



TRUST<sup>®</sup>  
hub

Firma Digital, Electrónica y Biométrica  
Gestión de Identidad  
Documentos y Notarización

GURUCUBE  
Trusted Identity  
Solutions 

## EL ENTORNO DE CONFIANZA MAS COMPLETO Y SEGURO

TrustHub® es la solución de identificación, autenticación, firma y notaría más moderna, completa y segura del mercado. Debido a su estructura modular que se articula parte en la nube y parte en local, proporciona una increíble variedad de configuraciones.

**SIGN** procesa todas las operaciones de firma, validación y sello gestionando por completo todo el ciclo de vida de los certificados.

**CIPHER** encripta documentos e informaciones sensibles de todo tipo inclusive datos biométricos, grafométricos y coordenadas GPS.

**ABIS** almacena y compara datos biométricos operando tanto como validador interno como interfaz digital hacia QTSP externos.

**IAM** es el gestor avanzado de identidad digital que identifica de forma segura y fehaciente los usuarios en TrustHub®.

**CHAIN** descentraliza las informaciones sobre las operaciones y los documentos notariandola en la Cadena de Bloque de BTC.

Cada núcleo funciona de forma completamente autónoma y reside en servidores distintos físicamente y lógicamente aislados. Con base de datos encriptadas y datos que necesitan ser integrados para ser congruentes, cualquier violación de sistema no comporta riesgo real para la privacidad de los usuarios.

La estructura modular de TrustHub® construida alrededor de sus nudos principales independientes, permite por un lado sectorizar la tipología de servicios erogados por medio de las APIs y por otro, relacionando de forma diferentes los nudos y su cronología de intermediación, llegar a proveer servicios completamente nuevos, diferentes, verticales y altamente personalizados en función de las necesidades.

## AUTENTICACION FUERTE Y FEDERACION DE USUARIOS

TrustHub® dispone de un avanzado sistema de autenticación y gestión de identidad basado en protocolos como OpenID Connect, OAuth2 y SAML que permite autenticar tanto los usuarios registrados directamente en TrustHub® como los que se encuentran registrados en el nudo independiente de SIGN o en otro IAM externo. Además, permite agregar segundos factores de autenticación con tokens OATH con Google Authenticator® o FreeOTP® e usar informaciones biométricas o grafométrica como 2FA o como autenticación directa.



Something you have



Something you know



Something you are

Trusthub® IAM soporta de forma nativa la autenticación simultanea de más usuarios a la vez en la misma sesión certificando así la presencia o asistencia contemporánea de un grupo de usuario en el mismo lugar o evento. Además, puede sincronizarse automáticamente con Microsoft® Active Directory®, directorios LDAP o los Servicios de Federación de Active Directory (ADFS). TrustHub® dispone además de una aplicación móvil propietaria de autenticación fuerte para iOS y Android (TrustHub® OATH)

## IDENTIFICACION BIOMETRICA

El sistema ABIS de TrustHub® puede almacenar de forma segura los datos biométricos de rostro, huellas, voz, palmas, iris y los datos grafométricos de la firma de cada usuario.

La base de datos biométricos se encuentra encriptada y físicamente y lógicamente separada de la base de datos personales IAM. Su potente motor de búsqueda permite la comparación de datos 1:1 y 1:N. Todas las informaciones son recolectadas bajo estándares NIST y se encuentran almacenada en formato ISO para garantizar una completa interoperabilidad y para poder efectuar comparaciones contra base de datos públicas y de QTSP.

