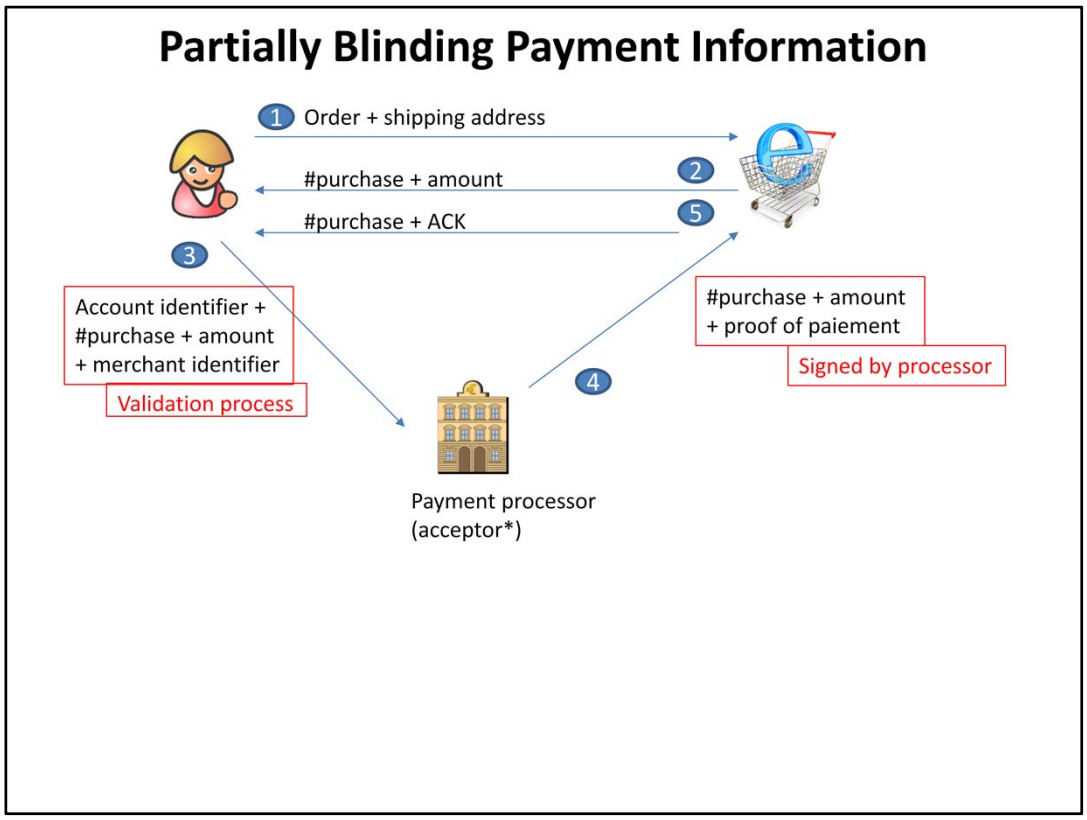


*This diagram does not preclude the payment (that is the fund transfer mechanism, push or pull). Actually, considering the structure proposed by Evert at the F2F in Utrecht, the payment processor performs the role of the "acceptor". Indeed, what a Point of sale terminal does :

- Perform the validation process of the buyer (PIN and card)
- Give a proof of payment to the merchant that the validation was correctly performed

