Internet-Scale Payment Systems
Ecosystem & Challenges

Malcolm Pearson
malcolmp@microsoft.com
Agenda

• Abstract Payment Flow
• Key Payment Challenges
• Payment Scenarios
• Payment Instrument Flows
  • Mobile
  • Kiosk
  • vCurrency
  • eWallet
  • Cards
  • Bank Transfer
• Needs for Standardization
Abstract Payment Flow - Online

Notes
• Network of many sources, merchants and payment instruments.
• Conceptually, source responsible for following user intent.
• Destinations & merchants may cascade.
Abstract Payment Flow- Full

Back-end issues
- Cash reconciliation
- Tax reporting
- Financials
# Key Payment Challenges

<table>
<thead>
<tr>
<th>Area</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network</strong></td>
<td>• Many Countries and Currencies&lt;br&gt;• Many Sources, Payment Instruments and Flows</td>
</tr>
<tr>
<td><strong>Security vs. Convenience</strong></td>
<td>Merchant Concerns&lt;br&gt;• Merchant expresses pricing&lt;br&gt;• Many pricing models&lt;br&gt;• Integrated merchant experience</td>
</tr>
<tr>
<td></td>
<td>Payment Source Concerns&lt;br&gt;• User agrees to pricing&lt;br&gt;• Payment sources follow user’s instruction</td>
</tr>
<tr>
<td><strong>Business</strong></td>
<td>• Already a long and rich history, many entrenched players</td>
</tr>
<tr>
<td><strong>Emerging Markets</strong></td>
<td>• Anticipating Different Cultural Norms&lt;br&gt;• Economic impact of cash-oriented commerce</td>
</tr>
</tbody>
</table>
## Payment Scenarios

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purchase physical Goods Online</td>
<td>• Relatively asynchronous payment flow permitted due to delays in physical delivery</td>
</tr>
<tr>
<td>Purchase Digital Goods</td>
<td>• Subscriptions to be used over a long period of time allow time and authorization</td>
</tr>
<tr>
<td></td>
<td>• Immediate use items (consumed in a game) cannot be taken back by merchant and cannot interrupt end user flow</td>
</tr>
<tr>
<td>Subscriptions. Payment Agreement Complexity</td>
<td>• Agreement to pay on a schedule</td>
</tr>
<tr>
<td></td>
<td>• Usage based subscriptions have variable pricing</td>
</tr>
<tr>
<td>Purchasing goods from physical stores. Roaming between mobile, tablet, TV and PC.</td>
<td>• Users expect continuity between online, mobile and physical store experiences</td>
</tr>
<tr>
<td>Consumer to consumer payments</td>
<td>• Gifting, sharing costs, informal payments</td>
</tr>
<tr>
<td>Returns and disputes</td>
<td>• Connecting payment and fulfillment</td>
</tr>
<tr>
<td>Securing payment material</td>
<td>• Target, Bitcoin</td>
</tr>
<tr>
<td>Backend</td>
<td>• Cash reconciliation</td>
</tr>
<tr>
<td></td>
<td>• Tax and Financial Reporting</td>
</tr>
</tbody>
</table>
Payment Mechanism Flows

Cash Kiosks & Retail centers
- Ucash
- Western Union
- CashU

Mobile Billing
- boku
- AT&T
- Orange
- Vodafone

eWallets
- PayPal
- QIWI
- MercadoPago
- Alipay
- Yandex

Bank Transfer
- DIRECT Debit
- iDEAL
- sofort
- Net Banking
- giropay

Others
- QQ Coin
- BillMeLater
- OXXO

Cash Cards
- paysafecard
- Fund With Cash - MoneyPak
- ItzCash

Cards
- VISA
- UnionPay
- MasterCard
- JCB

American Express
Mobile Billing
Pay via Mobile – Auth* via SMS
Leverage pervasive mobile billing networks

**Merchant Website, Online**
- User selects product
- Website generates price
- User select mobile account via phone #

**On User’s Mobile Device**
- Receive single-use SMS challenge
- Respond on phone
- Respond on Merchant Website

**Merchant Website, Online**
- User purchase is fulfilled
Pay via Mobile – Auth* via Mobile Network

Leverage pervasive mobile billing networks

On User’s Mobile Device
• User selects product
• Merchant generates price
• User selects to pay with “this” mobile account

