

RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: HT-W01

How Secure are Contactless Payment Systems?

Matthew Ngu

Engineering Manager
RSA, The Security Division of EMC

Chris Scott

Senior Software Engineer
RSA, The Security Division of EMC

CHANGE

Challenge today's security thinking



Apple Pay



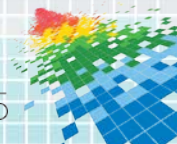
Visa payWave



paypass™

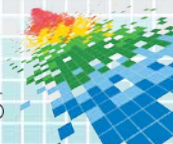


Google wallet

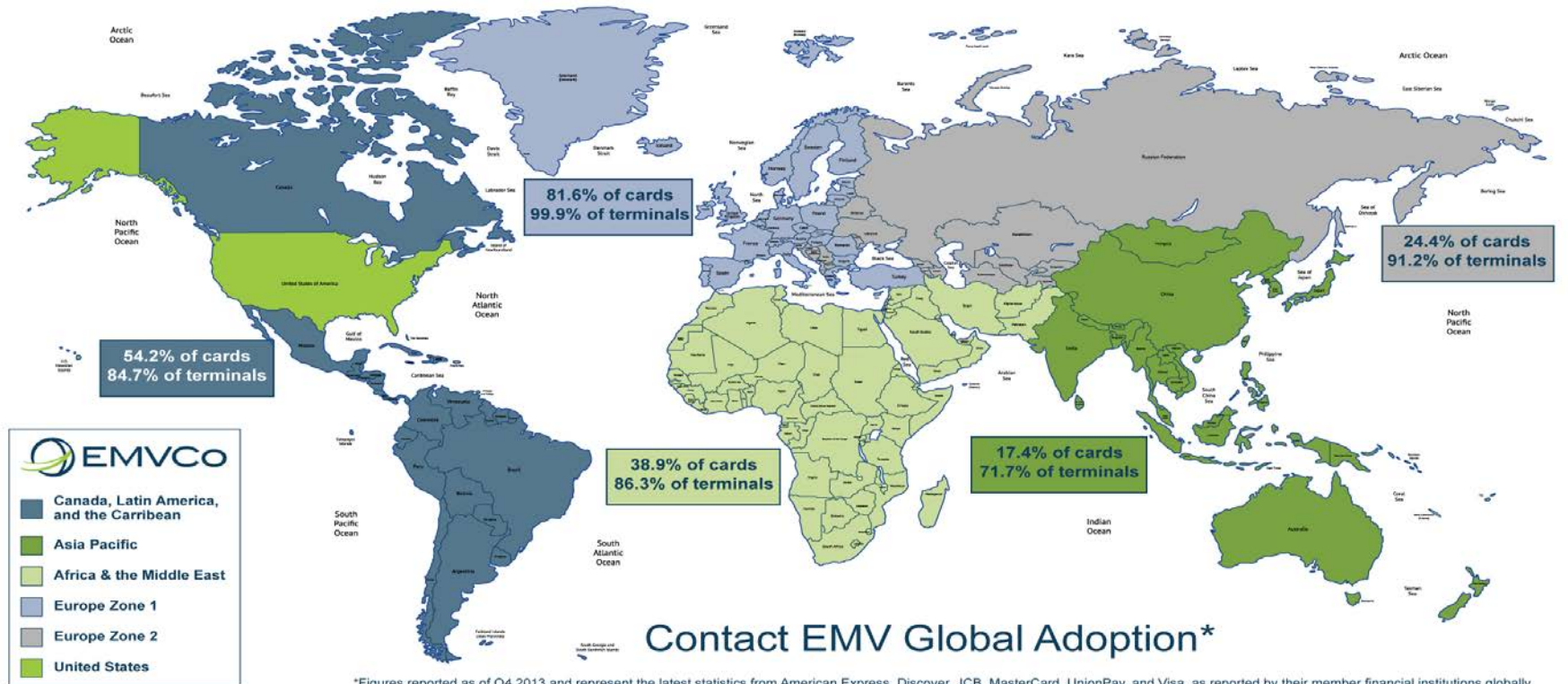


Some threat scenarios

- ◆ Can an attacker stand behind me and charge my card?
- ◆ Can an attacker read my EMV card?
- ◆ Can an attacker mount a high power reader in a van?
- ◆ Replay attacks?
- ◆ Can you think of anything else?

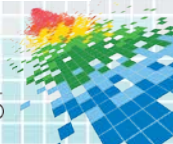


Global Adoption



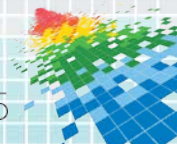
Contact EMV Global Adoption*

*Figures reported as of Q4 2013 and represent the latest statistics from American Express, Discover, JCB, MasterCard, UnionPay, and Visa, as reported by their member financial institutions globally. Figures do not include data from the United States. Figures are reported by region and do not imply country-by-country statistics.



