The Verex Process

Abstract

A new approach to goods authentication is described whereby the goods authentication process is embedded in a card payment transaction. This approach makes use of the payment infrastructure to fight brand and intellectual property piracy and addresses consumer assurance at the time of purchase.

The most effective implementation of the process is the one by which consumers are equipped with smartphones having the capability to scan NFC chips combined with a supporting a payment infrastructure.

Contents

Glossary and Abbreviations

EMV – an EMVco standard for smart card payment processing

NFC – Near Field Communication

NFC Tag – an unclonable microcomputer device capable of communicating with an NFC scanner and proving its authenticity to the scanner or an online service

PKI – Public Key Infrastructure

POS - Point Of Sale

RFID – Radio Frequency Identification

TAT – Tender Assurance Token

The Growing Problem of Counterfeit Goods

The International Chamber of Commerce (ICC) estimates that 5-7% of all world trade is in counterfeit or pirated merchandise. The total value of such "black market" goods is projected by the ICC to approach US$1.2 - 1.7 trillion by 2015, more than doubling in less than a decade.

Counterfeiting and piracy affects all industries, from electrical components to prescription drugs. These black market operations are increasingly migrating online, a channel that poses substantially higher monitoring and enforcement challenges than the physical distribution of counterfeit and pirated goods.

The luxury goods sector has increasingly become the target of counterfeiters, primarily due to the high margins, and most luxury brands. There are many brands affected by counterfeiting and brand piracy such as: Louis Vuitton, Rolex, Adidas, Nike, Canada Goose, Coach, Prada, and many more.

The Technology Responses to Piracy and Counterfeiting

The typical way to mitigate the risk of an item being counterfeited is to embed an unclonable digital tag into an item of merchandise and scan this tag using, for example, an NFC scanning device to ensure that the tag is authentic. This method cannot guarantee that the item is authentic but it deprives a potential fraudster from getting profit from piracy. Because every item has a unique, unclonable tag, in order to perpetuate a fraudulent sale, the fraudster must first purchase a real item to get an authentic tag, extract the tag from the item and sell a counterfeit item carrying the authentic tag. However, the fraudster will now have problems with selling the real item (to recoup the investment) because there is no longer a tag attached.

NFC tags are now widely commercially available in many form factors. For further information about just a few such vendors please see: Buy NFC Tags (The NFC Superstore), Tag Stand, and RFID Canada.

Descriptions and variations of the technology approaches to the brand authentication solution above have been discussed for many years. One example, published in 2001 can be found at http://www.lifecycleintegrity.com/Smart-Cert.htm.

There are many vendors with brand authentication solutions in the market. The most technically advanced among them is provided by Original 1. Their solution focuses on manufacturers and supply chain integrity rather than providing assurance of authenticity to retail consumers.

There are additional measures that prevent assurance tags from being extracted from the items in which they are embedded. It is impractical to extract a tag which is a part of an automobile computer, or a watch microprocessor, and there are a number of patents for electronic devices that detect tampering. Such sophisticated methods further reduce the risk of an item being counterfeited.

Another known method to mitigate the possibility of authentic tag reuse by counterfeiters is to provide a potential purchaser or inspector with pedigree data that describes the real item (colour, size, shape, labels) and its further disposition: manufacturing date, shipping date and address, and whether or not the item was sold. For examples, visit Inside Secure or watch the company's video on YouTube.

There are other approaches to authentication that make use of cloneable tags such as: barcodes, laser-engraved codes and passive RFID devices, among others. For example, see Videojet solutions for video imprints that can be applied to individual items of goods and SafeMedicine that represents a number of organizations fighting prescription drug forgery.

Other specialized, more esoteric authentication techniques are also available. One such method from Cypher Science makes use of a DNA tag (CypherMark) implanted in designer denim jeans. Another approach, laser-engraved diamonds, is available from Ajediam and JK Schmidt Jewellers. Most solutions involve the use of a scanner to access a tag description database in real-time and retrieve the pedigree information. Some vendors go further and provide the scanning device with the item ownership information about the person who bought the item and who owns it.

Most solutions, however, remain focused on inventory management and supply chain integrity, ensuring that merchants can be confident in what they sell and the manufactures can be confident in the parts and materials they use.

Since the advent of smart phones, firstly with barcode scanners and now with NFC scanners, merchants have started addressing the need to provide consumers with the ability to check the authenticity of goods at the point of purchase. See NXP for one example and the recent research at the European Bridge Project.

The Unique Verex Approach

Verex invented a new way to purchase goods with confidence by adding one more component to card-based payment transactions.

Before Verex, a payment card purchase transaction comprised such components as card authentication, cardholder verification, and payment authorization. Verex added one more component to the payment process, brand assurance, built directly and seamlessly into the transaction.

