TRUST hub®

e-Signature, e-Seal & Timestamp
Identity & Access Management
Document Notarization

GURUCUBE
Trusted Identity Solutions

THE SAFEST AND MOST COMPLETE ENVIRONMENT TO TRUST

TrustHub® is the most modern, complete and secure identification, authentication, signature and notarization solution on the market. Due to its modular structure that can be cloud-based or on-premise or a mix of the two, it provides an incredible variety of configurations.

SIGN processes all the signing, validation and sealing operations, managing the entire life cycle of the certificates.

CIPHER encrypts sensitive documents and information of all kinds, including biometric data, graphometric data and GPS coordinates.

ABIS stores and compares biometric data operating both as an internal validator and as a digital interface to external QTSP.

IAM is the advanced digital identity manager that securely and reliably identifies users on TrustHub®.

CHAIN decentralizes information about operations and documents by notarizing it in the BTC Block Chain.

Each microservice operates completely autonomously and is physically and logically isolated from the others. With encrypted databases and data that need to be integrated to be consistent, any system violation does not entail a real risk to users' privacy as single data breach does not expose any consistent data.

The modular structure of TrustHub® built around its main independent nodes allows, on the one hand, to sectorize the type of services provided through the APIs and, on the other, by relating the nodes and their intermediation chronology in different ways, to provide services completely new, different, vertical and highly personalized depending on the needs.

STRONG AUTHENTICATION AND USERS FEDERATION

TrustHub® is an advanced authentication and identity management system based on protocols such as OpenID Connect, OAuth2 and SAML that allows authenticating both users registered directly in TrustHub® and those registered into independent nodes of SIGN or into another IAM. In addition, it allows the addition of a second authentication factor with OATH tokens with Google Authenticator® or FreeOTP® and the use of biometric or graphometric information to be used as 2FA or direct authentication.

Trusthub® IAM natively supports the simultaneous authentication of more users at the same time in the same session, thus certifying the presence or contemporary assistance of a group of users in the same place or event. In addition, it can automatically synchronize with Microsoft® Active Directory®, LDAP directories, or Active Directory Federation Services (ADFS). TrustHub® also has a proprietary strong authentication mobile application for iOS and Android (TrustHub® OATH)

BIOMETRIC IDENTIFICATION

The TrustHub® ABIS system can securely store the biometric data of the face, fingerprints, voice, palms, iris and the graphometric data of the signature of each user. The biometric database is encrypted and physically and logically separate from the IAM personal database. Its powerful search engine allows 1:1 and 1:N data comparison. All information is collected under NIST standards and is stored in ISO format to guarantee complete interoperability and to be able to make comparisons against public and QTSP databases.

EMEA
Gurucube S.r.l.
Turin ITALY

LATAM
Gurucube S.A.
Córdoba ARGENTINA

Sales: sales@trusthub.cloud
Support: support@trusthub.cloud
Website: www.trusthub.cloud