Some US Statistics

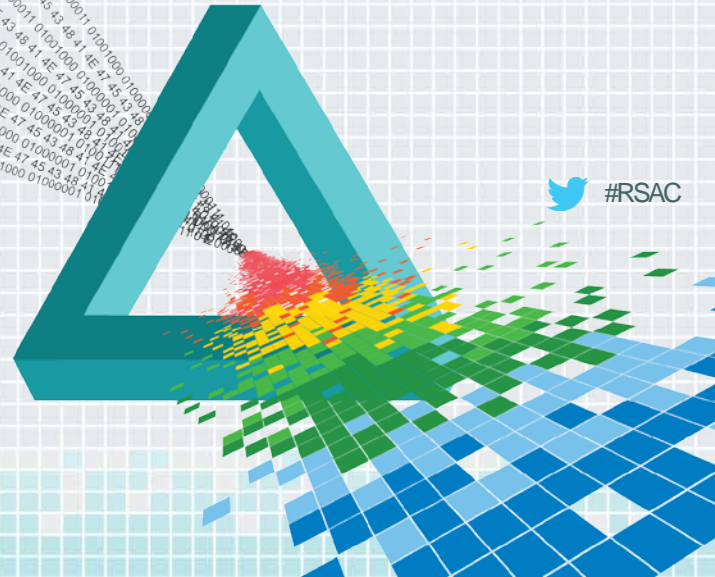
- ◆ 0.03% of transactions are EMV.
- ◆ 50,000 unique merchant terminal locations processed EMV transactions in 2014, compared to an estimated 12 million terminals that didn't do a single EMV transaction.
- ◆ Apple Pay and Google Wallet are currently only available in the US.
- ◆ To the end of November 2014, Apple Pay accounted for 1.7% of mobile payments whilst Google Wallet had a 4% share.
- ◆ Apple: \$2 of every \$3 spent in contactless transactions in the US in the lead up to Christmas were made via Apple Pay.



RSA[®]Conference2015

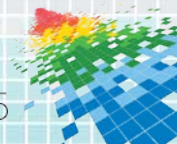
San Francisco | April 20-24 | Moscone Center

How does it work?



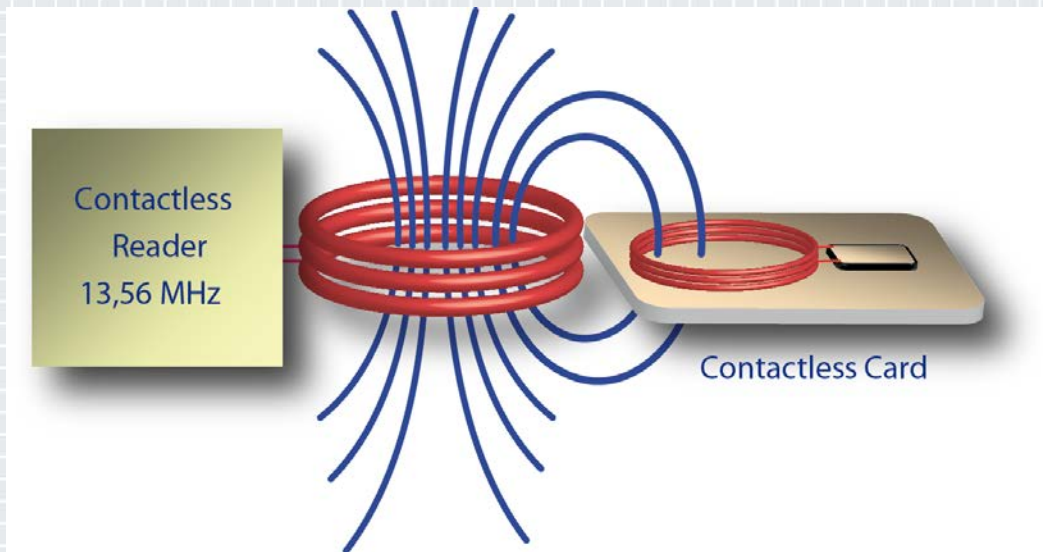
How does it work?

- ◆ Contactless Cards
- ◆ VISA PayWave / MasterCard PayPass
- ◆ Google Wallet
- ◆ Apple Pay

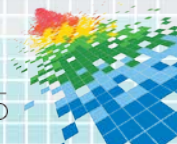


How does it work? Contactless Cards

Contactless cards use Near Field Communications (NFC) to send and receive data from the terminal using inductive coupling.