The major advantages of the Verex process are described below:

- **Payment association physical infrastructure reusability.** Verex uses the existing retail payment network infrastructure provided by payment associations, such as Visa, MasterCard and can be easily incorporated into technologies such as Google Wallet, ISIS Wallet.
- **Payment association legal infrastructure reusability.** When using a credit card, a consumer has no idea of the intricate web of rules and complex commercial relationships that protect the transaction's integrity. Verex transactions are automatically protected by the same rules as every day purchase transactions but have the added value of bringing the brand owners and manufactures into the chain of trust.
- **Transaction consistency.** When a Verex transaction is processed successfully, the pedigree database of items is changed to reflect the status of the goods or services (to "sold") and registers the transfer of ownership. The payment processing is completed concurrently. Within the Verex process, payment, ownership transfer, and item authentication are bound together. It is not possible for the payment to complete and the goods be taken away from the store without the consumer being confident in the brand authenticity and the ownership being transferred.
- **Premium Verex Services.** Additional services can be provided for consumers by Verex Club, such as warranty registration, instant rebate registration, loyalty points, coupons, etc.

Verex User Stories

The User stories provided in this section describe how the various participants (consumers, payment systems, financial institutions, payment technology vendors, brand owners, manufacturers, and retail stores) interact in the Verex process.

Note: none of the organizations cited as **examples** have implemented the Verex process nor have any expressed any intent or interest in Verex whatsoever. Also, the scenarios described below do not address every possible implementation of the Verex process.

John's Celebration – In-store Purchases

John has recently sold the patent for his invention to Google and wants to celebrate this event with his friends. For that purpose he decides to buy a bottle of Camus Cognac (a 750 ml bottle for $2,500). He also wants to make a present of a bottle of Russian Standard Vodka (1 L for $45) to his brother-in-law.

Having all this in mind, he heads to the nearest liquor store, named JoyStop, knowing that they display the Verex logo on the door.

The JoyStop sales clerk opens a vintage case where the expensive Camus Cognac is stored and presents a bottle to John. John finds a Verex logo on the bottle and taps it with his NFC enabled smartphone running the Verex app. The smartphone scans the NFC chip located inside the Cognac bottle cap. The chip proves its authenticity to the Verex app and informs John that the bottle itself has not been opened and that the storage conditions were within the temperature tolerances specified by the distiller. The chip also discloses some additional pedigree information to the smartphone. The smartphone then contacts the Verex Server.

From the Verex Server, the smartphone relays the description of **this particular** bottle and its contents including when it was shipped to JoyStop and that the bottle has not been sold. John is now convinced that he is buying the genuine article. He asks the clerk to bring **this particular** bottle to the checkout point while he continues to shop. (Due to the store policy such expensive goods cannot be kept in the consumer's shopping basket).

Next, John finds the aisle with Russian Standard Vodka, selects a bottle, and repeats the authentication process. John trusts JoyStop but read that up to 50% of Russian vodka (sold in Russia internally) is counterfeit. John wants his brother-in-law to have no doubt about the authenticity of this gift. Therefore, John selects a bottle carrying the Verex logo despite the fact he could buy the same bottle for 2 dollars less (but without a Verex tag) in another nearby liquor store. John puts the vodka bottle into his shopping basket and proceeds to checkout.

The cashier scans the Camus Cognac bottle with the POS NFC scanner. It is the same scanner used to scan NFC payment cards from Visa and MasterCard. She also scans John's Russian Standard Vodka bottle. The POS communicates with the Verex Server (see the next chapter how this can be implemented). The POS together with Verex Server verify the authenticity of the items and that the bottles are the same ones that John scanned with his smartphone. The latter step is performed to prevent inadvertent or fraudulent substitution prior to checkout.

As a result of this second authentication procedure, the Verex Server produces an electronic certificate of authenticity that is to be delivered to the payment infrastructure in the next phase of the Verex purchase transaction - the payment phase. At this point, John presents his credit card for payment.

The cashier examines the card and tells John that he is carrying a "regular" (not a Verex co-branded) credit card that will work perfectly well with the Verex transaction. She mentions that John might consider acquiring a JoyStop Verex co-branded MasterCard card (issued by J.P. Morgan-Chase Bank). John asks why he should acquire yet another credit card.

The cashier explains that if John orders the new card on the spot, the following will happen:

- First, as soon as the Verex payment transaction is completed, a $150 instant rebate provided by Camus will be immediately posted to John's new credit card account. If the regular credit card is used to purchase Camus Cognac, John will have to send a letter to Camus to claim the instant rebate, wait for a cheque in the mail and then deposit the cheque at a bank.
- Second, the particulars of his cognac bottle will be posted to John's Verex Club account, and everybody who has John's permission can visit the Verex Club website and assure themselves that John is the proud owner of this bottle. John could even sell this bottle to someone else in the future using this proof of ownership.
- Third, John does not need to pay for this bottle immediately. JoyStop will give him a credit for this purchase so John will pay off the balance of this purchase within the next 12 months.
- Fourth, John immediately starts earning Verex loyalty points.
- Fifth, John will receive electronic coupons from both Camus and Russian Standard for future promotions and discounts.