---

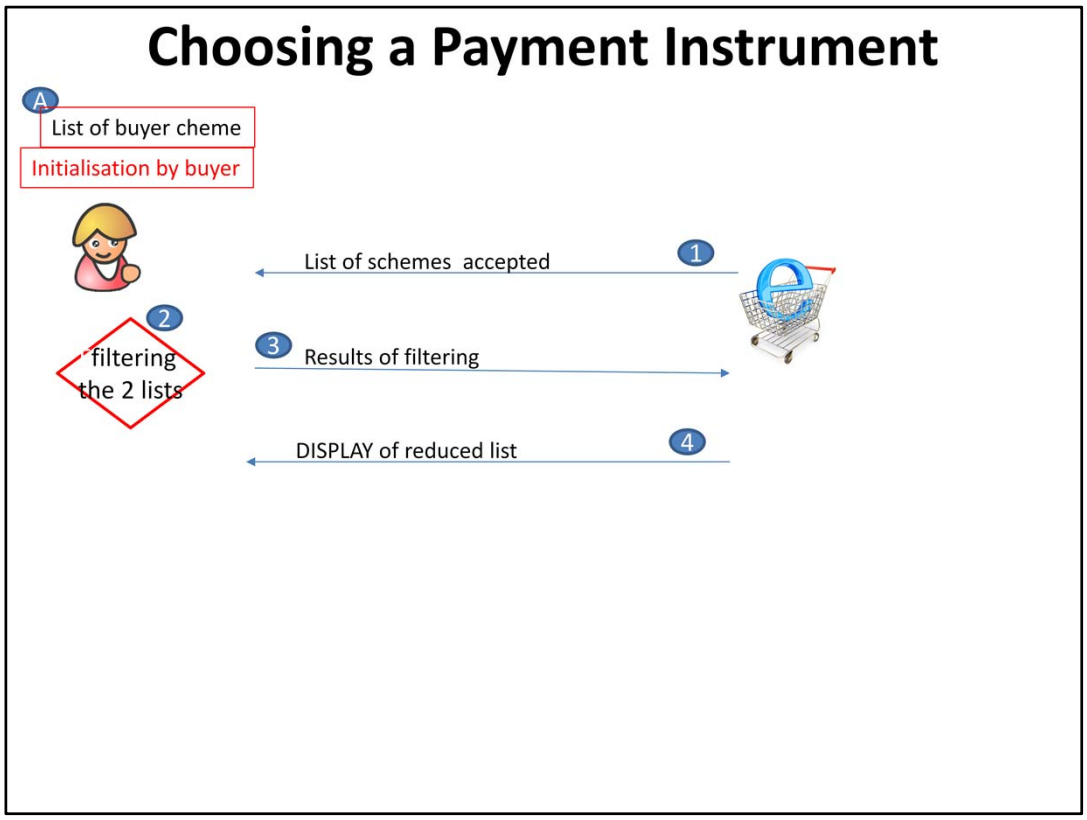
Leveraging variable degrees of pseudo-anonymity per requirements of the payment transaction.

Examples

Customer POV: Tibor orders 3 pounds of assorted chocolates from an online candy store. The store only needs Tibor's verified shipping address and a proof of payment to send him the chocolates. The verified shipping address and the proof of payment are made in a single request to Tibor's Payment Agent and both are delivered to the online candy store. Tibor's privacy is protected from the candy store, which did not require Tibor's name, email address, or any other personally identifying information to complete the transaction.

Merchant POV: An online candy store gets an order for 3 pounds of chocolate. The store requests a verified shipping address and a proof of payment from the customer in order to send the goods. After receiving both, the store ships the goods to the customer, not exposing themselves to any risk of accidentally leaking their customer's personal

information of payment data.
Payment Processor POV: PayCo is required to keep a certain amount of information on their customers for anti-money laundering / know your customer regulatory purposes. When a customer performs a transaction with a merchant, they would like to reduce the amount of information that's transmitted to the merchant while ensuring that they stay compliant with regulations. This enables the customer to stay pseudo-anonymous when dealing with merchants, but ensure that law enforcement have recourse in the event of illegal activity.



A- before payment, when the buyer initialises his user-agent with a list of schemes/ Example above is to try to understand what are the necessary identifiers for defining a schem

- PAN for card scheme
- Bank + name of scheme (Ideal example)
- QXBAN (example of SEPAmail)
- IBAN (SCT)
- IBAN (SDD CORE)
- IBAN (SDD B2B)

- Flows 1, 3 and filtering process at the user-agent could be in done in background

---

When a payer intends to make a payment, they are given a choice to pick among the intersection of the payment instruments they have available to them and the payment instruments that are accepted by the payee. Optionally, new payment instruments may be offered to them by the payee and provided as options by their payment agent.

Examples

Daniel wants to pay the taxi fare with his credit card. The cab company promotes the payment via its web site which offers, on Daniel's smartphone, to choose between several instruments offering different payment means: 1) the basic credit card (Visa, MasterCard, etc.) channel; 2) or an indirect aggregator (PayPal, Google checkout); 3) or the personal wallet detected as available on Daniel's phone.

Amantha downloads the latest version of her favorite game. It's only a couple of euros that she'd like to pay on top of her telecom operator's bill. The game store web site accepts payment via credit card and operator billing. Amantha selects the "operator billing" payment option.

Ricardo would like to pay for clothes at ThreadCo, a brick-and-mortar retailer, using software on his mobile phone. He taps his phone to checkout and notices that the purchase would be less expensive if he uses a department store digital credit card to complete the purchase. He applies for the card using a provided link, is approved for the digital credit card card, and completes the checkout process using his new card.