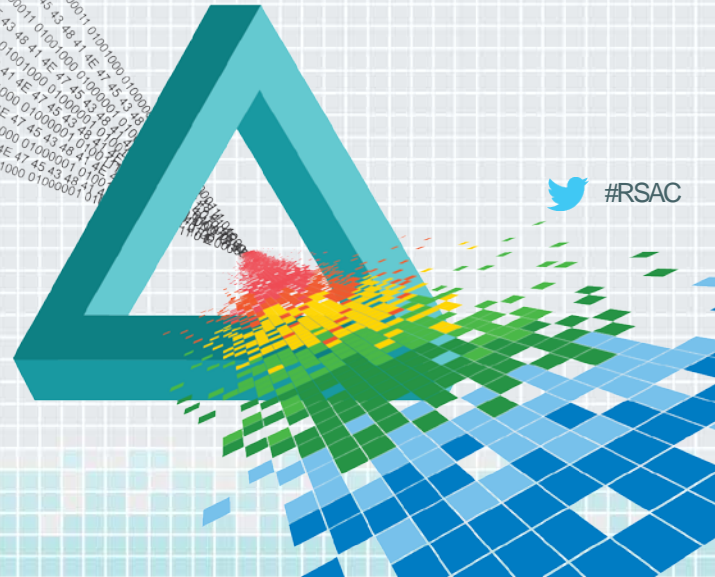
Source: rfid-handbook.de



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

How does it work? PayWave / PayPass



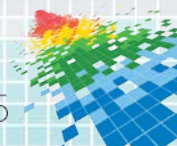
How does it work? PayWave / PayPass

Wait for merchant to enter amount.



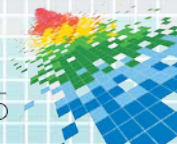
How does it work? PayWave / PayPass

Reader uses NFC to send and receive information with your card.



How does it work? PayWave / PayPass

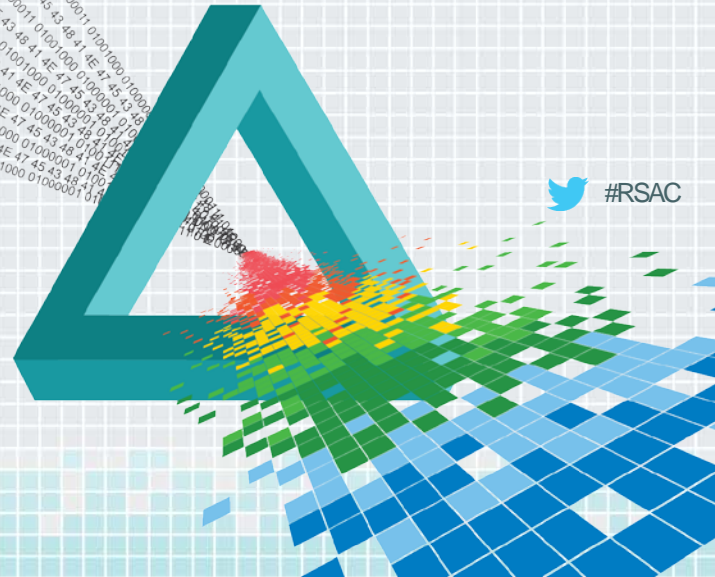
Dynamic data unique to every purchase protects your transaction data.



RSA[®]Conference2015

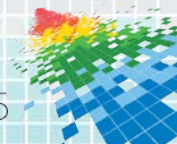
San Francisco | April 20-24 | Moscone Center

How does it work? Google Wallet



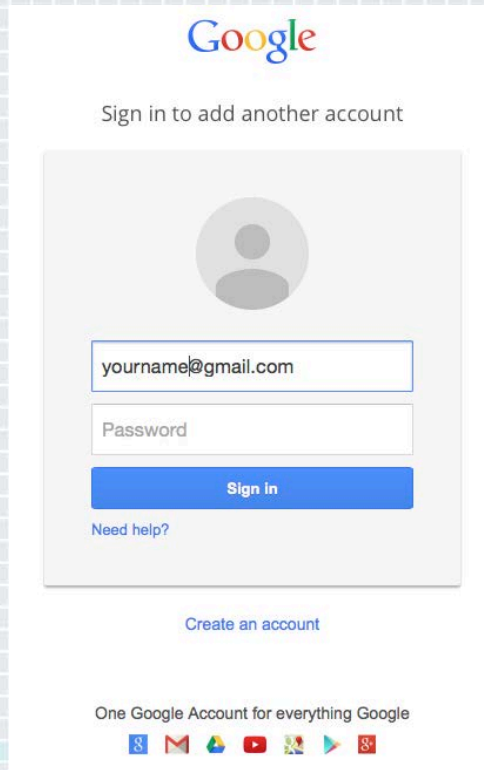
 #RSAC

How does it work? Google Wallet Prerequisites

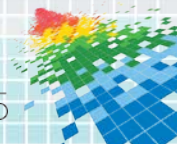


How does it work? Google Wallet – Setup

Login to your Google account.

