DUKPTの概要とその応用

タレスジャパン株式会社
住田　敦

■ はじめに

Webアプリケーションやデータベースのセキュリティーについては多くの書籍・雑誌で取り上げられ、幅広く知られていますが、電子決済系のセキュリティーについてはあまり知られていないのが現状と思います。よって、今回は電子決済系、特に昨今話題となっているスマートフォン等を使ったカード決済システムで注目されているセキュリティー・プロトコルであるDUKPTがどのようなシステムで使われ、どういった利点があるのかをご紹介します。また、この技術がその他の分野にも応用可能である点も併せてご紹介いたします。

■ DUKPTとは

旧来の電子決済では、決済を行う端末（小売り店舗等で金額を入力し、クレジットカードの情報を読み取るもの）から決済を処理するサーバまでの間は専用回線となっていましたが、現在は決済をiOSやAndroid端末などに決済用のハードウェアを組み合わせ、インターネットを経由して行うというケースが増えてきました。このようなケースで盗聴などの可能性を考えると、専用線を使う場合に比べ、より強固な通信の暗号化が必要となり、図1のような範囲の通信においてこのプロトコルの利点が注目されています。

まずDUKPTとはDerived Unique Key Per Transactionの略でANSI X9.24 part1にて規定されたプロトコルです。トランザクション毎にデータの暗号鍵を変えることで暗号通信のセキュリティー強度を上げることを目的としています。つまり、あるトランザクション・データが盗聴され、万が一鍵が推測されて復号化されたとしても他のトランザクションのデータまでデータ漏洩の影響が無いということが大きな特徴となっています。

しかしながら、複数の端末を使う場合に、トランザクション毎の鍵が同じになったり、どの鍵を使うかを通信経路上で交換してしまったりしたのではセキュリティー強度としてはあまり高いものになりません。よってDUKPTでは図2のような処理フローを採用しています。その大まかな流れは以下のとおりです。

1. サーバ側で暗号鍵用のシードを作成します。次に端末ベンダーは各端末固有情報を作成し、端末に渡すと同時にサーバ側にも渡します。サーバはこの情報

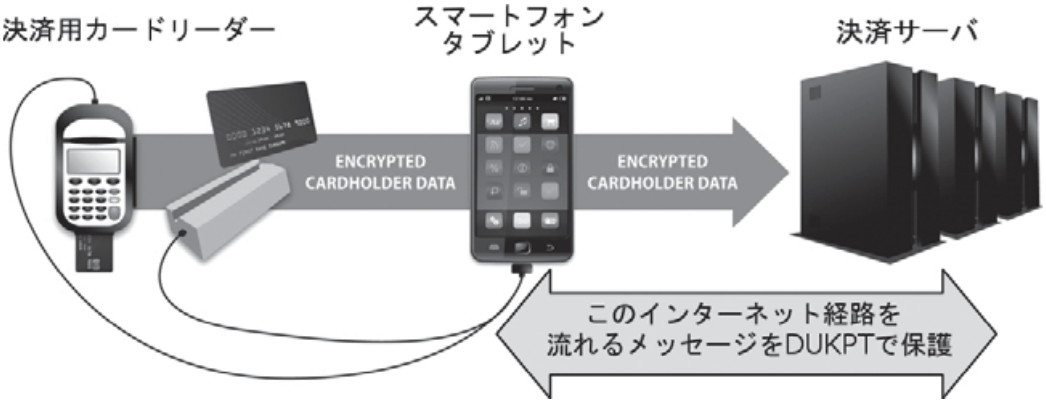

図1: DUKPTの適用範囲

を元に各端末固有の暗号鍵用のシードを作成し、それを端末に渡します。

2. 端末は初期化時といったタイミングでシード情報から鍵を作成し、その時点でシードを破棄します。端末側では作成された鍵から別の鍵を派生させていくという形でトランザクション毎の鍵を作成していきます。つまり、サーバとの通信毎にデータを暗号化して送りますが、この時、はじめから何番目に作った鍵かというトランザクション番号という情報と、どの端末であるかという端末情報を暗号化されたデータに付加し、サーバに送信します。
3. データを受け取ったサーバは、端末情報とトランザクション番号を元に、サーバ上のシード情報から暗号化鍵を生成し、データを復号化して取り出します。

■ DUKPT の利点

端末毎にシードが異なるため、同じ暗号鍵が使われるという可能性は低く、また鍵情報は通信経路上では交換されず、サーバ上でトランザクション毎に送られてきたデータを元に再計算されて使われるため、漏洩の心配もありません。

