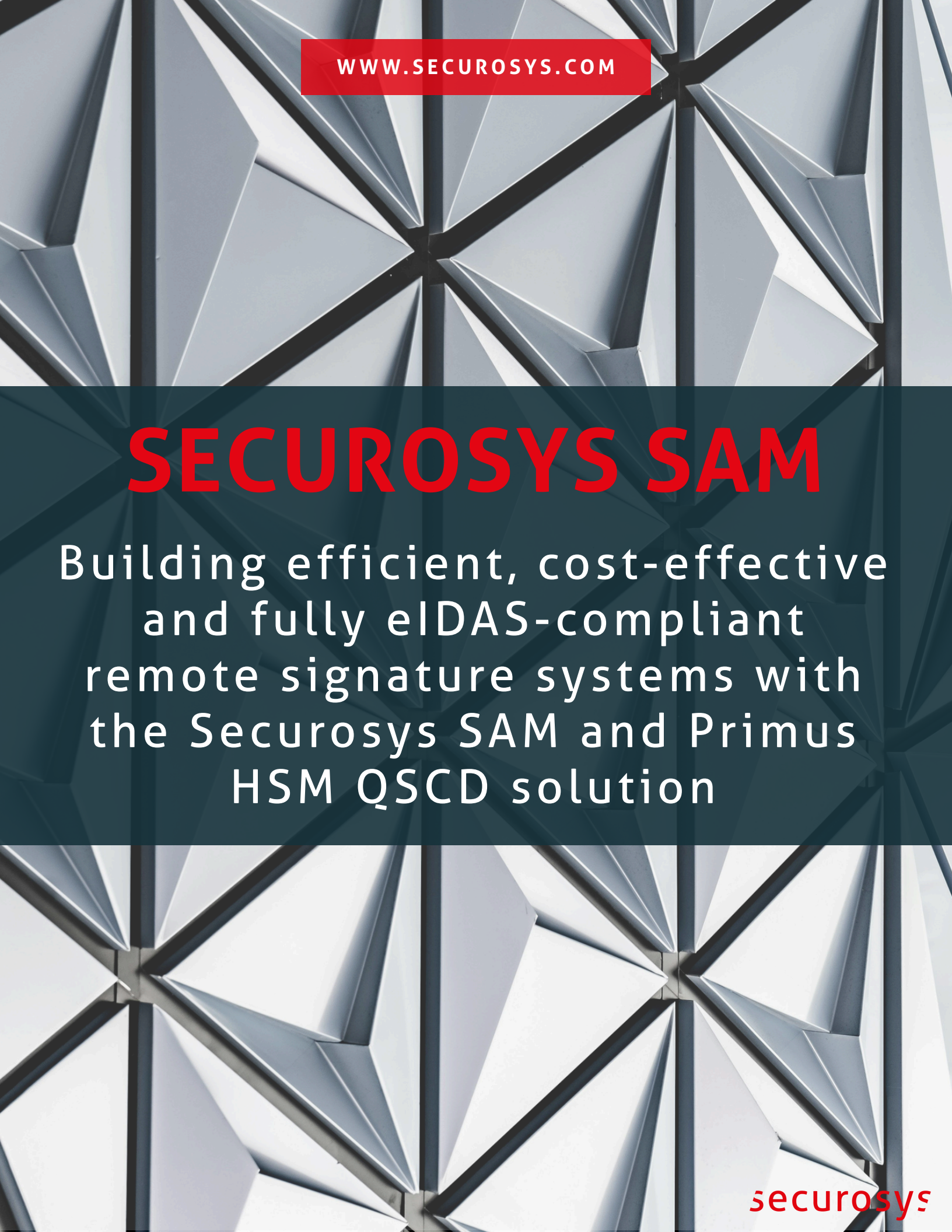


WWW.SECUROSYS.COM

SECUROSYS SAM

Building efficient, cost-effective and fully eIDAS-compliant remote signature systems with the Securosys SAM and Primus HSM QSCD solution

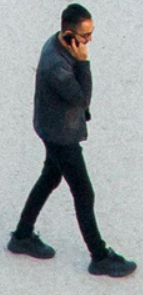
securosys

EXECUTIVE SUMMARY

In this paper we address the need for a Signature Activation Module (SAM) in remote signature systems complying with the EU's eIDAS regulations. We explain how the Securosys Smart Key Attributes (SKA) capability already addresses the need for strong authentication of the signing key's owner, uniquely enabling SAM functionality natively within a Securosys Primus HSM.

The EU's eIDAS regulation, these initials standing for Electronic IDentification, Authentication and trust Services, first came into effect in 2016. eIDAS also forms the basis for the ZertES regulation introduced in Switzerland in 2017: A Qualified Electronic Signature (QES), as defined under eIDAS, is considered the legal equivalent of a physical 'wet ink' signature.

