECC Support	Y	Not published	N	Y	Y	Y
	Virtual HSM version available and free to use	N	N	N	Y	N	Y
Performance	High performance versions available	Y	Y	Y	Y	N	Y
	Low performance versions available	Y	Y (Luna 100)	Y	Y	Y	Y

Hardware Security Module Comparison

4.2 Specification Matrix

Below are the specifications of individual components

Feature	Thales Luna HSM 7	Thales Luna 8	Thales Luna USB HSM	Entrust nShield 5c/5s	Entrust nShield Edge	Utimaco SecurityServer Se Gen2	YubiHSM 2 FIPS	Thales ProtectServer 3/3+
OS Support	Windows, Linux, Solaris, AIX Virtual: VMware, Hyper-V, Xen, KVM	Windows, Linux. Virtual: VMware, Hyper-V, Xen, KVM	Windows, Linux	Windows and Linux operating systems including distributions from RedHat, SUSE, and major cloud service providers running as virtual machines or in containers	Microsoft Windows 7 x64, 10 x64, Windows Server, 2012 R2 x64, 2016 x64, 2019 x64 • Red Hat Enterprise Linux AS/ES 6 x64, x86 and 7 x64; SUSE Enterprise Linux 11 x64 SP2, 12 x64, 15.1 x64 • Oracle Enterprise Linux 6.10 x64, 7.6 x64	Windows, Linux	Windows: Windows 10 Windows Server 2012 Windows Server 2016 Windows Server 2019 Linux: CentOS 7 Debian 8 Debian 9 Debian 10 Fedora 28 Fedora 30 Fedora 31 Ubuntu 1404 Ubuntu 1604 Ubuntu 1804 Ubuntu 1810 Ubuntu 1904 Ubuntu 1910	Windows, Linux
Cryptography	Full Suite B support Asymmetric: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES) with named, user-defined and Brainpool curves, KCDSA, and more Symmetric: AES, AES-GCM, DES, Triple DES, ARIA, SEED, RC2, RC4, RC5, CAST, and more Hash/Message Digest/HMAC: SHA-1, SHA-2, SM3, and more Key Derivation: SP800-108 Counter	PQC: ML-KEM, ML-DSA, LMS/HSS. RSA up to 4096 (PKCS#1 v1.5, OAEP, PSS); ECDSA/ECDH/ECIES on NIST, Brainpool and secp256k1 curves; X25519, X448, Ed25519, Ed448; AES (incl. GCM, XTS), ARIA, SEED; SHA-2, SHA-3, SHAKE; BIP32/SLIP10; MILENAGE, TUAK	Full Suite B support Asymmetric: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES) with named, user-defined and Brainpool curves, KCDSA, and more Symmetric: AES, AES-GCM, DES, Triple DES, ARIA, SEED, RC2, RC4, RC5, CAST, and more Hash/Message Digest/HMAC: SHA-1, SHA-2, SM3, and more Key Derivation: SP800-108 Counter	Full NIST Suite B implementation Asymmetric algorithms: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA (including NIST, Brainpool & secp256k1 curves), ECDH, Edwards (Ed25519, Ed25519ph) Symmetric algorithms: AES, AES-GCM, Arcfour, ARIA, Camellia, MD5 HMAC, RIPEMD160 HMAC, SEED, SHA-1 HMAC, SHA-224 HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC, Tiger HMAC, 3DES Hash/message digest: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160, SHA-3 (224, 256, 384, 512 bit) Elliptic Curve Key Agreement (ECKA) available via Java API and nCore APIs Elliptic Curve Integrated Encryption Scheme (ECIES) available via Java API,	Full NIST Suite B implementation Asymmetric algorithms: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA, ECDH, Edwards (X25519, Ed25519ph) • Symmetric algorithms: AES, Arcfour, ARIA, Camellia, CAST, DES, MD5 HMAC, RIPEMD160 HMAC, SEED, SHA-1 HMAC, SHA-224 HMAC, SHA-256 HMAC, SHA-384 HMAC,	RSA, DSA, ECDSA with NIST and Brainpool curves DH, ECDH with NIST and Brainpool curves AES, Triple-DES, DES MAC, CMAC, HMAC SHA-1, SHA2-Family, SHA3 (as from SecurityServer 4.10), RIPEMD Hash-based Deterministic Random Number Generator (DRNG) True Random	RSA 2048, 3072, and 4096 bit keys Signing: PKCS#1 v1.5 and PSS Decryption: PKCS#1 V1.5 and OAEP Elliptic Curve Cryptography (ECC) Curves: secp224r1, secp256r1, secp256k1, secp384r1, secp521r, bp256r1, bp384r1, bp512r1, curve25519 Signing: ECDSA (all except Ed25519), EdDSA (Ed25519 only) Derivation:	Asymmetric: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519) with named, user defined and Brainpool curves, and more Symmetric: AES, AES-GCM, AES-CCM, Triple DES, DES, CAST 128, RC2, RC4, SEED, ARIA plus others Hashing: SHA-1, SHA-2, SHA-3, MD5, MD2, RIPEMD 128, RIPEMD 160, DES MDC2 PAD1 and more