Motivations

Each payment instrument is registered with a set of attributes in order to filter, sort, and display them.

Each payment processor is registered and 'subscribes' to a the payment instrument it is able to provide.

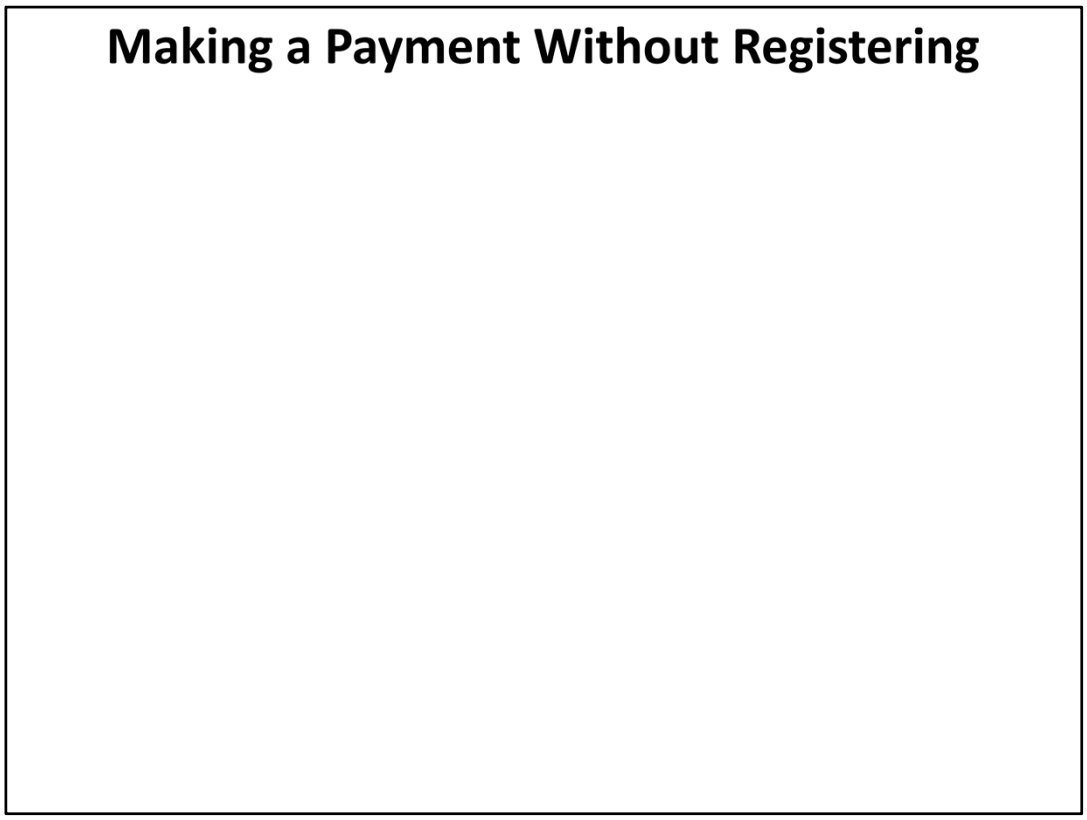
Each merchant provides a list of acceptable payment instruments.

A payment agent may attempt to optimize payment instruments on behalf of the customer by selecting for payment speed, loyalty benefits, price, or other conveniences.

Over time, each customer iteratively builds a list of preferred payment instruments for their commonly used merchants.

How are multiple payment instruments handled? Is there such a thing? There are two main approaches so far. The first is to treat loyalty cards, coupons, discount cards, and other similar items as types of credentials and the payment instrument as the mechanism that moves the value. The second is to explore how multiple payment instruments may be mixed together from different providers to complete a transaction.

Making a Payment Without Registering



It seems to me that this use-case is the same as "**Partially Blinding Payment Information**"

A payer goes to a payee storefront and initiates a payment without having to go through any registration process. During the payment process, the payer chooses which information to share with the payee which the payee then uses to identify the payer if future payments are made.

