SafeNet HSMs + Ascertia ADSS Server = Great Solutions

All SafeNet HSMs (except LunaXML) can all be used to great effect with Ascertia's ADSS Server, a multifunctional product that delivers the broadest range of e-security services in the world today. This document looks at the ways in which the two products work together.

Ascertia is a global leader in delivering functionally rich yet easy to deploy e-security solutions. The company focuses on digital signature creation, verification, timestamping and secure archiving products as well as eID validation. These key functions deliver the essential trust services needed by governments, financials, telco, healthcare and other organisations to conduct electronic business. Businesses need traceability, accountability and audit services plus clear originator authentication, signed approvals, assured data integrity and provenance to allow them to meet legislative, regulatory and internal controls requirements.

Ascertia's products enable these security options within a variety of environments, including:

PDF Signing Solutions (meets ISO PDF and ETSI PAdES signature standards)

ADSS Server offers advanced digitally signatures for PDF documents, using PAdES standards. Visible, invisible, certified, basic, timestamped or long-term signatures are supported.
SafeNet HSMs are used to hold keys and certificates for multiple users or corporate keys.

XML Signing Solutions (meets W3C and ETSI XAdES signature standards)

ADSS Server offers advanced XML DSig and ETSI XAdES signing (and encryption) for any data.
SafeNet HSMs are used to hold keys and certificates for multiple users or corporate keys.

Authorised Signing Solutions (confirms wilful signing for bulk documents)

This enables one or more employees to sign a request for an HSM based corporate key to be used to sign documents –this might be is a qualified to which access needs to be tightly controlled.

G2C Solutions

eID creation – ADSS Server offers CA services and works with smartcard management systems
eID validation – ADSS Server offers OCSP, SCVP and XKMS certificate validation services
Client SSL – ADSS server can be integrated with IAM systems to validate user identities
Document signing – ADSS Server and ADSS GoSign Applet enable advanced flexible signing
Citizen data encryption – Citizen data can be encrypted at the client and decrypted later
Signed receipts – transaction summaries, receipts, data items, log records can all be signed
SUMMARY – any data can be signed, verified, timestamped and long-term archived.
HSMs store top level keys, user keys, response signing, timestamp and archive keys

G2B & B2G Solutions

Tender Solutions – ADSS server offers advanced signing and encryption solutions to secure tender solutions and ensure that all submitted data is signed and encrypted. Encryption keys are recommended to be stored in HSMs and decryption takes place on the ADSS Server. Supplier signatures are verified and can be archive timestamped. Secure logs protect all transaction records.

Reporting Solutions – Business making reports or submitting data to government departments can sign and timestamp data, using keys stored in HSMs.
HSMs store top level keys, user keys, response signing, timestamp and archive keys

B2B solutions

ERP solutions – ADSS server offer very flexible, easy to integrate invoice signing solutions
CRM solutions – ADSS Server can generate keys and certificate for suppliers, partners, customers to interact with CRM web-pages and digitally sign documents using HSM based user signing keys.
HSMs store top level keys, user keys, response signing, timestamp and archive keys

Enterprise solutions

Keys and certificate generation – All employees can have centrally held keys and certificates generated for them and held on the server in an HSM, roamed keys can be generated and used for authorised access to server/HSM held qualified certificates.
HSMs store top level keys, user keys and archive keys

Firms can now safely cross the final hurdle of migrating paper-intensive processes to the digital world using Ascertia's products to clearly show document are signed-off and approved, prevent unauthorised changes, provide legal weight evidence & protect corporate reputations

Ascertia enables its partners and customers to answer these types of questions:

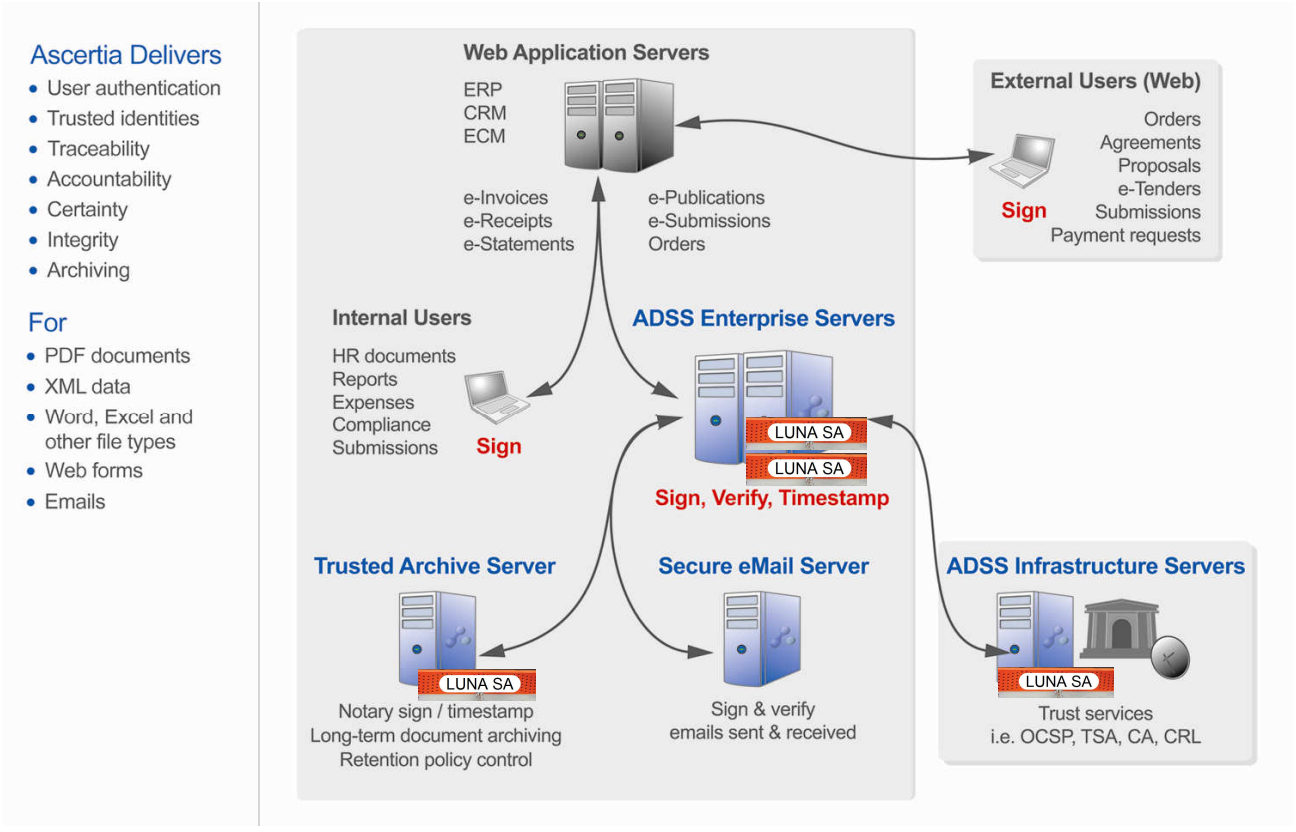
Who are you?
- Using Biometric / Smartcard / Tokens or soft Windows or Unix credentials
- Windows Logon, Windows applications
- Server Application logon
- Building access
- Real-time identity validation

Who signed the data and when?
- Signed PDF documents for global interoperability!
- Signed Office, XML or other files or web-forms
- When was this data timestamped?
- Can I be sure that the data has not been altered?
- Can this be used in a workflow process?

Traceability and Compliance
- When was this accessed?
- Who was the data originator, who approved, who released, when was this, were checks made?
- Can you confirm the signing time of the document?
- Can I enforce controls for my business processes?
- Will my digital signature be legally valid in 7 years?

Receipts, Invoices and Archiving
- Is it easy to ask suppliers to sign their offers?
- Can a signed PDF receipt be issued for that order?
- Is it easy to issue digitally signed invoices which can be verified by anyone?
- Can I verify and trust incoming documents?
- Can data be signed & timestamped & archived?
- Are these signatures legally accepted?

The following diagram illustrates how Ascertia's core technology can be used in many different ways to secure important information:



As a reminder, ADSS Server is able to:

- Sign PDF documents, XML data, Word, Excel, TIF, JPEG and other data and files
- Verify signed documents, digital identities (eIDs) for authentication, integrity & non-repudiation
- Act as a very effective commercial or enterprise Timestamp Authority and e-Archive Server
- Generate keys/certs and validate certificates from multiple CAs using OCSP / SCVP / XKMS.

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