Hardware Security Module Comparison

Feature	Thales Luna HSM 7	Thales Luna 8	Thales Luna USB HSM	Entrust nShield 5c/5s	Entrust nShield Edge	Utimaco SecurityServer Se Gen2	YubiHSM 2 FIPS	Thales ProtectServer 3/3+
	Mode Key Wrapping: SP800-38F Random Number Generation: designed to comply with AIS 20/31 to DRG.4 using HW based true noise source alongside NIST 800-90A compliant CTR-DRBG		Mode Key Wrapping: SP800-38F Random Number Generation: designed to comply with AIS 20/31 to DRG.4 using HW based true noise source alongside NIST 800-90A compliant CTR-DRBG	PKCS#11 and nCore APIs TUAK and MILENAGE algorithm support for mutual authentication and key generation (3GPP) NIST short-listed post-quantum cryptographic algorithms supported using the nShield Post- Quantum Option Pack	SHA-512 HMAC, Tiger HMAC, 3DES Hash/message digest: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160	Number Generator (TRNG acc. AIS31 class PTG.2) All algorithms included in product price	ECDH (all except Ed25519) Hashing functions: SHA-1, SHA-256, SHA-384, SHA-512 Key wrap: Import and export using NIST-approved AES CCM	Message Authentication Codes: SHA-1, SHA-2, SHA-3, MD2, RIPEMD128, RIPEMD160, DES MDC-2 PAD1, SSL3 MD5 MAC, AES MAC, CAST-128 MAC, DES MAC, DES3 MAC, DES3 Retail CFB MAC, DES3x9.19 MAC, IDEA MAC, RC-2 MAC, SEED MAC, ARIA MAC, VISA CVV Digital Wallet Encryption: BIP32 5G Cryptographic Mechanisms for Subscriber Authentication: MILENAGE and TUAK
Cryptographic APIs	PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL REST API for Administration	PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL; APIs for administration	PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL	PKCS#11 OpenSSL Java (JCE) Microsoft CAPI/ CNG Web Services (requires Web Services Option Pack) nCore	PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG, nCore, Web Services (requires web services option pack)	PKCS#11 Java Cryptography Extension (JCE) Microsoft Crypto API (CSP), Cryptography Next Generation (CNG) and SQL Extensible Key Management (SQLEKM) Cryptographic eXtended services Interface (CXI) Utimaco's high performance interface guarantees easy integration of cryptographic functionality into client applications	PKCS#11 API version 2.40 Microsoft CNG via the Yubico Key Storage Provider (KSP), both 32 and 64-bit DLLs Full access to device capabilities through Yubico's YubiHSM Core Libraries (C, Python)	PKCS#11, CAPI/CNG, JCA/JCE, JCProv, OpenSSL
Random	Designed to comply with	AIS 20/31 DRG.4	Random Number	AIS 20/31, and with SP 800-90B and		Hash-based	On-chip True Random	< Details unavailable at time of

