MOBILE-ID
Anytime, Anywhere

TRUSTED HUB

SIGNING & VERIFICATION APPLIANCE

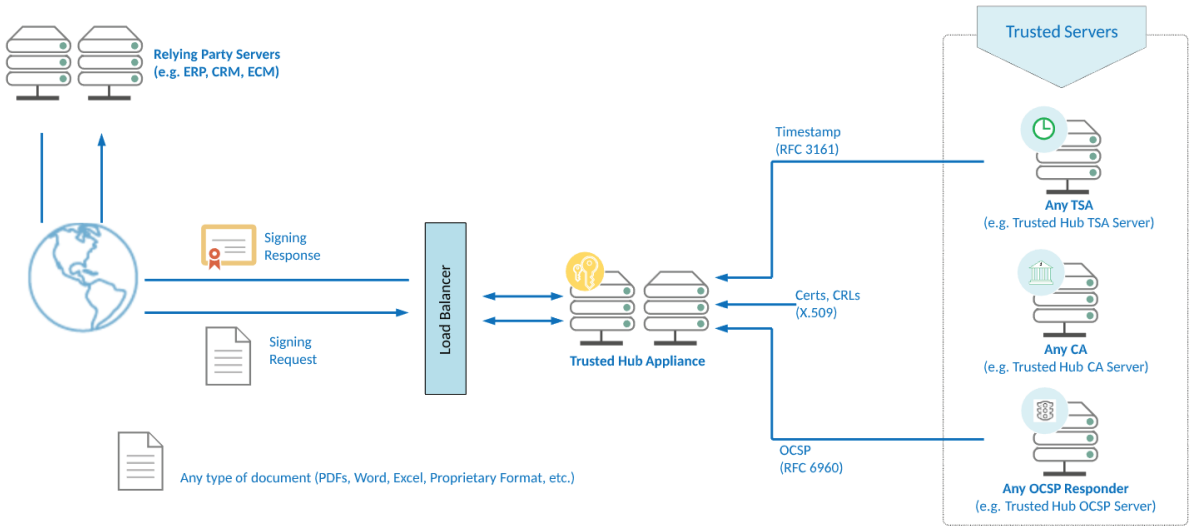
ETSI PAdES, XAdES, CAdES Signatures

What is the **Trusted Hub Appliance**?

Organizations continue to face a variety of pressures to provide enhanced security of documents, data and transactions. They need to provide better data integrity, non-repudiation, accountability, traceability and secure audit services to aid compliance with local legislation, regional directives and internal needs.

From a commercial and efficiency perspective there is also a strong drive to replace paper-based processes with secure, electronic ones. Digital signatures provide all of the security, user and/or organization identification services that are needed. Trusted Hub Appliance provides the high trust security services needed to create these and provide secure log evidence. Trusted Hub Appliance is compliant to the EN 319 142, EN 319 132, EN 319 122 and EN 319 102 standards.

Trusted Hub Appliance provides all of the ETSI PAdES, XAdES, CAdES digital signature trust services for a wide range of business documents, data and information workflows. It can be simply and easily integrated with ECM, CRM or ERP relying party via high speed APIs, CSC web services, Auto File Processor (Watched Folder) or even via Email. A minimum of application development or integration is required since Trusted Hub Appliance maintains all the management knowledge to understand how to sign, where to sign, with what keys, where these are kept, which CAs to trust how to validate certificates, etc. Thus small changes do not affect the applications.



The common use cases for **Trusted Hub Appliance** are:

Bulk signing of PDF, XML and other documents
such as invoices, reports, statements, etc.

- using Qualified or AATL or other high trust certificates
- using CSC web services or fast HTTP/S APIs
- using high level DotNet or Java APIs
- using Auto File Processor watched folder client
- using Secure Email Server

Signing keys and certificates can be held:

- in HSMs, in smartcards, in mobile devices, in software

User-based Qualified Remote Signing

- Trusted Hub Appliance and TSE Mobile ID enable Qualified Remote Signature creation using Level 2 Sole Control

User-based Advanced Remote Signing

- Trusted Hub Appliance supports advanced signature creation using AATL or other keys/certificates held centrally

User-based signing using local smartcards

- vSignPlugin Desktop is used to sign within web-browsers
- using Qualified or AATL or other keys/certificates

And finally, Trusted Hub Appliance powers GoPaperless. GoPaperless harnesses all this signing power within a market leading document workflow and digital signature approval application – see **gopaperless.mobile-id.vn** for details.

