Why Choose Ascertia for PDF Digital Signatures?

There are many vendors offering PDF signature products, however not all vendors are the same! Ascertia is a leader when it comes to PDF Signing products. Those who don't know the company often ask "why we are so confident" and "can we prove our claim"? To answer these questions we have prepared this solution sheet that summarises the breadth of capability within our products. It's a useful checklist to see if other vendors can match all of this! Ascertia offers:

- **A range of products to serve every need:** Ascertia is the only organisation that can deliver server and client based PDF signing products. So whether you need the full functionality of a desktop application, or automated server-side signatures or signing within a standard browser, using centrally held, roamed or locally held certificates, Ascertia has the right solution for your business need today and in the future.
- **Support for all types of PDF signatures:** There are many different types of standard PDF signatures and we support them all. Whether its visible or invisible signatures, certify signatures or approval signatures, basic signatures or Long Term Validation (LTV) signatures (with embedded timestamps and revocation info). We even provide automatic support for Adobe® CDS signatures.
- **More than just signing:** Our products provide PDF creation, PDF viewing, time-stamping, verification, encryption using certificates, and DLP features. A good example is our Go>Sign Client, which provides PDF document viewing, signing and DLP services to online applications.
- **PDF/A Support:** our digital signatures are PDF/A compliant, so that after being signed a document remains compliant with the PDF/A specifications. This is an essential standard for long-term archival and is also an ISO 19005 standard. Our products do not modify the document's meta-data unlike some vendors. Support for PDF/A-2 is planned.
- **PAdES Support:** ETSI PAdES Part 2, Part 3, Part 4 formats are already supported.
- **Centralised Trust Anchors:** When verifying digital signatures it's essential that there is a proper process for managing the final PKI Trust Anchors. Relying on the end-user to do this and manage the installation of the correct Root CAs, their maintenance and update is asking too much! In all our products we provide the option of using centralised signature verification. This allows organisational level control over which PKIs are to be trusted and also to what degree (assigning "levels" of trustworthiness). Getting a trusted "green tick" for a PDF signature in Ascertia's products can be set to only occur under the conditions defined by the organisation.
- **OASIS DSS support:** OASIS Digital Signature Specifications (DSS) is an important web services protocol for server-side signature creation & verification. It enables business applications to delegate all aspects of signing and verification to a trusted server. Ascertia supports the OASIS DSS protocol and also DSS-X profiles in ADSS Server.
- **ADSS Go>Sign Viewer:** This enables PDF documents to be displayed as a flattened "What You See Is What You Sign" (WYSIWYS) image of the document. It also offers Data Leakage Prevention (DLP) features that control cut/paste, printing, local saving of documents to provide tight controls. Go>Sign Viewer provides signature field management, plus signature creation using individual entity signing keys held centrally on ADSS Server or locally using Go>Sign Client.
- **ADSS Go>Sign Client:** This product offers a range of powerful features for local signing options:
  - Signing using locally held keys (e.g. on eID card or USB token) or server held keys, or roaming keys that are stored on the server & downloaded to when needed
  - Creation of long-term advanced electronic / digital signatures
  - Able to filter certificates so that busy managers automatically use the right certificate
  - Support for multi-lingual options and support for multiple environments
  - Supports for both a GUI or no GUI modes of operation
  - Support for local key generation and certificate management
- **Authorised Signatures:** Digitally signature laws require the digital signing process to be a "wilful act" on behalf of the signer. For server-side signatures to be recognised as qualified electronic signatures there needs to be proof that a signer authorised the signature to take place. There may also be many hundreds of documents that a signer needs to approve. Signing each one individually may take a

very long time! To overcome these issues ADSS Server offers a unique authorised signature feature. This allows one or more end-users to approve one or more documents to be signed centrally. The end-users sign the request to ADSS Server using locally held signing keys. Advanced profiles like "M out of N" authorisers can be set-up where multiple users need to provide approval before an important organisational-level signing key can be used. The authorised signing request structure allows the secure & efficient signing of many documents.

- **Complete PKI infrastructure:** Digital signatures require a Public Key Infrastructure (PKI). ADSS Server can be configured to provide a Certificate Authority (CA) for complete key and certificate management, CRL Issuance, OCSP Server and/or Time Stamp Authority (TSA) Services. Alternatively you can use an existing internal PKI or an external managed service provider as required. Implementing some PKI components internally using ADSS Server often has significant advantages in terms of costs, overheads, high-availability as well as management and control. Ascertia continues to add features to its ADSS Server and the latest additions include XKMS Server and Long-Term Archive and Notary Service (LTANS) Server modules.
- **Modular design:** Ascertia's design philosophy is highly-modular. This enables organisations to just license and use the functionality that is needed today. For example you can start with basic PDF signatures today and add new feature support easily and cost-effectively as required – such as adding timestamps to the signature or creating long-term advanced PDF Signatures.
- **Local hashing / Server-hashing:** For very large documents, signing on the server requires the document to be sent to the server, which can require high network and CPU resources. For this use case Ascertia enables local document hashing, so that only the document hash is sent to the ADSS Server for signing. In similar way, Ascertia allows only the document signature and hash value to be sent to the server for signature verification. This is helpful not only for performance but also document confidentiality and privacy!
- **Front-end business applications:** We also provides complete front-end business applications:
  - **Auto File Processor:** a sophisticated, automated watch folder signing application.
  - **Secure Email Server:** an MTA mail server that filters emails based on policy and signs/verifies/archives attachments using either PDF signatures or XAdES / CAdES.
  - **SigningHub:** a complete cloud based document workflow and approval application using Go>Sign Client for document viewing and signing and ADSS Server for verification.
- **Integrations with 3rd Party Applications:** Ascertia and its partners integrate the ADSS Server and ADSS Go>Sign Client products into leading 3rd party DMS, ERP, ECM and CRM systems, such as Microsoft SharePoint, Dynamics, Salesforce, Alfresco, SAP, Joomla, and KnowledgeTree. Roadmap integrations include: Documentum, Open Text and Oracle Stellent.
- **Long-term Archiving**: ETSI PAdES Part 4 provides the ability to produce PAdES LTV signatures and be able to add additional archive document timestamps to maintain the document validity. ADSS Archive Server also provides IETF LTANS long-term evidence archiving using separate Evidence Record Syntax objects – a technique used by organisations such as the British Library to protect its digital library data.

Summary

These items are the key technical features. We have not mentioned the ease of use features, the PDF signature appearance design features, the security, performance, high-availability features or the management and reporting features. We hope you agree that is an impressive list and we are right to consider ourselves leaders in PDF signature solutions. If you think we are missing something then we are keen to hear from you – Ascertia is constantly refining and enhancing its products.

For further information on any aspect of **PDF Digital Signatures** contact us on info@ascertia.com.