While Hardware Security Modules (HSMs) are critical components of any eIDAS system and enable the use of QES, most HSMs were not designed to strongly authenticate individual key owners. For this reason, the latest revision of the eIDAS standard mandates the use of a Signature Activation Module to ensure that any signing or sealing key can only be used by its rightful owner. While legacy HSMs require an external SAM element to be deployed, Securosys Primus HSMs include an embedded SAM based on our established and patented Smart Key Attributes feature.



INTRODUCTION TO THE EIDAS REGULATION AND ASSOCIATED TERMINOLOGY

eIDAS (Electronic Identification, Authentication and Trust Services) is a European Union regulation that establishes a framework for secure electronic transactions across borders. It aims to create a unified and trustworthy environment for digital interactions within the EU, ensuring the security and legal validity of electronic identification and trust services. Essentially, the purpose of eIDAS is for digital signatures to carry the same legal validity across the EU as wet ink signatures on paper. When we refer to a digital signature, we mean a cryptographic signature. This differs from a simple electronic signature, which uses no cryptography and is therefore more susceptible to tampering.

For many years, various local laws and guidelines across European member states governed digital certificates, digital and electronic signatures and trust services. The eIDAS regulation was designed to establish mutual recognition, ensuring that certificates and electronic IDs issued in one EU member state are recognized and accepted in others. This framework facilitates secure, cross-border access to services across the EU. eIDAS defines and regulates the elements within trust services like digital signatures and seals, website authentication, and time stamping, guaranteeing their reliability and legal validity. It aims to harmonize rules and standards for electronic identification and trust services across the EU, promoting interoperability and reducing barriers to digital transactions.

eIDAS also forms the basis of Switzerland's ZertES (Federal Act on Electronic Signatures in Switzerland) regulations. However, it should be noted that the two are distinct legal frameworks: digital certificates issued under Swiss law are not automatically recognized under eIDAS, and vice versa.

Equally, in the United Kingdom, the eIDAS regulations were incorporated into UK Law prior to Brexit, but "although UK eIDAS allows the legal effect of EU eIDAS qualified trust services to continue to be recognised and used in the UK, no reciprocal agreement currently exists. This means UK eIDAS qualified trust services are not automatically recognised and accepted as equivalent to qualified trust services in the EU".*[1]*

Within eIDAS, there are two distinct classes of digital signatures, referred to as Qualified Electronic Signatures (QES):

/ **Local Signing**: The user holds their key material on a smart card or USB token. This requires careful protection of the physical device as well as the installation of readers, drivers, and software on the user's computer(s). This approach may prevent the use of mobile devices such as smartphones and tablets for digital signatures.

[1] Information Commissioner's Office Website, https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation/, 2025

/ **Remote Signing**: The key material is stored centrally by a Qualified Trust Services Provider (QTSP). Many end-users and organizations have adopted this approach, valuing its reliability, security, and cost effectiveness.

Regardless of the approach, it is essential to protect the key material used for these signing operations. In Public Key Cryptography, which underpins digital signatures, it is the private key that holds all the power; thus, the system's security depends on its protection. For local signatures, this protection is typically ensured through a smart card or USB token – these devices are referred to as Secure Signature Creation Devices (SSCD). For remote signatures the protection is ensured by a Hardware Security Module (HSM).

Securosys CyberVault HSM. Image: Securosys SA

An HSM provides several functions, including:
/ **Strong key generation**. Most standard workstations and servers struggle to generate sufficiently random numbers as a basis for cryptographic key material. HSMs typically include a dedicated hardware-based Random Number Generator (TRNG) component, to ensure that any keys used are entirely random.
/ **Ongoing key protection**. All cryptographic operations, such as the encryption, decryption, or digital signing of data, code, and transactions, occur within the physical boundary of the device. This ensures that cryptographic keys are not in the memory of a physical or virtual server, where they would be exposed to attacks such as memory inspection, core dumps, snapshots and so on.
/ **Backup and recovery**. The most effective HSM designs ensure not only that the key is protected from being stolen, but also that it remains available in the event of hardware failure. This can be achieved through an HSM cluster, where key material is automatically synchronized across devices, or through a secure backup facility, where keys can be exported in strongly encrypted form to a USB drive or network.

In eIDAS, an HSM is referred to as a Cryptographic Module (CM). For local signatures the smartcard or USB token acts as the CM – the end user has sole control over it and is responsible for its usage and protection. Any QTSP offering qualified remote signing to their customer base must protect keys using what is known as a Type 2 QSCD. A Qualified Signature Creation Device (QSCD) is the combination of a Cryptographic Module and a Signature Activation Module (SAM). The SAM is mandated in an eIDAS architecture for remote signatures to ensure 'sole control' of signing or sealing keys by their rightful owner. Most HSM designs lack the ability to apply individual access control policies to all protected keys or to enforce strong authentication for key usage. The SAM component provides this functionality, enabling strong end-user authentication within the QTSP's system.

