IDENTITY PROVEN
TRUST DELIVERED

- > DOCUMENT SIGNING
- > eID VALIDATION
- > SIGNATURE VERIFICATION
- > TIMESTAMPING & ARCHIVING
- > APPROVAL WORKFLOW

ADSS Server compared with PDF toolkits

As trust solution experts we are often asked to explain the benefits that ADSS Server brings to an organisation rather than using cheaper PDF programming toolkits. The answer is all about providing effective management and security and also insulating applications from change. Good security practice requires that there is reasonable separation of responsibilities. ADSS Server delivers this by offering high level signature creation and verification services to support one or multiple applications. Each request is authenticated to see if the client application is registered, and can be allowed to access the requested signing or verification service profile.

Signing and Verification Profiles

Profiles are created within ADSS Server so that applications need only use high level calls, such as “sign this PDF using the invoice signature profile”. The profile defines all the other details:

- Whether to apply a simple signature or a certifying (locking) signature
- Whether to sign with a visible or invisible signature
  - If visible then where to sign on a page and which pages to sign on
  - What optional company logo and hand-signature images to apply
  - Which font to use and whether to embed this for PDF/A compliance
- What signature type to apply: basic signature, time stamped or long-term signature
- Which signing keys / certificates and thus which CRL/ OCSP/ TSA service providers to use
- Whether a smartcard or an HSM is to be used (PINs/Passwords are securely managed)
- Which optional signature certificate policies to enforce

Secure management

Toolkits do not offer security management, leaving the application to take responsibility for this crucial aspect. Cryptographic processes require effective control of key material and audit logs and ADSS Server offers full security management and controls actions using service profiles. Service profiles are defined and managed using strongly authenticated security operators using role based access control. A web-browser interface is provided to allow them to view, define or change policies (as their role permits). Operators can also define the nature and location of the signature field by opening the PDF within an interactive design tool. Applications can be optionally allowed to provide over-ride information such as setting the reason for signing, where to sign etc.

ADSS Operators control signature key/certificates, their assignment to signing policies, their type (software or hardware), the initial certification and subsequent renewal of certificates, the management of test and production keys & certificates. They can review application requests and ADSS Server responses and easily help developers understand why signing requests may fail, e.g. they have not been authenticated, they have asked for access to an HR key/certificate rather than a Finance invoice signing key/certificate, or perhaps the document is already signed and locked.

Should any problems be detected with back-end timestamp or CRL service availability then alerts can be sent to operators by email or SMS. All service requests and responses are stored in a secure transaction log and operators can decide if copies of all signed documents are to be kept in these logs. If any issue arises during test or production running detailed trace logs can be turned on and supplied to Ascertia for analysis – these are designed to contain no sensitive data, but they detail correct and incorrect server operations. This enables rapid global support and satisfied partners, customers and service providers.

In summary ADSS Server offers a complete solution for effective security management, it insulates applications from change, it simplifies development, operations and audit. Toolkits simply do not compare with this and they leave the fate of security management in the hands of developers.