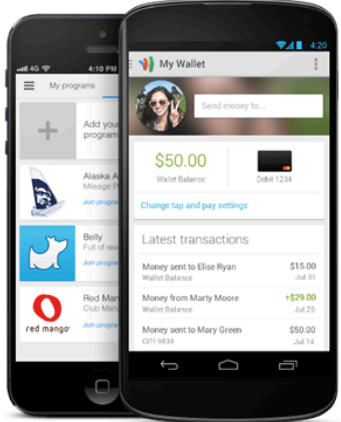


The screenshot shows the Google sign-in interface. At the top is the Google logo. Below it is the text "Sign in to add another account". A large grey circle with a person icon represents the user's profile. Below the profile icon are two input fields: the first contains "yourname@gmail.com" and the second is labeled "Password". A blue "Sign in" button is positioned below the password field. Underneath the button is a link that says "Need help?". At the bottom of the sign-in area is a link that says "Create an account". Below the sign-in area, there is a line of text: "One Google Account for everything Google". At the very bottom, there is a row of icons for various Google services: Search, Gmail, Google Drive, YouTube, Maps, and Google+.



How does it work? Google Wallet – Setup

Enter your credit card details on wallet.google.com.




Send money, carry less, save more

Send money wherever you go
Send money to friends and family using the Google Wallet app, site, or by attaching money in Gmail. [Learn more](#)

All your loyalty cards and offers in one place
Redeem great offers with Google Wallet from your favorite businesses to save when you shop. [Learn more](#)

Set up your Google Wallet

NAME AND HOME LOCATION

 Australia (AU) ▼

Chris Scott |

PAYMENT METHOD

Credit or debit card

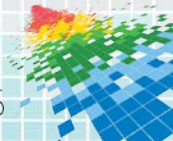
Card number

Expiration date / Security code

Billing address

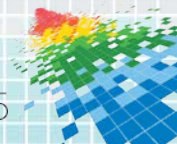
Billing address is the same as name and home location

Add a payment method later



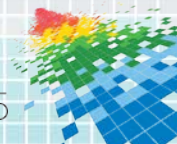
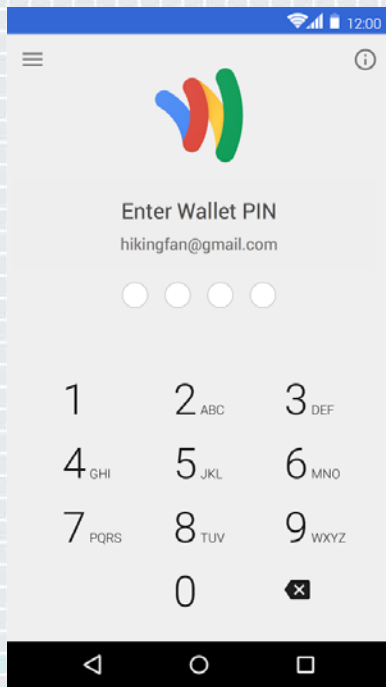
How does it work? Google Wallet – Setup

Verify your identity by providing Personally Identifiable Information (PII) such as name, address, date of birth, last four digits of Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN).



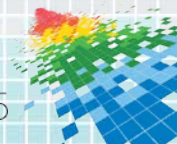
How does it work? Google Wallet – Setup

Create your Wallet PIN (different to phone PIN).



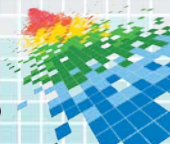
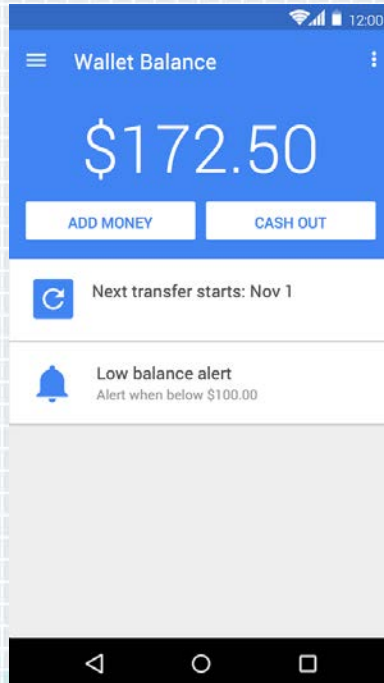
How does it work? Google Wallet – Setup

A MasterCard®-branded virtual prepaid debit payment card product, the Google Wallet Virtual Card, issued by Bancorp Bank will be installed on your phone.



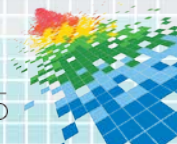
How does it work? Google Wallet - Payments

Add money to your Wallet (website or mobile app).



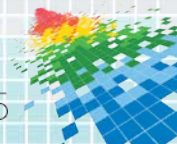
How does it work? Google Wallet - Payments

Bring the phone up to an NFC-enabled terminal.



