Veridocxが小規模企業と消費者にオンデマンドのセキュアなタイムスタンプを提供

Entrust nShield®ハードウェアセキュリティモジュール（HSMS）およびタイムスタンプ・オプションパックを活用したスタートアップ企業は、どのようにして否認防止タイムスタンプのwebサービスを簡単かつ手頃な価格で構築することができたのでしょうか？

目標: 否認防止タイムスタンプを新しい市場に導入する

オーストラリアのスタートアップ企業Veridocxは、消費者および小企業向けに極めて価値の高いサービスを提供したいと考えていました。それは、セキュアな否認防止タイムスタンプを手頃な料金で提供することでした。

デジタル文書のタイムスタンプは新しいテクノロジーではありませんが、これまでは多数の取引に対応する必要がある大企業によって主に開発されていました。Veridocxは、多くの消費者および小企業にも、知的財産の保護から、契約が締結された時間の確認、取引が発生した瞬間の特定など、タイムスタンプサービスを利用する理由があることを理解していました。それでも、消費者や小企業が簡単かつ手頃な料金で文書にタイムスタンプを利用する方法はありませんでした。封筒やEメールのヘッダーは簡単に改ざんできるため、郵送やEメールを通じたアイテムの送付は良い選択肢であるとは言えませんでした。第三者の立ち合いを求めて弁護士に文書を持ち込むのは高額な費用がかかり、不便でもありました。

> **«信頼できる拒否されないタイムスタンプを提供する能力において、Entrust nShieldタイムスタンプ・オプションパックに勝るものはありません。»**
>
> – Veridocx、技術担当取締役、Gavin Gregson

Veridocx

Veridocxは、わずか数ドルで、誰もが文書にタイムスタンプを取得でき、文書を識別できるオンラインサービスを提供するというシンプルなビジネスを考案しました。問題は、適切なタイムスタンプのソリューションを見つけることでした。自信を持ってこのサービスを販売するには、改ざんされない、信頼できるソリューションが必要でした。消費者が魅力を感じるためには、Veridocxのサービスは手頃な料金である必要がありました。そして、消費者のwebアプリケーションと簡単に統合できなければなりませんでした。

ソリューション: ENTRUST NSHIELD HSMsおよびタイムスタンプ・オプションパック

既製の機器の修正からカスタムのタイムスタンプ用ハードウェアの構築まで、様々なオプションを検討した結果、Veridocxは、Entrust nShield HSMsおよびタイムスタンプ・オプションパックがセキュリティ、手頃な料金、使いやすさのすべての要件を満たしていることを発見しました。

Entrust nShield HSMsおよびタイムスタンプ・オプションパックは同社のwebアプリケーションに簡単に統合でき、Veridocxチームは1日足らずでそれを設定し、稼働させました。これは、特にカスタムソリューションと比較すると、非常に手頃な料金でした。改ざんに強いEntrust nShield HSMとタイムスタンプ・オプションパックは、RFC 3161などの一般的なタイムスタンププロトコルをサポートし、FIPS 140-2レベル3に準拠しています。Entrust nShieldタイムスタンプ・オプションパックではタイムスタンププロセスをHSMで実行するため、Veridocxは顧客の内部および外部の誰もタイムスタンププロセスを改ざんできないことを保証することができました。

Entrust nShield HSMsとタイムスタンプ・オプションパックによって、Veridocxは誰でも非常に簡単にコスト効率の高いタイムスタンプを利用し、デジタルファイルを保管し、検証できるようにするソリューションを提供できます。ユーザーはveridocx.comにログインし、少額の手数料を支払い、ファイルをアップロードするだけです。ファイルはタイムスタンプを取得し、ユーザーは確認を受領し、タイプスタンプを取得したファイルをダウンロードするか、Veridocxのサイトで保管することができます。

Entrust nShield HSMsは、あらゆる実際のタイムスタンププロセスを処理します。Veridocxのウェブサイトは事実上、極めて柔軟性の高いタイムスタンプテクノロジーへの大規模なフロントエンドとして機能しています。

主な機能と導入メリット

- 高保証ハードウェアのセキュリティ。PKI対応アプリケーション、電子記録、コード署名に極めて正確なタイムスタンプを提供し、電子記録を強力な証拠に変換。
- アプリケーションとの統合が簡単。セキュアなタイムスタンプ機能とビジネスアプリケーションを簡単に統合し、デジタル署名文書（PDFなど）、アプリケーションコード、その他の電子的記録にタイムスタンプを提供。
- 正確で、監査可能なタイムスタンプ。時間の正確性と監査可能性に優れた、UTCに対し監査可能なタイムスタンプ。
- 改ざんに強いハードウェア。独立して認証された、改ざんに強いハードウェアにより、電子的なタイムスタンププロセスや鍵を保護。

アプリケーションと簡単に統合できるタイムスタンプソリューション。

Entrustのタイムスタンプソリューションは堅牢で、成熟し、Veridocxのwebアプリケーションと簡単に統合できたため、VeridocxはEntrustを選択しました。これにより、Veridocxは、顧客のために最高水準のサービスの構築に専念することができました。

