nShield Time Stamp Option Pack

Time stamping backed by high-assurance hardware security

HIGHLIGHTS

- Generates highly reliable and secure time stamps for electronic records

- Supports proof of receipt and non-repudiation for legal transactions

- Prevents unwanted rejection of signed code

- Creates auditable chain to central time source

- Rooted in FIPS certified nShield hardware security modules

A member of the Entrust nShield family of high-security data products, the Time Stamp Option Pack (TSOP) creates time stamps on digital artifacts that enable organizations to assuredly and efficiently attest to the origin and time of electronic events. The nShield TSOP provides secure and auditable time signing for electronic business transactions and document to provide authoritative proof of when an event occurred while ensuring the time stamps are secure, authentic, and auditable.

nShield TSOP operates within the certified boundary of the nShield Solo hardware security module (HSM), issuing time stamps that enforce the validity and legal weight of digital signatures and dates on digital documents. Unlike software-based systems in which administrators can easily manipulate time, the nShield TSOP protects time-stamping keys using nShield Solo tamper-resistant HSMs.

Learn more at entrust.com/HSM

nShield Time Stamp Option Pack

TECHNICAL SPECIFICATIONS

Functional capabilities	Protocols and interfaces	Compatibility

• Supports PKI-enabled applications, electronic records, and code signing
 	
• Facilitates long-term auditability and enforces non-repudiation
 	
• Highly accurate and auditable to UTC
 	
• Time-stamping application that runs inside nShield's tamper-resistant nShield CodeSafe environment to ensure the time stamp and data being stamped cannot be tampered with
	• PKIX time stamp protocol (RFC 3161), ETSI TS102 023 and 101 861
	
	• Support for extensions to RFS 3161 described by RFC 5816
	
	• Support for custom applications using optional toolkit (Java and C)
	
	• Authenticode for code signing applications
		• Integrates with Adobe Acrobat, LiveCycle, Microsoft Authenticode, and Office applications
		
		• Time-stamp signing algorithms:
		  – RSA (2048, 4096 bits)
		  – DSA (3072 bits)
		  – ECC: (NISTB,P & K curves), SECP 160r1, 256k1
		
		• Support for P7B certificate chains
		
		• nShield Solo XC Base F3, nShield Solo 500+ HSM
		
		(Please refer to the relevant nShield Solo data sheet for security certifications, safety and environmental standards, compliance, and other specifications.)

Integration	Management and monitoring	Operating systems
• The nShield TSOP is easy to integrate with business applications that time-stamp digital documents such as PDFs and software code including drivers and scripts. Common uses include financial transactions, lotteries and gaming, security logs, long-term archives, notarization, medical records, and code signing	• For streamlined operations, the nShield TSOP is remotely managed through a graphical web interface, and error notices are sent to the administrator by email	• Windows Server 2019 (64-bit) • Windows Server 2016 x64 • Windows Server 2012 R2 x64

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications, and data visit **entrust.com**

Learn more at
entrust.com

ENTRUST