John agrees and his Verex MasterCard card is issued immediately. The card is actually a payment "app" that is downloaded over-the-air to the Google Wallet in John's smartphone. John uses the new "mobile payment app" on the spot to complete the purchase transaction.

John taps his phone at the same POS, and the POS, combined with the MasterCard payment system infrastructure completes the payment component of Verex transaction. The payment infrastructure advises the Verex Server that the payment is authorized and the Server posts the sale of both bottles in its database and records John as the new owner of a Camus Cognac bottle. John receives the purchase completion advice together with the conformation of authenticity for both bottles at his smartphone. The POS prints the receipt. John heads home to celebrate.

Mary's Tires – Deferred Goods & Service Purchases/Warranty Registration

Mary needs to replace the tires on her car. She brings the car to an Active Green + Ross shop and chooses Michelin All Season tires. The particular tires she needs are not in stock so the shop orders the tires and Mary presents her Visa co-branded Verex card from the ISIS Wallet, stored on her smartphone.

A day later, Mary receives a message on her smartphone that her new tires (with the serial numbers displayed) were shipped by Michelin to the shop, and that the Verex tags built into the tires were scanned at the Michelin warehouse before shipping. The smartphone records the tires' unique product numbers in its Verex Club App.

Two days later, Mary brings her car to the shop, and the new tires are installed. Mary scans the tires with her smartphone and the Verex server confirm the tires' authenticity, and that the tires are indeed the same ones that were scanned at the point of shipping.

Mary presents her Visa Verex card (i.e. the ISIS wallet) at the POS for checkout. The Active Green + Ross clerk presents his personal digital tag-certificate to the POS. The POS, the Verex server, and the Visa payment infrastructure work together to complete the Verex transaction. All of the following steps happen in parallel:

- the payment is processed
- the tires are posted as sold in the Verex database, so nobody can reuse the same tags even if they find the way to extract them from these tires
- the tire ownership is transferred to Mary in the Verex database (now Mary can sell her car proving that it has the authentic Michelin tires)
- the Active Green + Ross shop is authenticated as genuine service provider
- The tires are authenticated as genuine
- Mary receives the transaction completion and service and goods authenticity confirmation at her smartphone
- Mary receives a $75 instant rebate from Michelin credited to her Visa Verex account
- the Michelin warranty for the tires is registered by Verex on Mary's behalf
- Mary receives electronic coupons from Michelin for her tire purchase discount (downloaded to her ISIS Wallet)
- Mary receives an electronic coupon from Active Green + Ross for a discount on future service (also downloaded to her ISIS Wallet).

Boris' Jacket – On-Line Purchases

Boris lives in Novosibirsk, Russia. The winters are very cold there and Boris saw a very warm and fashionable Canada Goose jackets in a nearby store. Boris wanted to buy a Canada Goose jacket but a friend of his, Peter, having just returned from a trip abroad told Boris that he saw something similar in China at 50% of the local selling price. Boris wants to make sure he purchases an authentic jacket that will last instead of investing in a potential knock-off.

Boris goes to the Canada Goose website and discovers he can buy a Verex authenticated jacket from Amazon.com. Boris has an American Express credit card (not a Verex card) and he places an online order for a Canada Goose jacket in his size. He also orders the courier delivery service from DHL. The payment transaction is initiated but will not yet be completed until the goods are delivered. This is one of the benefits of purchasing goods protected by Verex.

Two days later, Boris' jacket is manufactured and a Verex tag is personalized and embedded into the jacket. The tag is scanned at the warehouse just before shipment and the Verex Server sends an email to Boris: "Your jacket is ready". Boris also receives information including the serial number, color, and size and a reminder that the will be advised when the jacket actually ships.

A short while later, as promised, Boris receives a regular Amazon message confirming the shipment along with a DHL tracking number. A non-Verex transaction would have been completed right at this point and Boris' credit card would have been charged. When the Verex process is used, the payment systems, including Amex, will have amended their regulations so that the purchase amount is recorded on the Boris' credit card account records but there is no charge as yet. The transaction will only be completed when the item is delivered to Boris in Novosibirks.

A week later, a DHL courier knocks at Boris' door carrying a parcel. Boris scans the unopened parcel with his IPhone. The phone is equipped with a Device Fidelity NFC case that allows the phone to scan Verex NFC tags integrated with the Verex app.

The smartphone, interacting with the Verex Server, confirms the tag authenticity and displays the jacket description. At this point, Boris unpacks the parcel and compares the jacket with the information displayed on the smartphone screen.

Boris presents his AmEx card. The courier uses a portable POS to scan both the card and jacket's tag.

The Verex server and the AmEx payment infrastructure complete the Verex transaction started online by Boris several days before. It is only at this time that Boris' card is charged, and the item is marked as sold in the Verex database. Unfortunately, there is no ownership record put in the Verex database because Boris is not a member of the Verex Club.