Examples

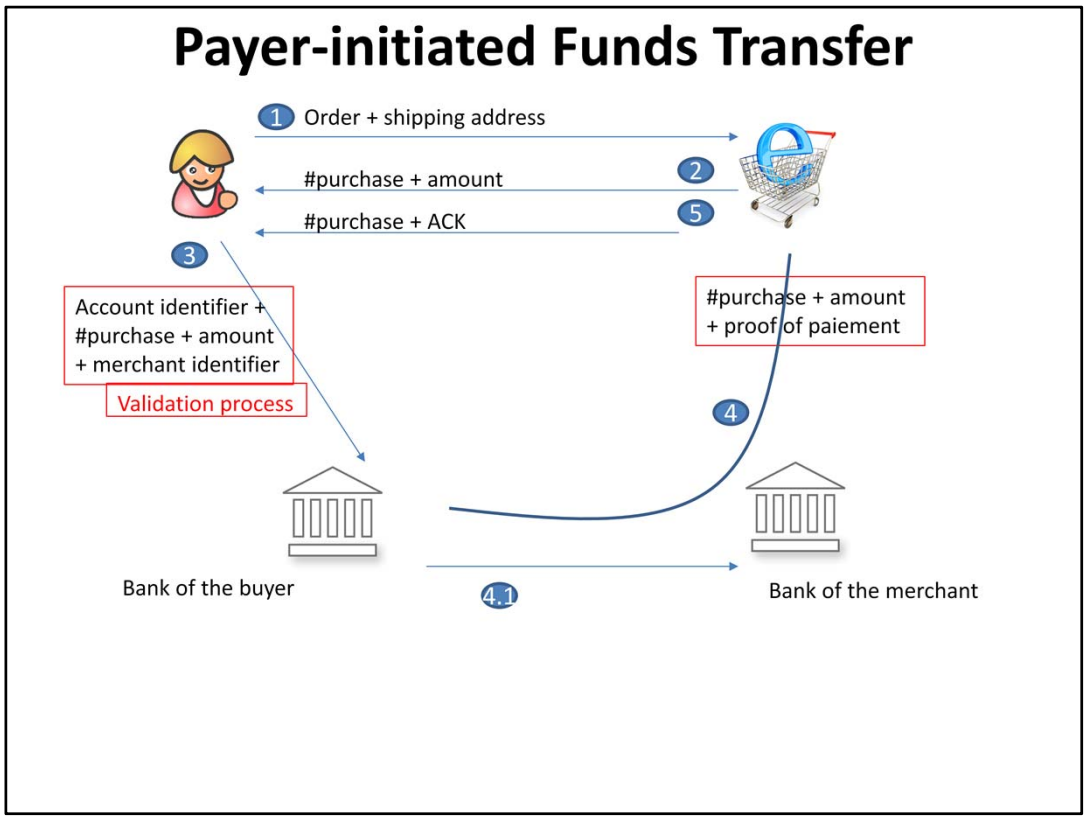
Customer POV: Lilith finds a song that she really likes through one of her favorite music blogs. Without registering with the blog, or the artists website, she initiates a purchase and is sent to the artist's website to show the proof of purchase and download the song. At no point did Lilith have to register for a user account, enter her credit card number, or email address.

Merchant POV: A proof of purchase for a song is shown to a merchant website. The proof of purchase is validated and the merchant website provides a download for the customer.

Motivations

There are a large number of "paywall" websites on the Web that require registration to use. In many cases, if the site isn't regularly visited by the customer, they abandon the transaction when they see the paywall requirement. Providing a mechanism to sell an inexpensive item to a customer without requiring registration would be of great benefit to not only the merchants selling goods and services, but customers that would like to

avoid lengthy registration processes.



This is globally the same mechanism as slide 1. The process need :

- A validation by the buyer
- A notification by the bank's buyer to the merchant
- A fund transfer

When payer-initiated funds transfer, the buyer (or user agent) should connect to its bank, performe the validation process asked by his bank. Then the bank :

- send the funds to the merchant bank
- send a real time proof of payment to the merchant
    - The more real-time the better
    - Could be trough the merchant bank (it implies sequential authentication, buyer bank to merchant bank, merchant bank to merchant)
    - Could be directly in any authentication mechanism of buyer bank to merchant available

---

When a customer wants to make a purchase, the merchant presents the customer with an electronic invoice which in turn can be presented to a payment processor. The payment processor then provides a validated proof-of-payment to the merchant via the customer's device or directly to the merchant.

