MOBILE-ID
Anytime, Anywhere

TRUSTED HUB

vSIGNPLUGIN DESKTOP™

Create, Verify & View Digital Signatures within a Web Browser

- Applies end-user digital signatures using Windows CAPI/CNG, Mac Keychain or PKCS#11
- Enables PDF, XML and PKCS#7/CMS signing and ETSI PAdES, XAdES, CAdES timestamped and long-term validation (LTV) signatures

Trusted Hub vSignPlugin Desktop makes it easy for end users to sign documents or data using locally held keys and certificates. Many countries have eID smartcards issued on smartcards and over 50 certificate service providers issue high trust AATL certificates that are automatically accepted within Adobe Reader. Trusted Hub vSignPlugin Desktop allows such smartcards, USB tokens or even local software tokens to create long-term validation, timestamped digital signatures.

vSignPlugin Desktop is the replacement for vSignPlugin Applet, a signed Java applet, now discontinued because web browsers no longer accept Java applets. vSignPlugin Desktop offers the same functionality in a simple to install desktop middleware application for Windows desktops and Mac OSX systems.

Support for Windows CAPI/CNG, Keychain and PKCS#11

Trusted Hub vSignPlugin Desktop has unmatched capability for creating PAdES, XAdES, CAdES, PDF, XML Dsig, PKCS#7/CMS signatures using local keys held within Windows or Mac OSX.

Full Control over the User Experience

The web-application developer has complete control over the look, feel and language of the user interface. Mobile-IDTM provides sample source code web-pages to show how a solution can quickly be deployed.

Rapid Development and Retro-fitting

Trusted Hub vSignPlugin Desktop is driven by the Trusted Hub Appliance vSignPlugin Service and this makes it easy for developers to add digital signature generation and verification options to any web-application. All signing complexities are handled by Trusted Hub Appliance products using high-level calls.

Enables Greater Usability and Fewer Mistakes

In many cases business managers and citizens do not know how to select the correct certificate for signing and so it makes no sense to ask them. Trusted Hub vSignPlugin Desktop can be instructed to look for the right certificate based on name, issuer, key usage, policy or other criteria and thus select the right one without asking the end-user.

Sign what you see (WYSIWYS) for PDF documents

Trusted Hub vSignPlugin Service has an option to display PDFs using a server-side viewer so that PDF documents can be displayed to users securely. The user is shown a flattened PDF before being asked to sign it, any existing signatures can be clearly seen and verified. All trust decisions are taken by Trusted Hub Appliance so that local trust decisions are not required.

Data Leakage Prevention (DLP)

The Trusted Hub vSignPlugin Viewer allows specific control over actions such as (a) saving a copy, (b) printing a copy and (c) the signature itself. These features help organizations to tightly control data and prevent loss/leakage.

Why use Trusted Hub vSignPlugin Desktop

- Works as part of a web-browser environment and these web pages can be updated and functionality immediately rolled-out – compare this with installed desktop software and the associated support and maintenance & new software roll-out overheads
- Supports a wide variety of PDF, XML and data/file/email signing formats, plus timestamped and long-term digital signatures (ETSI PAdES, XAdES and CAdES profiles)
- Supports automated digital certificate filtering to allow the relying party to control which local signing certificate is acceptable for use
- Works with the Trusted Hub vSignPlugin Viewer with controllable features for signature field creation, printing, downloading, plus visible signing and signature verification
- Trusted Hub vSignPluginViewer displays signature status and all signature appearance elements including hand-signature and company logos
- Supports Certified PDF signing using visible or invisible signatures, plus the ability to create new or use existing signature fields. Supports high trust AATL certificates
- Signs documents received from the server or documents held locally on user's systems
- Can optionally encrypt content using XML Encryption after signing as part of a secure upload process, e.g. for tenders, voting etc.
- Supports roaming credentials, where keys/certs are held in secure container on Trusted Hub Appliance and sent to the vSignPlugin Desktop at the time of signing
- Supported all modern HTML5 browsers
- Also able to generate keys and insert these into local key/certificate stores
- For the future ask about mobile device signing using strong authentication and authorization to sign using secured, centrally held keys and

Multi-lingual User interfacing

Trusted Hub vSignPlugin Service and vSignPlugin Desktop has been designed such that the user interface can be defined by the web-application developer. Thus all communication with the user can be made in whatever terms are required to make it easy to use. For example a signing action button could be presented as a Sign or Confirm or Accept button in their local language. Certificate selection and other interactions can be fully controlled by the application.

