ascertia

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 we keep being asked to explain the benefits that ADSS Server brings to an organisation as opposed to using alternatives such as some open source toolkits, some simple service models or a limited function product. The answer is all about management, flexibility and investment protection.

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

Verification / Validation Requirements	ADSS Server	Other Products
Can the product process PDF, XML, S/MIME and other PKCS#7 and CMS signed documents?	YES	Often limited to one or two formats
Can the product handle basic signatures, timestamped signatures, long-term signatures, PDF certified signatures?	YES	A very limited ability to cover this
Does the product allow the organisation to easily define the trust anchors (Root CAs and Issuer CAs) that are trusted?	YES	These often rely upon Windows
Can the product verify multiple signatures in a single call and return information on each of the signers	YES - returned via API	Detailed information is rarely returned
Can the product check both current and historic signatures by using a specified date & time in the past? Does it keep old CRLs from each trusted CA so that it can check the signature status in the past? For long-term signatures can it automatically use the embedded CRL/OCSP information if valid?	YES YES YES	Historic signatures are rarely handled Long-term signatures are often not handled
Does the Product have effective security controls and maintain protected event and transaction logs?	YES – including optional dual controls	Check carefully - some assume you will do this!
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 and OCSP 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	CRL – yes OCSP maybe!
Can a copy of the original document be kept within the transaction logs as evidence	YES	Usually a completely separate action
Can an 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 [work in progress]	Usually a completely separate project or product
Can the verification product just handle detached signatures to ensure privacy at the relying customer?	YES – also see ADSS Gateway	Some have issues being this flexible
Is the product designed to be used by both end-users, business relying parties and also managed service providers?	YES	Many are rather limited in scope

Verification Service Providers need ADSS Server

Verification / Validation Requirements	ADSS Server	Other Products
Does the product provide detailed logging of each transaction, the evidential information and filtering/searching and reporting generation capability?	YES	Limited functionality will exist at best
Can the calling client applications be authenticated using request signing and/or SSL client certificates? Can these clients be limited to only specific signature verification profiles?	YES	Sometimes an SSL client certificates capability
Can the product provide quality information on the signature algorithms, key lengths, hash algorithms and certificate policies associated with the signature and whether these meet the minimum local security policy requirements of the relying party?	YES	Unlikely
Does the vendor provide a client SDK for Java and .Net environments plus source code samples and example applications to make integration simple?	YES	Possibly
Can the solution be created on non-Windows platforms	YES	Possibly
Can high availability solutions be created without any extra effort?	YES	Possibly
Are a variety of FIPS 140-2 level 3 or CC EAL4 HSMs supported	YES	Possibly
Is an effective 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	Worth checking

ADSS Server enables organisations to check transactions 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://va.dnv.com) after an open global tender – our company and product flexibility was our key to success.

Further information is available on the usage scenarios and features and benefits of ADSS Server in the form of datasheets, detailed proposals and presentations. Consult Ascertia or your local partner for further information.