Hardware Security Module Comparison

Feature	Thales Luna HSM 7	Thales Luna 8	Thales Luna USB HSM	Entrust nShield 5c/5s	Entrust nShield Edge	Utimaco SecurityServer Se Gen2	YubiHSM 2 FIPS	Thales ProtectServer 3/3+
Numbers	AIS 20/31 to DRG.4 using HW based true noise source alongside NIST 800-90A compliant CTR-DRBG	with hardware noise source and NIST 800-90A HMAC_DRBG; dual entropy source including QRNG; external entropy supported	Generation: FIPS 140-2 approved DRBG (SP 800-90 CTR mode)	SP 800-90Arev1		Deterministic Random Number Generator (DRNG) True Random Number Generator (TRNG acc. AIS31 class PTG.2)	Number Generator (TRNG) used to seed NIST SP 800-90A Rev.1 AES-256 CTR_DRBG	writing >
Capacity	A/S700: 2MB A/S750: 16MB A/S790: 32MB	Luna 100: 128 MB; Luna 150: 1,024 MB; Luna 190: 4,096 MB	15.5MB	Unlimited (Only limited by client)	Unlimited (Only limited by client)	Internal: 64MB (PKCS#11 Database: 8MB) Store: RSA 2048 is 3300 Objects AES256 is 250K for 8MB DB External: (Only limited by client)	128KB 256 object slots Object types: – Authentication keys – Asymmetric private keys – Opaque binary data objects – Wrap keys – HMAC keys The potential to store up to: 127 rsa2048 or 93 rsa3072 or 68 rsa4096 or 255 of any elliptic curve type	4MB 8MB for FMs
Host Connectivity/Interface	4 Gigabit Ethernet ports with Port Bonding IPv4 and IPv6	4 x 10G SFP+ (fibre or RJ45 copper), 1 x 1G RJ45 BMC port	USB 2.0	2 x RJ45 [1 Gb/s]	USB port (1.x, 2.x compliant)	2 x RJ45 [1 Gb/s]	USB-A connector Universal Serial Bus (USB) 2.0	2 x RJ45 [1 Gb/s] (PSE 3) 4 x RJ45 [1 Gb/s] (PSE 3+)
Reliability	Dual hot-swap power supplies Field-serviceable components Mean Time Between Failure (MTBF) 171,308 hrs	Dual hot-swap power supplies and fans; MTBF 289,444 h (single module), 171,236 h (dual module)	N/A	All solid-state storage Field serviceable fan tray Dual hot-swap power supplies Full support for clustering HSMs and automated failover/load balancing Network bonding supporting active backup mode and 802.3ad mode MTBF 2 : 107,845 hours	N/A	MTBF 360,000 hours at 25°C / 77°F	Can withstand 500,000 read/write cycles Mean Time Between Failure (MTBF) is greater than 100 years in most commonly used environments, but may vary in harsher environments • Comes with a standard 1-year warranty	- Dual hot-swap power supplies (PSE 3+) - Mean Time Between Failure (MTBF) 165637 hours (PSE 3) - Mean Time Between Failure (MTBF) 171,308 hours (PSE 3+)



