



ENTRUST

Certicamaraがタイムスタンプ付き電子記録の正確性を検証

CerticamaraはEntrustのソリューションを採用し、監査可能なデジタルタイムスタンプによって、コロンビア政府が詐欺や汚職を防止できるようサポートしています。

2004年に設立されたCerticamaraは、コロンビア国内の企業や政府機関に安全なオンライントランザクション処理ソリューションを提供しています。同社の顧客は、電子的なやり取りにおいてサーバや組織のIDを検証するだけでなく、さらなる機能も提供するソリューションが必要であることを、ますます認識するようになりました。彼らはまた、改ざんできない方法を使用して、やり取りが発生した時間と、トランザクション内のデータが変更されていないことを検証できるようになりたいと感じていました。Certicamaraは顧客のニーズに応え、Entrust nShield®ハードウェア・セキュリティ・モジュール (HSM) と nShield タイムスタンプオプションパックを使用して、電子記録の時刻と出所を証明するタイムスタンプサービスを開発しました。

「多くの種類の電子トランザクション、プロセス、送信では、それらが発生した正確な時刻を把握することが重要です」と、Certicamaraのシステム管理者であるLeonardo Maldonadoは述べています。「これは特に、デジタル署名された電子文書に当てはまり、その答えとなるのがタイムスタンプである。Entrustのソリューションが安全なタイムスタンプを提供し、当社サービスを利用する企業や政府機関が、詐欺や不正からプロセスを保護できるようサポートしてくれる」

「Entrust nShield タイムスタンプオプションパックが安全なタイムスタンプを提供し、当社サービスを利用する企業や政府機関が、詐欺や不正からプロセスを保護できるようサポートしてくれる」

- Certicamara, Leonardo Maldonado氏

耐タンパ性アプライアンスのメリット

企業や政府機関が実行するプロセスの多くには、時間的制約があります。政府は通常、支払い期限を課し、罰金と手数料を設けます。従来の紙ベースのトランザクションでは、署名と物理的なタイムスタンプが、プロセスの発生を認証する機能を果たします。電子プロセスにおいても同様の方法に依存し、ソフトウェアアプリケーションやハードウェアアプライアンスが時間記録とともに電子記録にデジタル署名を行います。

すべてのデジタルタイムスタンプ方法が同等に安全で、簡単に統合できるわけではありません。ソフトウェアベースの方法では、デジタルスタンプは、サーバ内のタイムソースを使用してサーバによって発行されます。スタンプと時間はどちらも、ハッカーや悪意ある内部者によって不正操作される可能性があります。アプライアンスベースのタイムスタンプは、セキュリティを保護するために、コモンクライテリアEAL 4+およびFIPS140-2レベル3で検証された、保護された耐タンパ性環境内でスタンプの発行とタイムキーピングが行われるため、はるかに安全です。悪意ある内部者もハッカーも、デジタル署名プロセスに干渉することはできません。

要となる性能

Certicamaraは、Entrust nShield HSMとnShieldタイムスタンプオプションパックを選択する前に、ハードウェアベースのタイムスタンプソリューションをいくつかテストしました。

同社は、2つの理由によりEntrustソリューションを選択することにしました。まず1つ目の理由は、性能です。そして2つ目の理由は、Certicamaraには、Entrust nShield HSMを使用してきた長い（そして非常に成功した）歴史があったことでした。Chacon氏は、次のように説明しています。「トランザクションを遅くするようなスタンププロセスに用はない。Entrust nShield タイムスタンプ オプションパックは、電子記録に、約10ミリ秒につきデジタル署名1つをスタンプする。これに匹敵するオプションは他に存在しなかった。処理速度が遅いと、システムが効率的にサポートできる同時ユーザ数に悪影響を及ぼしてしまう。さらに当社には、5年以上にわたり、Entrust nShield HSMを使用してユーザ認証プロセスを保護してきた歴史がある。Entrustは常に問題のないセキュリティを提供してくれた」

