emSign

powered by emudhra

Document Signer Certificates for Tamper-Proof Digital Documents

Overview

With the ever-increasing use of digital communications and the online exchange of documents containing sensitive information, the necessity of ensuring the authenticity and integrity of these documents is paramount. The risk of unauthorized access by third parties can pose a significant threat, especially when the documents in question are of a highly sensitive nature. As a growing number of enterprises are transitioning towards digitization, the need for secure digital documents, both in transit and at rest, is more vital than ever.

Document signing certificates provide a solution to the security issues associated with digital documents, employing advanced encryption techniques and digital signatures. emSign offers document signing certificates that allow users to automate the document signing process comprehensively while preventing data tampering and data theft.

emSign

powered by emudhra

Business Challenges

Ensuring the integrity, authenticity, and non-repudiation of digital documents is a crucial factor in establishing trust and security. However, safeguarding these documents from tampering poses a substantial challenge due to the sophistication of current cyber threats. Digital documents, particularly those in transit, are vulnerable to risks posed by hackers, potentially leading to data breaches and data loss. This vulnerability compromises the confidentiality and integrity of these documents.

Document signing certificates that enable digital signing of documents effectively address these challenges, providing a means to secure data privacy, integrity, and authenticity. The digital signatures that underpin document signing certificates utilize cryptographic techniques to validate the origin and integrity of the documents.

The emSign Solution

emSign's document signing certificate offers comprehensive automation of the document signing process at an individual, department, or organization level. It prevents data tampering and data theft through robust document encryption.

emSign's document signing certificate maintains document integrity and authorship, thereby protecting intellectual property. It is designed to meet national, global, and industry-specific compliance requirements for digital signatures. It also facilitates the timestamping of documents to support time-sensitive transactions, audit trails, and non-repudiation. The certificate is available in three variants for both individuals and organizations: personal, professional, and corporate.

Key Benefits

- SVisual Trust Indicators: Detect document tampering using clearly defined visual indicators.
- Timestamping: Confirm the time and date of signing, and ascertain the validity of the signature.
- Multi-signature Workflows: Authenticate business-critical documents that require multiple signatures effortlessly.
- Automatic and Manual Signing: Both automatic (for bulk signing) and manual (for signing individual documents) signing options are available.
- 24x7 Support: Avail robust support along with a comprehensive library of resources for peace of mind.
- Regulatory Compliance: Document signing certificates from emSign comply with global standards and regulations, including GDPR, WebTrust, etc.

emSign

powered by emudhra

FEATURES	PERSONAL	PROFESSIONAL	CORPORATE
Signing key and delivery management	This signature certificate is issued to an individual to sign in their personal capacity without any relation to their place of work. Individual certificates are generally issued in a secure USB Token	This signature certificate is issued to an individual representing the organization in their capacity as an authorized signatory of the organization. These certificates are issued on a secure USB Token or alternately be provisioned in a Hardware Security Module (HSM)	This signature certificate is issued to the organization. Organization certificates undergo identity verification to verify the Organization's existence, latest status, and other such attributes. These certificates are issued on a secure USB Token or alternately provisioned in a Hardware Security Module (HSM)
Available certificate types	Standard – AATL (Adobe Approved Trust List) Web trust accredited	Standard – AATL (Adobe Approved Trust List) Web trust accredited	Standard – AATL (Adobe Approved Trust List) Web trust accredited
Ideal for	Individuals to sign in their personal capacity without any relation to their place of work/ organization/ department within an organization)	Signing (sealing) electronic documents as an organization (or a department within an organization by the respective authorized signatory)	Signing (sealing) electronic documents as an organization (or a department within an organization)
Validity	1-3 years	1-3 years	1-3 years
Timestamping	Available	Available	Available
Reissuance	Available	Available	Available

About eMudhra

eMudhra, a global provider of digital identity and cybersecurity solutions, specializes in digital signature certificates, Public Key Infrastructure (PKI) services, and robust authentication protocols. Our impactful presence in India and international presence have allowed us to support governments and enterprises in safeguarding their digital transactions and vital information.

eMudhra offers digital certificates, PKI-based solutions, authentication and identity governance services. With a strong presence in India and a global footprint, eMudhra helps organizations securely manage their digital transactions and protect sensitive information. Being a leading digital identity and cybersecurity solutions provider, eMudhra is now focused on futureproofing cybersecurity using Post Quantum Ready Cryptography and Zero-Trust Identity Governance model.