Hardware Security Module Comparison

Feature	Thales Luna HSM 7	Thales Luna 8	Thales Luna USB HSM	Entrust nShield 5c/5s	Entrust nShield Edge	Utimaco SecurityServer Se Gen2	YubiHSM 2 FIPS	Thales ProtectServer 3/3+
Certifications	FIPS 140-3 Level 3 (certificate #4684); previously FIPS 140-2 Level 3 – password and multi-factor (PED) Certificate #3205 QSCD for eIDAS compliance Common Criteria Certification (PP 419 221-5)	In process: FIPS 140-3 Level 3, Common Criteria EAL4+ (EN 419 221-5), eIDAS 2 QSCD	FIPS 140-3 Level 3 (G7, certificate #4962); previously FIPS 140-2 Level 2 and Level 3 BAC & EAC ePassport Support	FIPS 140-3 Level 3 BSI AIS 20/31 compliant eIDAS and Common Criteria EAL4+	FIPS 140-2 Level 2 and Level 3 (historical)	FIPS 140-2 Level 3* (historical); u.trust GP HSM Se-Series: FIPS 140-3 Level 3 (#5223)	FIPS 140-3 Level 3 (v2.4, certificate #5302); FIPS 140-2 Level 3 (v2.2, historical)	FIPS 140-2 Level 3* (historical); FIPS 140-3 Level 3 pending
Compliance	- UL, CSA, CE - FCC, CE, VCCI, C-TICK, KC Mark - RoHS2, WEEE - TAA	UL, CSA, CE, FCC, RoHS3, WEEE, TAA, 80 PLUS Platinum	- UL, CSA, CE - FCC, KC Mark, VCCI, CE - RoHS, WEEE	UL, CE, FCC, RCM, Canada ICES, RoHS2, WEEE, REACH	UL, CE, FCC, RCM, and Canada ICES RoHS2, WEEE	CE, FCC Class B UL, IEC/EN 60950-1 CB certificate RoHS II, WEEE	FCC CE WEEE ROHS	- UL, CSA, CE - FCC, KC Mark, VCCI, CE - RoHS, WEEE - India BIS [IS 13252 (Part 1)/IEC 60950-1]
Management	M of N support for division of command	Quorum (M of N) and multi-factor authentication; APIs and CLI; container-based multi-tenancy	M of N support for division of command	M of N Support nShield Remote Configuration (available on Serial Console-configured models) nShield Remote Administration (purchased separately) nShield Monitor (purchased separately)	M of N support	M of N Support	Mutual authentication and secure channel between applications and the YubiHSM 2 YubiKey authentication Role based Access Control M of N unwrap key restore via the YubiHSM Setup Tool M of N key splitting for backup and recovery Network sharable	Password + OTP
Logging	Syslog	rsyslog; secure audit logging		Secure audit logging Syslog diagnostics support and Windows performance monitoring	Secure audit logging	Secure audit logging	Internal and host event logs limited to 62 lines.	Syslog
Monitoring	SNMP	BMC out-of-band diagnostics and hardware utilisation metrics		SNMP monitoring agent	SNMP monitoring agent	SNMP	SNMP	SNMP
Performance (Signing)	over 20,000 ECC and 10,000 RSA Operations per second for high	Not published (Thales claims up to 10x Luna 7 for	1024 RSA: 200 tps 2048 RSA: 63 tps P256 ECC: 43 tps	Base: 2048 RSA: 580 tps Mid: 2048 RSA: 3,460 tps High: 2048 bit RSA: 11,680 tps	2048 RSA: 2 tps 4096 RSA: 0.2 tps	SE12 (LAN) 2048 RSA: 16 2048 RSA (Bulk):	2048 RSA: +7 tps	Figures not available for 2048 bit RSA PL25

Feature	Thales Luna HSM 7	Thales Luna 8	Thales Luna USB HSM	Entrust nShield 5c/5s	Entrust nShield Edge	Utimaco SecurityServer Se Gen2	YubiHSM 2 FIPS	Thales ProtectServer 3/3+
	performance use cases	classical and 100x for PQC)	ECIES: 20 tps AES-GCM: 71 tps			16 4096 RSA: 2 4096 RSA (Bulk): 2 SE52 (LAN) 2048 RSA: 75 2048 RSA (Bulk): 80 4096 RSA: 11 4096 RSA (Bulk): 11 SE500 (LAN) 2048 RSA: 580 2048 RSA (Bulk): 2100 4096 RSA: 90 4096 RSA (Bulk): 220 SE1500 (LAN) 2048 RSA: 780 2048 RSA (Bulk): 3200 4096 RSA: 150 4096 RSA (Bulk): 360	• RSA-2048-PKCS1-SHA256: ~139ms avg • RSA-3072-PKCS1-SHA384: ~504ms avg • RSA-4096-PKCS1-SHA512: ~852ms avg • ECDSA-P256-SHA256: ~73ms avg • ECDSA-P384-SHA384: ~120ms avg • ECDSA-P521-SHA512: ~210ms avg • EdDSA-25519-32Bytes: ~105ms avg • EdDSA-25519-64Bytes: ~121ms avg • EdDSA-25519-128Bytes: ~137ms avg • EdDSA-25519-256Bytes: ~168ms avg • EdDSA-25519-512Bytes: ~229ms avg • EdDSA-25519-1024Bytes: ~353ms avg • AES-(128 192 256)-CCM-Wrap: ~10ms avg • HMAC-SHA-(1	1024 RSA: 25 tps PL220 1024 RSA: 220 tps PL3500 1024 RSA: 3,500 tps

Feature	Thales Luna HSM 7	Thales Luna 8	Thales Luna USB HSM	Entrust nShield 5c/5s	Entrust nShield Edge	Utimaco SecurityServer Se Gen2	YubiHSM 2 FIPS	Thales ProtectServer 3/3+
							256): ~4ms avg	
							• HMAC-SHA-(384 512): ~243ms avg	