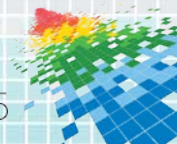
How does it work? Google Wallet - Payments

Phone will ask you to authenticate the payment with Wallet PIN.



How does it work? Google Wallet - Payments

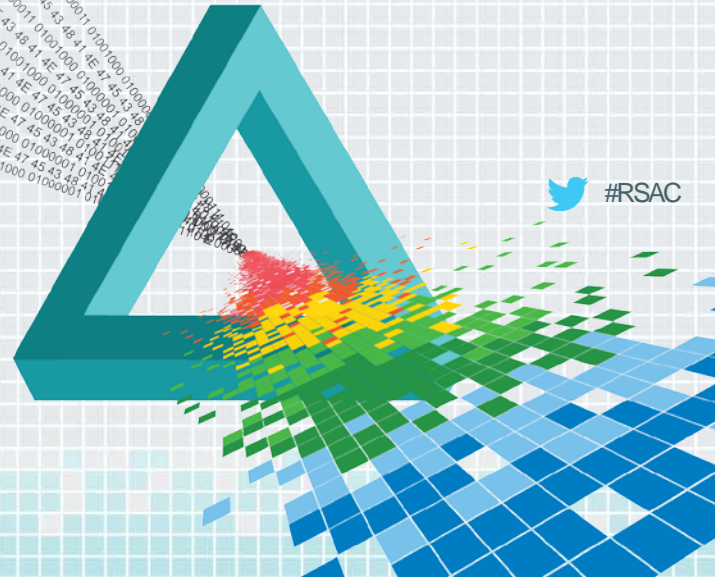
- ◆ Phone transmits the Google Wallet Virtual Card information to the merchant's terminal, not your real credit card information stored on Google's servers.
- ◆ Transaction completed as normal using credentials for current payment only.



RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

How does it work? Apple Pay



 #RSAC

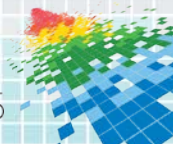
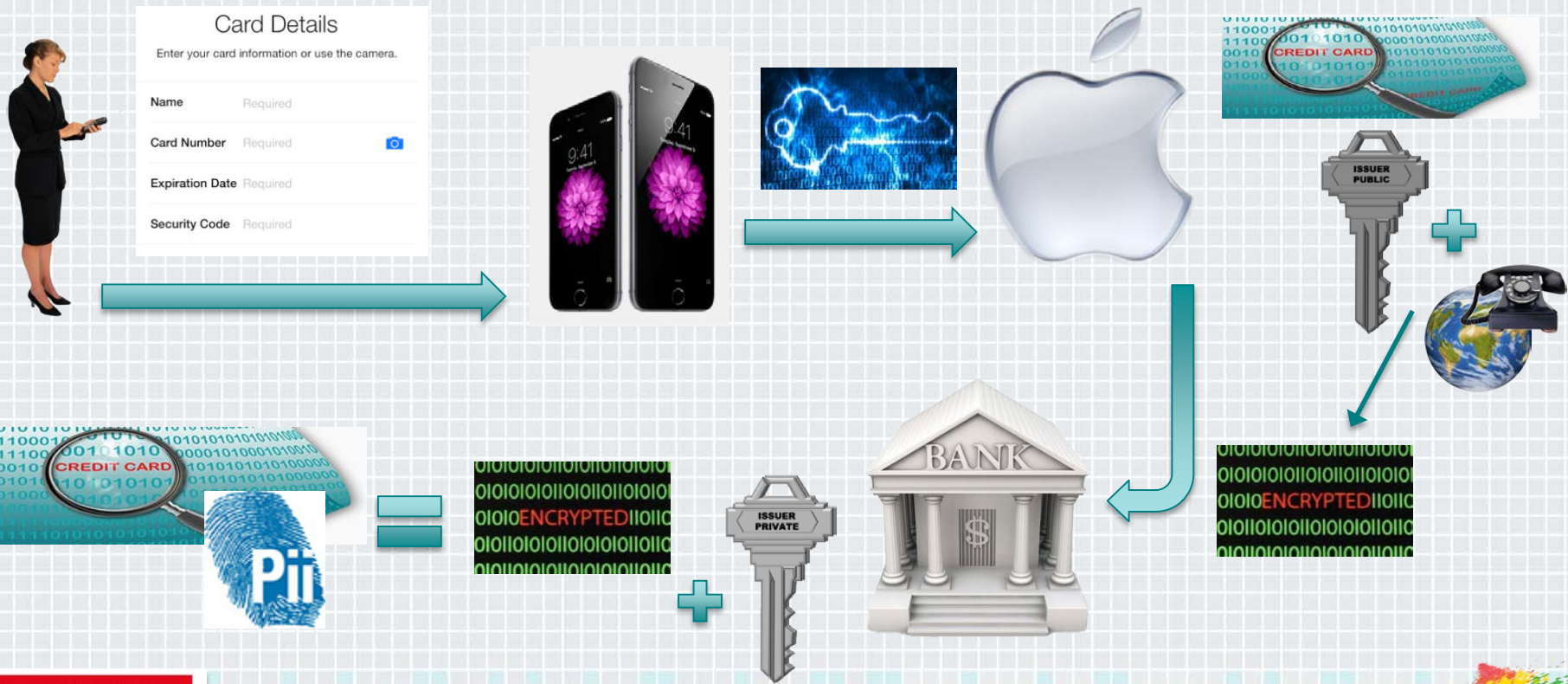
How does it work? Apple Pay Prerequisites