Example Usage Scenarios

Trusted Hub vSignPlugin Service and vSignPlugin Desktop can be used in a range of relying party scenarios, e.g.:

- e-Banking applications where end-users must sign and upload financial data or documents as part of payments or loans environment or approve centrally held documents
- e-Government applications where citizens wish to communicate with local and central services to register, update information, request changes, request new services, pay taxes or even vote
- e-Government applications where citizens wish to communicate with local and central services to register, update information, request changes, request new services, pay taxes or even vote
- e-Business applications where web forms or documents must be signed by employees or customers as part of a web-based workflow system
- Integration of digital signatures within ECM, ERP or CRM based workflow systems. A document can be viewed and signed within the vSignPlugin Desktop. The application can ask Trusted Hub Appliance to verify the signature and continue with the required workflow
- e-Tendering applications where suppliers must sign an encrypt their documents as part of a secure online submission process

Advanced Functionality

Working with the Trusted Hub Appliance a timestamp can be appended to the end-user signature and CRL or OCSP-based certificate validation data can also be embedded to create long-term signatures. Signed documents and data can additionally be verified via the Trusted Hub Appliance verification service.

Enhanced Trust with Reduced Complexity

For visible PDF signatures Trusted Hub vSignPlugin Service manages the other complexities that include signature appearance, obtaining a timestamp, obtaining certificate chain status information. The PDF can also be certify signed and locked. All these parameters are configured within signing profiles on the Trusted Hub Appliance.

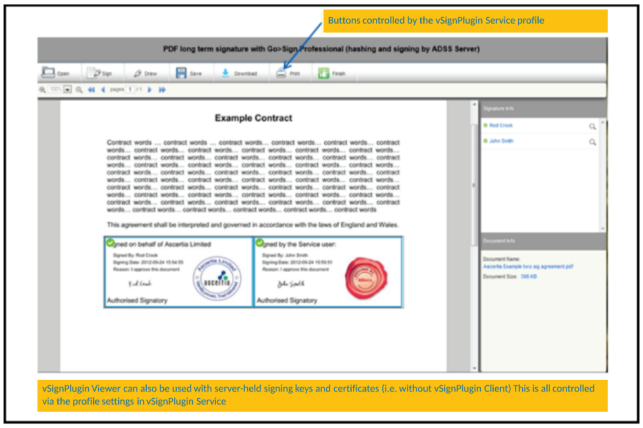
When using the optional PDF viewer, users may also be allows to draw signature fields. Where a signature field exists the user can click within it to initiate signature creation. For greater control over trust the status of the signature is displayed based on Trusted Hub Appliance decisions rather than local desktop trust decisions.

Multiple Key Stores

Two factor authentication ensures extra security for the signing process and Trusted Hub vSignPlugin Desktop supports most desktop/laptop key stores so that it can work with both software-based keys or secure smartcards/USB tokens.

Trusted Hub vSignPlugin Desktop also supports roamed credentials. This is a solution where the signing keys are generated and stored in a secure software container which is uploaded to the Trusted Hub Appliance. The secure container is delivered to the user's Trusted Hub vSignPlugin Desktop whenever the user wishes to sign a document. This is a cheaper alternative to smartcards or USB tokens but still provides tight user control over the signing keys. vSignPlugin Desktop can also locally generate keys and manage certificates for Windows CAPI/CNG CSP key stores.

Screenshot of Trusted Hub vSignPlugin Viewer



Trusted Hub vSignPlugin Service and Trusted Hub vSignPlugin Desktop Standards Compliance:

Signature generation:	PDF signatures, ETSI PAdES, CAdES and XAdES (ES/-T/-C/-X/-X/-Long/-A), XML DigSig, CMS/PKCS#7 Works with Trusted Hub Appliance to deliver timestamps, validation data and enhanced signature formats
Signature verification:	Uses Trusted Hub Appliance to manage trust anchors and verification using CRL and OCSP based status checking
Time stamping:	Uses Trusted Hub Appliance to manage RFC3161 TSAs
Token Support:	Various CAPI/CNG and PKCS#11 compliant software, smartcards or tokens/middleware
Operating Systems:	Windows 10, Windows 7, Mac OSX 10.4 Tiger and above
Browsers:	vSignPlugin Desktop works with any modern HTML 5 browser including Edge, Chrome, Firefox etc.
Interfaces:	SOAP/XML or HTTP/S APIs in Java or .NET or via WSDL web-services

MOBILE-ID
Anytime, Anywhere
Mobile-ID Technologies and Services Joint Stock Company
www.mobile-id.vn
info@mobile-id.vn
1900 6884