簡単な実装

Entrust nShield タイムスタンプオプションパックは、Certicamaraの既存のアプリケーション環境にタイムスタンプを統合するための、JavaおよびC言語開発フレームワークを提供しました。Entrust nShield タイムスタンプオプションパックは、監査可能かつ正確な時間をサーバに提供します。トランザクションやその他の電子記録の処理にCerticamaraの安全なネットワークを使用している顧客は、タイムスタンプも利用できるようになりました。

「デジタル署名とタイムスタンプは、紙や物理的な署名よりも安全であると当社は信じている。手書き署名は偽造することができるが、Entrust nShield タイムスタンプオプションパックを使用することで、偽造、不正操作、改ざんから署名プロセスを保護することができる。」

- Certicamara, Alex Chacon氏

「Entrust nShield タイムスタンプオプションパックには非常に感心した」と、Chacon氏は述べています。「これにより、タイムスタンプとビジネスアプリケーションの統合が容易になった。また、柔軟な実装も可能となった。今日、当社のお客様は、すべてのプロセスまたは特定のトランザクションに、安全かつ監査可能なタイムスタンプを追加するオプションを利用することができる」

汚職の撲滅

Certicamaraの顧客の多くは、監査可能なタイムスタンプを使用した電子記録の安全が検証がもたらすメリットを直ちに理解しました。例えば、Certicamaraのサービスを長年にわたり利用しているコロンビアの運輸省は、オンライン車両登録プロセスに安全なタイムスタンプを採用し、同様に、同国財務省は、コロンビアの金融機関が促進するオンライン取引に安全なタイムスタンプを導入することにしました。

またタイムスタンプは、新たなプロセスを可能にします。コロンビア政府は現在、汚職防止を目的としてタイムスタンプを使用する、購入プロセスを導入しています。

政府の請負業者は、Certicamaraシステムを通じて商品やサービスを提供するために入札書が提出する必要があります。Entrust nShield タイムスタンプオプションパックが、各入札書にデジタル署名するため、誰かに賄賂を渡して競合する入札を事前に確認したり、正式な提出期限後に不正に入札書を送信したりすることはできません。

「Entrust nShield タイムスタンプオプションパックは、正確な提出時刻を示すデジタル証明書を使用して入札書に署名する」と、Maldonado氏は説明します。「誰にも入札ルールを不正操作することはできない。これは、より効率的な電子プロセスを可能にしなから、汚職を防止するための簡単な方法である」

より多くのサービスとより多くのセキュリティ

Certicamaraは、Entrustソリューションを導入したタイムスタンプサービスにより、コロンビアにおいて、正確かつ監査可能な電子記録に対するニーズをより効率的に満たすことができると確信しています。



Entrustを使用するメリット

- 電子記録に監査可能なタイムスタンプを提供
- 効率的かつ費用対効果の高い電子プロセスの実現
- 詐欺や汚職の防止をサポート
- タイムスタンプとアプリケーションとの迅速かつ簡単な統合を実現

「タイムスタンプは、電子プロセスの法的に重要なさまざまな側面を検証するための簡単な方法である」と、Chacon氏は話します。「これにより、お客様は、監査および検証が可能でなければならないプロセスであっても、紙ベースの非効率的なビジネス方法から自信を持って移行することができる。実際のところ、デジタル署名とタイムスタンプは、紙や物理的な署名よりも安全であると当社は信じている。手書き署名は偽造することができるが、Entrust nShield HSMとnShield タイムスタンプオプションパックを使用することで、偽造、不正操作、改ざんから署名プロセスを保護することができる」

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、支払いや国際取引、電子政府サービスへのアクセス、そして企業ネットワークへの認証において世界中でより安全で円滑なユーザ体験が求められています。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ネットワーク、そして150カ国以上におよぶ顧客に支えられ、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