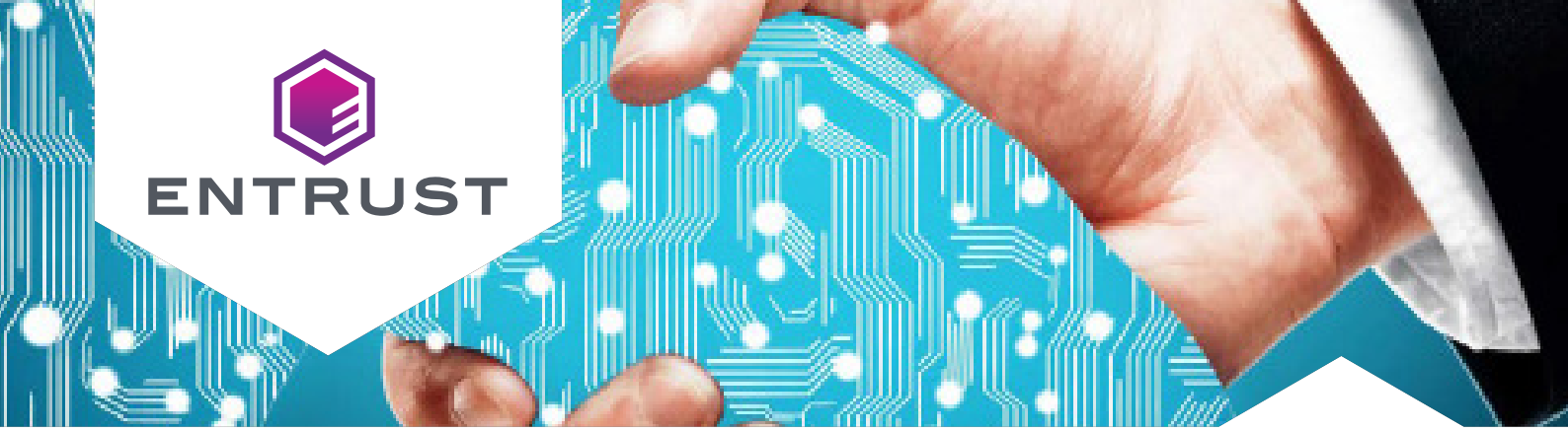

# Entrustは、チュニジアのデジタルインフラストラクチャの保護を支援します

**課題：チュニジアのデジタル経済の成長と、市民へのセキュリティの提供を支援する**

2015年、チュニジア政府は「デジタルチュニジア2020」を開始しました。これは、オンライン政府サービスとeコマースを充実させることにより、国のデジタル経済を強化することを目的とした計画です。イニシアチブの成功の基本は、公的および民間のオンラインサービスとeコマースに対するチュニジアの市民の信頼と自信を確立することでした。電子取引に対する米国の最高レベルの信頼を代表する国家デジタル認証機関（NDCA）は、デジタル取引のセキュリティを支える国家公開鍵基盤（PKI）を再設計するため、「デジタルチュニジア2020」の基礎プロジェクトに着手しました。

プロジェクトを成功させるには、既存のPKIからスムーズかつ迅速に移行すると同時に、実装後に強化された信頼サービスを提供する必要があります。さらに、PKIは、デジタル認証に関する新しい厳格な規制に準拠する必要があります。

**ソリューション：ENTRUST NSHIELD HSMによって保護された新しいPKI**

チュニジアの政府PKIを現代化するには、最新の利用可能な最高のハードウェアとソフトウェアをインストールし、可用性、信頼性、サービスの質を向上させる必要があります。PKIで使用されるルート鍵を保護するには、NDCAは、ソフトウェアのみのソリューションで機密情報を処理することはリスクが高いため、ハードウェアベースのソリューションが必要であることを認識していました。

# チュニジア共和国

## NDCAはPrimeKey + Entrustを選択

NDCAは最適な機能とセキュリティを得るために、PrimeKeyの新しいPKIとEntrustのハードウェアセキュリティモジュール（HSM）という2つの重要なコンポーネントを組み合わせたソリューションを選択しました。Entrust nShield® HSMは、機密性の高い取引中に認証局（CA）の秘密鍵をホスト・保護することにより、PKIにセキュリティを提供します。

NDCAは、PKIを保護し、次のような取引を保護するために、Entrust nShield HSMの2つのモデルを使用しました。

- 電子商取引を行う消費者ならびにB2B取引およびB2G取引を行う企業の電子IDの認証
- オンライン納税および申告、税関および外国貿易の申告の電子提出、電子請求書、電子バンキングサービスなどのオンライン取引の保護
- チュニジアのオンライン電子調達システムであるTunEPSを使用した、政府の提案依頼書に応答する企業の検証
- eパスポートやeIDカードなどのドキュメントのチップに保存される、署名の作成および生体認証データ、その他の個人識別情報（PII）などの情報の認証

