Security & Authentication in Acquiring Retail Payments

CPSS – World bank Forum On Retail Payments
Perugia, 19th March 2013

Gary Munro

consult hyperion
securing tomorrow's transactions

THE WORLD BANK
Working for a World Free of Poverty

Agenda

consult hyperion
securing tomorrow's transactions

- **Consult Hyperion**
- **Risks & Security in Retail Payments**
- **Authentication & Transaction Types**
- **Impact of Mobile**
- **Future Security & Authentication**

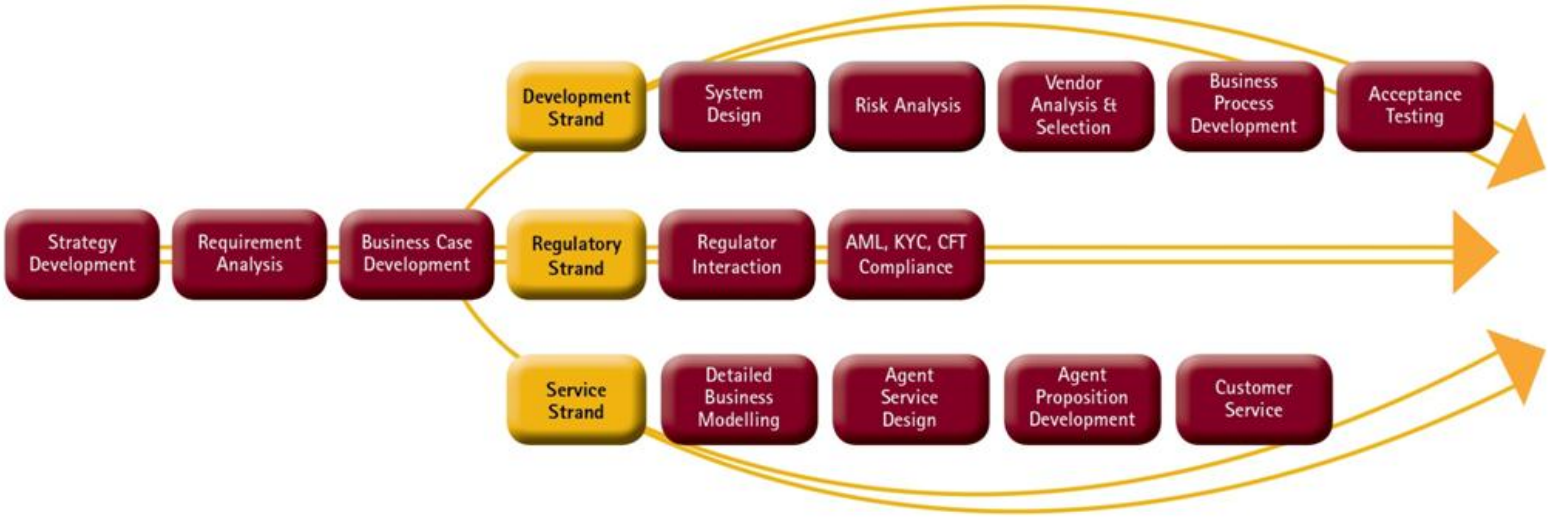
Introduction to

Consult Hyperion

consult hyperion
securing tomorrow's transactions

Consult Hyperion has helped some of the world's leading organisations to make the right technical and commercial choices within and around EMV, mobile, contactless and NFC-enabled payments and transit ticketing.

Consult Hyperion acts as the "Client's Friend", adding product strategy, technical, regulatory, compliance and information security expertise into project teams within organisations considering deploying innovative new payment or identity services.



Agenda

consult hyperion
securing tomorrow's transactions

Who Are Consult Hyperion?

Risks & Security in Retail Payments

- Transaction Risks
- Use of Authentication

Authentication & Transaction Types

Impact of Mobile

Future Authentication

Risks

consult hyperion
securing tomorrow's transactions

Cardholder

-**Payment integrity**

Merchant

-**Not being paid**

-**Liabilities**

- Technology
- Fraud
- Data Breach

-**Unauthorised account access**

-**Reputational risk**

Acquirer

-**Terminal Security**

-**Criminal Merchant**

-Card skimming

-Money laundering

-**AML fines**

Issuer

-**Security**

-3D secure not supported

-**Fraud**

Authentication in Card Payments

consult hyperion
securing tomorrow's transactions

Cardholder | Merchant | Acquirer | Issuer

Signature CVM

Offline Data Authentication

PIN CVM
Transaction Certificates
Signed Transactions
3D Secure

Agenda

consult hyperion
securing tomorrow's transactions

Who Are Consult Hyperion?