Veridocx

Veridocxチームは1日足らずで、Entrust nShield HSMsとタイムスタンプ・オプションパックをVeridocxのプラットフォームに設定し、統合しました。

ENTRUSTのソリューションには他にも大きな利点がありました。

否認防止。Veridocxチームにとって、これは譲れない条件でした。チームは誰もタイムスタンプの偽造や改ざんができないことを約束し、証明できる必要がありました。タイムスタンプ鍵はハードウェア・セキュリティ・モジュールで安全に保護されているため、Veridocxは、タイムスタンプはハッカーやその他の外部の脅威、内部の脅威にも晒されないことを知っていました。必要であれば、監査可能なセキュリティトレイルを使用して、誰もEntrust nShield HSMsにハッキングし、タイムスタンプを修正または改ざんしていないことを証明できます。

セキュリティ。管理者が時間値を簡単に操作できるソフトウェアベースのシステムとは異なり、Entrust nShield HSMsは、独立して認定された改ざん防止ハードウェアのタイムスタンプ鍵を保護します。

品質。ハードウェアの品質が高いため、インストールや運用が簡単になり、こういった状況で発生する多くの困難なセキュリティや信頼性の問題を解決しました。

サポート。Veridocxチームは、Entrust nShield HSMsの品質だけでなく、ビジネス面および技術面の両方で受けるサービスとサポートも優れていることに気が付きました。

評判。Veridocxは、現在可能な最高のセキュリティと評判の高いタイムスタンプテクノロジーで構築したサービスを販売しようと考えており、それにはEntrustが最適でした。

手頃な料金。Veridocxは、カスタムソフトウェアや既製のハードウェアを使った独自のシステムを構築するよりも、はるかに少ない費用でEntrustのタイムスタンプソリューションを導入することができました。

ENTRUST NSHIELD HSMsとタイムスタンプ・オプションパック

Entrust nShield HSMsとEntrust nShieldタイムスタンプ・オプションパックは、正確な時間を記録し、セキュアなタイムスタンプを作成します。作成時間、記入時間、あるいは電子記録およびアプリケーションに関連した他のイベントの日時を記録します。精度が高く、改ざんに強い電子的なタイムスタンプソリューションを実装することにより、組織はデジタル記録に使用されたタイムスタンプの正確性を検証し、様々な重要なプロセスの完全性および監査可能性を改善することができます。

法的およびコンプライアンスの目的のために、時間証明のついた電子文書の署名を必要とする組織に最適なEntrust nShield HSMsとタイムスタンプ・オプションパックは、金融取引、宝くじ、ゲーム、セキュリティログ、承認ワークフロー、長期アーカイブ、電子ラボ記録、コード署名などの他の一般的なアプリケーションにも使用できます。

管理者が時間値を簡単に操作できるソフトウェアベースのシステムとは異なり、Entrust nShield HSMsは、独立して認定された改ざん防止ハードウェアのタイムスタンプ鍵を保護します。

Entrust nShield HSMsは、FIPS 140-2レベル3およびコモンクライテリアEAL 4+に準拠し、独立した国の原子時計に安全な時間のトレーサビリティのため、協定世界時（UTC）に対し監査可能な極めて正確なタイムスタンプを提供します。

Veridocx

ENTRUST NSHIELDタイムスタンプ・オプションパック

機能

- PKI対応アプリケーション、電子記録、コード署名をサポート
- 長期的な監査可能性、否認防止を実現
- UTC（協定世界時）に対して非常に正確な監査が可能
- 独立した国の原子時計に対し、セキュアな時間のトレーサビリティ
- 改ざん防止タイムスタンプのコンポーネント

プロトコルとインターフェース

- PKIXタイムスタンププロトコル（RFC 3161）、ETSI TS 102 023および101 861
- オプションのツールキットを使用したカスタムアプリケーションのサポート（JavaおよびC）
- コード署名アプリケーション用のAuthenticode

互換性とアップグレード可能性

- Entrust Time Source Master Clockと合わせて実装可能
- Adobe Acrobat、LiveCycle、Microsoft Authenticode、Officeと統合
- 最新リリースのソフトウェアにアップグレード可能

ENTRUSTについて

Entrust は信頼される認証、支払い、データ保護を実現することで、動き続ける世界をセキュアにしています。今日、人々はこれまで以上に、国境を越えた移動、買い物、電子政府サービスへのアクセス、企業ネットワークへのログインといったさまざまな場面で、シームレスで安全なユーザー体験を求めています。Entrust はこうしたインタラクションの要となり、他にはない多様なデジタルセキュリティと認証発行ソリューションを提供しています。2,500人を超える従業員、グローバルパートナーのネットワーク、150か国以上に顧客を擁するEntrustは、世界で最も信頼されている組織から信頼されています。

詳細は下記URLをご覧ください。
entrust.com/ja/HSM

ENTRUST

お問い合わせ：
HSMinfo@entrust.com