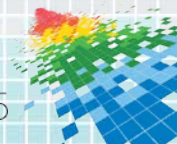
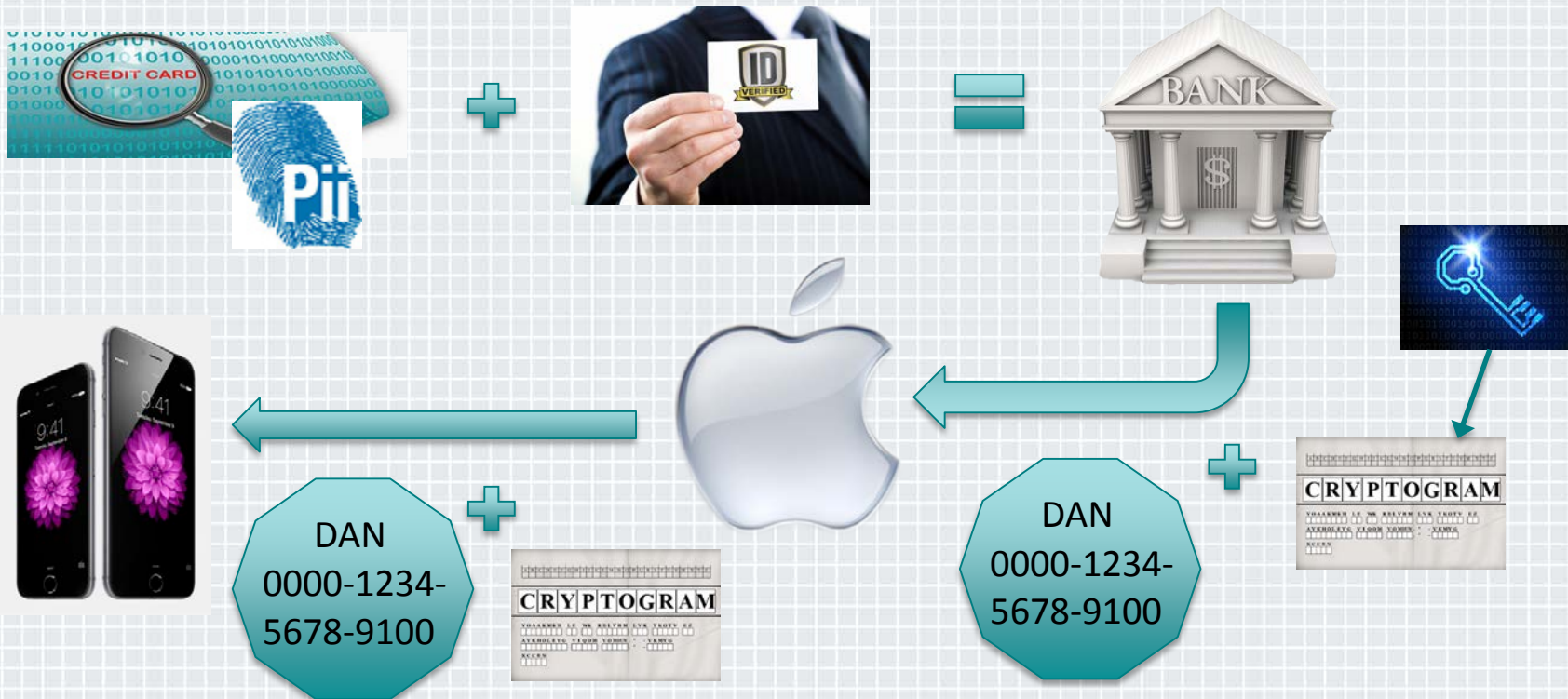
or



How does it work? Apple Pay - Setup

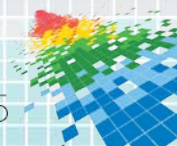


How does it work? Apple Pay - Setup continued

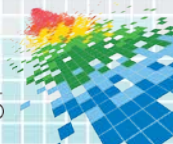


How does it work? Apple Pay – Payments

- ◆ Bring the phone or watch up to an NFC-enabled terminal.



