Exploring eIDAS solutions and CEN TS 419241

The new EU regulation 910/2014 (eIDAS) aims to boost trust and convenience in secure and seamless cross-border electronic transactions by promoting the widespread use and uptake of electronic identification and trust services. It defines electronic identification (eID) and electronic Trust Services (eTS) as key enablers and central building blocks of the Digital Single Market. The eIDAS regulatory framework and standards is expected to increase the efficiency and global competitiveness of European businesses and private sector.

As part of its support of eIDAS, Ascertia is tracking various secondary level legislation and standards for compliance testing and certification. There is particular interest in the CEN TS 419241 technical specification that defines the "Security Requirements for Trustworthy Systems Supporting Server Signing (TW4S)".

The focus of these security requirements is to allow high trust unique-per-user keys and certificates to be created, stored, securely accessed, revoked and deleted on server based solutions with appropriately high levels of security. This will allow Advanced and Qualified Electronic (Digital) Signatures to be created on business documents and data providing appropriate certifications have been obtained. In essence users will be able to strongly authenticate themselves using strong authentication mechanisms and authorise a TW4S compliant system to create a high trust advanced electronic (digital) signature. This has many efficiency and ease of use benefits when compared to the traditional smartcard/ token based local signing solutions.

At a high-level TW4S recognises two different levels of user authentication for demonstrating "sole control" over the user's server-held signing keys. The first level is where the signing application authenticates the user. The second level requires 2-factor authentication and also that this must be enforced from within an HSM. For server-side Advanced Electronic Signatures sole control at level 1 is sufficient however for server-side Qualified Electronic Signatures, the solution must implement sole control at level 2.

Currently only the first part of this specification is available and additional parts are expected later in 2016. Although the final requirements and protection profiles will only be known at this time, Ascertia is preparing a solution that will meet this specification. The following sections explain this in more detail.

Ascertia ADSS Signing Server

The Ascertia ADSS Server is a cryptographic services engine and already provides sophisticated cryptographic key management features including:

- Working with multiple HSMs either as load-balanced configuration or as fall-back options using PKCS#11, CAPI/CNG and even Azure Key Vault and Amazon AWS Cloud HSM
- Able to create large number of user keys and securely export and store these outside of the HSM using Key Encrypting Keys (KEKs) - this ensures that user keys and certificates are held securely within the ADSS Server Key Manager database and can be used immediately on all other live servers with local HSMs or networked HSMs
- Can create long-term, short-life or even one time use certificates
- Integrates with a range of external CAs using online certification protocols (as well as traditional offline) and also supports multiple internal CA instances
- Can manage enterprise keys with certificates being securely issued remotely from another ADSS Server instance
- Able to support RSA, ECDSA and SHA-2 secure algorithms as well as support for larger key lengths

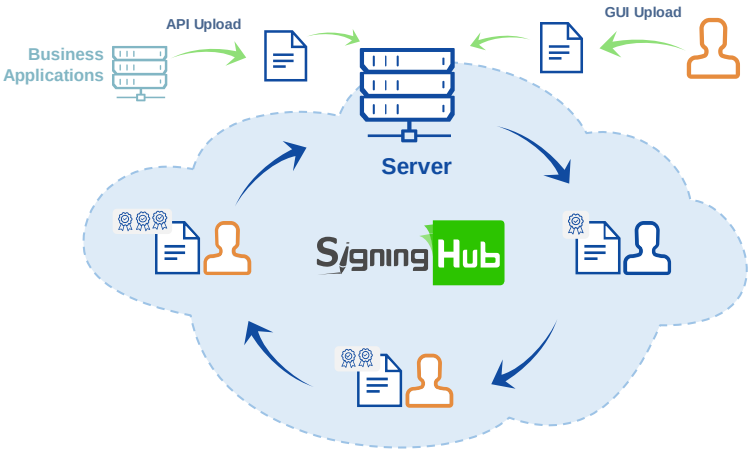
Ascertia SigningHub

SigningHub is Ascertia's document signing, workflow and approval status tracking product that is powered by ADSS Server.

SigningHub Cloud or Enterprise

Four modes of use:

- Direct user interaction to upload documents and send to others
- Tight integration with the business application – invisible to the user
- Loose integration for applications with no suitable user web-browser interface
- Advance integration via connectors Salesforce, SharePoint, Dynamics



SigningHub manages users, supports multiple authentication mechanisms and controls access to documents they are entitled to review and sign. SigningHub internally relies on the ADSS Server for its core e-Trust services.

