Create, Verify and View Digital Signatures within a Client Browser

ADSS Go>Sign Applet™

- Applies **end-user** digital signatures
- Handles PDF, XML and PKC#7 / CMS formats
- Supports local hashing and ETSI P/X/C/AdES timestamped and long-term signatures
- Supports advanced PDF viewing

ADSS Go>Sign Applet has been designed to make client-side digital signatures easy to implement and use. It removes all the difficulties associated with local installed software. In multi-third party environments such as business to business, business to customers or government to citizens there is a clear need for browser based zero-installation signing. No organization wishes to own the problems that might arise from installing and using desktop software and increasingly organisations do not allow this.

ADSS Go>Sign Applet is a perfect solution for client-side signing. It has been designed to enable busy, non-technical people to sign documents and data. It works with modern browsers to allow citizens and businesses to go green, eliminate paper and avoid postage and handling costs.

Full Control over the User Experience

The web-application developer has complete control over the look, feel and language of the user interface. Ascertia provides sample source code web-pages to show how a solution can quickly be deployed. The aim is to use language that is meaningful to the business and the end-user and eliminate confusing technical terms.

Rapid Development and Retro-fitting

ADSS Go>Sign Applet and ADSS Server make it easy for developers to add digital signature generation and verification options to any web-application. All signing complexities are handled by ADSS products using simple high level calls.

Enables Greater Trust

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. The application can command Go>Sign to look for a specific certificate based on name, issuer, key usage, policy or other criteria and thus select the right certificate without involving the end-user. The application can retrieve details of the selected certificate to show to the user. It may also need to show messages such as 'insert your eID card' where no suitable certificate exists.

What You See Is What You Sign (WYSIWYS)

ADSS Go>Sign Applet has two options: Go>Sign Standard includes functionality for creating PDF, XML and PKCS#7 and CMS signatures. Local hashing is supported as is the ability to filter certificates based on various criteria; support for CAPI and PKCS#11 stores is also included.

Go>Sign Professional adds the ability to use a built-in PDF viewer so that PDF documents can be displayed to users within the secure confines of the applet. The user is shown a flattened PDF before being asked to sign it. The signed document can then be re-shown to the user if required.

Why use ADSS Go>Sign Applet

- 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.
- Very simple to use for senior business users, when compared with complex "thick" desktop applications.
- Supports automated digital certificate filtering to allow the business application to control this and other aspects.
- Supports local digital signature creation including PDF, XML and PKCS#7 / CMS. Supports Certified PDF signing, visible and invisible signatures, new and existing signature fields.
- Signs documents received from the server or held locally on user's systems.
- Supports timestamped and long-term digital signatures including ETSI PAdES, XAdES and CAdES profiles. [P].
- Provides full support for PDF CDS signatures and optional PDF viewing to allow users to see the document before signing [P].
- PDF Viewer displays signature status and all signature appearance elements including hand-signature and company logos [P]
- Can encrypt content using XML Encryption after signing as part of a secure upload process [P]
- Supports roaming credentials, where keys/certs are held in secure container on ADSS Server and sent to the applet at the time of signing [P]
- Supported on various browsers and platforms

[P] = Requires ADSS Go>Sign Professional license

Data Leakage Prevention (DLP)

The ADSS Go>Sign Applet PDF viewer allows specific control over actions such as (a) saving a copy, (b) printing a copy and (c) the signature itself. These features help organisations to tightly control data and prevent loss / leakage.

Create, Verify and View Digital Signatures within a Client Browser

Multi-lingual User interfacing

ADSS Go>Sign Applet 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.

Go>Sign Professional includes a PDF viewer applet and this can use local language tables to communicate appropriately with end users.

Example Usage Scenarios

ADSS Go>Sign Applet can be used in a range of business application 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-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 Go>Sign Applet. The application can ask ADSS Server 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 ADSS Server 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 ADSS Server verification service.

Enhanced Trust with Reduced Complexity

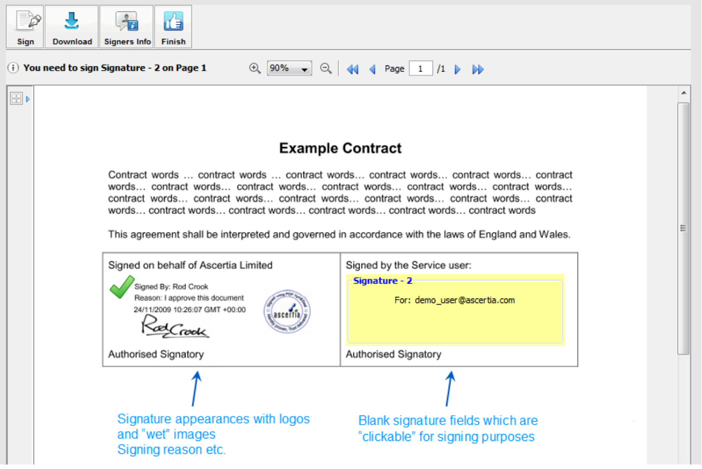
For visible PDF signatures ADSS Server manages the other complexities that include signature appearance, obtaining a timestamp, obtaining certificate chain status information. The PDF can also be certify signed and locked. All these parameters are configured within signing profiles on the ADSS Server.

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 ADSS Server decisions rather than local desktop trust decisions.

Multiple Key Stores

Two factor authentication ensures extra security for the signing process and ADSS Go>Sign Applet supports both Windows CAPI and PKCS#11 key stores so that it can work with both software-based keys or secure smartcards/USB tokens.

ADSS Go>Sign Applet 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 ADSS Server. The secure container is delivered to the user's ADSS Go>Sign Applet 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.



You need to sign Signature - 2 on Page 1

Example Contract

Contract words ... contract words ... contract words

This agreement shall be interpreted and governed in accordance with the laws of England and Wales.

Signed on behalf of Ascertia Limited	Signed by the Service user:
Signed By: Rod Crook Reason: I approve this document 24/11/2009 10:26:07 GMT +00:00 Rod Crook	Signature - 2 For: demo_user@ascertia.com
Authorised Signatory	Authorised Signatory

Signature appearances with logos and "wet" images Signing reason etc.

Blank signature fields which are "clickable" for signing purposes

Screenshot of ADSS Go>Sign Professional PDF Viewer

ADSS Go>Sign Applet 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 ADSS Server to deliver timestamps, validation data and enhanced signature formats
Signature verification:	Uses ADSS Server to manage trust anchors and verification using CRL and OCSP based status checking
Time stamping:	TSP (RFC3161) via ADSS Server
Token Support:	Various CAPI and PKCS#11 compliant smartcards or tokens and middleware
Operating Systems:	Windows XP, Windows Vista, Windows 7, Windows 2003 / 2008 Server, Linux, MAC
Browsers:	Internet Explorer v7+, Firefox 3+, Chrome 3+, Opera 10, Safari (soon)
Interfaces:	Javascript

Ascertia Limited
Web: www.ascertia.com
Email: info@ascertia.com
Tel: +44 1256 895416 US: +1 508 283 1890
40 Occam Road, Guildford, Surrey, GU2 7YG, UK

Digitally Signed By: Rod Crook
Reason: I approve this document
22/11/2011 16:19:53 GMT +00:00
Rod Crook

Sales Department
ascertia
Identity proven, Trust delivered