Verification Service Providers need ADSS Server!

Signature Verification is rapidly becoming an over-used term. Many product and service providers claim to offer verification services to meet business needs. As trust solution experts Ascertia keeps being asked to explain the benefits that ADSS Server brings to an organisation as opposed to using alternatives such as open source toolkits, simple service models or limited function products. The answer is all about functionality, support for standards, security management, flexibility and investment protection.

The following requirements are common to all internal systems or service providers:

Verification / Validation Requirements	ADSS Server	Other Products
Can the solution process PDF, XML, S/MIME and other PKCS#7 and CMS signed documents?	YES	Often limited to one or two formats
Can the solution handle basic signatures, timestamped signatures, long-term signatures, PDF certified signatures?	YES	Usually a limited ability to cover this
Can the solution handle ETSI XAdES, CAdES and PAdES signed documents with support for multiple extended signature formats?	YES	Often a limited capability
Does the solution allow the organisation to easily define the trust anchors (Root CAs and Issuer CAs) that are trusted?	YES	Often limited to Windows trust lists
Can the solution verify multiple signatures in a single call and return information on each of the signers?	YES returned via API	Detailed information is rarely returned
Does the solution support OASIS DSS protocol and DSS-X Verification Reports with the ability to offload application from complex coding?	YES using profiles	A limited capability at best
Can the solution check both current and historic signatures and after a grace period, using a specified time in the past?	YES	Historic signatures are rarely handled
Can basic signatures be enhanced to long-term signatures (CAdES and XAdES) as part of the verification process?	YES	Usually a limited ability to cover this
Can the solution keep old CRLs from each trusted CA so that these can be used to check the signature status in the past?	YES	Rarely seen
For long-term signatures can the solution automatically use the embedded CRL/OCSP information if valid?	YES	Often a limited capability
Does the solution have effective role based access security controls and maintain protected event and transaction logs?	YES	Check carefully this is rarely seen!
Can a high availability load-balancing configuration be immediately deployed? On platforms other than Windows? and supporting a range of HSMs?	YES YES YES	Most have issues being this flexible!
Can both CRLs, OCSP, XKMS or even SCVP services be used to check the signer's status? Can a sophisticated validation policy be configured to define the order in which these mechanisms are used, and how to locate and communicate with the back-end status providers?	YES support for multiple profiles allow a range of possibilities	CRL is common OCSP is rarer Support for XKMS and SCVP is very unusual
Can a copy of the original document be kept within the solution's transaction logs as evidence?	YES As an option	Usually a completely separate action
Can a notary archive action be associated with the verification action such that a long-life archive signature and timestamp are applied within an LTANS compliant archive?	YES With in-built TSA & LTANS modules	Usually a completely separate project or product

Verification / Validation Requirements	ADSS Server	Other Products
Is there a solution option for extracting and sending only the signatures from documents to ensure privacy at the relying customer?	YES - see ADSS Gateway	Most have issues being this flexible
Is the solution designed to be used by both end-users, business relying parties and managed service providers?	YES	Often a limited capability
Does the solution provide detailed logging of each transaction, the evidential information & filtering/searching?	YES	Often a limited capability
Does the solution provide an in-built capability for service summary and detailed service reporting?	YES	Often a limited capability
Can the calling client applications be authenticated using request signing and/or SSL client certificates? Can these clients be limited to only use specific signature verification profiles?	YES YES	Most have issues being this flexible
Can the solution provide a standard based approach to providing quality information on the signature algorithms, key lengths, hash algorithms and certificates associated with the signature and whether these meet the minimum local security policy requirements of the relying party?	YES follows the PEPPOL specifications	Rarely seen
Does the solution provide a Client SDK for Java and .Net environments plus source code samples and example applications to make integration really simple?	YES	Worth checking
Can the solution be created on Windows, Solaris and Linux platforms with support for 32 and 64 bit processing?	YES	Worth checking
Are various FIPS 140-2 level 3 or CC EAL4 HSMs supported?	YES	Worth checking
Is an effective security management environment maintained that protects the authentication mechanisms, the verification policies, the validation policies, the keys, certificates, operator and system event logs and the transactional logs?	YES meets CWA 14167-1 requirements	Worth checking

ADSS Server enables organisations to check transactional validity at the server. Some people advise allowing the end-user to determine if the data is to be trusted, however Ascertia does not recommend this approach – if the data cannot be trusted then why present it to busy managers?

As can be seen ADSS Server has been designed to cope with a changing e-business world in which multiple document formats will be used, with multiple signature formats and other properties. Although requirements may seem clear now there is usually a clear need for investment protection so that changing business requirements do not lead to a project being scrapped and restarted because of a lack of flexibility.

ADSS Server was selected as the core technology of the DNV Validation Authority Service (http:/www.dnv.com) after an open global tender – our approach and product functionality and flexibility was our key to success. BBS (http://www.bbs.no) now runs this service and has renamed it as the Global Verification Service.

ADSS Server and ADSS GoSign Applet can also provide very effective signing solutions that can use the verification solution features described above. Further information is available on the usage scenarios and features and benefits of ADSS Server in the form of datasheets, detailed proposals, presentations and live verification demos on the Ascertia website. Consult Ascertia or your local partner for further information.