Processes and Interfaces

The following sections describe one of several possible implementations of the Verex process. Variations will depend on the particular technological and business environment of the implementation.

Preliminary Item Authentication

Before buying an item of merchandise in a store, a customer wants assurance that the item is authentic.

The process described below pertains to both in-store and online purchase scenarios. The main difference between the two is that the seller verification steps during an on-line purchase are performed by a warehouse or shipping clerk instead of a store clerk.

The process is illustrated in Figure 1. The consumer uses a smartphone which communicates with the NFC tag or scans a barcode. The tag sends an authentication check request to the Verex Server. The Server responds with information that enables the consumer to determine whether the item is genuine.

This information includes the item description, the description of the store to which the item was shipped, and the item disposition: shipped, ready for sale, sold, returned, revoked, etc. based on what the manufacturer decides is relevant.

If the Server is not accessible from the smartphone some essential information from the NFC tag can be displayed instead, so the consumer may still be able to make a preliminary judgment on the authenticity of the tag. This off-line method is not recommended when either barcodes or cloneable tags are used.

This preliminary authentication process is optional but highly desirable, especially where purchasing high-value, luxury goods.

The tag can also contain records that certify certain properties of the item, such as electronic safety certificates, excise stamps, goods quality ratings, service provider's license, recycled content etc. In this case, the Verex Server provides assurance of the attached electronic certificates.

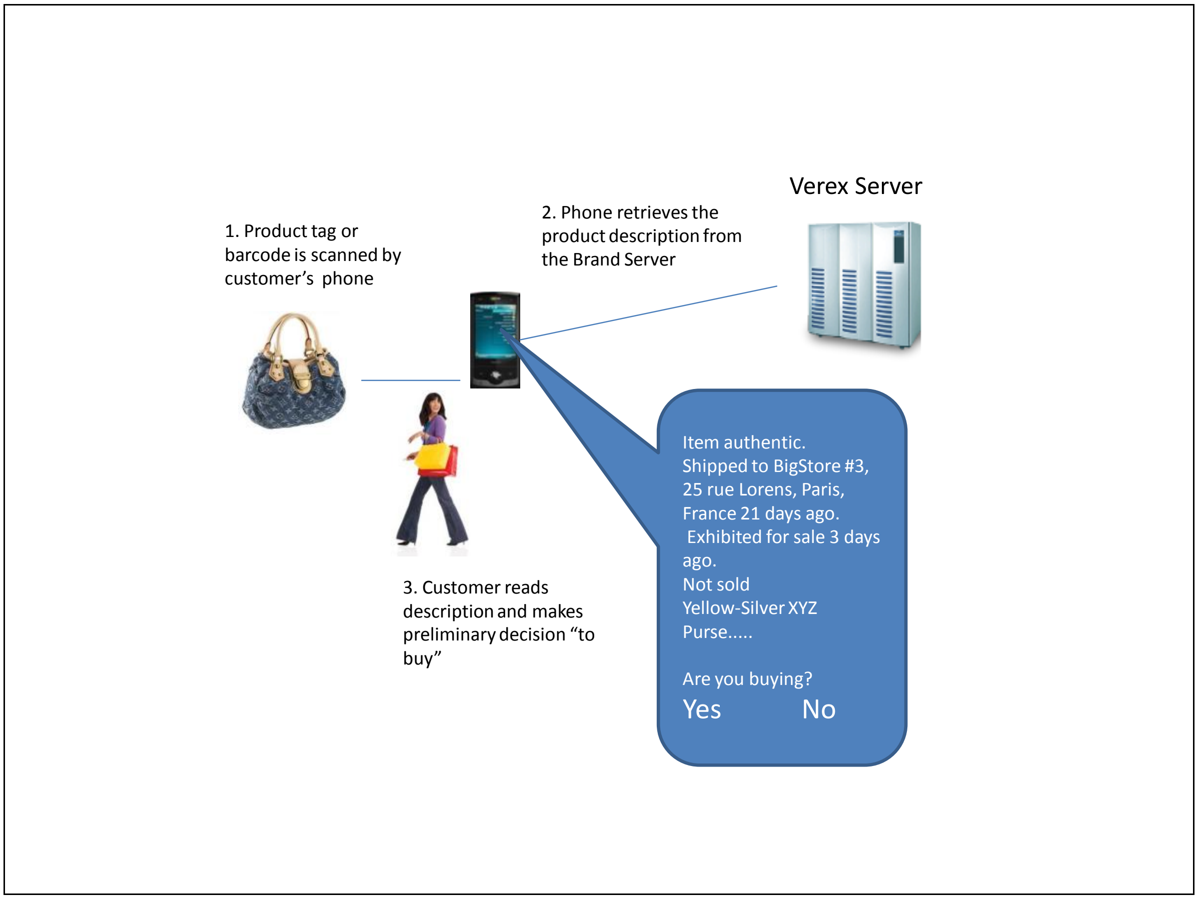
Verex Server
1. Product tag or barcode is scanned by customer's phone
2. Phone retrieves the product description from the Brand Server
3. Customer reads description and makes preliminary decision "to buy"
Item authentic.
Shipped to BigStore #3, 25 rue Lorens, Paris, France 21 days ago.
Exhibited for sale 3 days ago.
Not sold
Yellow-Silver XYZ Purse.....
Are you buying?
Yes
No