How does it work? Apple Pay – Payments



How does it work? Comparison

Contactless Implementation	Stores Primary Account Number (PAN)	Customer Authentication
Pay Wave/ Pay Pass	Yes, in secure element on card	None below threshold amount, PIN or signature above threshold amount
Google Wallet	Yes, on Google servers in cloud	PIN (different from phone unlock PIN)
Apple Pay	No, PAN only required during registration	iTouch or Passcode



RSA[®]Conference2015

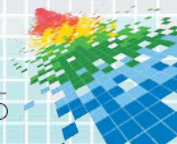
San Francisco | April 20-24 | Moscone Center

Security Analysis

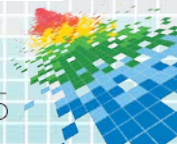
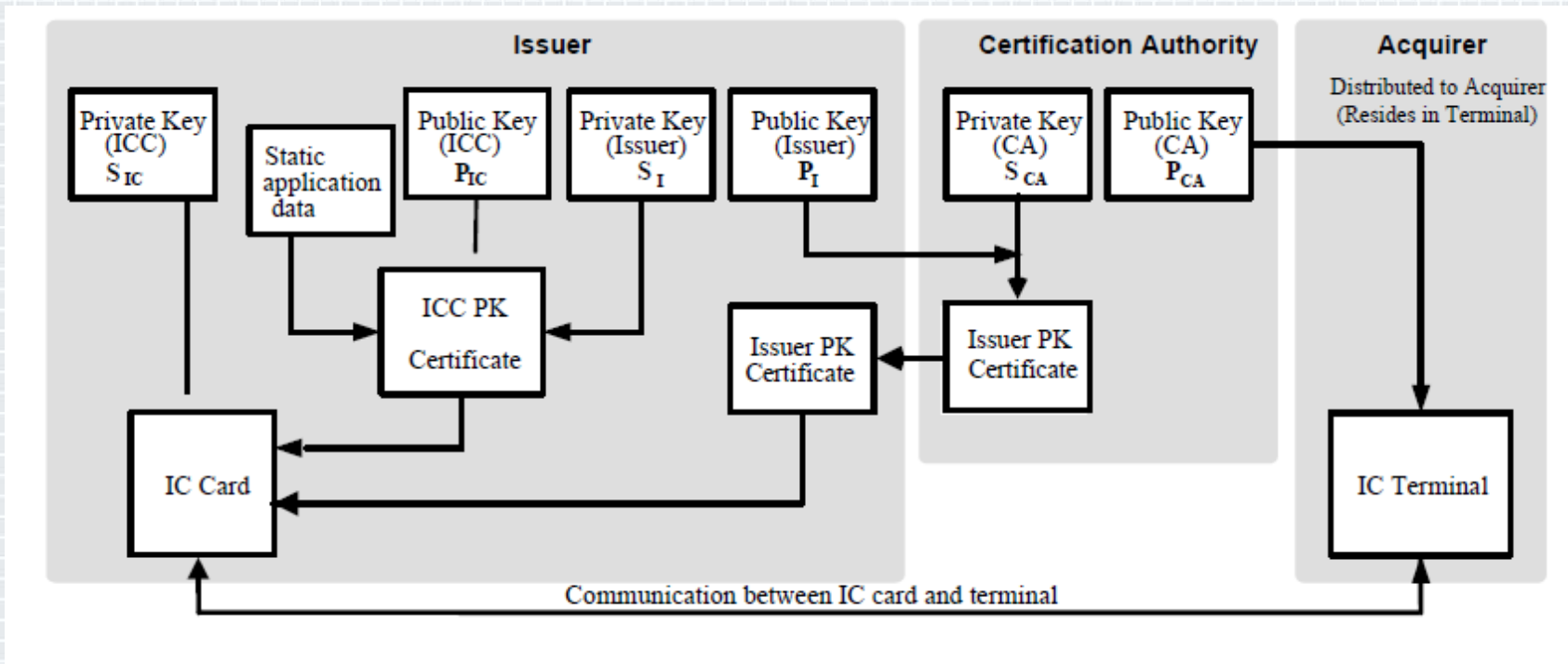


What are the Security Features?

- ◆ Secure Element, Trusted Execution Environments.
- ◆ EMV for preventing card fraud.

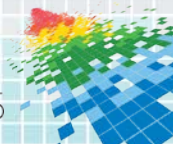


From EMVCo: PKI



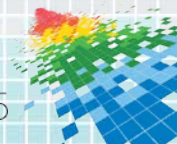
What is protected with EMV?

- ◆ Authenticity of the cards (protects against counterfeit cards).
- ◆ Payment transactions by adding dynamic data unique to each transaction.
- ◆ PINs and keys stored in secure part of card (TEE or SE). PIN encrypted between PIN pad and card.
- ◆ A standard is only as good as its implementation.