Mobile operator validates
• Trust user identity due to mobile network transport or SIM
• Trusts purchase description due to marketplace app on device
• Validates and reserves funds

Purchase fulfilled
• Mobile or otherwise
Pay via Mobile – QR Code, auth via Mobile

Leverage pervasive mobile billing networks, transfer payment devices

**Merchant Website, Online**
- User selects product
- Website generates price
- Website generates QR code

**On User’s Mobile Device**
- Purchase details retrieved via QR code
- Purchase details forwarded to Mobile Operator

**Mobile operator validates**
- Trust user identity due to mobile network transport or SIM
- Trusts purchase description due to marketplace app on device
- Validates and reserves funds

Also applies to physical goods and inter-personal payments of gifts

**Merchant Website, Online**
- User purchase is fulfilled
**Mobile Flows**

- **Strength**: Low fraud
- **Challenge**: Regionally specific solutions, cost, flexibility
- **Need**: Payment Federation

<table>
<thead>
<tr>
<th>Phase</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invoicing</td>
<td>1...2</td>
</tr>
<tr>
<td>Payment</td>
<td>10...12</td>
</tr>
<tr>
<td>Reconciliation</td>
<td>20, 21</td>
</tr>
</tbody>
</table>
## Mobile Device as Payment Instrument Wallet

<table>
<thead>
<tr>
<th>Approach</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conventional Card Wallet</td>
<td>• Susceptible to similar fraud problems as conventional cards</td>
</tr>
<tr>
<td>Authentication Mechanism</td>
<td>• Device receives invoice</td>
</tr>
<tr>
<td></td>
<td>• Device verifies user’s consent</td>
</tr>
<tr>
<td></td>
<td>• Device generates secure statement of user-payment authorization</td>
</tr>
<tr>
<td></td>
<td>• Bank must generate source authorization to verify and reserve funds</td>
</tr>
</tbody>
</table>
## Ideal Mobile Solution Technical Elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Notes</th>
</tr>
</thead>
</table>
| End User Authentication        | • Possession of mobile device + ???  
                                  • Leverages Mobile Operator Network or SIM security |
| User Payment Authorization     | • Performed within mobile device  
                                  • TPM                                                                 |
| Source Payment Authorization   | • Mobile operator verifies funds availability  
                                  • Need for common format to express Source payment Authorization       |
| Merchant to Source Network     | • Facilitates Merchant’s ability to scale to trust multiple payment sources |
Cash Kiosks and Retail Centers
Online + Retail Centers
Example: Boleto

**Merchant Website, Online**
- User selects product
- Website generates price
- User selects and prints Boleto

**At Retail Center [Merchant 2]**
- User presents Boleto and cash to cashier
- Cashier accepts cash and scans Boleto to record payment

**Merchant Website, Online**
- User purchase is fulfilled
Online + Retail Centers
Example: ChinaUnicom

**At Retail Center Kiosk**
[not ChinaUnicom]
- User selects product and price
- User selects and prints Payment Slip

**Cell # 12093847**
Topup: 456 RMB
Time Date
QR Code

**At Retail Center Counter**
- User presents slip and cash to cashier
- Cashier accepts cash and scans slip to record payment

**On cellphone**
- Balanced topped up
- Available for other payments
Online + Retail Centers
Example: Qiwi

**At Retail Center Kiosk**
- User selects account to pay into
- User selects price
- Deposits cash

**Merchant Website, Online**
- User purchase is fulfilled
Invoice Cash Kiosk Flows

**Strength**: Low fraud

**Challenge**: Some methods are not automated, Async

**Need**: Common encoding, network of sources

<table>
<thead>
<tr>
<th>Phase</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invoicing</td>
<td>1…4</td>
</tr>
<tr>
<td>Payment</td>
<td>10…12</td>
</tr>
<tr>
<td>Reconciliation</td>
<td>20, 21</td>
</tr>
</tbody>
</table>
# Ideal Kiosk Solution Technical Elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>End User Authentication</td>
<td>• Not an issue because cash is presented</td>
</tr>
<tr>
<td>User Payment Authorization</td>
<td>• Not an issue because cash is presented</td>
</tr>
<tr>
<td>Source Payment Authorization</td>
<td>• Kiosk or cashier verifies cash presented</td>
</tr>
<tr>
<td></td>
<td>• Variable quality identifying payment targets. Boleto is rigorous. Qiwi is highly dependent on user correctly typing payment account ID.</td>
</tr>
<tr>
<td></td>
<td>• Need for common format to express Source payment Authorization</td>
</tr>
<tr>
<td>Merchant to Source Network</td>
<td>• Facilitates Merchant’s ability to scale to trust multiple payment sources</td>
</tr>
</tbody>
</table>
Virtual Currency Flows