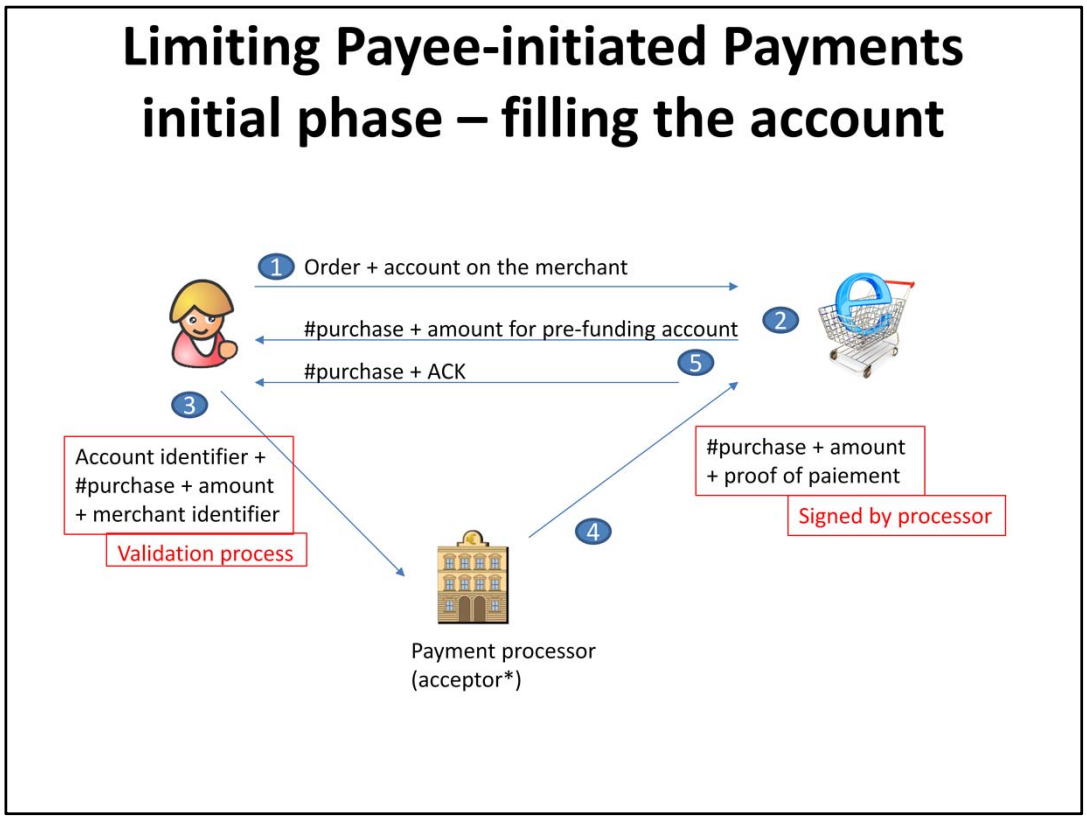
Examples

Customer POV: John goes to CandyCart.com and clicks "buy" to purchase chocolates. His browser re-directs him to his payment processor which asks him to approve the purchase. He approves the purchase, his payment processor transmits the funds to the

receiving account, and his browser is re-directed back to CandyCart.com with the proof of payment.
Merchant POV: A customer selects 5 items to purchase. The merchant system presents an electronic invoice (either a total only or with a breakdown of the transaction), including the merchant's identifier, to the customer's device. The customer's device returns a proof of payment that is digitally signed with the customer's payment processor's private key.
3-Corner Payment Processor POV: A customer sends an electronic invoice, including the merchant and customer identifiers, to the payment processor. The customer and the merchant use the same payment processor. The payment processor checks the customer and merchant for validity, posts the requested amount to the merchant's account, and then generates a proof of payment for the merchant. The payment processor then returns a signed digest of the invoice plus a digest of the proof of payment to the customer's device. The customer's device delivers the proof-of-payment to the merchant system to prove that funds have been transferred.
4-Corner Payment Processor POV: A customer sends an electronic invoice, including the merchant and customer identifiers, to the payment processor. The customer and the merchant use different payment processors. The payment processor checks the customer and merchant for validity, and initiates a transfer of the requested amount to the merchant's account via a payment clearing mechanism. Once the payment processor has received a verification that the payment message was received by the acquirer, it then generates a proof of payment for the merchant. The payment processor then returns a signed digest of the invoice plus a digest of the proof of payment to the customer's device. The customer's device delivers the proof-of-payment to the merchant system to prove that funds have been transferred.

Motivations

For this use case, the customer asks the payment processor to initiate payment to the merchant directly, preventing the need for sensitive customer information to be shared with the merchant, which keeps the merchant out of "PCI scope." No direct communication between merchant and payment provider is required for this use case. It may be possible to create an electronic receipt format that satisfies the requirements for this use case as well as others.