Trusted Hub Appliance provides high-level security services whilst removing all the lower-level complexities from the business environment. Trusted Hub Appliance administrators define acceptable policies and profiles as well as how they will be applied and how they will be presented. They then permit or deny client applications the right to use these, e.g. the "invoice signing" profile should only be allowed by the specific finance department invoicing application.

There are various ways in which **Trusted Hub Appliance** can be integrated with relying party:

CSC Signing Capabilities

>> Sign various document/data formats
- PDF, Office, XML, File, Form (PKCS#7) and S/MIME

>> Sign using various format options
- Embedded – e.g. PDF, Office, XML-DSig
- Wrapping – e.g. PKCS#7/CMS/XML-DSig
- Detached – e.g. XML-DSig, PKCS#7, CMS
- Plus timestamps (PAdES-T, XAdES-T, CAdES-T, and -A)
- Plus validation status (PAdES, XAdES, CAdES)
- PAdES PART 2/3/4 signatures

>> Notary/archive/timestamp/evidence archive
- LTANS Archiving, plus PAdES-A, CAdES-A, CAdES

>> For use with any internal or external document
- Signing using corporate or user, server or client key/certs
- Local signing uses vSignPlugin Desktop

CSC Verification Capabilities

>> Verify & Trust various document/data formats
- PDF, Office, XML, File, Form (PKCS#7) and S/MIME

>> Verify various signature types
- Embedded – e.g. PDF, Office, XML-DSig
- Wrapping – e.g. PKCS#7/CMS/XML-DSig
- Detached – e.g. XML-DSig, PKCS#7, CMS

>> Special options
- Add/check timestamp information (XAdES, CAdES, PAdES-T)
- Add/check validation status information (AdES-X-L-A) PAdES part 2, 3, 4, 5 signatures
- Detached – e.g. XML-DSig, PKCS#7, CMS

>> For use with any internal or external document
- Signing using corporate or user, server or client key/certs
- Local signing uses vSignPlugin Desktop

With so many options Mobile-ID™ and its delivery partners can help you to define the best options to meet the various business, legislative and regulatory needs and reduce the risks and costs involved in creating, sending, receiving and storing unprotected business documents. The multiple capabilities of Trusted Hub Appliance can be used to solve today's needs and also offer tremendous investment protection to meet the changing needs of tomorrow.

Trusted Hub Appliance has been designed to meet the needs of SMEs, large multi-national organizations, managed service providers and regional trust schemes. It does this by providing flexibility, resilience, scalability, combined with well-designed internal security, management, audit logging and reporting that is designed to meet CWA 14167-1 requirements for trustworthy systems.

For bulk signing of invoices and other documents review the Auto File Processor option for Trusted Hub Appliance. To sign existing PDFs being emailed from ERP system such as SAP look at the Secure Email Server option.

Trusted Hub Appliance also supports Qualified Seals when used together with QTSP services. Speak to Mobile-ID™ or our local partners about this option.

Trusted Hub Appliance Standards Compliance:

Interface standards	CSC services (including over SSL/TLS), high speed HTTP/S protocols, Auto File Processor (AFP) Watched folders, Secure Email Server for email support, Java and .NET APIs
Algorithms and keys	RSA 1024/2048/4096/8192, ECDSA 256/384/521, SHA1/256/384/512, RIPEMD
Signature generation	PDF, PDF/A, XML DSig, PAdES 2/3/4, XAdES, CAdES (ES/-T/-C/-X/-Long/-EPES/-A), PKCS#7, CMS, S/MIME
Signature verification	One or multiple ETSI PAdES, XAdES, CAdES, PDF, XML DSig, PKCS#7, CMS and S/MIME signatures
Signature enhancement	Enhances PAdES 3,4,5, XAdES and CAdES signatures to include timestamp and certificate status data
Certificate validation	Requests validation using OCSP, CRLs, Delta CRLs, DPD/DPV or even XKMS and SCVP
OCSP & Time stamping	Has an RFC 6960 OCSP client and an RFC 3161 timestamp client as standard
HSM Support	PKCS#11 or CAPI/CNG compliant HSMs, smartcards or tokens, Gemalto/SafeNet, Thales, Utimaco Cloud HSMs including Azure Key Vault, Amazon AWS Cloud HSM
Operating Systems	Windows Server 2016/2012 R2/2012/2008 R2, Linux (RedHat, Centos, SuSe, others), Solaris (on request)
Databases	SQL Server 2016/2014/2012, Oracle 12c/11g, PostgreSQL 9, 8, MySQL 5.x (Percona & Oracle), Azure SQL
Trust Server Options	**Mobile-ID Trusted Network CA, TSA and OCSP Servers can also be used to provide advanced trust infrastructure services**