**Strength:** Low fraud

**Challenge:** Adoption, Governmental Support

**Need:** Business guarantees and Reporting

<table>
<thead>
<tr>
<th>Phase</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invoicing</td>
<td>1...2</td>
</tr>
<tr>
<td>Payment</td>
<td>10...12</td>
</tr>
</tbody>
</table>
eWallets

• eWallet performs similar function to source bank
  • Holds balances
  • Authenticate user payment authorization
  • Generate source payment authorization

• Combine with other strategies to fund eWallet balance
  • Kiosk
  • Mobile
  • Conventional credit card
  • ACH
**Wallet Flows**

**End User**

1. [1] Purchase()
2. [2] GenerateInvoice()
3. [3] Redirection
5. [10] Authentication

**Merchant**

1. [1] Purchase()
2. [2] GenerateInvoice()
3. [3] Redirection

**Wallet Service**

- **Authentication**

**Source Bank**

1. [20] Transfer
2. [21] Cash Reporting

**Merchant Bank (dest.)**

- [21] Cash Reporting

**Strength:** Low fraud

**Challenge:** Regionally specific solutions, Abrupt UX

**Need:** Payment and Authentication Federation

<table>
<thead>
<tr>
<th>Phase</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invoicing</td>
<td>1...4</td>
</tr>
<tr>
<td>Payment</td>
<td>10...12</td>
</tr>
<tr>
<td>Reconciliation</td>
<td>20, 21</td>
</tr>
</tbody>
</table>
## Ideal Wallet Solution Technical Elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>End User Authentication</td>
<td>• Typically implemented by the wallet provider</td>
</tr>
<tr>
<td>User Payment Authorization</td>
<td>• Performed within wallet provider</td>
</tr>
<tr>
<td>Source Payment Authorization</td>
<td>• Wallet provider verifies funds availability</td>
</tr>
<tr>
<td></td>
<td>• Need for common format to express Source payment Authorization</td>
</tr>
<tr>
<td>Merchant to Source Network</td>
<td>• Facilitates Merchant’s ability to scale to trust multiple payment sources</td>
</tr>
</tbody>
</table>
Online Credit Card Flows - Actual

**Scope of Trust**

<table>
<thead>
<tr>
<th>Phase</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purchase</td>
<td>1...6</td>
</tr>
<tr>
<td>Cash to merchant</td>
<td>10, 11</td>
</tr>
<tr>
<td>Reconciliation</td>
<td>20, 21</td>
</tr>
<tr>
<td>Dispute</td>
<td>30+</td>
</tr>
</tbody>
</table>

**Strength**: Broad North American adoption, smooth UX

**Challenge**: Anti-Fraud and Dispute complexity & Cost

**Need**: Secure payment instructions
Ideal Banked Technical Solution

*principle: minimize scope of trust*

```
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Authentication Service</td>
</tr>
<tr>
<td>1</td>
<td>User-Authoizes-Payment</td>
</tr>
<tr>
<td>2</td>
<td>Bank-Authoizes-Payment</td>
</tr>
<tr>
<td>20</td>
<td>Cash Recon</td>
</tr>
<tr>
<td>30</td>
<td>Reporting</td>
</tr>
</tbody>
</table>

End User

Merchant

Source (Bank)

Destination (Bank)

Authentication Service

Tax and Financial Governance
```
## Ideal Banked Solution Technical Elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Notes</th>
</tr>
</thead>
</table>
| End User Authentication       | • Secure channel between end user and authentication service prevents replay  
                                 | • Authentication service could be delegated outside the bank, but must be trusted  
                                 | • Many banks have invested significantly in their own solutions already                                                        |
| User Payment Authorization    | • User states intent to make a payment (authorize).  
                                 | • Authorization specifies source, target merchant, invoice, quantity and time  
                                 | • Statement is tied back to secure authentication of the user  
                                 | • A single authorization statement could authorize multiple payments                                                         |
| Source [Bank] Payment Authorization | • Bank verifies validity of Payment Authorization, tied back to End User  
                                      | • Bank verifies and reserves availability of funds through credit or debit  
                                      | • Bank produces trustable statement of funds availability  
                                      | • Merchant may fulfill as soon as Source Payment Authorization is available                                                   |
| Merchant to Source Network    | • Facilitates Merchant’s ability to scale to trust multiple payment sources                                                              |
Bank Transfer