Figure 1. Preliminary Authentication

Tag Requirements

The Tag has the following characteristics:

- Stores its private and symmetric encryption keys securely (to prevent tag cloning).
- Generates its own unpredictable number to avoid attacks from a fraudulent POS
- Proves its authenticity to a POS and Verex Server. The elements of offline and online integrated circuit card authentication prescribed by EMV can be used for this purpose. The scanning device (e.g. smartphone) sends an unpredictable number to the tag and the tag responds with the electronic signature of the POS and smartphone unpredictable numbers. The signature can be PKI-encrypted and verified off-line by the phone without a connection to the Verex Server. However, the connection to the Verex server is the best practice.
- Possess additional electronic certificates that certify certain properties of the item (such as excise marks, safety certificate, etc.), the tag can prove the authenticity of these certificates.

- Possesses the description of the static parameters of item of goods or services. These are parameters that do not change, such as the description of the goods appearance, date of manufacture, expiration date, etc.
- Scannable in a contactless way that does not require a power supply. A good technology candidate from that point of view is NFC.

Since all phones are not yet capable of communicating with NFC tags, the tag should also possess an alternative scannable form factor, such as a barcode. Barcode scanning capability is available on almost every smartphone equipped with a camera. (The barcode tag is a passive, read-only device with relatively small data capacity and unlike Verex NFC tags, it is cloneable. When barcodes or clonable tags are implemented, online access to Verex assurance services is required to provide the phone with reliable merchandise pedigree data and also to detect barcode reuse, (e.g. sale of another item with a cloned or reused barcode).

Smartphone or Scanner Requirements

The smartphone or an alternative (e.g. warehouse or shipping) scanning device must have the following characteristics:

- Built-in NFC scanner capable of communicating with tags. Google-Android smartphones have such capability. In the absence of built-in functionality, viable alternative solutions exist from suppliers such as Device Fidelity, inventors of NFC scanners as a form factor built into a microSD card or phone.
- If the NFC scanner is not present, the smartphone must have a barcode scanning device (basically, a camera).
- The presence of a Verex software application that communicates with the tag via NFC or optical (barcode) channel and with the Verex server via Wi-Fi or cellular data communication subsystem.
- A unique identifier known to the Verex Server so the server can send a message or a data package to this smartphone. The identifier can be permanent (for Verex Club members) or session-based for all other consumers. The consumer’s Verex electronic certificate, securely stored in the smartphone, may be required for members of the Verex Club.

In-Store Checkout Phase of the Verex Transaction Process

The checkout phase (see Figure 2) begins when the goods are presented to the checkout cashier. The cashier scans all items that display the Verex logo. In case of service authentication, the certificate tags are scanned. Items that are not Verex-protected items are scanned at the same time and, possibly, with the same POS scanning device. Adding Verex process need not impact current checkout processing.

The store POS communicates with tags in the same way the consumer’s smartphone. The POS aggregates the tag data from all scanned items and sends the information in bulk to the Verex Server.

The tag scanning can be done (preferably) via the NFC channel, so the tag is challenged with the POS unpredictable number, and returns the signed authentication data (or cryptogram). An alternative way of scanning is via the barcode.

The payment card (or the payment application) data is read at the POS. If a Verex-co-branded card is tendered, the POS captures the Verex Club membership identification number (member ID).

When all items and the card have been scanned, the POS sends an Assurance Request message (comprising all tag information and possibly the member ID) to the Verex Server. Optionally, tags can also contain electronic certificate records that certify certain properties of the item. The certificate data and the data that proves the certificate authenticity is also included in the Assurance Request.