REMOTE SIGNING WITH EIDAS 2.0

In the previous section, we introduced the concept of remote signing. Remote signing removes the requirement for local security hardware, allowing users to sign from various connected devices, such as mobile phones, tablets and laptops, where using tokens or smartcards may prove impossible or unwieldy. Even when suitable drivers and physical interfaces to insert those SSCD devices are available, connection and compatibility issues can generate a significant volume of technical support calls and downtime. Additionally, these portable tokens are easily lost by end users, creating further administrative overheads.

We also established that, in a remote signing architecture, keys are held remotely for users by a Qualified Trust Services Provider (QTSP) within a Qualified Signature Creation Device (QSCD or SCDev). There are extensive eIDAS and European Telecommunications Standards Institute (ETSI) standards defining the requirements for these systems. Under eIDAS Regulation (EU) No 910/2014, any device managed on behalf of a user by a QTSP can only be considered a QSCD when duly operated by that QTSP in accordance with the regulation. Links to the relevant standards documents are provided later in this white paper. In April 2024, the (EU) 2024/1123 updates to the eIDAS Regulation were introduced. These amendments, which came into effect on May 20, 2024, are referred to as eIDAS 2.0.

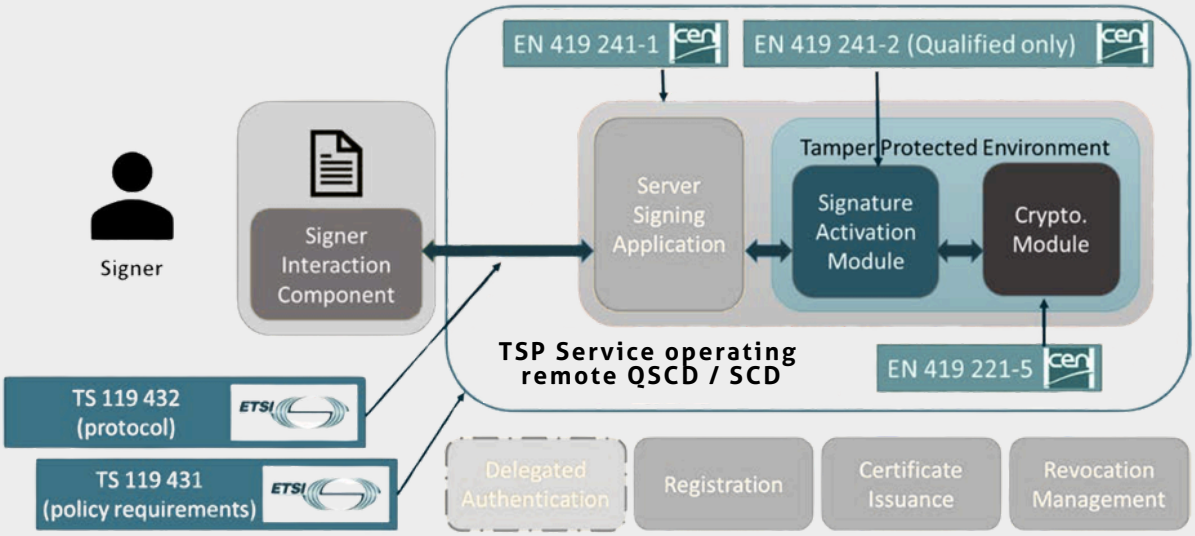


Figure C.1: Scope of standards on the different remote signing components

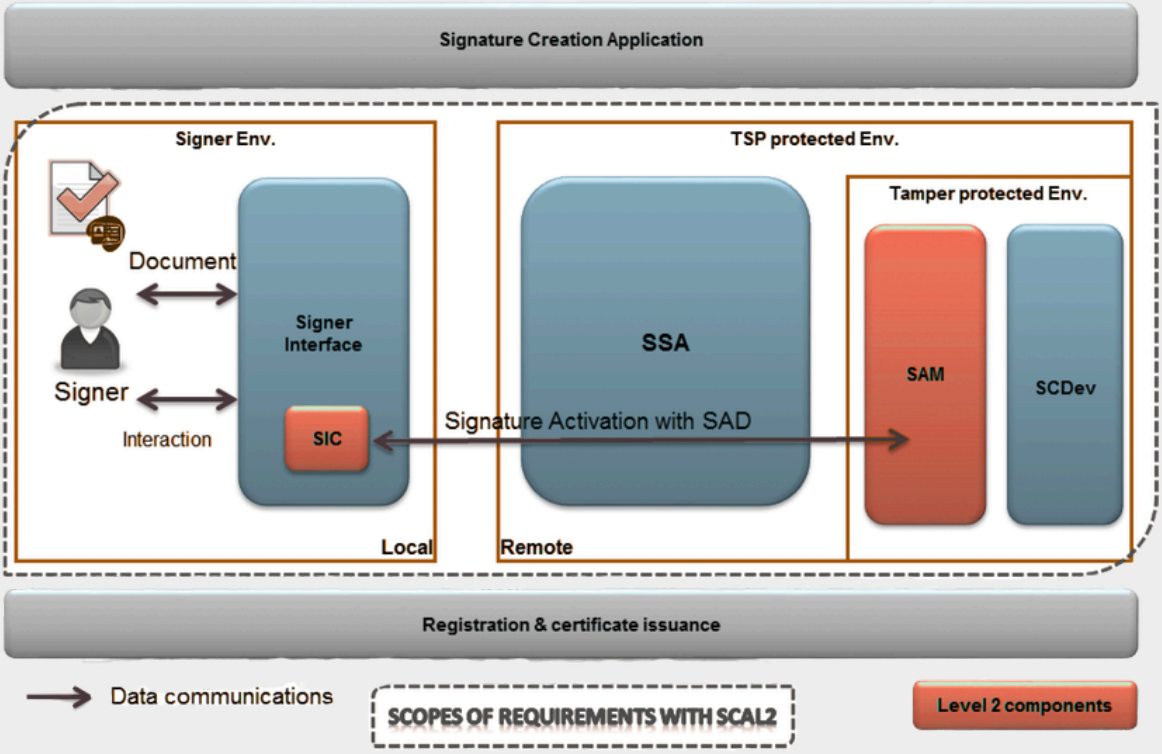
The diagram above is included in ETSI TS 119 431-1 V1.3.1 (2024-12) – "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev" and illustrates the standards applicable to any eIDAS 2.0 remote signing architecture. The Signature Activation Module (SAM) is depicted, defined under EN 419 241-2 ("Trustworthy Systems Supporting Server Signing – Part 2: Protection profile for QSCD for Server Signing"), specifically for qualified signing, introduced as part of eIDAS 2.0.