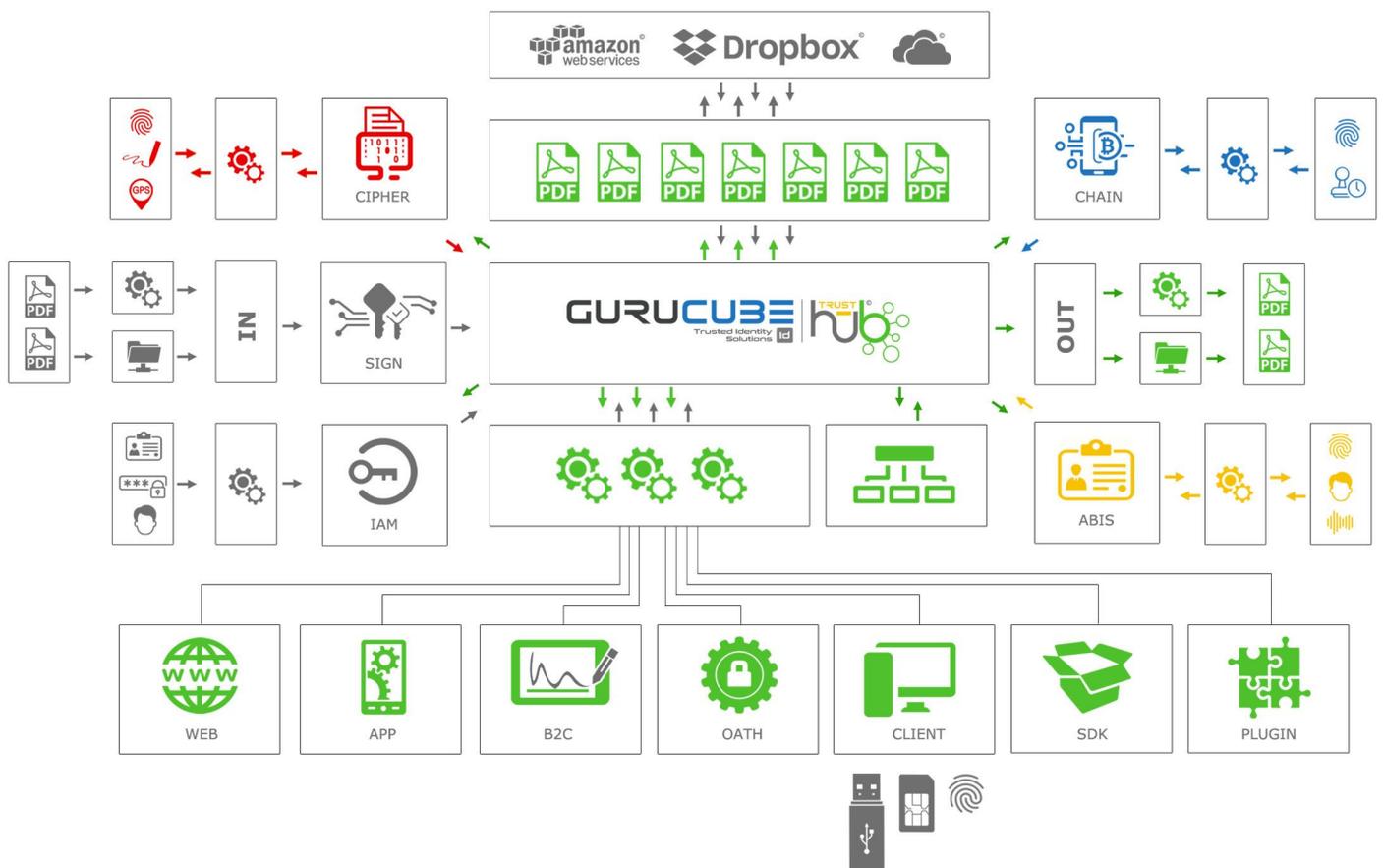
## ENROLAMIENTO DIGITAL BIOMETRICO PRESENCIAL Y REMOTO

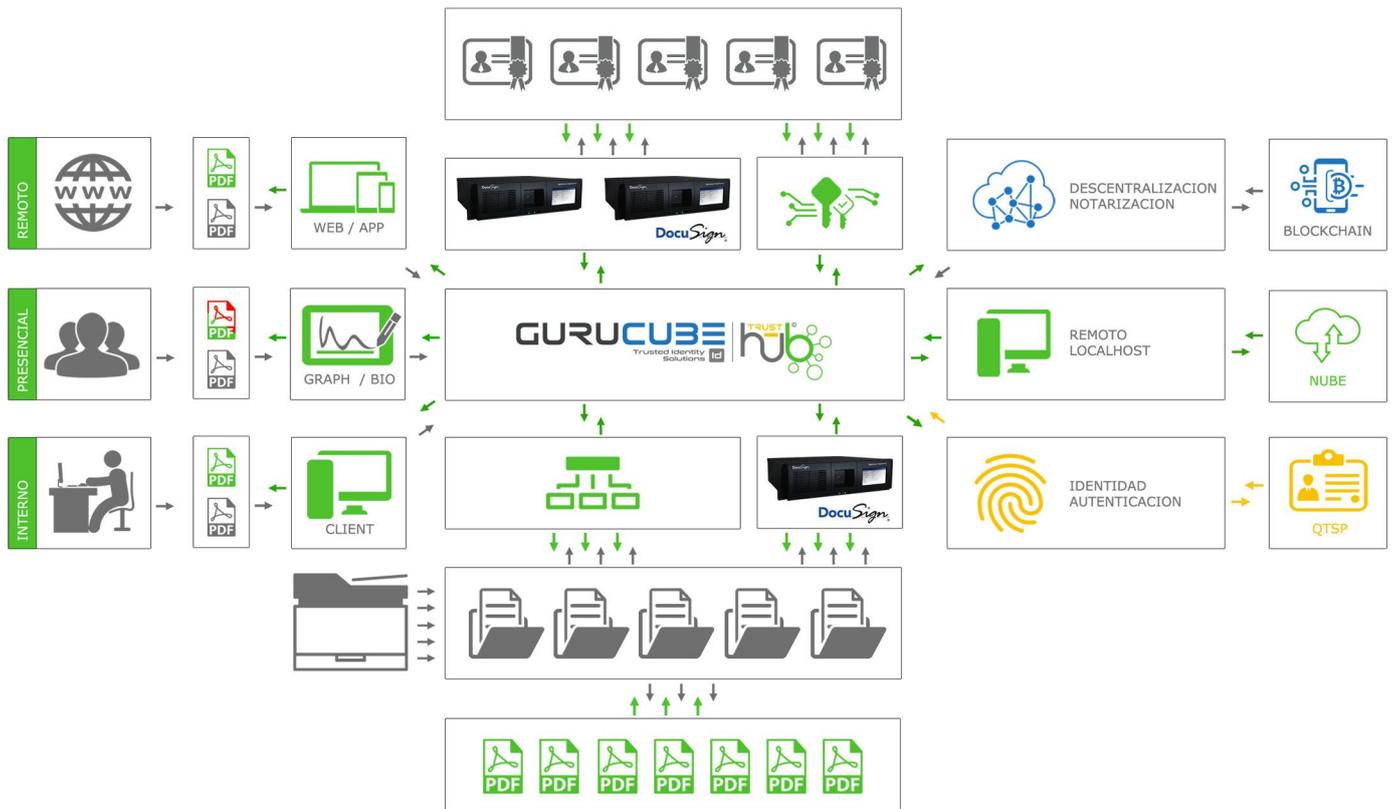
Además del enrolamiento con validación por Mail o SMS bajo estándar eIDAS (deducido), TrustHub® provee un proceso de enrolamiento biométrico presencial con huellas dactilares o remoto con rostro y prueba de vida. Los datos biométricos pueden ser encriptados y almacenado localmente en el ABIS de TrustHub® para una eventual verificación a posteriori o ser validados en tiempo real contra servicios web de Entidades Públicas o QTSP. TrustHub® mantiene un registro de las entidades habilitadas a la certificación de identidad. En función de la localización aplica las reglas preestablecidas de validación que otorgan valor legal en cada País. TrustHub® garantiza la interoperabilidad de los datos biométricos recolectado, la separación lógica y física entre base de datos, la inalterabilidad de los mismos y el pleno cumplimiento de las normas sobre datos personales.