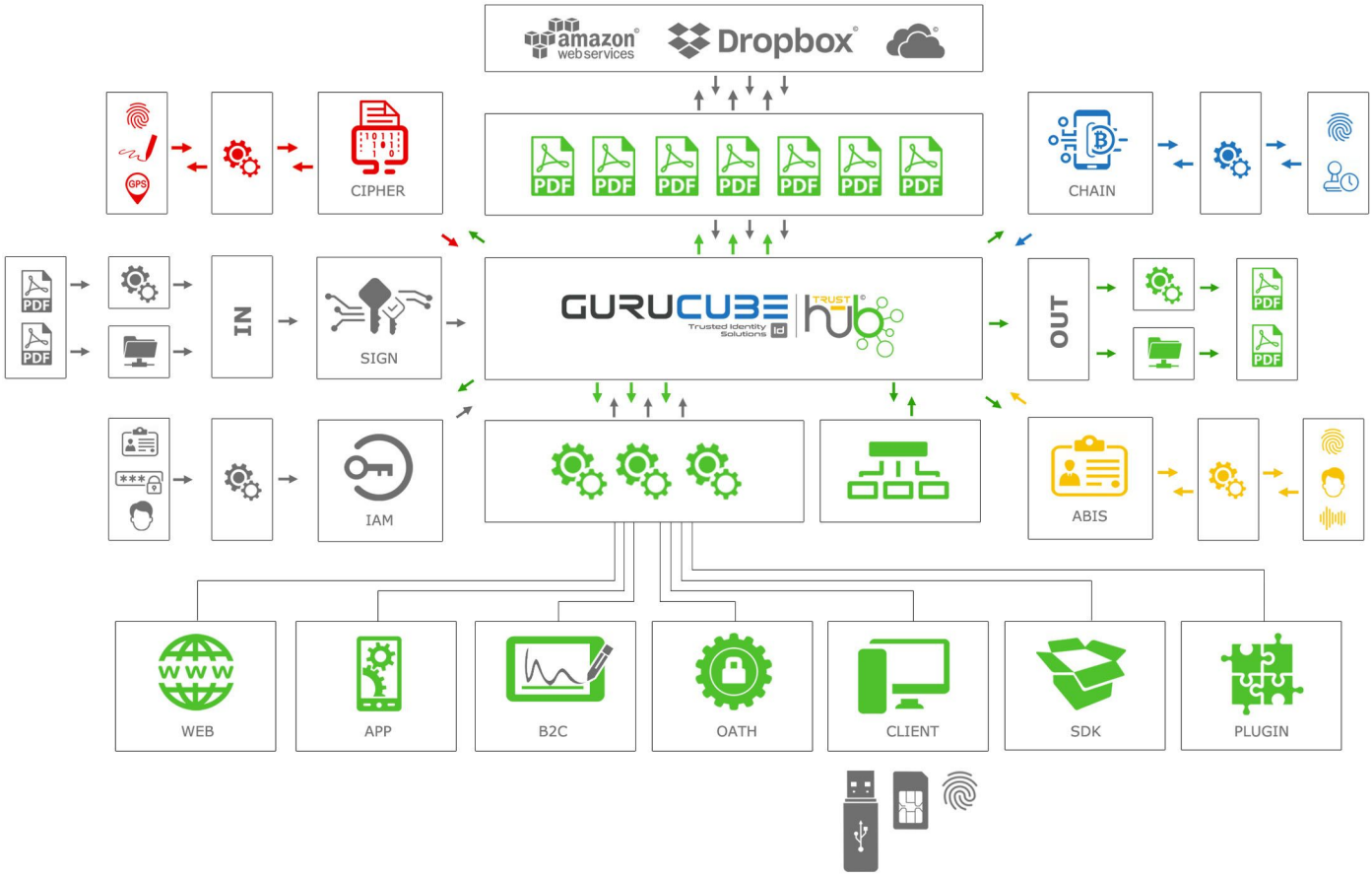
PRESENTIAL AND REMOTE BIOMETRIC ENROLLMENT

In addition to enrollment with validation by Mail or SMS under the eIDAS standard (deducted), TrustHub® provides a presential biometric enrollment process with fingerprints or remote with face and proof of life. The biometric data can be encrypted and stored locally in the TrustHub® ABIS for possible subsequent verification or be validated in real time against web services of Public Entities or QTSP. TrustHub® maintains a registry of the entities qualified for identity certification. Depending on the location, it applies the pre-established validation rules that grant legal value in each Country. TrustHub® guarantees the interoperability of the biometric data collected, the logical and physical separation between databases, their inalterability and full compliance with the regulations on personal data.