https://www.etsi.org/deliver/etsi_ts/119400_119499/11943101/01.03.01_60/ts_11943101v010301p.pdf. Page 29. V1.3.1, December 2024.

The SAM's role in this architecture is to ensure that users retain sole control over their signing keys. The eIDAS regulations define two distinct levels of sole control:

/ Sole Control Assurance Level 1 (SCAL1)
Under SCAL1, signing keys are used under the sole control of the signer, with a low level of confidence. The Server Signing Application (SSA), as shown in the diagram above, is entirely responsible for authentication in software.

/ Sole Control Assurance Level 2 (SCAL2)
Under SCAL2, signing keys are used under the sole control of the signer, with a high level of confidence. In this case, the Signature Activation Module, also illustrated above, handles user authentication within a tamper-protected environment.



TUnder SCAL2, the authorized signer's use of their signing key is enforced by the Signature Activation Module (SAM), as is illustrated in the above diagram from CEN EN 419 241-1[MA1] . The signer is supplied with a Signer Interface, also referred to as the SIC (Signer Interaction Component). Through this interface, the signer supplies Signature Activation Data (SAD) to the SAM using the Signature Activation Protocol (SAP), thereby enabling the use of the corresponding signing key.

file:///C:/Users/martina.alig/Downloads/ETSI%20standards%20for%20trust%20services%20and%20digital%20signatures%20-%207%20Remote%20signingV2.pdf

securosys

GRANULAR KEY CONTROL WITH SMART KEY ATTRIBUTES (SKA)

Hardware Security Module (HSM) designs are typically very effective at protecting machine identities - a relatively small number of keys used by a set of server applications. However, their limitations become apparent when there is a requirement to protect user identities, where the HSM must protect much larger numbers of keys for exclusive use by their owners, each requiring individual authentication actions for every key operation.

Granular Key Control

Most HSM designs suffer from shortcomings around authentication. Once an application or system has been authenticated, all keys stored within an HSM partition - another name for a subset of key material stored within an HSM - can be accessed without additional checks. This creates a potential risk, as it would allow attackers to use sensitive key material to sign or decrypt transactions, simply by installing rogue code on an authenticated host systems. In contrast, Smart Key Attributes (SKA) technology enables every individual key protected by a Securosys Primus HSM to be assigned its own specific usage policies.