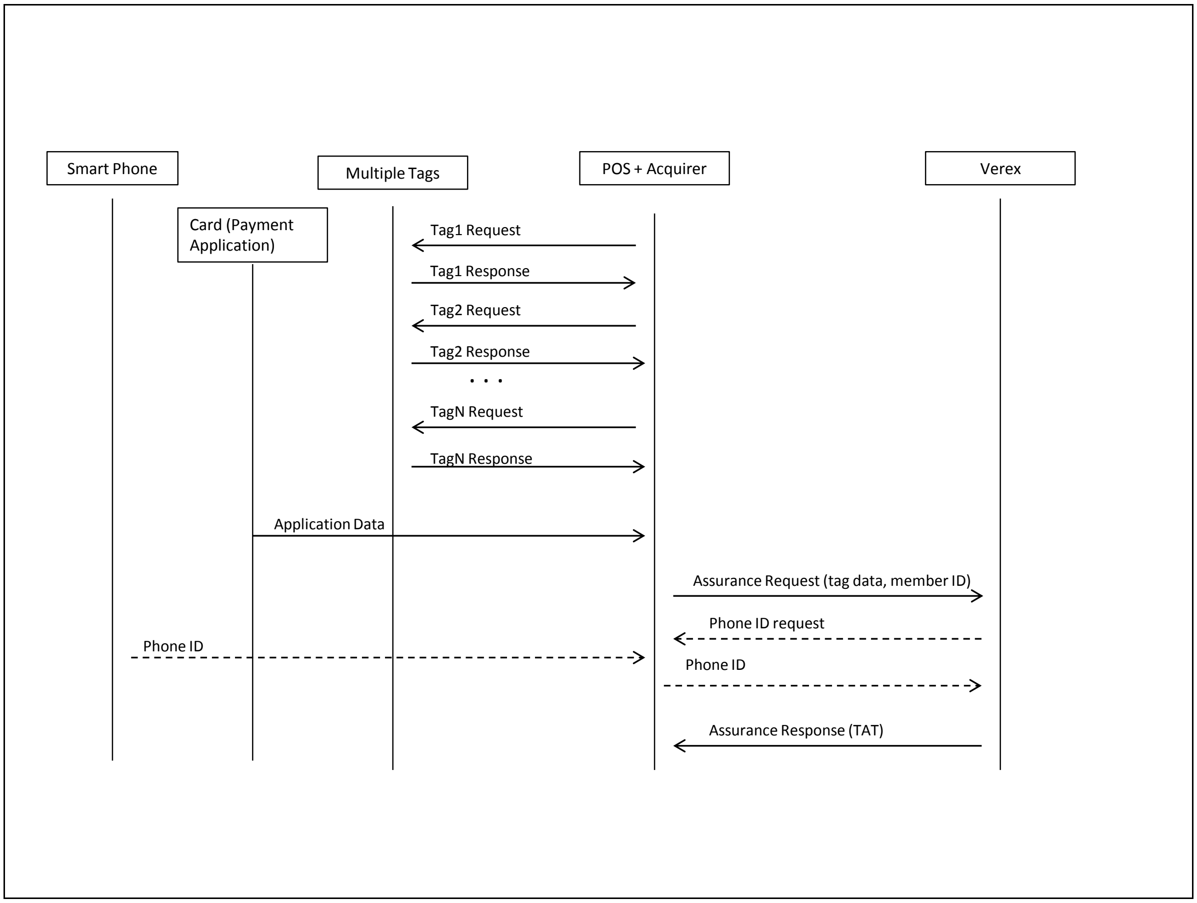

Figure 2. Goods Authentication at Checkout

Optionally, the Verex Server may request the phone identifier from the POS if the Server is not able to identify the smartphone that was used at the Preliminary Authentication phase. In this case, the cashier asks the consumer to present the phone for scanning either via NFC, barcode displayed on the phone screen, Blue Tooth, etc. The POS sends this information to the Verex Server as well. If the payment card application is embedded in the phone, the phone has already been scanned once and the second scanning may not be required.

The Verex Server authenticates all presented tags and, when possible, matches the tag data with tag data scanned at the Preliminary Authentication phase. If not all items authenticated or matched successfully, the smartphone and the POS are advised, and additional corrections may take place.

At the end of the item authentication process, the Verex Server creates the list of all successfully authenticated items, attached electronic certificates, and related amounts, signs the list with the Verex electronic signature and returns the signed list to the POS in the Assurance Response message. This list is called hereafter the Tender Assurance Token (TAT). In some implementations it may be sufficient to include only the electronically signed digest of the item list in the TAT. The electronic signature used to create TAT can be a PKI-based. It can also be based on the symmetric encryption where the secret key is shared between Verex and the payment infrastructure.

The process of communication between the POS and the Verex Server outlined above can be implemented either directly between the POS and Server or indirectly via a POS proxy, such as a store server, a store network server, acquiring processor server, acquirer server, or payment association network.

After the TAT is obtained from the Verex Server the transaction authorization request is sent to the payment infrastructure by the POS. The request will comprise all usual authorization request data fields. In addition, the TAT is included in this request.

The payment infrastructure verifies the TAT signature, and if it is correct, proceeds with the payment step of the Verex transaction. If the payment is authorized by the payment infrastructure, a transaction completion advice is sent to the Verex Server. This advice can be sent by any element of the payment infrastructure: the payment card issuer, the payment association network, the acquiring processor, merchant server, or even the POS. The implementation of this step depends on the specific business and technological environment.

