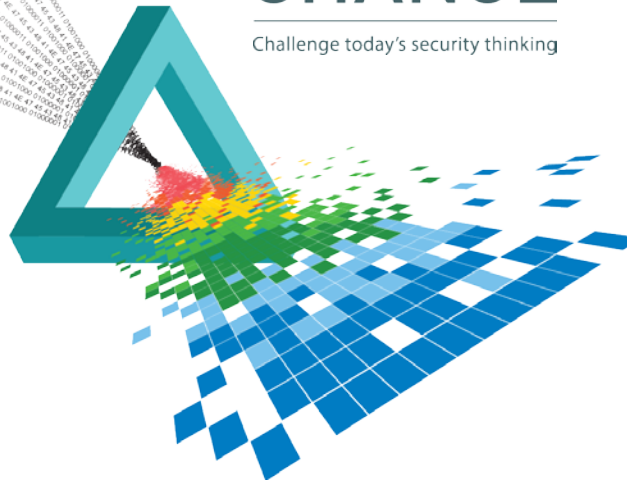
RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking



SESSION ID: SPO-W09B

How Next Generation Trusted Identities Can Help Transform Your Business

Chris Taylor

Senior Product Manager
Entrust Datacard
@Ctaylor_Entrust

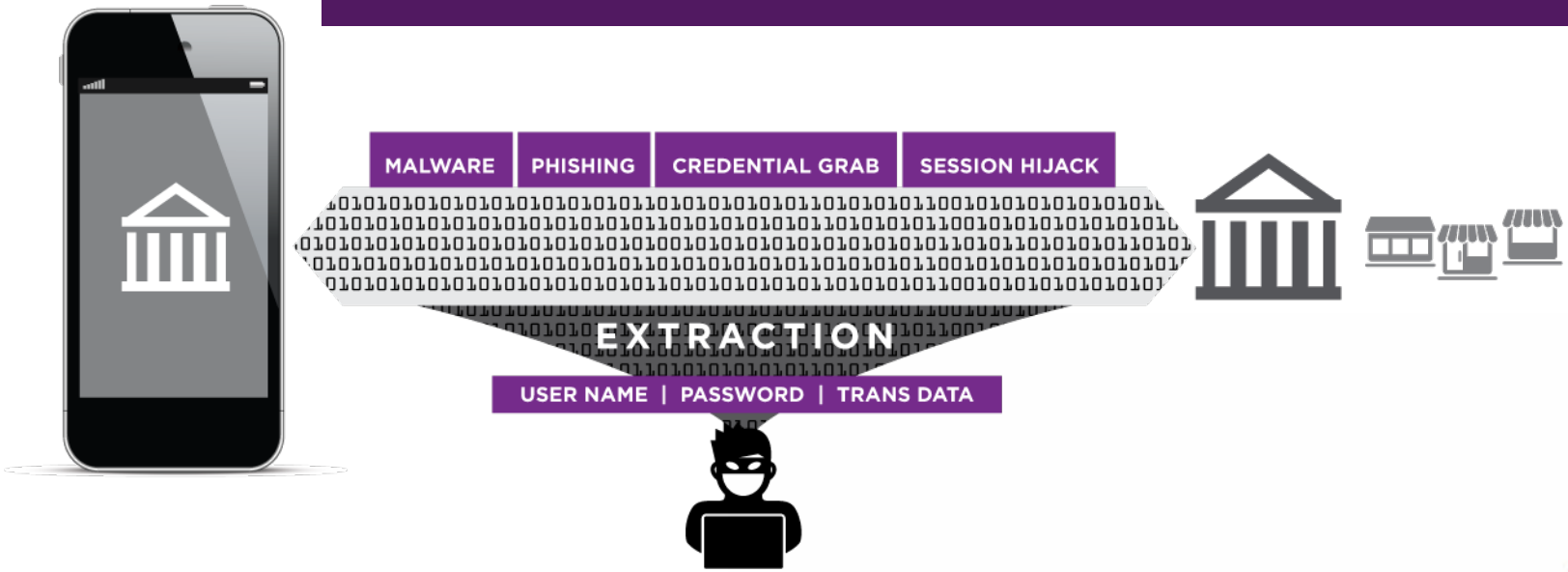
Identity underpins our PERSONAL life

Entrust Datacard

Identity underpins our WORK life

So, what's the problem?

TOO MANY IDENTITIES, TOO MANY PASSWORDS



Mega-breaches target password weaknesses

POLITICS CYBERCRIME

This Could Be the End of User Name and Password

Massimo Calabresi @calabresim | Feb. 9, 2015

Anthem, J.P. Morgan hacks could lead to tougher online security.

A top New York State regulator is "very likely" to impose new cyber-security rules on much of the banking and insurance industries after high profile cyber-intrusions at Anthem and [redacted] tell TIME.