Applications and Use Cases

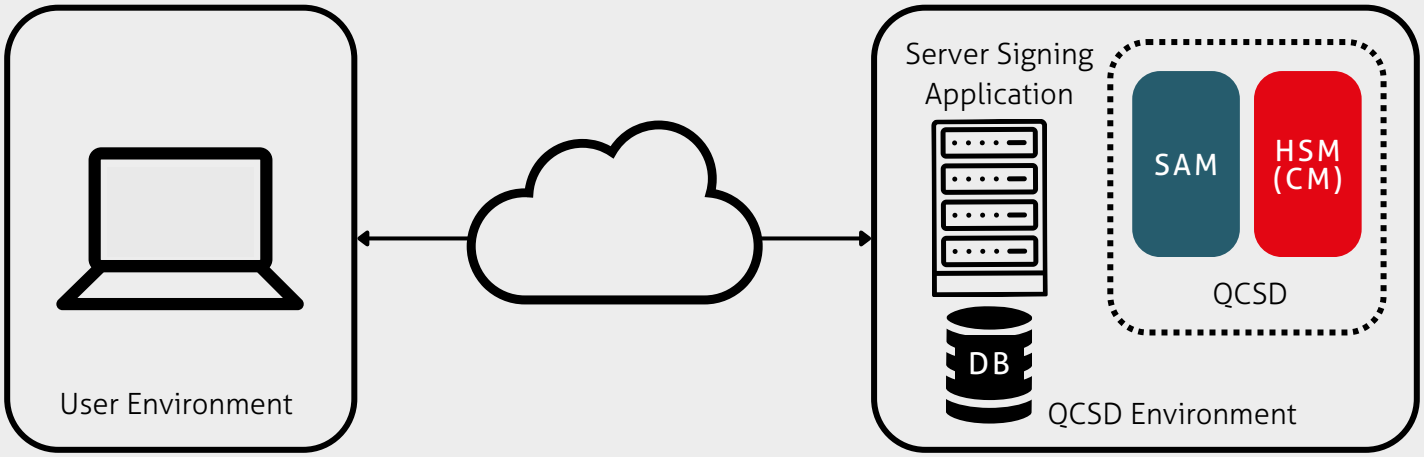
This fine-grained authorization capability enables companies to establish rules governing HSM operations on a per-key basis. Organizations can define authorization policies that align directly with specific business processes by assigning key material with corresponding SKA rules. Naturally, some processes require more complex key usage controls, depending on their sensitivity and context. Common use cases include individual signing keys, such as those used for remote qualified signatures, and multi-key access related to electronic company seals, which may require multiple signatures from two or more parties. SKA has also been widely adopted in demanding cryptocurrency implementations.

Potential applications might include:

/ Digital signatures (remote signing service with authorization)
/ Digital seals (requiring multiple approvals)
/ Timed approvals
/ Multiple approvals within different timeframes (for example, gathering authorization from three out of a group of five separate approvers within a four-hour timeframe, or obtaining a single authorization from any of six different approvers within a week)
/ Multiple approvals across different departments and/or groups within a single business entity (for example obtaining approvals from the Board of Directors, the CFO, and perhaps the Purchasing Department Manager)
/ Multiple approvals across different departments and/or groups within a single business entity (for example obtaining approvals from the Board of Directors, the CFO, and perhaps the Purchasing Department Manager)

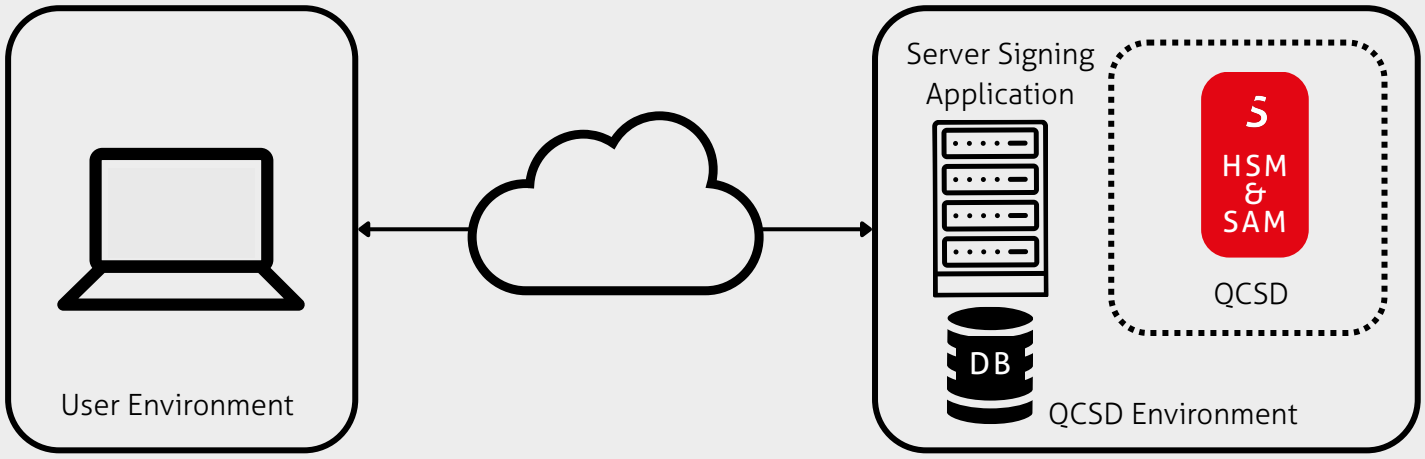
THE SECUROSYS SIGNATURE ACTIVATION MODULE

The diagram below depicts the combination of a Hardware Security Module operating in conjunction with a Signature Activation Module to act as a full Qualified Signature Creation Device for an eIDAS remote signing architecture. In terms of the relevant standards, under eIDAS a QSCD (Qualified Signature Creation Device) is defined as the combination of an HSM (known as a Cryptographic Module/CM in eIDAS and certified under Common Criteria EAL 4+ with Protection Profile CEN EN 419 221-5) and a SAM (Signature Activation Module, certified to CEN EN 419 241-2).