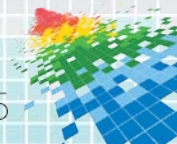
What are the Security Features?

- ◆ Payment tokens for protecting PAN.



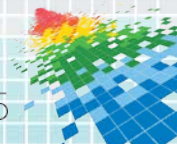
What is protected with tokenisation?

- ◆ PAN and card expiry date are protected.
- ◆ Viability of stolen data is minimised by limiting the domain in which the token is valid.
- ◆ Merchant liability is limited by not processing or storing actual cardholder PAN.



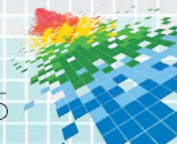
What are the Security Features?

- ◆ Multi factor authentication during payment transaction (Wallet and Pay).
- ◆ Contactless card does not need to leave your hand for payment.



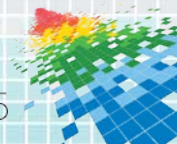
What are the weak points and threats?

- ◆ Stolen EMV contactless card can be used to make small payments (below PIN limit).
- ◆ Malware on the device or reader.
- ◆ Stolen card details can *possibly* be registered with electronic wallets and then used – depending on ID&V process of Issuer.
- ◆ Static authentication data.



The threat scenarios again...

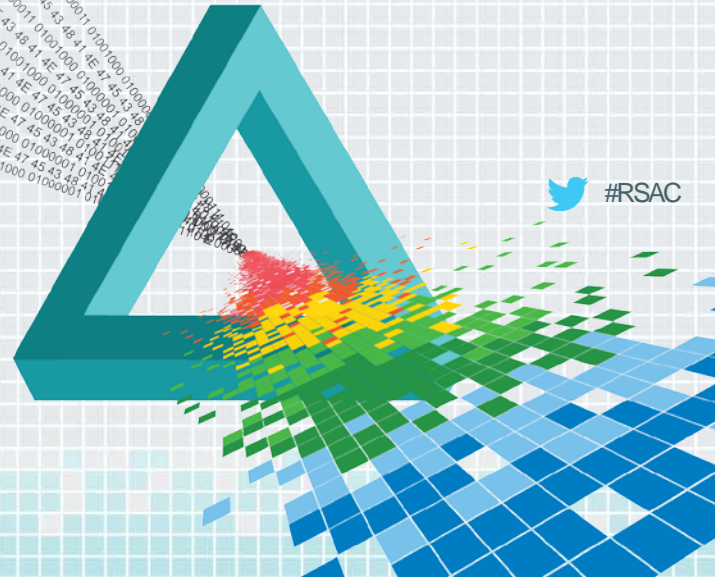
- ◆ Can an attacker stand behind me and charge my card different amounts in quick succession?
- ◆ Can an attacker read my EMV card and encode PAN on a mag stripe card?
- ◆ Can an attacker mount a high power reader in a van?
- ◆ Replay attacks?



RSA[®]Conference2015

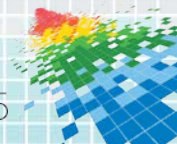
San Francisco | April 20-24 | Moscone Center

How can I APPLY what I
have learned?



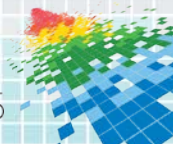
If I am a Merchant, Bank, Processor...

- ◆ Use a combination of EMV and (back-end) tokenisation.
- ◆ Realtime authorization, ie no offline transactions.
- ◆ Phase out mag stripe cards – data from chip card can be transferred onto mag stripe.
- ◆ Do not send activated cards by mail.
- ◆ Monitor usage patterns and implement other fraud detection measures.
- ◆ Secure issuer and card private keys; card MAC master keys. Isolate from corporate network and include physical interlocks for access.
- ◆ Biometric authentication on card or just simple button that has to be pressed to enable chip to be energized.



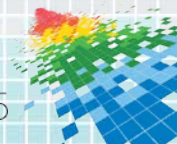
If I am a Consumer?

- ◆ Do metal card sleeves really work?
- ◆ Tell your bank when you travel.
- ◆ Check your statements regularly.
- ◆ Protect your PIN.
- ◆ Enable iPhone “locate my phone” feature.
- ◆ Set limits on transactions.



Summary

- ◆ EMV Contactless, Google, Apple Pay
- ◆ Contactless payments systems are not fraud-proof.
- ◆ But more secure than mag stripe-based systems.
- ◆ More/as convenient, more secure than cash.
- ◆ Mostly simple measures can be taken to improve security.
- ◆ Novel approaches are required to improve convenience and bring down cost of implementation.



Any Questions?

- ◆ Matthew Ngu: matthew.ngu@rsa.com
- ◆ Chris Scott: chris.scott@rsa.com

