cosign by arx The Digital Signature Company

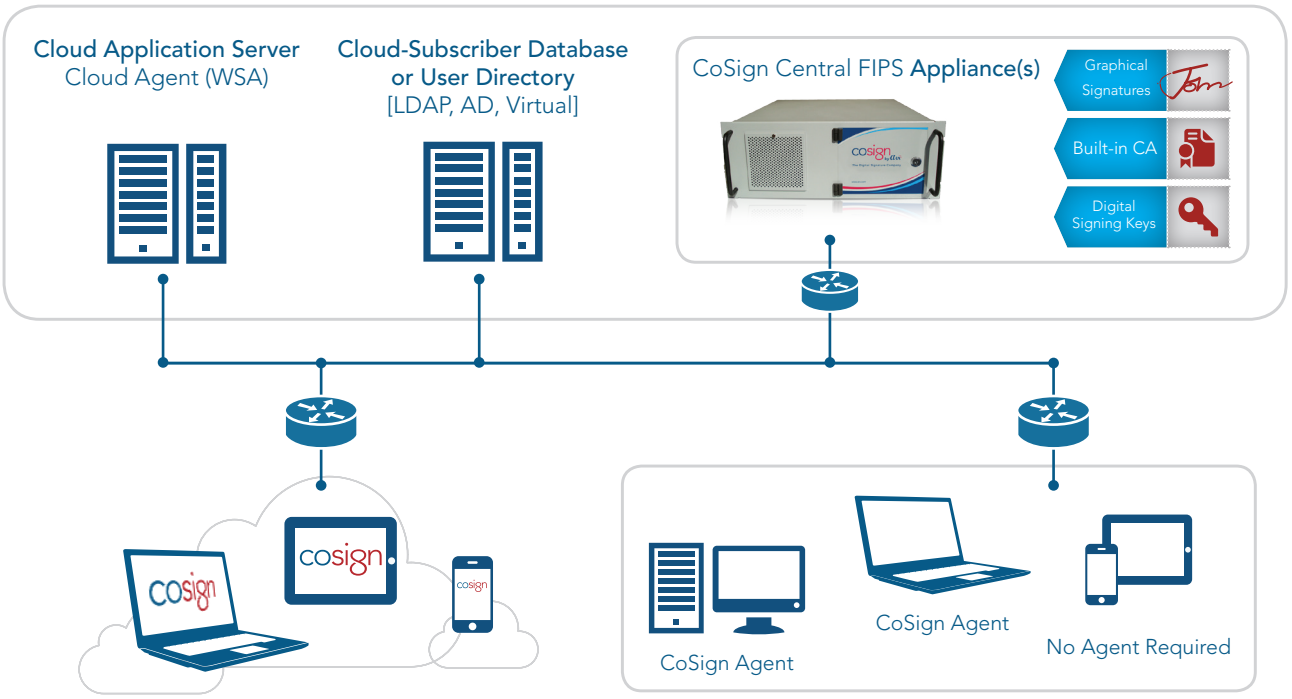
CoSign: The Proven Digital Signature Engine for Applications in the Cloud

CoSign by ARX, the most widely used digital signature solution, was recognized as "the strongest digital signature solution" in the Forrester Wave: E-Signatures 2013 report. Millions of people at businesses, governments and cloud services around the world use it every day to easily add secure digital signatures to documents in many formats and applications.

CoSign, which was designed from the ground up as an enterprise grade signing system based on global standards, meets the most demanding requirements for Cloud applications. It is the only digital signature system proven to comply with the strictest technical standards, regulations and business requirements across vertical industries and geographies. Anyone can verify CoSign digital signatures for signer identity and intent, as well as document integrity, without requiring proprietary validation software.

The high-speed, high-capacity, network-attached CoSign digital signature engine has both FIPS 140-2 level 3 and Common Criteria EAL4+ certification. It offers a comprehensive digital signature solution that incorporates centralized key and certificate management, all the necessary signature automation features, and a high-availability/load-balancing/redundancy option.