• Batch implementation
• Low transaction cost
• Two way transactions
  • Push – secure, like Kiosk Scenarios
  • Pull – trusts merchant, like North American Credit Card. Similar fraud risk, but currently less exploited because less accessible.
• Ideal flow applies
  • Automated push based on secure authorization
Bank Transfer Current

End User

[1] Show Invoice

[4] Fulfillment

[2] User-Authorizes-Payment

Merchant

[20] Cash Recon


Receiving Bank

[10] Transfer Credit or Debit

Sending Bank

[30] reporting

Tax and Financial Governance

[30] reporting

[30] reporting

[30] reporting
Ideal Bank Transfer

End User

[1] Show Invoice
[2] User-Authorizes-Payment
[0] Authentication

[4] Fulfillment

[2] User-Authorizes-Payment

Merchant

[20] Cash Recon
[20] Cash Recon Network

Source (Bank)

Fulfillment Source to Destination ONLY

[10] Transfer Source to Destination ONLY

[20] Cash Recon

Destination (Bank)

[30] Reporting

Authentication Service

[30] Reporting

Trust Network

Tax and Financial Governance
# Ideal Bank Transfer Solution Technical Elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Notes</th>
</tr>
</thead>
</table>
| End User Authentication         | • Secure channel between end user and authentication service prevents replay  
|                                 | • Same requirements as credit card                                   |
| User Payment Authorization      | • Same requirements as credit card                                   |
| Source [Bank] Payment Authorization | • Bank verifies validity of Payment Authorization, tied back to End User  
|                                 | • Bank verifies and reserves availability of funds through credit or debit  
|                                 | • Bank produces trustable statement of funds availability               |
|                                 | • Payment processing may still be batched                             |
| Merchant to Source Network      | • Facilitates Merchant’s ability to scale to trust multiple payment sources |
## Ideal Payment Solution: Secure Network

<table>
<thead>
<tr>
<th>Element</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invoice</td>
<td>• States target of funds</td>
</tr>
<tr>
<td></td>
<td>• Ties prices with product to be delivered</td>
</tr>
<tr>
<td>End User Authentication</td>
<td>• Secure channel between end user and authentication service prevents replay</td>
</tr>
<tr>
<td></td>
<td>• Authentication service could be delegated outside the bank, but must be trusted</td>
</tr>
<tr>
<td></td>
<td>• Many banks have invested significantly in their own solutions already</td>
</tr>
<tr>
<td>User Payment Authorization</td>
<td>• User states intent to make a payment. Statement tied back to authenticated user</td>
</tr>
<tr>
<td></td>
<td>• Authorization specifies source, target merchant, invoice, quantity and time</td>
</tr>
<tr>
<td></td>
<td>• A single authorization statement could authorize multiple payments</td>
</tr>
<tr>
<td></td>
<td>• Experience integrated with merchant.</td>
</tr>
<tr>
<td>Source [Bank] Payment Authorization</td>
<td>• Bank verifies validity of Payment Authorization, tied back to End User</td>
</tr>
<tr>
<td></td>
<td>• Bank verifies and reserves availability of funds through credit or debit</td>
</tr>
<tr>
<td></td>
<td>• Bank produces trustable statement of funds availability</td>
</tr>
<tr>
<td></td>
<td>• Merchant may fulfill as soon as Source Payment Authorization is available</td>
</tr>
<tr>
<td>Merchant to Source Network</td>
<td>• Facilitates Merchant’s ability to scale to trust multiple payment sources</td>
</tr>
<tr>
<td>Cash Reconciliation</td>
<td>• Matches multiple user payments into single bank deposits from sources</td>
</tr>
<tr>
<td>Reporting</td>
<td>• Transaction details from source banks, target banks and merchant</td>
</tr>
<tr>
<td></td>
<td>• Used in financial reporting and taxation</td>
</tr>
</tbody>
</table>