Risks & Security in Retail Payments

Authentication & Transaction Types

- Face to Face Retail Payments
- Online Retail Payments

Mobile POS

Future Authentication

Face to face retail payments

consult hyperion
securing tomorrow's transactions

Chip & Sig

- Merchant validation

Chip & PIN

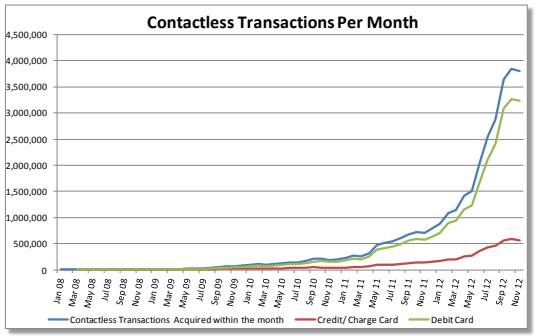
- Cardholder Authentication

Contactless

- No CVM
- Offline Transactions

Risk mitigation

- Transaction limit
- Transaction counters



Face to face payments NFC

Single issuer solutions

Secure Element based

Mobile App Passcode

Higher Value Payments

- Cardholder Device CVM

Mobile Wallets

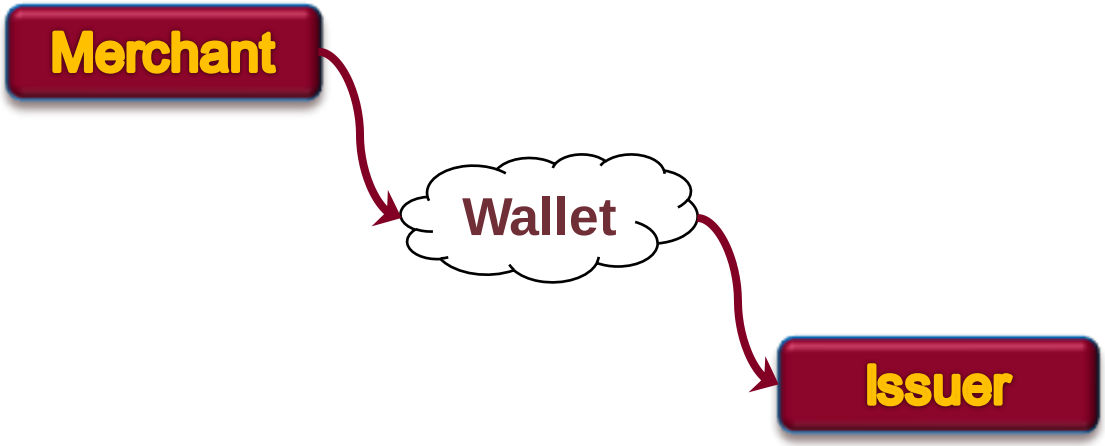
- Payment
- Loyalty

Complex ecosystem

Multiple TSMs

Face to face payments
Decoupled debit

consult hyperion
securing tomorrow's transactions



Debit transaction at Merchant

- Passcode
- CDCVM

Cloud based wallet

- User name password

CNP Transaction

- Negative interchange
- Monetisation of data

Online retail payments

consult hyperion
securing tomorrow's transactions

CNP / Card on File

- Rising Fraud
- 3DSecure
  - Password
  - Adaptive Auth – RBA / KBA

Online Wallets

- PayPal
- Issuer based
- Fees
- Password based Access

V.me by Visa

PayPal

BUY WITH MasterPass

Agenda

consult hyperion
securing tomorrow's transactions

Who Are Consult Hyperion?

Risks & Security in Retail Payments

Authentication & Transaction Types

Mobile

- Growing the merchant base

Future Security & Authentication

Mobile POS

consult hyperion
securing tomorrow's transactions

Opportunity to significantly grow Merchant base

- Mobile merchant
- Sole trader
- Merchant On-boarding

Allows development of low cost card acceptance infrastructure

- Secure
- Effective across large geographies
- Mobile telecoms infrastructure

Mobile Money

consult hyperion
securing tomorrow's transactions

Mobile centric banking

- Money transfers
- P2P
- Direct payments

Moving into retail payments space

- Mobile front end to ACH payments
- Protecting the mobile front end

Fundamo

M-PESA

Pingit

Agenda

consult hyperion
securing tomorrow's transactions

Who Are Consult Hyperion?

Risks & Security in Retail Payments

Authentication & Transaction Types

Mobile

Future Security & Authentication

- The something present transaction

Future Authentication

consult hyperion
securing tomorrow's transactions

Strong Authentication has typically involved the use of hardware tokens:

- Smart Cards
- One time password tokens

These are costly to issue and manage and can be inconvenient.

Technology solutions:

- Trusted Execution Environments
- Identity Protection Technology

FIDO alliance

- Multi-solution

There is therefore considerable interest in new authentication techniques that do not require specific secure hardware devices.

Future Authentication

consult hyperion
securing tomorrow's transactions

Risk based authentication: Uses contextual information, such as transaction and session details, compared against previous behaviour to provide a risk-based score.

Knowledge based authentication: Uses previously recorded challenge / response questions. Typically the questions selected for an individual are random taken from a large set of possible questions to mitigate phishing and guessing attacks.

Voice Biometrics: This is particularly relevant in the context of the mobile channel and can be combined with KBA.

Location: Location (derived from network or GPS) is another tool that can be used to reduce risk. Location is not usually consideration an authentication factor per se.

Future Authentication

consult hyperion
securing tomorrow's transactions

Device Fingerprinting: Device information, e.g.

- serial numbers
- software versions
- hardware clock skew

used to confirm services are accessed from known devices. This does not authenticate the consumer, but is an addition tool to reduce risk.

Keystroke dynamics: Process of continuously monitoring the manner and rhythm in which an individual types characters on a keypad. Most interestingly it turns authentication from being a one-time event to be a continuous process. There are however potential legal issues, plus security issues due to the technique being very similar to spyware.

Future Authentication

consult hyperion
securing tomorrow's transactions

Conclusion:

Level of authentication at POS is dependant upon the risk profile.

None of the above techniques is a panacea. Instead there are a range of authentication techniques that may be used depending on the context, channel and level of assurance required for a particular transaction.

In card payments, we have a polarised view that either a transaction is:

- Card Present (strong authentication)
- Card Not Present (weak authentication)

Technology introduce the possibility of intermediate levels of authentication:

- The **Something Present** transaction.

Security & Authentication in Acquiring Retail Payments

consult hyperion
securing tomorrow's transactions

Thank you

For Further Information

consult hyperion
securing tomorrow's transactions

About Consult Hyperion

www.chyp.com

gary.munro@chyp.com

+44 1483 301 793

About Mobile Payments

twitter @chyppings

browse http://www.chyp.com

listen http://www.tomorrowstransactions.com

comment http://www.digitalmoneyforum.com/blog