5 Resources

5.1.1 Thales

<https://cpl.thalesgroup.com/encryption/hardware-security-modules/network-hsms>

<https://cpl.thalesgroup.com/encryption/hardware-security-modules/usb-hsm>

<https://thalesdocs.com/gphsm/ptk/protectserver3/docs/Home.htm>

<https://thalesdocs.com/gphsm/ptk/protectserver3/docs/PDF/Migration.pdf>

<https://data-protection-updates.gemalto.com/2021/05/03/thales-protectserver-3-hsms-now-available/>

https://thalesdocs.com/gphsm/luna/6.2.4/docs/network/Content/administration/scalable_key_storage/sks_using.htm

Luna 8 Network HSM product page

Introducing Luna 8 (Thales announcement, 4 August 2026)

Luna 7 FIPS compliance and validated firmware versions

ProtectServer 3 FIPS validation status

5.1.2 Entrust

<https://www.entrust.com/digital-security/hsm/products/nshield-hsms/nshield-connect>

<https://www.entrust.com/-/media/documentation/datasheets/entrust-nshield-connect-ds.pdf>

<https://www.entrust.com/digital-security/hsm/products/nshield-hsms/nshield-edge>

<https://www.entrust.com/-/media/documentation/datasheets/entrust-nshield-edge-ds.pdf>

<https://www.entrust.com/products/hsm/nshield-5c>

<https://www.entrust.com/blog/2024/06/entrust-nshield-5s-hardware-security-module-achieved-common-criteria-eal4-certification>

nShield 5c data sheet

Migrating from nShield XC to nShield 5 (end of sale information)

5.1.3 Utimaco

<https://hsm.utimaco.com/products-hardware-security-modules/general-purpose-hsm/securityserver-se-gen2/>

<https://hsm.utimaco.com/products-hardware-security-modules/general-purpose-hsm/securityserver-cse/>

https://hsm.utimaco.com/wp-content/uploads/2017/09/UTIMACO_Product_Brief_CSe_A4_20210118_final.pdf

https://hsm.utimaco.com/wp-content/uploads/2017/09/Utlimaco_Datasheet_SeGen2_A4_EN_Ir_20170512.pdf

u.trust General Purpose HSM Se-Series

u.trust GP HSM Se-Series FIPS 140-3 Level 3 certification

5.1.4 Yubi HSM

<https://www.yubico.com/au/product/yubihsm-2-fips/>

<https://www.yubico.com/products/hardware-security-module/>

<https://resources.yubico.com/53ZDUYE6/at/q4bsft-z2wi8-fo7aag/213367-Collateral-YubiHSM2-Product-brief-update-r3.pdf>

<https://resources.yubico.com/53ZDUYE6/at/k76bjgrqv9mfxkkg53gt3f/213134-YubiHSM2-solution-brief-r2.pdf>

https://developers.yubico.com/YubiHSM2/Usage_Guides/YubiHSM2_for_ADCS_Guide/Backing_Up_Key_Material.html

https://developers.yubico.com/YubiHSM2/Usage_Guides/YubiHSM2_for_ADCS_Guide/Key_Splitting_and_Key_Custodians.html

YubiHSM 2 FIPS 140-3 v2.4 product page

Yubico FIPS 140-3 validation announcement

YubiHSM 2 logging (62 entry log store)

Security Advisory YSA-2024-03

5.1.5 Other devices

Below is a short list of other providers of HSMs. The list is not exhaustive.

- Atos / Eviden Trustway Protezione
- Crypto4A
- Cryptomathic
- Engage Black
- Fortanix
- Futurex
- Marvell LiquidSecurity
- Nitrokey NetHSM
- Quintessence Labs
- Securosys
- Ultra (formerly AEP and HSM now discontinued)
- Cloud:
 - AWS Cloud HSM
 - Cogito Hardware Security Module as a Service (HSMaaS)
 - Cogito Key Management as a Service (KMaaS)
 - Google Cloud Key Management
 - Microsoft Azure Dedicated HSM (closed to new customers; successor is Azure Cloud HSM)
 - StrongKey