ascertia | IDENTITY PROVEN TRUST DELIVERED

ADSS SERVER SAM APPLIANCE

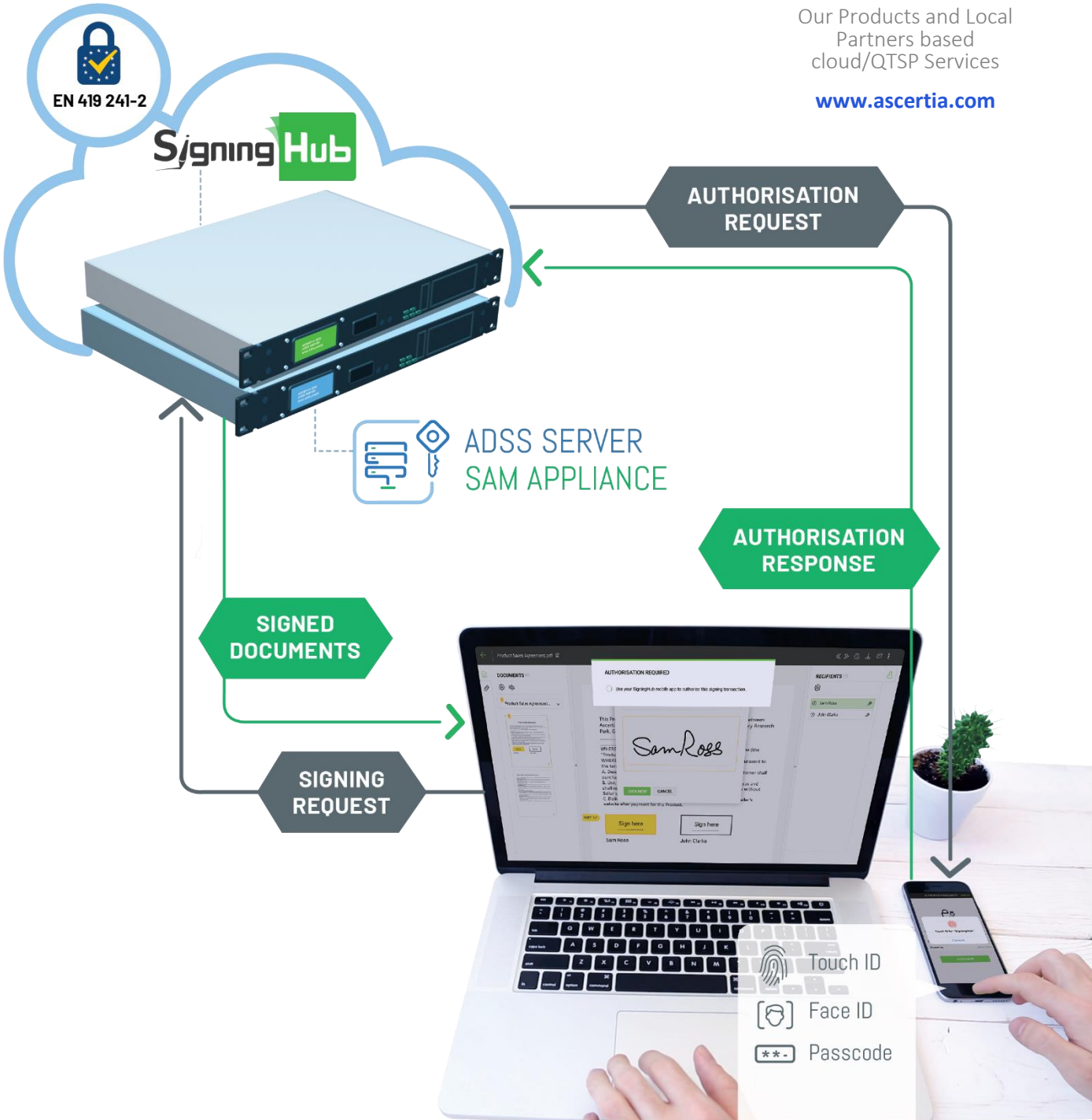
COMMON CRITERIA EN 419 241-2 CERTIFIED

LEADERS IN REMOTE SIGNING

ASK US ABOUT

Our Products and Local Partners based cloud/QTSP Services

www.ascertia.com



KEY FEATURES

- Ascertia's ADSS Server SAM Appliance is the first product to achieve Common Criteria EAL4+ certification against the eIDAS ETSI EN 419241 standard and the EN 419 241-2 Protection Profile with Level 2 Sole Control.
- Seamless integration with Ascertia's SigningHub and ADSS Server products and the new Ascertia Go>Sign mobile app for authorising signing actions from mobile devices.
- A secure Trusted Path authorisation mechanism provides the CEN "Signature Activation Protocol (SAP)" requirements and ensures only the key owner can authorise the use of their centrally held signing key.
- The SAP allows the user to review the "data to be displayed" and decide if this adequately describes what they are being asked to sign, if so they authorise the use of their remote signature.
- Includes Utimaco's most powerful HSM which is CC EAL4+ certified meeting the EN 419 221-5 protection profile – use to generate, protect and process all user signing keys. The ADSS Server SAM Service can also be configured to just run in software on Windows or Linux for testing or evaluation purposes. It can use software crypto, a software HSM simulator or a PKCS#11 HSM.
- A high performance 1U hardware appliance that meets FIPS 140-2 Level 3 criteria.

ADSS SERVER SAM APPLIANCE STANDARDS COMPLIANCE

EN 419 241-1
Trustworthy System Supporting Server Signing: Part 1 General System Security Requirements

EN 419 241-2
Trustworthy System Supporting Server Signing: Part 2 Protection Profile for QSCD for Remote Signing
Ascertia ADSS Server SAM Appliance is CC EAL 4+ certified

EN 419 221-5
Protection Profiles for TSP Cryptographic Modules – Part 5: Cryptographic Module for Trust Services
Ascertia ADSS Server SAM appliance - includes a certified HSM

TS 119 431-1
Policy and security requirements for TSP service components operating a remote QSCD / SCD

TS 119 431-2
Policy and security requirements for TSP service components supporting AdES digital signature creation
Ascertia is working in ETSI Special Task Force 539

TS 119 432
Protocols for remote digital signature creation
Ascertia is working in ETSI Special Task Force 539

ⓘ Many other relevant standards that TSPs must also consider e.g.: PAdES, XAdES, CAdES profiles, standards for certificate issuance, timestamping etc.