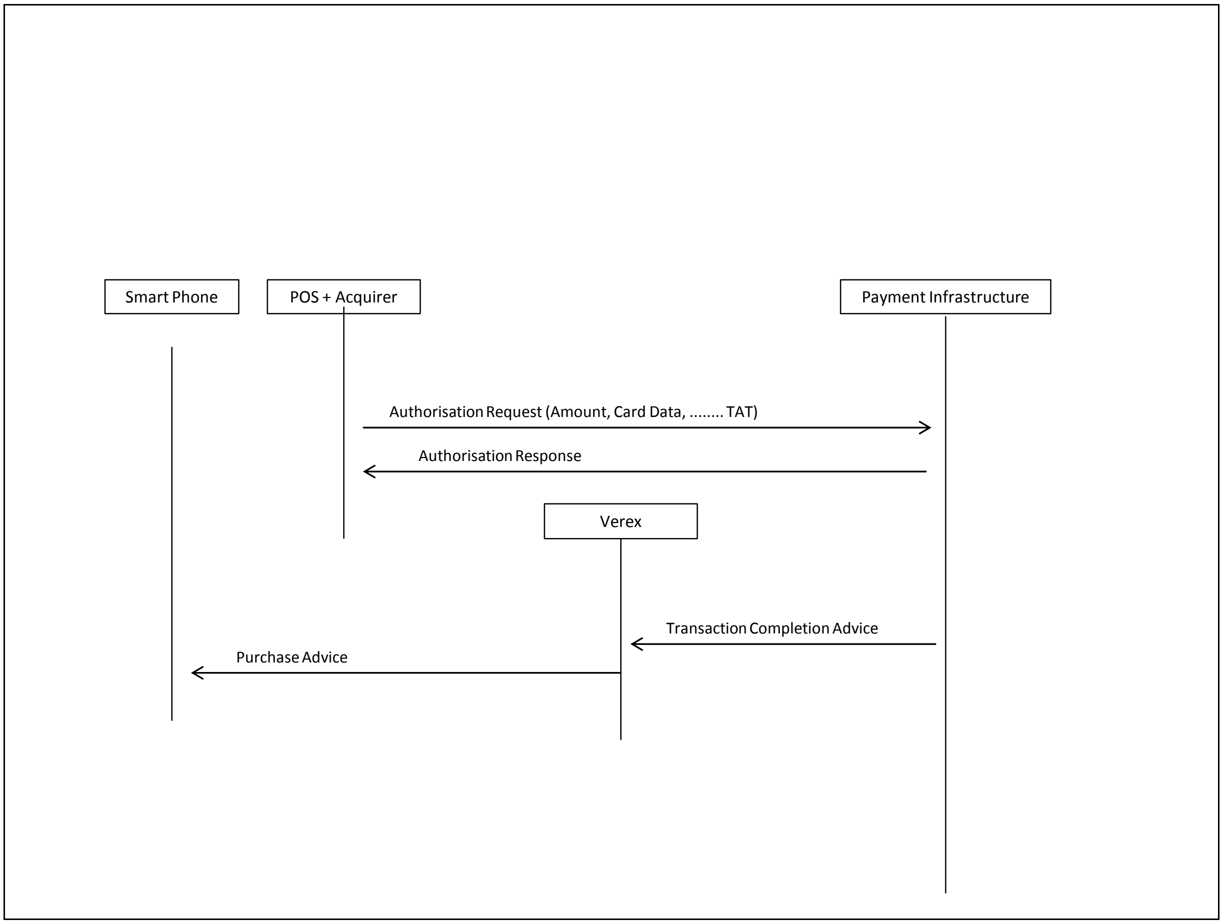

Figure 3. Verex Transaction Completion

After the Verex Server receives the transaction completion advice, it sends the purchase advice to the consumer’s smartphone, assuring the consumer that all purchased items and attached electronic certificates are authenticated and the items are exactly the ones the consumer has chosen.

Verex Post-Purchase Processes

Verex Premium Services

If the Verex transaction was originated by a Verex co-branded card, the Verex Server executes additional optional, value-added functions as configured by the brand owners or merchants based on the particular purchased items. This can include automatic warranty registration, ownership tracking, instant rebates, coupons, etc.

Reconciliation

Verex charges fees to the brand owners based on the sold items and the purchase amounts and compensates the entities representing payment infrastructure participants.

Verex charges financial institutions issuing Verex co-branded cards for Verex club services. The financial institutions may impose charges to the cardholders as they see fit and within the framework arranged between Verex and the appropriate payment association.

Verex Process Variants

Online Purchase

When the consumer selects an item online, this item may not necessarily be the one that is ultimately shipped. In some cases involving unique products, the exact item will certainly be chosen. In most other situations though, it will be one of many of its kind. In other cases the item may not yet have been manufactured at the time of online order. Individualization of the purchased item comes later, before its shipment.

At the time of the online order, after the card pre-authorization, the online store informs the consumer that the Verex item authentication will follow at shipment. This notification must be regulated under payment association rules (e.g. take place within a certain number of days).

At the time of shipment, the item (or items) is scanned and a TAT is created by the Verex Server. The Verex Server sends the message (email) or directly informs the consumer’s Verex smartphone application about the tag (e.g. a digital signature) and the item in the shipment.

