



ENTRUST

Veridocx brings on-demand secure time stamping to small business and consumers



How Entrust nShield® hardware security modules (HSMS) and Time Stamp Option Pack enabled a startup to easily and affordably build a web-based service for non-repudiable time stamping.

THE GOAL: BRING NON-REPUDIABLE TIME STAMPING TO A NEW MARKET

Startup Australian company Veridocx wanted to offer an extremely valuable service to consumers and small businesses: secure, non-repudiable time stamping at an affordable price.

While time stamping for digital documents is not a new technology, it was previously primarily deployed by larger organizations with the need for higher numbers of transactions. Veridocx knew many consumers and small businesses had reasons to use a time stamping service – from protecting intellectual property to verifying the time a contract was signed to pinpointing the moment a transaction occurred. Yet there were no easy and affordable ways for consumers and small businesses to time stamp documents. Sending items through the mail or via email wasn't a good option – envelopes and email headers could be easily tampered with. And taking a document to a lawyer for a third party witness was expensive and inconvenient.



There's nothing out there that comes close to the Entrust nShield Time Stamp Option Pack, in terms of being able to provide reliable and non-repudiable time stamps. >>>

– Gavin Gregson, Technical Director, Veridocx

LEARN MORE AT [ENTRUST.COM/HSM](https://www.entrust.com/hsm)

Veridocx developed a simple business proposition: to provide an online service that lets anyone obtain a time stamp for a document and identify the document positively – for just a few dollars. The challenge would be to find the right time stamping solution. It would need to be tamperproof and reliable in order to sell the service with confidence. It would have to be affordable if Veridocx was to offer the service at rates consumers would find attractive. And it would have to integrate easily into their web application.

THE SOLUTION: ENTRUST NSHIELD HSMs AND TIME STAMP OPTION PACK

After considering a variety of options – from modifying off-the-shelf equipment to building custom time stamping hardware – Veridocx discovered that Entrust nShield HSMs and Time Stamp Option Pack satisfied all their requirements for security, affordability and ease of use.

The Entrust nShield HSMs and Time Stamp Option Pack was easy to integrate into their web application – the Veridocx team had it up and running in less than a day. It was highly affordable, especially compared with the cost of a custom-built solution. The tamper-resistant Entrust nShield HSM together with the Time Stamp Option Pack supports recognized time stamping protocols such as RFC 3161 and is compliant with FIPS 140-2 Level 3. By performing the time stamping process within the HSM, the Entrust nShield Time Stamp Option Pack allows Veridocx to assure its customers that no one outside or inside the company can tamper with the time stamping process.

With Entrust nShield HSMs and Time Stamp Option Pack, Veridocx is able to offer a solution that makes it extremely

easy for anyone to cost-effectively time stamp, store and verify any digital file. Users simply log onto veridocx.com, pay a small fee and upload a file. The file gets a time stamp, the user gets verification and the time stamped file can then be download or stored on the Veridocx site for safekeeping.

The Entrust nShield HSM handles all of the actual time stamping process – the Veridocx website essentially serves as a large front end to an extremely flexible time stamping technology.

KEY FEATURES AND BENEFITS

- High-assurance hardware security. Perform highly accurate time stamping for PKI-enabled applications, electronic records, and code signing – transforming electronic records into strong evidence.
- Easy integration with applications. Integrate secure time stamping functionality easily with business applications to time stamp digitally signed documents (e.g. PDFs), application code, or other electronic records.
- Accurate, auditable time stamps. Get superior time accuracy and auditability, with time stamps auditable to UTC.
- Tamper-resistant hardware. Protect the electronic time stamping process and keys through independently certified, tamper-resistant hardware.

A TIME STAMPING SOLUTION THAT INTEGRATES EASILY WITH APPLICATIONS

Veridocx chose Entrust because its time stamp solution was robust, mature and easy to integrate into the Veridocx web application. This enabled Veridocx to focus on building top-notch services for their customers.

It took the Veridocx team less than a day to configure and integrate the Entrust nShield HSM and Time Stamp Option Pack into their platform.

THE ENTRUST SOLUTION ALSO OFFERED OTHER SIGNIFICANT BENEFITS:

Non-repudiability. This was essential to the Veridocx team. They needed to be able to promise and prove that no one could forge or tamper with a time stamp. With the time stamp keys securely protected in a hardware security module, Veridocx knew their time stamps were safe from hackers and other external threats, as well as from any internal threats. If it was necessary, they could use auditable security trails to prove that no one could have hacked into the Entrust nShield HSM to modify or tamper with a time stamp.

Security. Unlike software-based systems in which administrators can easily manipulate time values, Entrust nShield HSMs protect the time stamping keys in independently certified, tamper-resistant hardware.

Quality. The quality of the hardware made installation and operation easier and solved many of difficult security and reliability problems that arise in an implementation of this kind.

Support. The Veridocx team discovered that the quality of Entrust nShield HSM was matched by the excellence in service and support they received on both the business and technical side.

Reputation. Veridocx wanted to be able to market their service as having been built with the most secure and reputable time stamp technology available today, and Entrust fit the bill.

Affordability. Veridocx was able to implement the Entrust time stamp solution at a cost that was far less than building their own system with custom software and off-the-shelf hardware.

ENTRUST NSHIELD HSMs AND TIME STAMP OPTION PACK

Entrust nShield HSMs together with the Entrust nShield Time Stamp Option pack keep accurate time and create secure time stamps to record creation time, filing time, or the timing of other events associated with electronic records and applications. By deploying a highly accurate and tamper-resistant electronic time stamping solution, organizations can verify the accuracy of time stamps used for digital records and improve the integrity and auditability of a broad range of critical processes.

Ideal for organizations that need electronic document signing with proof of time for legal and compliance purposes, Entrust nShield HSMs together with the Time Stamp Option Pack can be used for other common applications including financial transactions, lotteries and gaming, security logs, approval workflows, long-term archives, electronic lab books, and code signing.

Unlike software-based systems in which administrators can easily manipulate time values, Entrust nShield HSMs protect time stamping keys in independently certified, tamper-resistant hardware.

Entrust nShield HSMs are validated to FIPS 140-2 Level 3 and Common Criteria EAL 4+, and can provide highly accurate time stamps auditable to Universal Coordinated Time (UTC) for secure time traceability to independent national atomic clocks.



ENTRUST NSHIELD TIME STAMP OPTION PACK

Functional capabilities

- Supports PKI-enabled applications, electronic records and code signing
- Facilitates long-term auditability and enforces non repudiation
- Highly accurate and auditable to UTC
- Provides secure time traceability to independent national atomic clocks
- Tamper-resistant time stamping component

Protocols and interfaces

- PKIX time stamp protocol (RFC 3161), ETSI TS 102 023 and 101 861
- Support for custom applications using optional toolkit (Java and C)
- Authenticode for code signing applications

Compatibility and Upgradeability

- Can be deployed with Entrust Time Source Master Clock
- Integrates with Adobe Acrobat, LiveCycle, Microsoft Authenticode and Office
- Software upgradeable to latest releases

ABOUT ENTRUST

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.



Learn more at

entrust.com/HSM



ENTRUST