POS システムにおける DUKPT 鍵管理の仕組み

- 2021 年 3 月 19 日投稿
- Intertrust

POS システムには、カード会員のデータを保護し、取引の不正を防ぐためのさまざまな仕組みがあります。これらの仕組みのほとんどはサーバー側で機能しているため、消費者や販売店からは見えません。一方で、POS システムもハッカー攻撃の標的となっていることから、システムの開発者にとって実態を正しく理解することが重要です。この不正なアクセスを防ぐ仕組みの中で、DUKPT 鍵管理スキームは、POS セキュリティに不可欠な暗号化プロトコルの 1 つです。

DUKPT 鍵管理とは？

DUKPT（Derived Unique Key Per Transaction）は、1980 年代後半に VISA が開発した鍵管理方式で、ANSI X9.24 guidelines for Retail Financial Services Symmetric Key Management の Part 3 に定められています。DUKPT では、決済のトランザクション毎に 1 回限りの暗号鍵を使用するため、1 つの鍵が侵害されても他の取引やシステムの内容までたどり着くことが容易ではないため、情報漏洩リスクを最小限に止めることができます。このワンタイムキーは、公開されることのない秘密鍵を使って生成されます。

POS システムで DUKPT が重要な理由

DUKPT 鍵管理は、金融業界で広く使用されている標準であり、POS トランザクションにおけ

るサイバー犯罪や不正行為を大幅に削減する効果があります。しかし、どんな暗号アルゴリズムも、その鍵を手に入れることができれば破られる可能性があり、一般的に、暗号化方式で最も脆弱なポイントは、暗号化側と復号側の間で鍵が共有されるときです。POS トランザクションでは、POS デバイス(決済端末)がデータを暗号化し、決済サービスプロバイダがそれを復号しますが、上記脆弱性のリスクを回避するため暗号化/復号化鍵を共有せずにデータを復号化する DUKPT 鍵管理スキームが使われます。

DUKPT では、POS デバイスが固有の派生鍵と固有の KSN（Key Serial Number）を生成します。POS デバイスは、ワンタイムキーでデータを暗号化し、暗号化されたデータと KSN を決済サービスプロバイダに送信します。決済サービスプロバイダは、固有の KSN の情報を使用して同じ鍵を生成し、データを復号化します。

DUKPT の鍵管理の仕組み

DUKPT プロセスでは、まずサーバー側でシステム鍵(Base Derivation Key: BDK)を用いてトランザクション毎に異なる暗号鍵を生成します。 BDK はサーバー側で安全に保管され、公開されることはありません。同じ BDK を多くの POS デバイスに使用することができます。

POS デバイスでは、初期設定の際に BDK と端末の固有 ID 情報（通常は POS デバイスのシリアル番号）を使用して、 初回鍵が作成されます。初回鍵は、固有の Key Serial Number(KSN)とともに POS デバイスにインストールされます。

KSN は、端末の固有 I D 情報と内部トランザクションカウンターの数字に基づいて生成されます。初回鍵は新たに派生する鍵を生成するために使用された後、POS デバイスから消去されます。トランザクション毎に派生鍵の 1 つがトランザクションデータの暗号化に使用され、トランザクションカウンタの数字に基づいて固有の KSN が生成されます。

暗号化されたデータ、KSN、およびその他のトランザクションデータは、決済サービスプロバイダに送信されます。この時点で、ワンタイムキーは POS デバイスから消去され、トランザクションがカウントされます。

決済サービスプロバイダ側では、KSN を使用して関連する BDK を検索し、演算をしてそのトランザクションで使用された POS デバイスの初回鍵を再生成します。初回鍵は、デバイス側で行われたのと同様のプロセスを経て、そのトランザクションのワンタイムキーを生成します。

それを使用してデータの復号化と必要なプロセスが実行されますが、使用された鍵情報は保持されません。

上記 POS システムにおける DUKPT 鍵管理のサマリー

1. システム鍵(Base Derivation Key: BDK)と POS デバイスの Key Serial Number（KSN）を使用して、DUKPT 初回鍵が作成されます。
2. DUKPT の初回鍵は POS デバイスにインストールされます。
3. 初回鍵は、固有の KSN を持つ派生鍵のグループを作成するために使用され、その後、POS デバイスから消去されます。
4. トランザクション中、派生鍵の 1 つ（セッションキー）とその KSN がトランザクションの暗号化に使用されます。
5. KSN カウンタがトランザクションの数値を修正します。
6. データが送信された後、セッションキーと KSN は、必要に応じて派生鍵を作成するために使用され、その後鍵は消去されます。

whiteCryption® Secure Key Box™ は DUKPT をサポートしています

DUKPT による鍵管理は、POS システムのセキュリティを大幅に向上させ、取引情報を安全に保つことができますが、実装が煩雑で、暗号の専門知識が必要になる場合があります。whiteCryption® Secure Key Box™ は、決済システムの開発者が、ソフトウェアベースの POS セキュリティ機能に加えて、より迅速に安全で PCI 基準に準拠したアプリケーションを構築できるように、DUKPT をサポートしています。また、動的な鍵の暗号化に対応しているため、初回鍵のインジェクション時にも鍵を保護することができます。

Secure Key Box™ は、whiteCryption 社が提供をする業界をリードするホワイトボックス暗号化ソリューションです。Tap to Phone アプリケーションの構築、 PCI CPoC 基準に準拠するために必要なものについては、ホワイトペーパーをご覧ください。

Intertrust Technologies は、豊富な経験と業界をリードするアプリケーション・セキュリティ・ソリューションを提供しています。アプリケーションと暗号鍵の高度な保護を通じて、お客様のアプリケーション、ビジネス、顧客をどのように保護するかについては、Intertrust Technologies Japan ホームページをご覧いただくか、japan-sales@intertrust.com にお問い合わせください。