このような利点に加え、通信にセッションという考え方は無いため、例えばトランザクション番号 n 番の通信の後に、番号 n+5 番に対応するデータがサーバに送信されたとしても、サーバは n+5 と端末情報の 2 つの情報を元に暗号化鍵を計算するだけです。

つまり、n+1 から n+4 番の情報やそれに対応する鍵

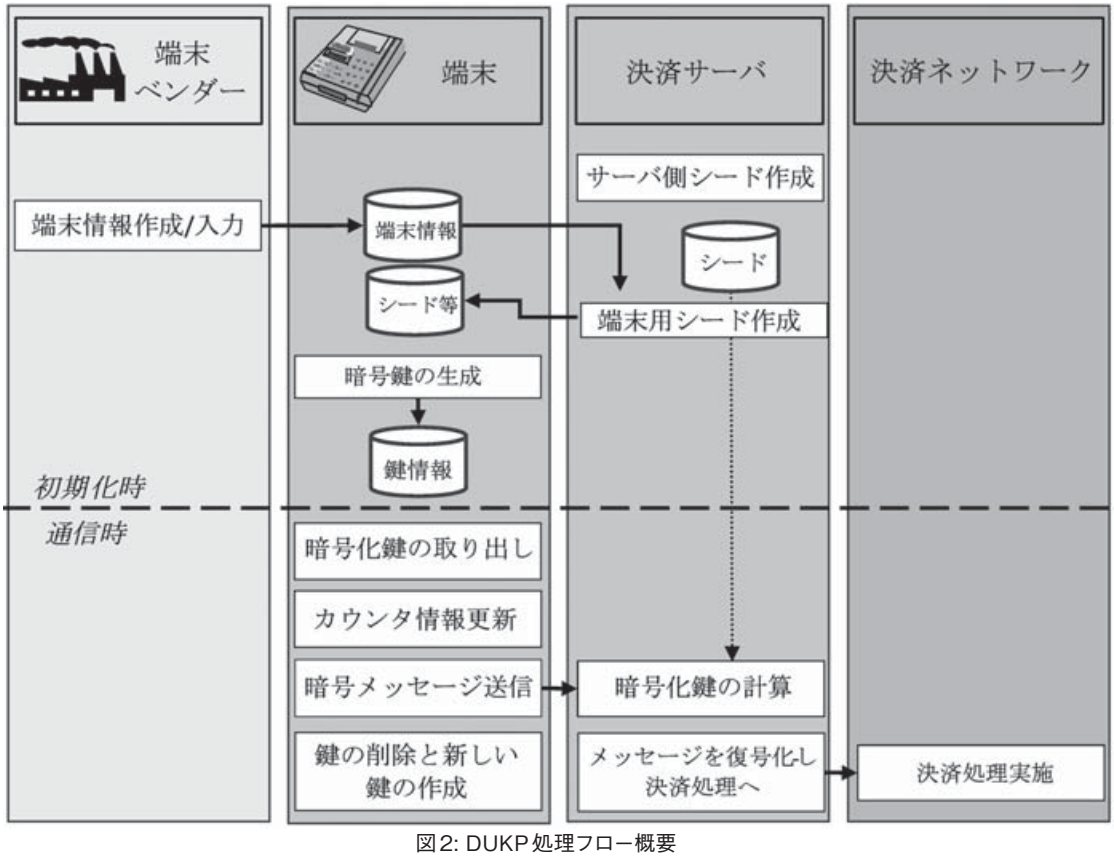

図 2: DUKP 処理フロー概要

の情報はn+5番の鍵を生成するために不要であるということも特徴の一つとなっています。

先に、インターネットを使うことにより、強固な暗号化が必要になると述べました。

鍵を1回1回変えることが出来る以外にも、このDUKPTという方法を使ったほうが良い理由があります。

従来の決済系の通信は、専用回線のみが使われていたため、PIN（決済で使用される暗証番号）のみを暗号化していました。この場合であれば、PINを確認するロジックと端末間で何かしらの鍵の共有の仕組みがあれば問題はありませんでした。しかしながら、インターネットを経由する場合にはそれ以外の情報、例えば決済ではPAN（クレジットカードのカード会員番号）といったものも暗号化すべきであると、決済系のグローバルセキュリティー基準であるPCI DSS（国際ペイメントブランドのVISA, MasterCard, American Express, JCB, Discoverの5社が策定）でも求められています。この場合、カードの中の個々の情報を使うロジックごとに鍵を管理していくという方法よりも、メッセージの電文すべてを暗号化してやり取りをしたほうが効率的になります。そのような通信の中で、アプリケーション両端を結んだ暗号化通信を決済系ではP2PE（Point 2 Point Encryption）と呼びますが、以前はベンダーごとにその実装が異なるため、マルチベンダーの環境に適応するには考慮点がありました。しかしながら、スタンダードであるDUKPTをベースにしたソリューションを用いればベンダーをまたがった暗号化ソリューションが容易に実装可能となるといった利点が出ます。