## NOTARIZACION DE ARCHIVOS EN CADENA DE BLOQUE

TrustHub® CHAIN es un sello de tiempo basado en la cadena de bloque de BTC definido como proceso de notarización. Permite notarizar una operación a la vez o generar grupos de operaciones notarizadas. Este componente a la par de TrustHub® CIPHER es transversal a todas las otras herramientas ya que además de constituir un servicio por sí mismo, es utilizado internamente para proveer sello de tiempo a todos los eventos generados. No obstante basarse en tecnología distribuida TrustHub® CHAIN garantiza la inmediatez de la operación de sellado gracias a un avanzado sistema de calendarios.

TrustHub® dispone de un espacio encriptado propio y está integrado con S3®, OpenKM, Google Drive, Dropbox®, y OneDrive®. Además gracias a TrustHub® CLIENT provee acceso a documentos físicamente ubicados en localhost.





## MODULO PROXY

TrustHub® PROXY permite trasladar localmente el proceso remoto de firma con la ventaja de no tener que enviar en ningún momento los documentos más confidenciales afuera de la intranet segura de la empresa, ahorrar ancho de banda importante en el caso de firmas en lotes o de documentos de grandes dimensiones y de poder personalizar el proceso de firma y la firma en si en el documento según requerimientos específicos, sin renunciar a los beneficios de la custodia centralizada de los certificados.

## HSM COMO SERVICIO

TrustHub® puede funcionar como servicio de integración con HSM remotos, es decir que por medio de su API RESTful proporciona una potente interfaz de conexión segura con HSMs DocuSign® DSA o Entrust® (solos o conectados en cluster) ubicados en cualquier lugar del mundo. En esta configuración TrustHub® constituye una capa lógica y funcional por arriba de la interfaz estandar #PKCS11, proporcionando un control completo y centralizado sobre las llaves de firmas almacenadas en cada HSM.

## ENCRIPCIÓN DE DATOS SENSIBLES BIOMETRICOS O DE LOCALIZACION

TrustHub® CIPHER puede encriptar documentos para hacerlos visibles únicamente bajo una específica clave de decrepitación. De la misma forma puede encriptar datos biométricos como huellas dactilares, palmas, rostros, iris, voz y en general cualquier dato que se necesite archivar de forma segura y no alterable para hacerlo resistente frente una auditoria o un análisis forense. También puede encriptar datos de georreferenciación para garantizar legalmente la efectiva presencia en un dato lugar en un momento específico.

Las APIs RESTful de TrustHub® permiten una rápida y completa integración de todas las funcionalidades de identificación, autenticación, firma y notaría con cualquier otra aplicación. Pueden ser utilizadas con diferente lenguaje de programación y en diferentes plataformas incluyendo aplicaciones en .PHP, .NET y JAVA. Para la integración en Java es disponible además una librería específica que permite reducir aún más el tiempo del desarrollo.

## VALIDACION A LARGO PLAZO

TrustHub® SIGN soporta el formato PAdES-LTV. De esta forma un documento PDF y PDF/A (ISO19005) firmado digitalmente con un certificado activo al momento de la firma, seguirá viéndose valido también después de su vencimiento. Para que este tipo de firma muestre su característica de Validación a Largo Plazo (LTV) es necesario incorporar al proceso un sello de tiempo calificado x.509 (TSA).

## FIRMA BIOMETRICA Y GRAFOMETRICA

TrustHub® SIGN permite firmar documentos usando datos biométricos (ISO / IEC 19794-8), grafométricos (ISO / IEC 19794-7) o cualquier otro signo grafico o dato adicional. Como medida de seguridad y en el respeto de las normas Europeas e Internacionales sobre el tratamiento de datos sensibles, ante de guardar el objeto grafométrico o biométrico con todas las informaciones de velocidad, aceleración, presión, inclinación, tiempos entre otras o las coordenadas y tipo de las minucias de la huella en el repositorio del PDF, los mismos son encriptados por el CIPHER de TrustHub® que luego sella el documento con un certificado digital. En caso de repudio o contestación de firma, TrustHub® provee la llave de decriptación del objeto grafométrico o biométrico necesario para el análisis forense.