This could be performed in two phases :

- Creating and filling the account (prepaid)
- Spending

A payer visits a payee's website and initiates a payment. The payer's payment processor presents them with an option to assign a pay-as-you-go token with a specific spending limit (and/or other limitations) for future purchases with the payee. An option is also presented to require the display of a receipt when a purchase occurs (and/or other interactions), or to perform the purchase in the background with no interactive purchase process required.

Examples

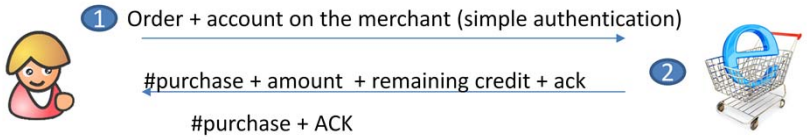
Customer POV: Yanos visit's his favorite financial news site, which requires articles to be purchased if the customer does not have a subscription. Yanos initiates a purchase. The website, in the payment request, requests a multi-use payment token from Yanos' payment processor to spend up to $15 a month on Yanos' behalf when he purchases certain for-pay articles. Yanos' payment processor asks him if he would just like to perform a one-time purchase, or grant the payment token to the news site. Yanos doesn't want to be bothered to approve a $0.50 purchase, as he does many of them on the website, so he authorizes the initial payment and also authorizes the multi-use payment token. The multi-use payment token is delivered to the financial news site along with proof-of-purchase for the initial article he intended to buy.

Merchant POV: An online video game company following a freemium business model would like to enable in-app purchases for their content. In order to do so, they would like to request a multi-use payment token from their customer. They enable a button in their game that requests a multi-use payment token and when a customer approves it, the company stores it in their systems. The multi-use payment token is only good for 3 months and has a spending limit that is set by the customer.
Payment Processor POV: A payee's payment processor receives a request for a multi-use payment token from a payer via the payee's device. The payment processor ensures that the details of the payment token are acceptable to the payee, enables them to add constraints to the payment token, and upon approval, grants a unique identifier for the payment token to be returned to the merchant. The payment token is always linked between a payer's source account and a payee's destination account such that the theft of the payment token does not result in the ability of the thief to move money from the payer's source account to an arbitrary payee.

Motivations

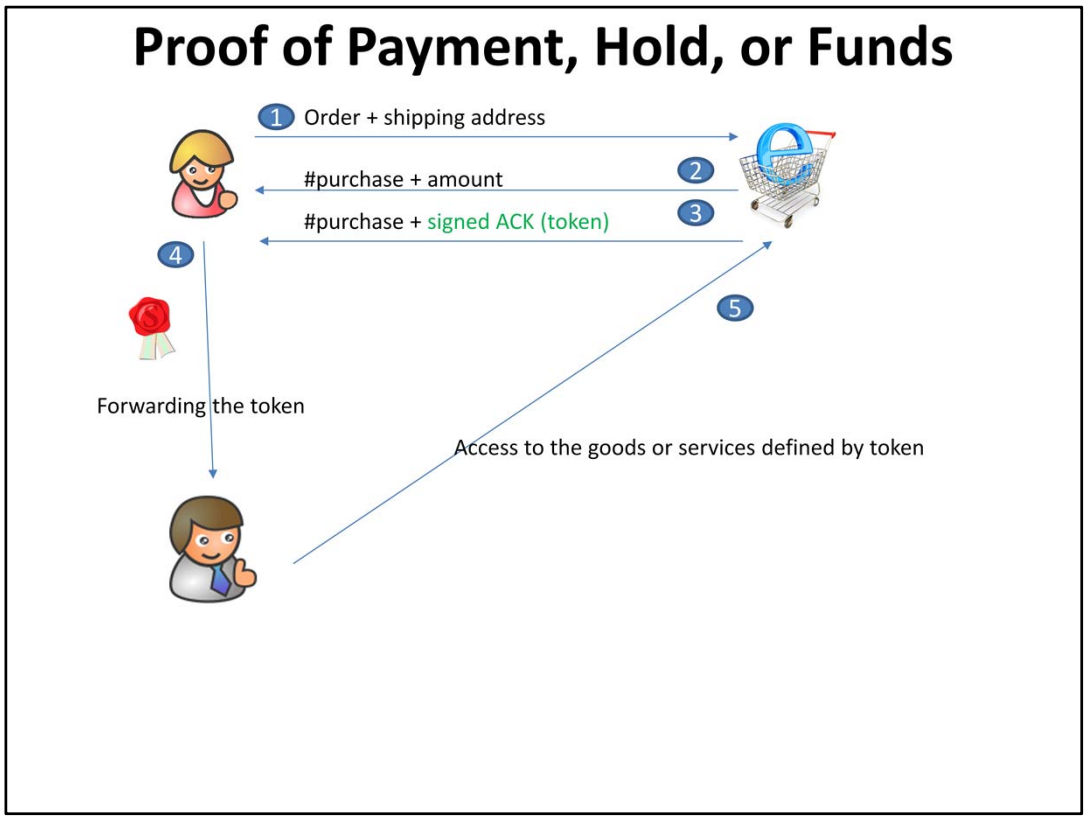
There are a number of types of purchases that don't require the full attention of the payer when they happen. For example, an in-game purchase for an item that costs $0.05 is not necessary until a pre-set limit set by the payer is reached. It is important to not make the payment experience cumbersome for markets that perform micro-payments, or require the processing of many repetitive payments. If the payment authorization step can be automated to the point of disappearing without creating a bad customer experience or generating fraud, then it should be eliminated.