■ DUKPT の考慮点

ここまでDUKPTの利点を挙げましたが、重要な考慮点が2つあるので、それをご紹介します。

1つめとして、端末側でシードを元に暗号化鍵を生成すると前にご紹介しましたが、シードから生成できる鍵の個数に上限があり、その上限に達した場合には新しいシードを端末側に配布する必要があります。この配布の仕組みは、DUKPTの規定の範囲外となります。しかしながら、このシード情報が盗まれた場合には端末のなりすましといった問題が発生するため、電子メールの添付ファイルとして送信して手作業にて端末にUSBキーか何かでコピーをするというやり方は推奨されません。しかしながら、シードを更新する必要のある端末が出るたびに、専用のエンジニアがジュラルミンケースにシード情報の入った記憶媒体を入れて持ってきて更新作業を厳重に実施していくというのも、端末の数や人件費を考えると現実的ではありません。

このような考慮点を解決するため、DUKPTを実装した製品を提供しているベンダーは、Remote Key Loadingという仕組みで端末に対してシード情報を遠隔地から配布する仕組みを実装しています。Remote Key Loadingに規定はありませんが、多くのベンダーは基本的にはPKIをベースにした暗号通信により安全にシード情報を配布する仕組みを提供しています。

2番目として、DUKPT自体に端末とサーバの相互認証といった仕組みは無いため、例えば端末に入れている鍵のシード情報が盗まれればその端末の偽造は可能となりますし、サーバ側のシード情報が盗まれれば偽造されたサーバが決済情報を集めてしまう可能性があります。こういった場合に備え、DUKPITでは端末側のシード情報は初めの鍵作成の時点ですぐに破棄するという実装となっています。しかしながら、サーバ側はクライアントから送られた情報での鍵の再計算のために持ち続ける必要があるため、HSM(Hardware Security Module）といった外部のセキュア・ハードウェアにシード情報を安全に保持しておくことが現実には推奨されています。

■ DUKPT の応用的な適用例

ここまで、DUKPTの仕組みとその利点、決済系でどのように使われるかをご紹介しましたが、他の分野にもこの仕組みは適用可能です。

例えばファイルをファイルサーバにアップロードする仕組みへの応用が考えられます。

製造業の分野において、重要な設計図情報などのファイルをアップロードする場合、情報漏洩に備えて通信経路を暗号化することは必須であり、そのようなセキュリティーはすでに実装済みのシステムは多いと思います。しかしながら近年の標的型攻撃の手法から考えると、ファイルサーバでファイル受け取った時点で復号化してしまうと、そのサーバがハッキングされた場合にはサーバ内で情報を奪取されてしまうという危険性が生じます。ここで、図3のようにファイルをストレージにストアするまで暗号化ファイルごとに異なる鍵で暗号化して送信すれば、暗号化されているために奪取されたとしても情報を読むことが出来ませんし、もし仮に1ファイルのみの情報が解読され、漏洩さえたとしてもそれ以外のファイル情報は別の鍵で守っているため、漏洩から守ることが可能となります。

こういった利点に加え、ストレージ側において、ファイルごとに暗号化した鍵をすべて、どこかに保持しておくという必要は一切無いということも利点の一つです。1つ1つのファイルに対して、何番目の鍵を使ったかという情報だけを付加しておけば、復号化のタイミングで鍵を計算すれば良いだけですので、大量の鍵をどうやって守るかを考える必要はなく、シード情報だけに重点を置いて保守をすれば良いという形となります。ただし、端末側での鍵の再生成の仕組みはDUKPTの規格としては提供されていませんので、端末側に再度送る場合には、そこでサーバからクライアントへの新規のDUKPTのトランザクションを発生させて新しい鍵で再暗号化して端末に送るといった仕組みを別途考える必要があります。

■ おわりに

電子決済という重要度の高い情報を取り扱う分野にて使われているセキュリティー技術の1つとして、DUKPTをご紹介しました。

セキュリティー技術は、適用分野が増えるにつれて、特定分野固有のものが増えていますが、そのようなものの1つとして今回知っていただくのと同時に、他の分野に適用すると新たな利点が生まれるものがあるといった観点で、今後のソリューション作成の一助としていただければ幸いです。

図3: DUKPT応用例