As previously established, the SAM component of a QSCD solution ensures that all users within a QTSP system retain sole control of their signing keys. This requirement emerged because the majority of HSM designs originated in the last century, long before the introduction of strict regulatory frameworks such as eIDAS. Traditional HSMs provide limited controls over individual key usage – once an HSM or a 'partition' (subset) of the HSM has been authorized or 'activated' using the right credentials, any key stored there can be used with no further verification. Consequently, a standalone SAM becomes a vital component, but one that must be developed in-house or purchased by any QTSP. This SAM functionality must also be certified, maintained and re-certified repeatedly throughout the entire lifecycle of the remote signing offering.

In the previous section, we introduced the Smart Key Attributes (SKA) functionality. This technology allows every key protected within a Securosys Primus HSM to be assigned its own distinct, individual rules and criteria. SKA was originally designed with eIDAS compliance in mind, supporting additional multi-signature (multi-party) controls and powerful conditional policies. These features, widely adopted by Securosys customers for cryptocurrency deployments, can also be used to manage access to company seals in eIDAS-based architectures. This existing foundation allows a Primus HSM, uniquely, to operate as a full QSCD without additional software. It is only necessary to enable 'SAM Mode' for the partition of the HSM being used by the Server Signing Application (a partition being the mechanism for separating key material within a Primus HSM device), thereby eliminating the need for an external SAM, as shown below.



This integrated approach offers several benefits for QTSPs providing remote signing services to their customer base:

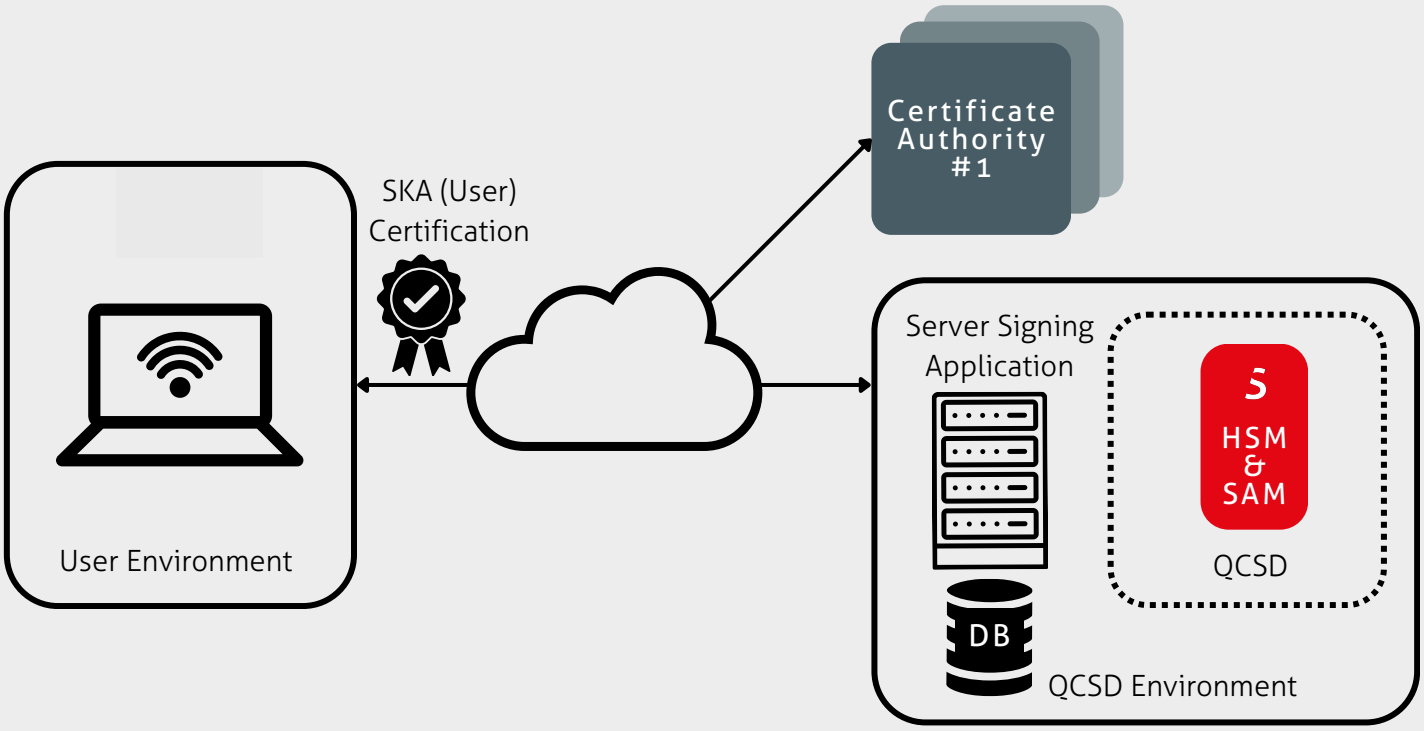
/ No SAM development or certification required.
There is no need to develop your own SAM functionality or put it through certification. This saves any QTSP considerable time and expense. Development and certification are typically estimated at around 18 months, with associated costs exceeding 500,000 USD.