Working in conjunction with ADSS Server, SigningHub also the user to sign:

(a) using a locally held key and certificate – which can be a Qualified Certificate on an QSCD (the new name for SSCD)

(b) using a mobile held key and certificate – which can also be a QC on a QSCD. SigningHub supports communication with the mobile apps that support this

(c) using a centrally held key and certificate which can be held protected in software, OR held within a CC EAL4+ HSM, OR securely generated, wrapped, exported from a CC EAL4+ HSM and held within the SigningHub database, and then at the time of signing the wrapped key is sent back to the HSM, securely unwrapped and used for secure signing within the HSM and then securely deleted from the HSM

With the sophistication that is offered in terms of user authentication, key and certificate management, and of course document management Ascertia already provides a solution which can be self-certified as compliant with TS 419241 Level 1 sole control – which as explained previously is sufficient for Advanced Electronic Signatures using server-side signing.

Support for Level 2 sole control will be provided during 2016 and will be achieved by:

- Working with the Verisec Freja Mobile solution to support 2-factor user authorisation of signing requests at time of server-side signing using a secure channel
- Making the authorisation decision to allow signing using a secure process running inside the HSM, thus providing a trusted channel between the user and the HSM

This solution will be formally certified as eIDAS Level 2 compliant once the relevant Protection Profiles are standardised. This is required for those business use cases where Qualified Electronic Signatures are necessary.

Ascertia has unique advantages in being able to leverage its relationships with key security vendors such as Verisec whilst providing an efficient and user-friendly interface. SigningHub and ADSS Server software run on physical or virtualised systems, on private or public cloud platforms, Microsoft Azure or Amazon AWS. Our signing process includes strong evidential

measures to ensure that the intention to sign was clear and the signing action was clearly understood and a wilful act. The features that differentiate SigningHub from other options are:

- SigningHub is not just a signing engine, it offers a complete multi-user document workflow and digital signature approval solution. It manages the approval lifecycles from document preparation, sending notifications, to workflow status tracking, signing and event logging and evidencing
- SigningHub quickly enables people and applications to create a document workflow with digital signature approval by multiple parties using sequential, parallel or individual flows
- It supports full corporate re-branding and localisation
- It is an EU solution with no US Patriot Act or Safe Harbor implications when running in-house or via a non-US hosting service
- It can be delivered as an on premise product to allow organisations to easily meet their data protection and data residency requirements
- Makes the digital signature process easy for non-technical people whilst delivering strong authentication, integrity, non-repudiation and encryption
- Leverages the value of existing Enterprise, National, Global or EU Qualified PKIs by its ability to interwork with multiple PKIs simultaneously
- Creates long-term signatures that are good for 10, 15 or 20+ years and these can be refreshed into the future when longer timeframes are demanded (supports both the traditional PAdES Part 2 as well as latest PAdES Part 4 standards)
- Supports groups, delegation, form field entry and initials
- Helps users to prevent common mistakes such as completing all actions prior to signing and signing in the right place
- Supports a full range of desktops and browsers plus iOS and Android mobile devices
- Provides strong security using a WYSIWYS (what you see is what you sign) interface
- Supports current open standard document formats
- Future-proofed by offering central signing, local signing and mobile signing
- Intuitive and quick to learn, very quick to deliver with excellent support services

Summary

ADSS Server provides a very rich set of features for supporting different signature types, configuring different signing profiles and linking these to business applications. OASIS and ETSI standards are well supported as are other important standards such as PEPPOL signature/certificate quality levels.

Given the sophistication of signing options using server-held keys and certificates, roamed keys and certificates and local hashing and signing, ADSS Server can be used to deliver TW4S solutions to various business applications.

SigningHub uses strong authentication options and authorisation services and makes it easy for users to review and sign documents using eIDAS compliant digital signature mechanisms. SigningHub delivers much more than just a signing engine, it fully manages the document approval lifecycle from preparation to sign-off by multiple parties, notifying each person when it's their turn to sign and allowing document owner to keep an eye on the document approval status. SigningHub includes the ability to set-up flexible service plans for a multi-tenanted system together with built-in billing module for online and offline payments – thus a complete solution for commercialising document signing and approval services. External identity service providers e.g. STORK Pan-European Proxy Services (PEPS) or corporate Active Directory Federation Services are supported where based on standard SAMLv2 protocol.

Ascertia has world class products and a clear strategy to ensure it keeps providing products that provide ***the most secure way to sign***.