BLOCK CHAIN FILES NOTARIZATION

TrustHub® CHAIN is a time stamp based on the BTC blockchain defined as a notarization process. It allows notarizing one operation at a time or generating groups of notarized operations. This component, along with TrustHub® CIPHER, is transversal to all the other tools since, in addition to constituting a service by itself, it is used internally to provide a time stamp for all generated events. However, being based on distributed technology, TrustHub® CHAIN guarantees the immediacy of the sealing operation thanks to an advanced calendar system.

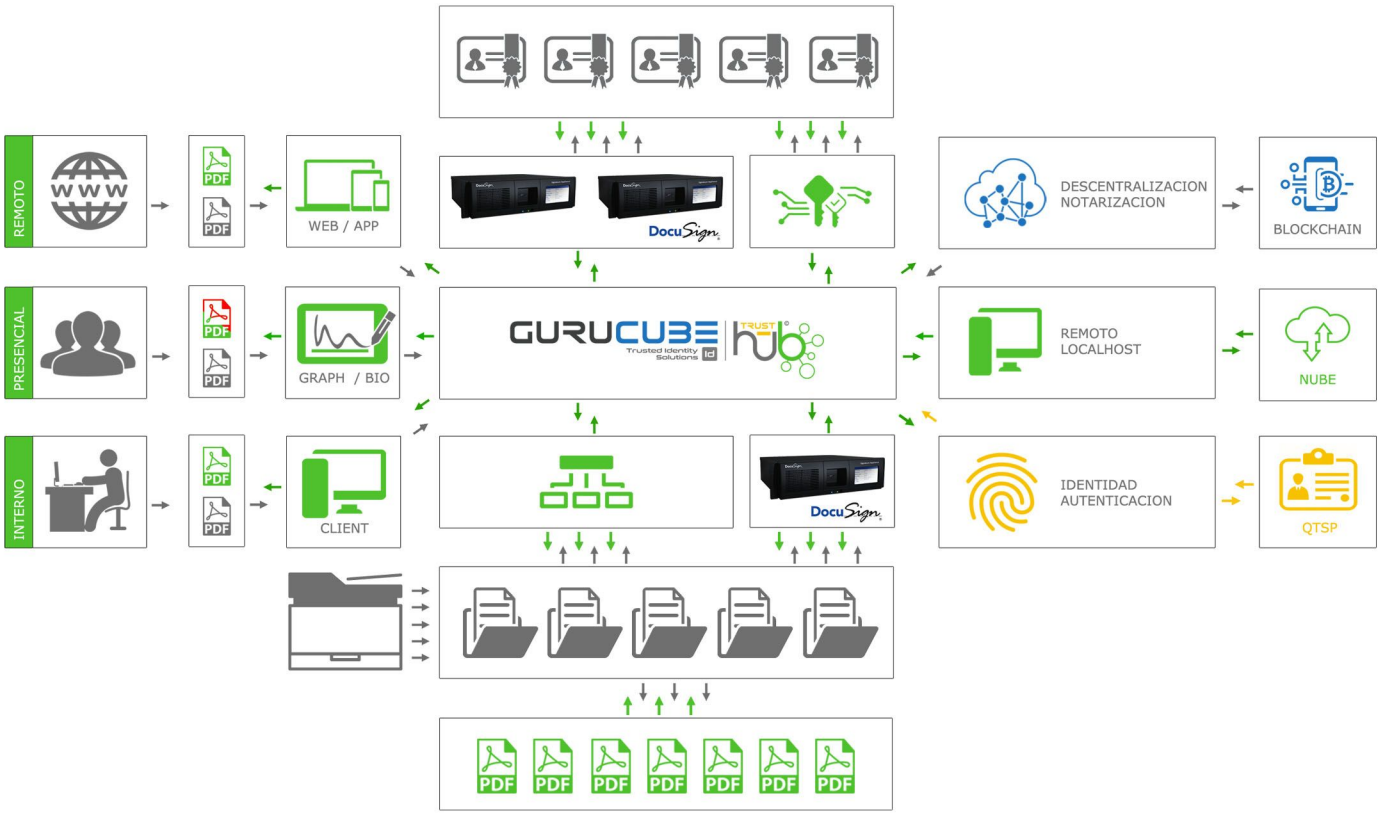
TrustHub® has its own encrypted space and is integrated with S3®, OpenKM®, Google Drive®, Dropbox®, and OneDrive®. In addition, thanks to TrustHub® CLIENT, it provides access to documents physically located on localhost.