Limiting Payee-initiated Payments phase 2– spending



This could be performed in two phases :

- Creating and filling the account (prepaid)
- Spending



A payer intiates a transaction for a good or service from a payee resulting in a standardized, cryptographically signed, machine-readable proof-of-payment, proof-of-hold, or proof-of-funds. Entities involved in the transaction (payer or any payee) may then use the proof to assess whether or not the payer should have access to the good or service.

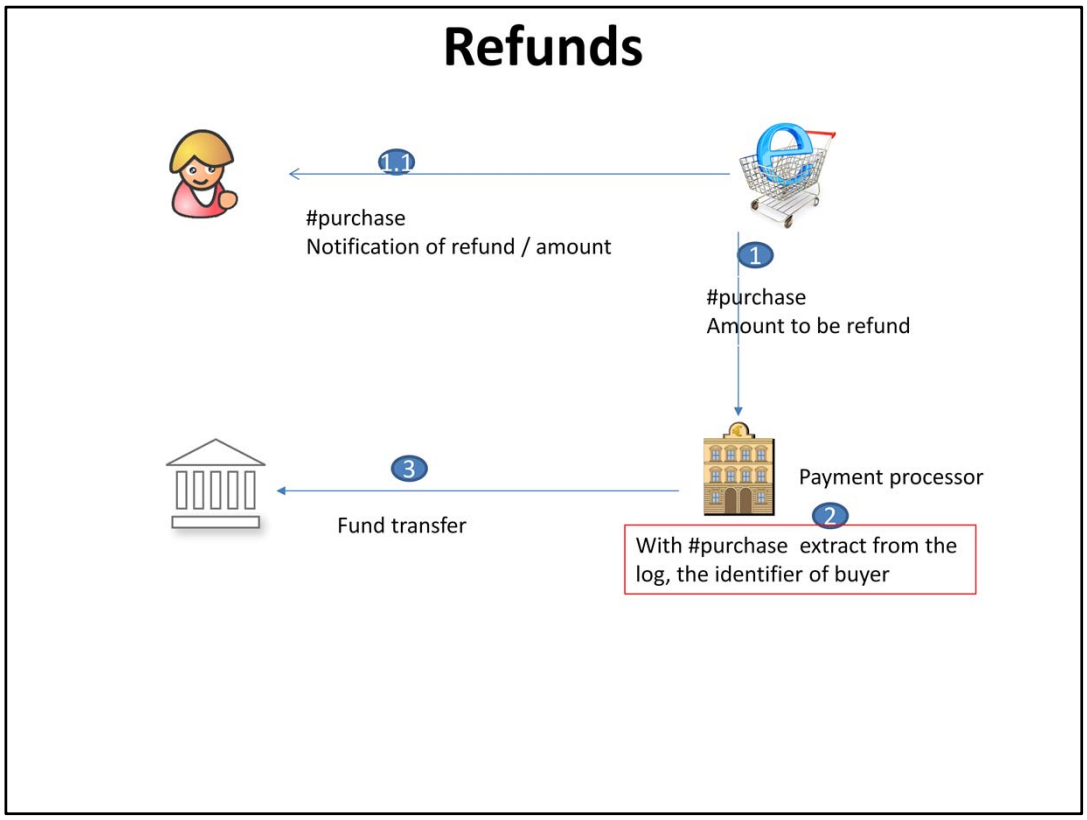
Examples

Customer POV: Jeff buys a lot of heavy metal music through the "Buy this track" function on his car radio. When he buys a new car, he wants to transfer his collection and provides all of the proof-of-payment data to show that he has already paid for the songs.

