ADSS Go>Sign Client ™

Enabling local digital signatures for Microsoft Windows and macOS

ADSS Server is a well-proven, standards-based product that can be deployed on premise for enterprise use or within a managed service as part of a cloud service. It can meet the most demanding needs by providing high throughput and high availability. As a strategic product for Ascertia, it offers support for the latest Windows and Linux operating systems, databases and HSMs.

Enabling Local Digital Signatures

In the digital world it is critical to be able to prove who you are transacting with and who has signed a digital document or transaction, digital identities, issued by highly trusted providers need to be generated and stored in a way that ensures only holder of the identity is authorized to use the credential, this in turn provides confidence that signature applied to a document or transaction was performed by the holder of the identity and proves the identity was under the control of the induvial. Cryptographic smartcards and USB tokens provide a secure certified environment for users to generate and store these digital identities compared to software based identities that can be copied and have no certified protection mechanisms to prevent an attacker from trying to access the digital identity of the holder..

Many types of project make use of smartcard based digital identities for highly regulated schemes for digital signatures and authentication, these include:

- National eID schemes
- AATL Trust Service Providers
- Enterprise Corporate ID's

The ADSS Go>Sign Client allows such smartcards, USB tokens or even local software based digital identities to create long-term validation, timestamped digital signatures.

ADSS Go>Sign Client makes it easy for end users to sign documents, data and transactions using locally held keys and certificates.

Go>Sign Applet was the first client and used a signed Java applet. This approach worked well until 2016 but now most browsers no longer accept Java applets. Go>Sign Desktop is a simple to install client that offers the same functionality for Windows and Mac OSX.

Key Features

- **Broad technology support:** Supports a wide variety of PDF, XML and data/file/email signing formats, plus timestamped and long-term digital signatures (ETSI PAdES, XAdES and CAdES profiles)
- **Simplified User Experience:** Supports automated digital certificate filtering to allow the business applications to control which local signing certificate is acceptable for use.
- **Roaming Credential Support:** Supports roaming credentials, where keys/certs are held in secure container on ADSS Server and sent to the Go>Sign Client at the time of signing.
- **Digital Identity Generation:** Supports generating keys and certificates in local key/certificate stores as well as 3rd party smartcard and USB tokens.
- **Standards Support:** Support for Windows CAPI/CNG, Token and PKCS#11
  ADSS Go>Sign Client has unmatched capability for creating PAdES, XAdES, CAdES, PDF, XML Dsig, PKCS#7 / CMS signatures using local keys held within Windows or macOS.

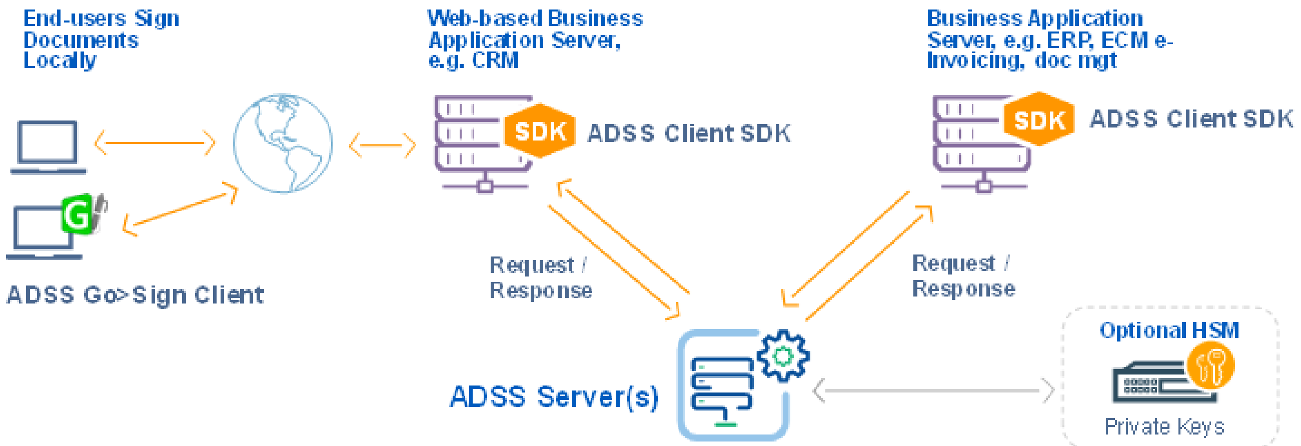
ADSS Client SDK at a Glance

ADSS Client SDK provides APIs for signing, verification and encryption, using OASIS DSS, APIs for certificate management using CMC, certificate validation using OCSP, SCVP and XKMS and archiving services using LTANS (as well as ETSI AdES-A signing).

ADSS Server provides high level security services whilst removing all the lower-level complexities from the business environment. ADSS Server administrators define acceptable policies and profiles as well as how they will be applied and how they will be presented. They then permit or deny client applications the right to use these, e.g. the “invoice signing” profile should only be allowed by the specific finance department invoicing application.

ADSS Client SDK enables this interaction and simplifies the task. It is quite possible to get an initial application integrated within just four hours – this is feedback from one of our customers that downloaded our evaluation software and with no prior knowledge added signing to their documents.

The following diagram illustrates how ADSS Client SDK is used to advantage within ERP, ECM CRM applications today for internal and external sign-off and approval, signature verification, bulk document signing and indeed any trust service request made to ADSS Server.


End-users Sign Documents Locally
ADSS Go>Sign Client
Web-based Business Application Server, e.g. CRM
SDK
ADSS Client SDK
Business Application Server, e.g. ERP, ECM e-Invoicing, doc mgt
SDK
ADSS Client SDK
Request / Response
Request / Response
ADSS Server(s)
Optional HSM
Private Keys

Further Information

With so many options Ascertia and its partners can help to define the best options to meet various business, legislative and regulatory needs and reduce the risks and costs involved in creating, sending, and receiving and storing e-business documents. The many capabilities of ADSS Server can be used to solve today’s needs and also offer tremendous investment protection to meet the changing needs of tomorrow.

ADSS Server has been designed to meet the needs of SMEs, large national and multi-national organisations, managed service providers and regional trust schemes. It does this by providing flexibility, resilience, scalability, combined with strong internal security, management, audit logging and reporting.

ADSS Client SDK is a comprehensive solution for developers to PKI enable business applications.

- Supported Operating Systems:
  Microsoft Server 2022, 2019, 2016
  Linux RedHat, SUSE, CentOS, Ubuntu

M Hathaway

Mike Hathaway | Chief Product Officer

About Ascertia

Ascertia provides digital trust for people, devices, data and documents for everybody from individuals to Enterprises and Governments. Ascertia’s PKI and digital signature technologies serve a global customer base and partner network via direct and indirect sales channels.

For more info

info@ascertia.com

www.ascertia.com