/ No dependency on third-party SAM providers.
There is no need to purchase an additional external SAM from a third-party. The entire QSCD (CM/HSM and SAM) is delivered by the same supplier. This reduces cost, ensures ongoing compatibility and simplifies technical support. There is no risk of the HSM and SAM suppliers deciding to discontinue their collaboration following a disagreement, change of ownership or strategic decision to move away from a particular market. Many customers have experienced the impact of such situations over the years.

/ Full SAM security within the HSM boundary.
Smart Key Attributes are defined and processed entirely within the tamper-protected physical boundary of a Securosys Primus HSM. This fully satisfies the security requirements for SAM operation, entirely removing the need to execute additional custom logic within the HSM or to develop against or license secure execution functionality.

/ Seamless integration.
Calls from the signing application to the HSM remain unchanged. There is no need to completely rewrite HSM calls in existing code, that already use the Securosys REST API, JCE or PKCS#11 APIs.

SAM Mode is enabled per partition in each Primus HSM, allowing a mix of eIDAS and non-eIDAS key usage within the same hardware. User identification is achieved via PKI certificates, as shown in the diagram below and described in detail in the following section.
Added title lines for better structure, let me know what you think.

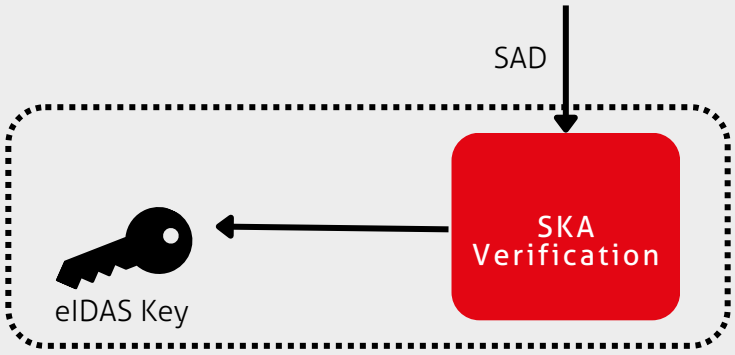


High-level architecture diagram – The user obtains a certificate from the Certificate Authority, which is then used to authorize signing requests passed through SSA on to QSCD where signing key is stored.

We started this section by outlining the standards required for a full Qualified Signature Creation Device (QSCD). The first-generation Securosys Primus HSM design was certified for EAL 4+ (PP CEN EN 419 221-5) by OCSI in Rome, April 14, 2021. This certification remains valid until April 14, 2026. Renewal of this certification, and re-evaluation of the Primus HSM as a QSCD including SAM, according to EN 419 241-2, is currently in progress. Full re-certification will be achieved before the end of Q4 2025.

CONFIGURING THE SECUROSYS SIGNATURE ACTIVATION MODULE

Previously in this white paper, we introduced the concept of sole control. As established, the role of the Signature Activation Module (SAM), is to verify the identity of the owner of each cryptographic key within an eIDAS remote signing architecture. It handles the authorization of key usage, ensuring that data can only ever be digitally signed under the sole control of its rightful owner.



Incoming Signature Activation Data verified against SKA policy within the Primus HSM to control key usage.

Assigning an owner to a signing key is achieved through the Smart Key Attributes (SKA) functionality. These SKA parameters are defined when each key is created. [RS1] [RS2] Identity provision is delegated through the use of standard X509 certificates, which are used to identify the owner of each key. These certificates are obtained from a Certificate Authority (CA). This can be a commercial, public, external CA such as DigiCert, Sectigo. GlobalSign, GeoTrust or SwissSign, or an internal, privately managed CA system. An array of multiple CAs can be specified where required. Each CA must be whitelisted within the HSM configuration so that valid user certificates issued by that CA are trusted. [RS3] This CA whitelisting can only be performed by a privileged manager - for a Primus HSM this role is the Security Officer (SO) or Partition Security Officer (PSO). Note that in SAM Mode, full certificates are onboarded into the SKA policy, not just the public key.

Once the 'root' or top-level certificate [MA4] for a CA has been imported, individual user certificates issued under that root CA are now trusted for use within the system, provided the common name and signature are valid and correct. The specific SKA attribute relating to SAM usage is 'sam-approved';

Attribute	Meaning of True	Meaning of False	Allowed Changes	Comments
sam-approved	SKA key can be used for SAM approval.	SKA key can NOT be used for SAM approval. or SAM not activated	Set by HSM. Not user-modifiable	Signature Application Module (SAM) for eIDAS use cases.

