Secure Digital Signing with SAP and SafeNet Hardware Security Modules from Gemalto

SAP software utilizes electronic documents to streamline business operations and communication across departments, such as procurement, manufacturing, customer service, sales, finance, and human resources. Together with SafeNet HSMs from Gemalto, businesses gain a secure, trusted solution for secure digital signing.

Secure Digital Signing with SAP Solutions and Gemalto HSMs

As organizations transition from paper to digital, a simple, secure solution to streamline business processes and initiatives is needed. Together, SAP and Gemalto offer the ideal solution that not only cuts time but costs associated with traditional paper-based document signing. The combined solution allows users to digitally sign documents, files, forms, and transactions anywhere while ensuring data integrity, signer authenticity, and regulatory compliance.

Using Digital Signatures with SAP Solutions

SAP software utilizes electronic documents to streamline business operations and communication across departments, such as procurement, manufacturing, customer service, sales, finance, and human resources. These solutions speed up the time to market, provide for effective, real-time business processes, and improve the overall utilization of corporate resources. With the integration of electronic documents and digital signatures, SAP management solutions allow organizations to reap many rewards, including but not limited to:

- Automated operational processes
- Faster reporting across all business lines
- Increased confidence in data integrity
- Enhanced vendor relationships

Benefits of Digital Signatures

- Easy to Use – Digitally sign and seal electronic documents with ease
- Expedite Business Processes – Replace handwritten signatures and paperwork, and reduce the approval process time for multiple authorizing signatures
- Paperless Office – Reduce costs associated with traditional paper-based processes
- Legal Compliance – Digitally signed electronic documents improve compliance posture

Enhancing Digital Signatures with Gemalto’s SafeNet Hardware Security Modules

SafeNet HSMs augment digital signatures for two fundamental reasons: performance and security. From a performance standpoint, signing operations are extremely processor-intensive, and the longer the key, the greater the processing effort required. NIST recommends using keys that are at least 2048 bits in order to provide adequate security. At this length, there is a significant load on the CPU, and to be CPU-independent, hardware acceleration is needed to provide a large number of both key generation and signing operations. Thus, organizations need to offload all cryptographic functions to a dedicated HSM with its own dedicated crypto processors to ensure adequate performance and prevent overloading the host server.
Moreover, utilizing SafeNet HSMs for all signing operations is a matter of basic security. After all, the entire security structure of digital signatures is built upon the foundations of cryptographic keys so the private keys must be kept strictly private, secret, and secure. Without proper security measures protecting both the signing process and underlying cryptographic keys, our ability to trust digital signatures is put in jeopardy.

### The Advantages of Secure Digital Signing with SAP and Gemalto

Together, SAP and Gemalto efforts provide a secure and seamless digital signing solution, enabling organizations to achieve:

- **Streamlined Business Processes** – Replace handwritten signatures and paperwork with digital documents and legally compliant certificate-based signatures, and reduce approval process timelines for multiple authorizing signatures.
- **Reduce Costs** – Reduce costs associated with traditional paper-based processes (i.e., paper, printing, ink, faxing, postage, and processing time).
- **Non-Repudiation** – Gemalto and SAP solutions integrate to provide non-repudiation of documents or transactions. Digitally signed documents and transactions are sealed electronically, providing evidence of signer and document authenticity and guaranteeing document integrity and are thus resistant to fraud and tampering. Utilizing a hardware-based device ensures users that the private keys are never exposed outside the module, ensuring the integrity of signed documents.
- **High Assurance** – With PKI-based trusted credentials, the level of assurance is typically higher than that of electronic signatures protected only by a password. Class 2 and Class 3 certificates assigned to Individuals and Organizations from country-specific Central Certificate Authorities (e.g., CCA of India) or other approved Certificate Authorities which are deemed acceptable as per the court of law can only be issued on FIPS 140-2 Level 2 or higher certified devices like SafeNet HSMs.
- **Compliance** – Utilizing standards-based digital signatures and X.509 certificates in accordance with regulatory and legal mandates maintains the integrity of documents. SAP and Gemalto enable compliance with security and privacy standards, including country-specific regional legal framework, FIPS-validated cryptographic modules, NIST test suite validation, and JITC/SAFE/IdenTrust certification, all of which combine to provide a powerful, dependable, and interoperable digital signature solution.

### How Digital Signing Works

1. **User views document**
   - User views document, fills in form fields, chooses credential, and clicks signature field to approve

2. **Signing process**
   - User initiates signing for smart card token pin to authenticate to credentials stored on the hardware token or smartcard

3. **Document received**
   - Adobe Acrobat or Adobe Reader® validates signature from trusted CA. Recipient views signed document

### Digital ID Protection

Secure certificate issuance and key management provided by HSMs

### About SAP

Headquartered in Waldorf, Germany, SAP is the world’s largest inter-enterprise software company, and the world’s third-largest independent software supplier overall. SAP employs over 28,909 people in more than 50 countries. Their professionals are dedicated to providing high-level customer support and services. For more information, visit [www.sap.com](http://www.sap.com).

### About Gemalto’s SafeNet Identity and Data Protection Solutions

Gemalto’s portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments, and transactions—from the edge to the core. Gemalto’s SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

---

**Contact Us:** For all office locations and contact information, please visit safenet.gemalto.com

**Follow Us:** blog.gemalto.com/security