USB接続型のEntrust nShield Edge HSMは、オフラインルートCAの鍵の生成および管理に使用されます。ネットワーク接続型のEntrust nShield Connect HSMは、次のような様々なサービスを実行します。

- 証明書失効ステータス取得のためのオンライン証明書ステータスプロトコル（OCSP）トランザクションのサポート
- パスポートやeIDチップに保存されている生体認証情報および電子情報の証明書の発行および署名を行う政府署名サーバ上での、鍵および鍵を使用した取引の保護

NDCAは、Entrust nShield HSMを2つのデータセンターにインストールしました。1つはオリジナルデータ用で、もう1つはバックアップおよびディザスタリカバリ用です。

Entrustは、HSMと統合サポートの提供に加え、NDCAの技術チームにEntrust nShield HSMの最大活用方法に関するトレーニングも提供しました。

## 積極的なコラボレーション

Entrustは、PrimeKeyと直接連携するイニシアチブを取り、ソリューションの設計とテストに必要なリソースとサポートを提供しました。この直接的かつ積極的なコラボレーションにより、プロジェクトがスムーズに実施され、最適化された統合ソリューションが生み出されました。

# チュニジア共和国

**ソリューションについて**

## Entrust nShield HSM

Entrust nShield HSMは、安全な暗号化処理と鍵管理のための改ざん防止環境を提供します。nShield HSMは、FIPS 140-2レベル2およびレベル3、コモンクライテリア認定、eIDAS準拠であり、高い効率を維持しながら、暗号化システムの確立された新しいセキュリティ標準を満たしています。

Entrust nShield HSMは、組織の最も重要なアプリケーションの暗号化操作と鍵を分離して保護し、PKI、SSL / TLS、コード署名などの幅広いアプリケーションの暗号化、デジタル署名、鍵管理を実行します。Entrust nShield HSMは、高保証ソリューション、およびソフトウェアのみの暗号化よりも優れた保護を提供します。Entrust nShield HSMはすべての主要なアルゴリズムをサポートし、世界クラスのトランザクションレートパフォーマンスを備えています。

Entrust nShield HSMと独自のnShield Security Worldアーキテクチャを使用することで、必要な容量のみを購入し、ニーズの変化に応じてソリューションを簡単に拡張することができます。

## Entrustの主要なソリューションの利点

- 改ざん防止ハードウェア内で暗号化鍵および操作を保護し、ソフトウェアのみのソリューションよりもセキュリティを大幅に強化する。
- 認定ソリューションを信頼する– Entrust nShield HSMは、FIPSやコモンクライテリアなどの厳しい標準に対して認定されており、eIDAS規則に準拠する。
- 独自のEntrust nShield Security Worldアーキテクチャを使用して、鍵管理を維持し、進化するニーズに応じて拡張可能なHSMセットを構築する。


**詳細をチェック：ENTRUST.COM/ja/HSM**

# チュニジア共和国

## Entrustを利用する理由は？

### Entrust HSMはFIPS 140-2レベル2および3、コモンクライテリア認定、eIDAS準拠です。

Entrust nShield HSMは、プロジェクトに必要な厳格なFIPS、コモンクライテリア、eIDAS標準を満たしています。Entrustは、イタリアの認証機関であるOCSIを通して、nShield SoloおよびConnect HSMにコモンクライテリア EAL4 +認証を取得しています。1999/93 EU指令の下で、この認定により、Entrust nShield HSMはSSCD（セキュア署名生成デバイス）テータスを取得しました。この認定は、eIDAS 2014規制への準拠も提供します。

### Entrust nShield HSMはNCDAにより実証されたソリューションです

Entrust nShield HSMは、以前のNDCAプロジェクトで正常に展開されました。Entrustは高品質のソリューションを提供し、代理店のニーズに対応していたため、NDCAは国の新しいPKIを安全に維持するために、競争の激しい入札でEntrustを選択することを躊躇しませんでした。

## ENTRUSTについて

Entrustは、信頼性の高い本人認証、決済、データ保護を可能にすることにより、世界の動きを安全に維持します。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、これらすべてのインタラクションに対応した、他では見られない広範なデジタルセキュリティおよび資格情報発行用ソリューションを提供しています。2,500名以上の従業員とグローバルパートナーのネットワークを備え、150か国以上における顧客から支持されているため、世界における多くの委託組織から信頼を得ていることは不思議ではありません。

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**