EMEA
Gurucube S.r.l.
Turin ITALY

LATAM
Gurucube S.A.
Córdoba ARGENTINA

Sales: sales@trusthub.cloud
Support: support@trusthub.cloud
Website: www.trusthub.cloud



PROXY MODULE

TrustHub® PROXY allows the remote signature process to be transferred locally with the advantage of not having to send the most confidential documents outside the company's secure intranet at any time, saving significant bandwidth in the case of batch or document signatures of large dimensions and of being able to personalize the signature process and the signature itself in the document according to specific requirements, without giving up the benefits of centralized custody of the certificates.

HSM AS A SERVICE

TrustHub® can function as an integration service with remote HSMs, meaning that through its RESTful API it provides a powerful secure connection interface with DocuSign® DSA or Entrust® HSMs (alone or connected in a cluster) located anywhere in the world. In this configuration TrustHub® constitutes a logical and functional layer above the standard #PKCS11 interface, providing complete and centralized control over the signing keys stored in each HSM.

ENCRYPTION OF SENSITIVE BIOMETRIC OR GPS DATA

TrustHub® CIPHER can encrypt documents to make them viewable only under a specified decryption key. In the same way, it can encrypt biometric data such as fingerprints, palms, faces, irises, voice and, in general, any data that needs to be archived in a secure and non-alterable way to make it resistant to auditing or forensic analysis. You can also encrypt georeferencing data to legally guarantee the effective presence in a data place at a specific time.

TrustHub® RESTFul APIs allow a fast and complete integration of all identification, authentication, signing and notarization functionalities with any other application. They can be used with different programming languages and on different platforms including .PHP, .NET and JAVA applications. For integration in Java, a specific library is also available that allows further reduction of development time.

EMEA
Gurucube S.r.l.
Turin ITALY

LATAM
Gurucube S.A.
Córdoba ARGENTINA

Sales: sales@trusthub.cloud
Support: support@trusthub.cloud
Website: www.trusthub.cloud

LONG TIME VALIDATION

TrustHub® SIGN supports the PAdES-LTV format. In this way, a digitally signed PDF and PDF/A (ISO19005) document with an active certificate at the time of signing will continue to be valid even after its expiration. In order for this type of signature to show its Long-Term Validation (LTV) attribute, it is necessary to incorporate an x.509 (TSA) qualified time stamp into the process.

BIOMETRIC AND GRAPHOMETRIC SIGNATURE

TrustHub® SIGN allows you to sign documents using biometric data (ISO / IEC 19794-8), graphometric data (ISO / IEC 19794-7) or any other graphic sign or additional data. As a security measure and in compliance with European and International regulations on the processing of sensitive data, before saving the graphometric or biometric object with all the information on speed, acceleration, pressure, inclination, times, among others, or the coordinates and type of the minutiae of the fingerprint in the PDF repository, they are encrypted by the TrustHub® CIPHER which then seals the document with a digital certificate. In case of repudiation or signature challenge, TrustHub® provides the encryption key of the graphometric or biometric object necessary for forensic analysis.

QR CODE

TrustHub® marks each document with a unique QR code, which allows the authenticity of the document to be validated at any time.

COMPLETE CONTROL OVER THE ENTIRE SIGNATURE PROCESS

TrustHub® SIGN guarantees complete control over the documents throughout the entire signing process as they never leave the encrypted repository.