The merchant makes the shipment and informs the consumer about the shipment in the regular way with the following variations from the standard non-Verex process:

a) The shipment must be arranged through a courier service supporting Verex process.
b) The consumer’s credit card is not charged at the shipment as the Verex payment transaction has not yet been completed. It will be completed at the item delivery. This must be regulated by payment association rules.

Upon delivery, the Verex transaction is completed in the way similar to the completion of an in-store transaction. As before, the transaction begins by sending an authorization request to the payment association with the TAT included.

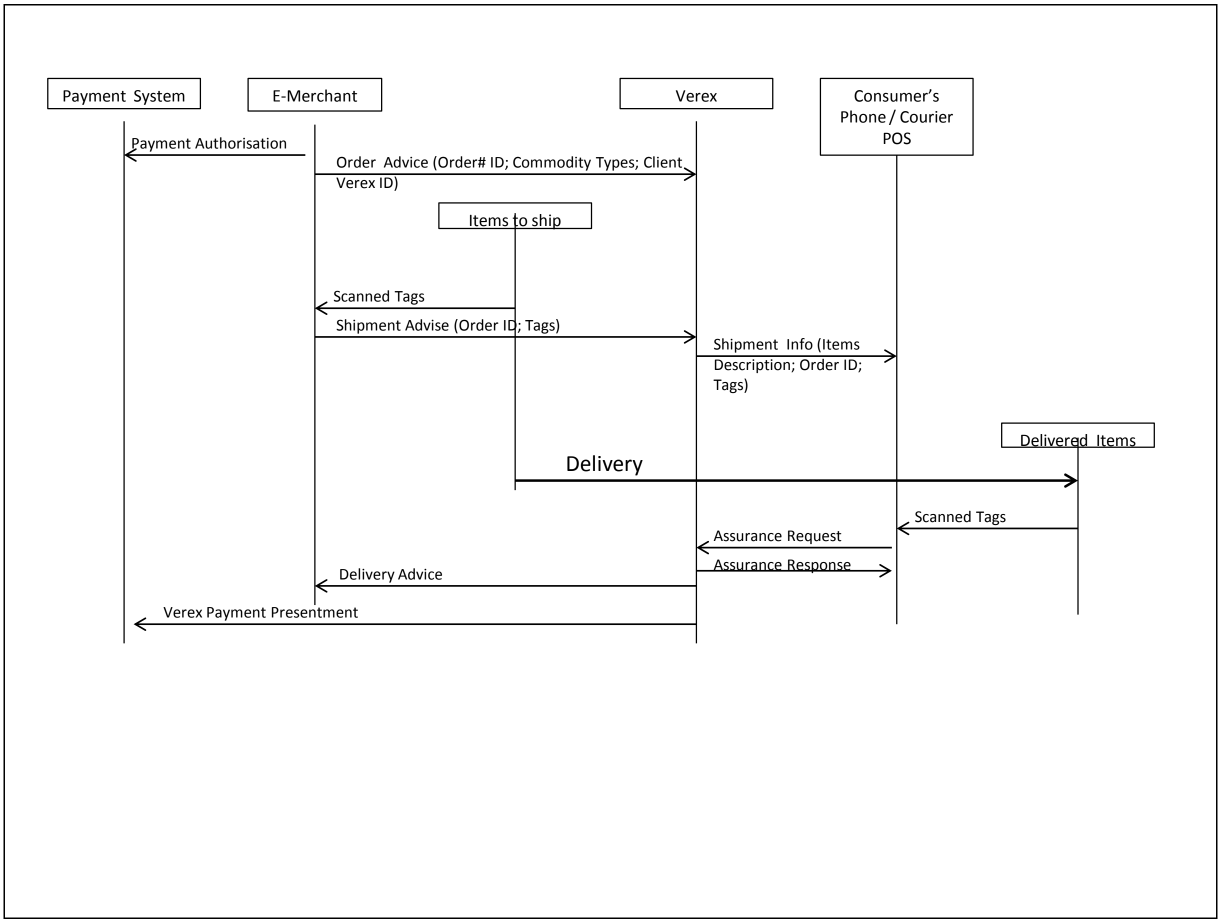
Payment System
E-Merchant
Verex
Consumer's Phone / Courier POS
Payment Authorisation
Order Advice (Order# ID; Commodity Types; Client Verex ID)
Items to ship
Scanned Tags
Shipment Advise (Order ID; Tags)
Shipment Info (Items Description; Order ID; Tags)
Delivered Items
Delivery
Scanned Tags
Assurance Request
Assurance Response
Delivery Advice
Verex Payment Presentment

Figure 4. Verex Online Variation

Offline Variations

Secure elements in the smartphone, NFC tag capabilities, and the smartcard payment application (EMV) permit the delegation of certain functions of a card issuer and the Verex Server to those elements, enabling transaction to be completed offline with some follow-up functions taking place by both Verex and the payment infrastructure back office.