ADSS Go>Sign Applet - Flexible Client-side Signing

ADSS Server enables business processes to sign PDF Documents, XML data and other files data, and Emails in multiple different ways, including:

- **Server-side signing** (using corporate keys / certificates for the organisation or department or role)
- **Server-side signing** (using end-user keys / certificates protected by an authorisation mechanism)
- **Client-side signing** (using local keys /certificates held inside a Windows key store, or smartcard or within a PKCS#11 environment, e.g. on non-Windows systems)

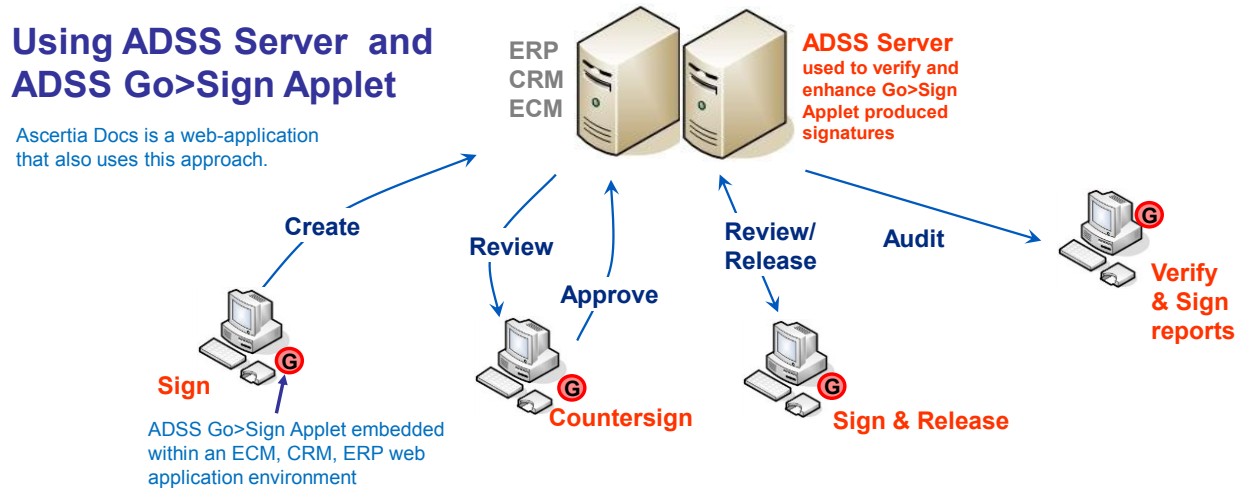
Client-side signing sounds easy enough, but various solutions have problems with this capability, in particular the typical requirement for local software installation. For multi-third party environments (e.g. Business to business, Banks to their corporate or retail customers) there is a very strong requirement to have zero-installation signing – no organisation wishes to own any problems that arise from forcing people to install and use desktop software, and indeed some organisations do not allow this.

Ascertia has created a perfect solution for this, ADSS Go>Sign Applet. Go>Sign Applet addresses a range of business and technical requirements and shows that, although simple in concept, the ADSS Server and Go>Sign Applet combination is incredibly powerful and flexible. The following points highlight the key advantages of this solution:

- **Provides total business control**:
  Go>Sign Applet allows the web-application developer to have complete control over the look and feel and language of the user interface, Ascertia provides sample web-pages to show how quickly a solution can be deployed and how easily the business can own the interaction with the customer, using terms that are meaningful to the business and the end-user (rather than using technical terms decided by Ascertia or other internal or external developers).
- **Maximises simplicity for the end-user**:
  ADSS Go>Sign Applet has been designed to make it easy for busy managers the application can control the signing process completely and thus ensure the user does what is expecting in terms of reviewing and signing the document.
- **Enables great trust control**:
  The application can control whether to ask the user to select a certificate from a list of acceptable certificates or it can instruct ADSS Go>Sign Applet to find a certificate from one or more CA issuers and use this to sign the data. In reality business managers find it hard to choose the correct certificate and would prefer not to be asked the question. The business application can instruct Go>Sign Applet to filter certificates based on common name, issuer name, key usage and other elements, thus removing any confusion from the busy end-user.
- **Simple, small, effective:**
  ADSS Go>Sign Applet works with ADSS Server to minimise complexity within the applet and thus ensure it is as small as possible whilst having advanced functionality such as support for timestamps and long-term signatures.
- **Support multiple business documents and data**:
  ADSS Go>Sign Applet can sign PDF documents as well as forms and other files and even web-mail. Documents can be signed and uploaded or downloaded and signed, they can be hashed locally or centrally the signature or the whole document can be returned. ETSI XAdES, CAdES and PAdES (PDF) signatures and multiple formats are all supported.
- **Supports the expected certificate stores:**
  Go>Sign Applet is able to select certificates from with the Windows CAPI key and certificate store and on non-Windows systems a PKCS#11 interface can be selected – thus multiple smartcards and USB tokens can be used and well as software keys and certificates. Go>Sign Applet can also generate keys and create a certificate signing request for Windows CAPI CSP/CNG.
- **Reduced application complexity** with enhanced trust.
  ADSS Server can be used to control signing or Go>Sign Applet can display and draw signature fields and add the signer's details. Signature verification takes place on ADSS Server and ADSS Go>Sign Applet displays the result within its PDF viewer.

- **Provide trust services after signing:**
  The application needs to check that the signer's certificate is acceptable - ADSS Server provides all the trust policy controls needed to check that the end-user signature is verified and can be trusted. PEPPOL trust ratings are also supported.
- **Handles advanced functionality:**
  Working with the ADSS Server a timestamp can be appended to the end-user signature and the OCSP-based certificate validation data can also be embedded to create long-term signatures. OASIS DSS and DSS-X web-services are also provided.
- **Excellent application development support:**
  ADSS Go>Sign Applet is delivered together with ADSS Client SDK and clear documentation and source code examples are provided to make development easy.

ADSS Server and ADSS Go>Sign Applet are expected to be used within simple or complex business workflows to provide the trust, traceability and integrity services needed to ensure strong internal controls and accountability. The following diagram summarises the ways in which Go>Sign Applet can be used to sign and approve document workflows:



The core signing functionality is within Go>Sign Applet and the policy controls reside within the application or alternatively within ADSS Server. The ADSS Server security management interface ensures that only role-privileged operators can change these policies and if required dual controls can be enabled so that 'four-eyes' control can easily be applied.

Licensing is flexible and cost effective for Go>Sign Applet – the licenses are just an extension of the ADSS Server licenses. A single per-server charge enables use of the applet and then multiple users are licensed across the environment (irrespective of the number of servers).

ADSS Go>Sign Applet is suitable for a wide variety of deployment scenarios; ask us for information on how it can be used to suit a range of needs including:

- Web-based signing of PDF documents
- PDF document viewing and DLP
- Signing of XML, forms and local files
- Local KeyGen and certificate management
- Time-stamping and long-term signatures
- Handling encryption for files, emails, PDFs

Ascertia is a world-leader at providing flexible, scalable and easy to manage solutions that outpace all other approaches in meeting today's constantly changing demands.

Need more information?

Ask us for further information on how we can deliver trust services that protect your business documents and workflow processes info@ascertia.