The Cloud Application's Domain



ARX | 855 Folsom St. Suite 939, San Francisco, CA 94107 | Tel. (415) 839-8161 | www.arx.com | sales@arx.com

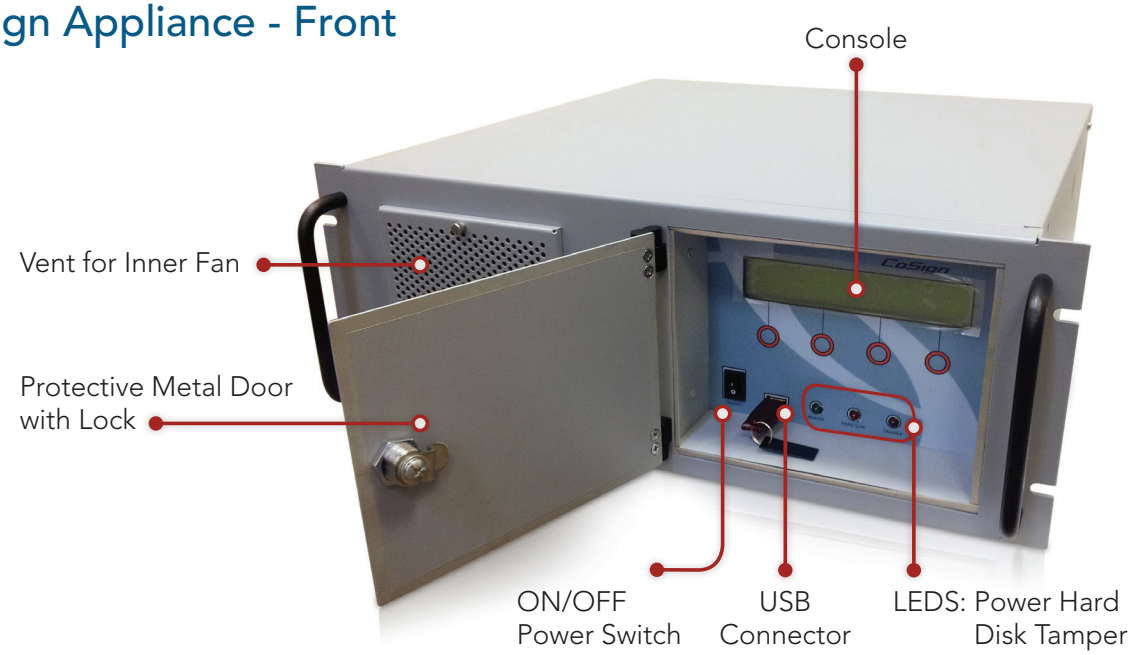
Key Features:

- **Standard digital signatures:** CoSign signatures adhere to global PKI standards, providing signers with sole control over their signature credentials (private key and certificate). It complies with CEN-TS-419241 technical specification level 2.
- **Management security:** CoSign is NIST FIPS 140-2 level 3 validated and Common Criteria EAL4+ certified. The CoSign appliance is a highly secure, tamper-evident device, incorporating strict security measures to protect the signature keys. All the signature keys are stored within the CoSign device itself and all signature operations are performed within the secure enclosure of the CoSign device.
- **Document security:** Word, Excel, PDF and many other types of documents can be signed with CoSign while remaining securely within the enterprise domain. This is achieved by installing a CoSign Agent on the signer's (Windows) desktop and/or on any of the content servers (such as SharePoint, OpenText Content Server, Oracle WCC and Alfresco ECM).
- **Scalability, redundancy, high availability and high performance:** Through its flexible scalable architecture CoSign can support millions of users, while a single appliance is capable of 1500 signature operations per second. More than one CoSign appliance can be configured for hot backup and operation in an Active-Active mode. The load balancing capability ensures that the signature-request load is distributed among all production CoSign appliances. The internal user-database that holds the signature keys is securely synchronized among all the servers so that if one of the servers goes offline, the others continue serving the users.
- **Disaster recovery and secure backup:** The entire internal credential database can be backed-up to an encrypted backup file (FIPS approved mechanism), and can only be restored in a fresh CoSign appliance that shares the same Master Key.
- **Web-based signing app:** CoSign Web App is the most secure online signing app, enabling anyone to easily add digital signatures to their PDF, Word and Excel documents from desktop and mobile/tablet web browsers while ensuring maximum security.
- **CoSign Signature APIs:** High-level Signature APIs enable convenient integration with any application. They can be used with any development language on any platform including PHP and .NET apps. Standard cryptographic APIs are also supported including Microsoft CAPI/CAPI NG, PKCS#11 and JCE/JCA.
- **CoSign Web Agent API:** Using the CoSign Web Agent API, developers can easily integrate CoSign with any web application. It enables a user to preview a document in a browser on any computer or mobile/tablet device and then digitally sign it.