## QR CODE

TrustHub® marca cada documento con un código QR univoco, lo que permite validar en cualquier momento la autenticidad del mismo.

## CONTROL COMPLETO SOBRE TODO EL PROCESO DE FIRMA

TrustHub® SIGN garantiza un control completo sobre los documentos a lo largo de todo el proceso de firma ya que en ningún momento dejan el repositorio cifrado.



HSM remoto



Token USB



Smart Card

En el proceso de firma con HSM el concepto de custodia de las llaves como lo de seguridad del proceso mismo de firma, es intrínseco ya que se lleva a cabo en HW certificado Common Criteria EAL4+ o FIPS 140-2 Nivel 3 ubicado en la infraestructura custodiada por TrustHub®. El proceso de firma con Token o Smart Card a cambio podria introducir ventanas de posibles alteraciones ya que el mismo se desarrolla localmente en la PC del firmante, fuera del perimetro controlado. Sin embargo, también en esta condición, TrustHub® SIGN garantiza la seguridad del proceso disponibilizando para la firma únicamente el hash del documento mientras que el original queda guardado. Sucesivamente verifica y compara los hashes usando el certificado recibido para firmar definitivamente el documento remoto.

## REGISTRO ELECTRONICO DE OPERACIONES

El registro electrónico de operaciones de TrustHub® registra todos los datos relacionados con la conexión de los usuarios y su actividad en la plataforma. El registro es inalterable, cada operación recibe un sello de tiempo y se descentraliza en la Cadena de Bloque de BTC.

## CERTIFICACIONES

El software y el servicio cumplen con los estándares eIDAS (identificación electrónica y servicios fiduciarios para las transacciones electrónicas) y con los estándares técnicos de interoperabilidad y seguridad de NIST, ETSI, ISO, W3C, OASIS, IETF, Microsoft® y Adobe®.

## ALGORITMOS CRIPTOGRAFICOS

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

## ENTIDADES CERTIFICADORAS COMPATIBLES

TrustHub® SIGN puede almacenar y disponibilizar certificados calificados emitidos por cualquier Entidad Certificadora Nacional (Firma Digital Calificada), Internacional (AATL) o Entidad Europea de Certificación (QTSP) además de emitir sus propios certificados digitales disponiendo de una AC interna (confianza controlada).

## PARTNERS INTERNACIONALES



## PARTNER LOCAL

Sello distribuidor / partner local

### Modalidades de firma

- PAdES, CAdES (P7M) y XAdES
- One Shot y por lotes
- HSM, Tokens y Smart Cards
- Grafométrica y Biométrica
- LTV, TSL, CRL y OCSP
- Validación condicional de firmas
- e-Seal (eIDAS)

### Sello de tiempo

- x.509 v3 RFC3161
- TSA y TTP (Tercero de confianza)

### Características ABIS

- Templates ISO / IEC 19794
- MINEX III (NIST)
- CIPHER

### Gestión de identidad

- Centralizada y distribuida
- Integración IAM (Keycloak®)

### Métodos de autenticación

- Usuario/contraseña
- SoftTokens OATH (Google Authenticator®)
- Biométrica con TrustHub® ABIS
- Grafométrica (Wacom®)
- RADIUS® / OAuth2 / OpenID Connect
- Fido® U2f Security Keys
- SAML

### Gestión de documentos

- Bóveda virtual encriptada
- Nube (S3®, Dropbox®, OneDrive®)
- Localhost con TrustHub® CLIENT

### Interfaces de integración

- TrustHub® RESTful API
- PKCS#11 HW Interface

### Directorios sincronizables

- Microsoft® Active Directory®
- Directorios LDAP
- Active Directory Federation Service (ADFS)

### HSM compatibles

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

### Normas de referencia

- eIDAS Compliance (electronic IDentification, Authentication and trust Services)