HSM remoto | Token USB | Smart Card

In the signing process with HSM, the concept of custody of the keys as the security of the signing process itself, is intrinsic since it is carried out in Common Criteria EAL4+ or FIPS 140-2 Level 3 certified HW located in the guarded infrastructure. by TrustHub®. The signing process with Token or Smart Card in return could introduce windows of possible alterations since it is developed locally on the signer's PC, outside the controlled perimeter. However, even in this condition, TrustHub® SIGN guarantees the security of the process by making only the hash of the document available for signature while the original is saved. It then verifies and compares the hashes using the received certificate to definitively sign the remote document.

ELECTRONIC REGISTRATION OF OPERATIONS

TrustHub®'s electronic transaction log records all data related to users' connection and activity on the platform. The registry is unalterable, each operation receives a time stamp and is decentralized in the BTC Block Chain.

CERTIFICATIONS

The Software and Service comply with eIDAS (Electronic Identification and Trust Services for Electronic Transactions) standards and NIST, ETSI, ISO, W3C, OASIS, IETF, Microsoft® and Adobe® technical standards for interoperability and security.

EMEA
Gurucube S.r.l.
Turin ITALY

LATAM
Gurucube S.A.
Córdoba ARGENTINA

Sales: sales@trusthub.cloud
Support: support@trusthub.cloud
Website: www.trusthub.cloud

CRYPTOGRAPHIC ALGORITHMS

RSA keys 1024-4096 bit (PKCS#1); Secure Hash Standard (SHA-1, SHA-256, SHA-384, SHA-512).

COMPATIBLES CERTIFICATION AUTHORITIES

TrustHub® SIGN can store and make available qualified certificates issued by any National Certifying Entity (Qualified Digital Signature), International (AATL) or European Certification Entity (QTSP) in addition to issuing its own digital certificates with an internal CA (controlled trust).

INTERNACIONAL PARTNERS

DocuSign®
wacom®
ENTRUST® SECURING A WORLD IN MOTION
GlobalSign® GMO INTERNET GROUP
HID® Powering Trusted Identities
openkm® KnowledgeManagement

LOCAL PARTNER

Distributor seal / local partner

SIGN
- PAdES, CAdES (P7M) y XAdES
- One Shot and Recurrent
- HSM, Tokens and Smart Cards
- Graphometric (Wacom®) and Biometric (HID®)
- LTV, TSL, CRL and OCSP
- e-Seal (eIDAS)

TSA
- x.509 v3 RFC3161
- TSA and TTP (Trusted third party)

ABIS
- Fingerprint, Face, Voice, Iris, Graphometric
- Templates ISO / IEC 19794
- MINEX III (NIST)

CIPHER
- SHA-512 RSA 1024-4096 bit

IAM
- User/Password
- SoftTokens OATH (Google Authenticator®)
- Biometric with TrustHub® ABIS
- RADIUS® / OAuth2 / OpenID Connect
- Fido® U2f Security Keys
- SAML
- Centralized and Distributed ID
- Third party IAM Integration (Keycloak®)
- Microsoft® Active Directory®
- Directorios LDAP
- Active Directory Federation Service (ADFS)

CLOUD | CLIENT
- Internal Encrypted repository
- Integrations (S3®, OpenKm®)
- Localhost with TrustHub® CLIENT
- Distributed File System (IPFS)

API
- TrustHub® RESTful API
- PKCS#11 HW Interface

HSM
- DocuSign® DSA 7.1 Common Criteria EAL4+
- EnTrust® HSM nShield FIPS 140-2 Nivel 3

Compliance
- eIDAS Compliance

(**e**lectronic **ID**entification, **A**uthentication and trust **S**ervices)

NIST PCI DSS COMPLIANT COMMON CRITERIA CERTIFIED EAL4+

Rev 4.7.5

EMEA
Gurucube S.r.l.
Turin ITALY

LATAM
Gurucube S.A.
Córdoba ARGENTINA

Sales: sales@trusthub.cloud
Support: support@trusthub.cloud
Website: www.trusthub.cloud