- **Active Directory and LDAP synchronization:** CoSign users can be managed via automatic synchronization with Microsoft Active Directory, an LDAP directory, or the Active Directory Federation Services (ADFS). When a user is added to the organization's service directory, a signer is automatically created in CoSign. Similarly, any change made in the service directory is automatically reflected in CoSign, which also supports Single Sign On.
- **Application connections:** CoSign integrations are available for many popular document, content and workflow management systems including Microsoft SharePoint, OpenText Content Server, OpenText eDOCS, Oracle WebCenter Content, Documentum, SAP, Alfresco, K2, Nintex, HP Trim, TeamCenter, AutoCAD and others. CoSign connections enhance these applications by adding the ability to sign documents from directly within them.
- **Graphic signature images:** CoSign provides the option to stores graphic signature images alongside a user's signature key. During the signing process, the user can add their graphic signature alongside their digital signature.
- **Authentication:** A variety of user authentication methods can be used including directory or domain subscriber-name-passwords, One Time Passwords, Tokens (such as smartcards and USB-based security tokens), RADIUS or OATH-based authentication, biometric fingerprint devices, LexisNexis InstantID and SAML 2.0.
- **Certificate Authority (CA) support:** In addition to advanced certificates, which can be issued by the internal CA (controlled trust) within the appliance, CoSign can also use qualified certificates issued by an external or subordinate Trust Center, CDS and AATL certificates issued by an Adobe-trusted CA, and certificates issued by an automatic web-trusted CA.
- **Auditing and monitoring:** The CoSign audit log records signature operations, errors and maintenance events, and can be collected by an external Syslog server. CoSign can be monitored using the standard SNMP protocol.
- **Compliance:** CoSign complies with the US E-SIGN Act, US UETA, EU eIDAS (Electronic Identification and Trust Services for Electronic Transactions in the Internal Market) regulation, EU VAT Directive, FDA 21 CFR part 11, HIPAA, USDA and SOX. In addition, it complies with the technical interoperability and security standards of NIST, ETSI, ISO, W3C, OASIS, IETF, Microsoft and Adobe.
- **Cryptographic algorithms:** RSA 1024-4096 bit (PKCS#1); Secure Hash Standard (SHA-1, SHA-256, SHA-384, SHA-512); and Triple-DES and AES only to secure the credential database, backup files, and SSL and IPSec sessions.
- **Key Generation:** Internal FIPS-approved PRNG algorithm. Random seed is generated from a dedicated hardware source (internal smartcard).

Physical and Electrical Characteristics: Built-in 1 Gigabit Ethernet NIC; Dimensions: w 19" (48.3cm); d17.5" (44.50cm); h7" (4u) 17.8cm. Weight: 30lbs (13.6kg). Electrical rating of power supply: Voltage - 00-240 Vac; Frequency: 60/50 Hz; Current: 10 A; Power consumption: 250 Watt, 850 BTU/h; EMC (EN 55022, EN 55024, FCC), UL, and CB Certified.

CoSign Appliance - Front



CoSign Appliance - Rear