Customer POV: Willie buys e-tickets for a football game, but his mobile phone is stolen while standing in the queue. Since he has a receipt and identifies himself, he can still get in to watch the match.

Customer POV: Renne checks into a hotel and is asked for a deposit for any damages to the room. She uses her phone to provide a proof-of-hold until she checks out of the hotel, at which time the hold on her funds will be released.

Merchant POV: Rockinradio, smoothSounds, and classicClassic are independent specialised music retailers. They accept proof-of-purchase from each other to provide a track that is in their online catalogue even if it was originally bought from another provider.



1. We consider that the merchant do not have the “scheme identifier” of the buyer for refund
    1. in card scheme, the buyer identifier for refund is the PAN,
    2. in the Sepa Credit transfer, the buyer identifier is the IBAN, but the merchant is not supposed to know it

---

The funds that are transmitted from payer to payee are reversed after a decision by a merchant, regulatory authority, or payment processor.

Examples

Customer POV: Pele buys a slice of pizza at a local restaurant and is accidentally charged for five slices of pizza. He notices the mistake after he pays and requests a refund, which the restaurant manager approves. The overcharged funds are returned to his account.

Merchant POV: A customer claims that a blender that they purchased online was faulty and returns the product to the merchant. The merchant provides the customer with a refund in the form of store credit based on the return policy.

Regulator POV: A financial crimes regulator identifies a criminal syndicate that is operating via a number of fake identities. The fake identities are flagged and an electronic message is sent to all payment processors to reverse all payments sent to the fake identities.

Applying Coupons and Loyalty Cards to a Payment

A payee can associate a membership card, coupon, or similar token with a transaction to receive a discount or other benefits.

Examples

Customer POV: Cory shops for groceries at his local ChowMart. When he starts the checkout process via the automated kiosk, the machine asks him to tap his phone to transmit his ChowSavingsCard info to get discounts on items he's purchasing. He taps his phone, selects his card and taps his phone again to transmit the card information to the kiosk, which shows him how much of a discount he is receiving because of the card.

Merchant POV: ChickenHut requests loyalty cards from frequent customers in order to provide discounts. When customers tap their phone, a cryptographically verifiable token that was issued by ChickenHut is transmitted from the phone to the point of sale device and verified for authenticity.

Motivations

Coupons and loyalty cards are two discount mechanisms that may be used by a customer before performing a final payment. While coupons and loyalty cards vary wildly in their associated benefits, a merchant or manufacturer must ensure that each one is authentic. In order to ensure the authenticity of a coupon, loyalty card, or information stored therein, it is important that all information is cryptographically verifiable. It is also important for the point-of-sale devices to be able to add information to the locally-stored loyalty cards for use in off-line scenarios.

Performing a Payment in Multiple Phases

Transactions over a certain amount may require a preliminary check on the availability of funds to complete the transaction. These transactions may also have a provision to perform a hold on the funds until the product or service is delivered and the transaction is complete.

Examples

Customer POV: George pulls up to a pump at a petrol station. His in-vehicle application recognizes the station location and the pump, and asks if he wants to approve a fill up. He answers "yes" and is prompted for which method of payment he would like to use. He makes his selection, exits the vehicle, lifts the nozzle, selects the grade of fuel, and fills his car. When he returns to his vehicle, an electronic receipt for the purchase is displayed by his in-vehicle application.

Customer POV: Doris uses her mobile application to approve fuel fill-up for her van. She realizes after exiting her vehicle that the site is not ADA compliant, and so she cannot access the pumps. She uses her mobile application to cancel the transaction.

Merchant POV: FuelCo's in-store control system gets a message from a payment processor that pump 14 should be approved for a fill-up. The message includes a single use cryptogram that can be used to prove authorization. The equipment arms the pump and allows the fueling to proceed. On completion, the merchant system sends the actual amount to pay along with the single use cryptogram back to the payment processor.

Motivations

Delivering services or products that are difficult to "undo", such as performing an oil change, dispensing fuel, or renting a car, are examples of situations which may require a two-part transaction.

This use case highlights the need for a two part transaction. The first part either checks

availability or reserves funds, and the second completes the transaction with the actual amount. There are many different ways these two segments can be completed.