The above is a snippet from the complete SKA attributes table in our documentation. Further details on the use of SKA and enabling SAM functionality can be found in the Securosys documentation:
https://docs.securosys.com/ska/overview
https://docs.securosys.com/ska/Concepts/attributes/#access

ABBREVIATIONS

CA - Certificate Authority
CEN - Comité Européen de Normalisation (European Committee for Standardization)
CM - Cryptographic Module (an HSM)
eIDAS - Electronic Identification, Authentication and Trust Services
ETSI - European Telecommunications Standards Institute
HSM - Hardware Security Module
PKI - Public Key Infrastructure
PP - Protection Profile
QES - Qualified Electronic Signature
QSCD - Qualified Signature Creation Device
QTSP - Qualified Trust Services Provider
RNG - Random Number Generator
SAD - Signature Activation Data
SAM - Signature Activation Module
SAP - Signature Activation Protocol
SCAL1/SCAL2 - Sole Control Assurance Levels 1 and 2
SCDev - Signature Creation Device
SIC - Signer Interaction Component
SSA - Server Signing Application
SSCD - Secure Signature Creation Device
USB - Universal Serial Bus

REFERENCES

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0910-20241018

Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance)
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016D0650

ETSI EN 319 411-1 V1.4.1 (2023-10)
"Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements"
https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.04.01_60/en_31941101v010401p.pdf

eIDAS 2.0 | Updates, Compliance
https://www.european-digital-identity-regulation.com/

ETSI TS 119 431-1 V1.3.1 (2024-12)
"Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev"
https://www.etsi.org/deliver/etsi_ts/119400_119499/11943101/01.03.01_60/ts_11943101v010301p.pdf

Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur, ZertES)
https://www.fedlex.admin.ch/eli/cc/2004/788/de

UK Information Commissioner's Office – "What is the eIDAS Regulation?"
https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation/#:~:text=Although%20UK%20eIDAS%20allows%20the,trust%20services%20in%20the%20EU.

SUMMARY

The 2024 eIDAS regulation updates mandate the use of a Signature Activation Module (SAM) for remote qualified signing. All Qualified Trust Services Providers (QTSPs) face various decisions when deploying the most efficient architecture possible to meet the requirements of eIDAS 2.0. As discussed in this paper, the Securosys approach offers many significant benefits, including:

/ **Modern design.** While most legacy HSM architectures predate eIDAS, the Securosys Primus design was directly influenced by these concepts. The Smart Key Attributes (SKA) feature is native to the HSM, enabling a more elegant solution for delivering integrated SAM functionality. This same modern architecture allowed Securosys to introduce comprehensive, high-performance Post Quantum Cryptography algorithms ahead of the market.
/ **Integrated, comprehensive solution.** Deploying a Primus HSM removes the need to build your own SAM functionality or purchase a standalone SAM component from a third party.
Technical Support for your combined QSCD solution will come from a single supplier, one with a long-term commitment to the HSM market.
/ **Single API.** SAM modules are typically developed by separate organizations or engineering teams, requiring developers to juggle multiple unrelated APIs. The Securosys approach consolidates these interfaces, simplifying development and integration.
/ **No competitive challenges.** Securosys does not supply PKI or Signing Server solutions; our exclusive focus is on delivering best-in-class Hardware Security Modules.
/ **Online testing available.** Customers and partners can obtain online access to our CloudHSM Sandbox to test HSM/QSCD and SAM functionality with an actual HSM device. This ensures that test results accurately reflect real-world production behavior, while also eliminating the inherent risks of software simulators that could be subject to reverse engineering or compromise.
/ **Full certification.** Re-certification will be completed before the end of Q4 2025, achieving full QSCD certification for the Primus HSM, including SAM, according to EN 419 241-2.
As standards evolve in the future, the complete Securosys QSCD solution will be re-certified, ensuring continued compatibility and avoiding potential scenarios where HSM and custom, third-party or standalone SAM offerings are at different stages of certification and compatibility.

The Securosys Primus HSM range, with its Secure Key Attributes technology and native SAM Mode, represents the optimal solution for any eIDAS QSCD requirement.

For more information about our solutions, or to evaluate Securosys Primus HSMs and our Signature Activation Module technology, please contact us directly:
https://www.securosys.com/en/contact

ABOUT US

Securosys SA, headquartered in Zurich, Switzerland, is a renowned industry leader specializing in cybersecurity, encryption, as well as digital identity and online keys protection. Founded in 2014, Securosys' hardware security modules (HSMs) secure transactions exceeding 100 billion euros daily on the Swiss banking system SIC (under the supervision of the Swiss National Bank) as well as the Swiss stock exchanges SIX and SDX. Over half of the world's Tier 1 banks and numerous technology companies trust the HSMs developed and manufactured by Securosys in Switzerland.

Securosys' comprehensive HSM solutions, available both on-premises and as a service in the cloud, are certified to the highest security standards, including FIPS and Common Criteria. Designed for diverse industries including finance, healthcare, and government, Securosys HSMs offer unparalleled features such as independent, cryptographically secure partitions, patented policy-based individual key protection, and cloud readiness. The devices support hybrid signatures, ensuring a seamless transition from classical to post-quantum cryptographic (PQC) algorithms.