Scott Eels—Bloomberg/Getty Images

Benjamin Lawsky superintendent of the New York State Department of Financial Services, speaks during a Bloomberg Television interview in New York on Nov. 24, 2014.

The move could spell the beginning of the end for a decade-long debate among state and federal regulators over whether to require companies to go beyond the simple user name and password identity checks required

Criminals used a third-party vendor's user name and password to enter the perimeter of [redacted] network. These stolen credentials alone did not provide direct access to the company's point-of-sale devices.
The hackers then acquired elevated rights that allowed them to navigate portions of

Early investigations in the [redacted] case suggest foreign hackers used the user name and password of a company executive to get inside

How Hackers Infiltrated Banks

Since late 2013, an unknown group of hackers has reportedly stolen $300 million — possibly as much as triple that amount — from banks

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Alert (TA14-212A)
Backoff Point-of-Sale Malware

Original release date: July 31, 2014 | Last revised: August 27, 2014

PoS malware dubbed "Backoff" which has been discovered exploiting businesses' administrator accounts remotely and exfiltrating consumer payment data.

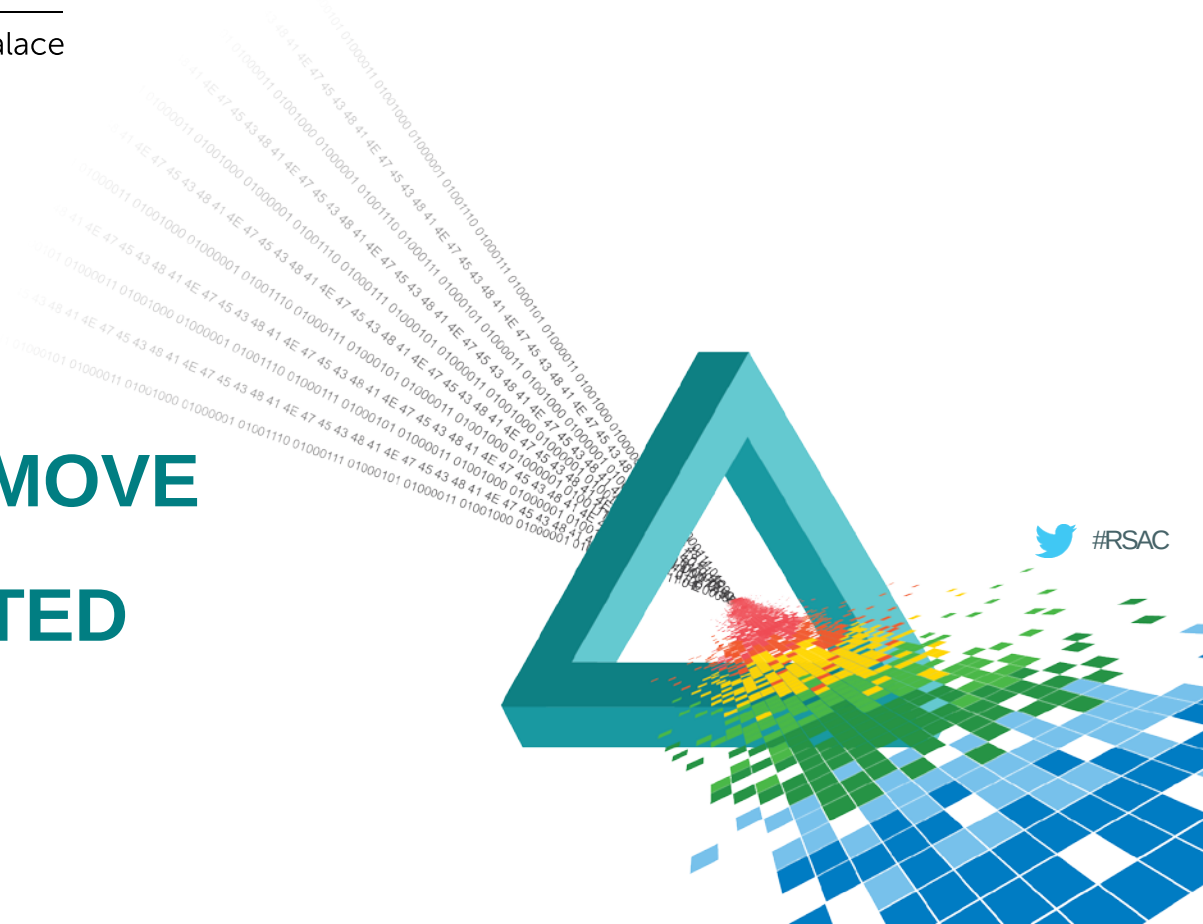
Hackers obtained system administrators' passwords to pull of the mega-hack against [redacted] servers, according to reports. This will come as no surprise to IT professionals.

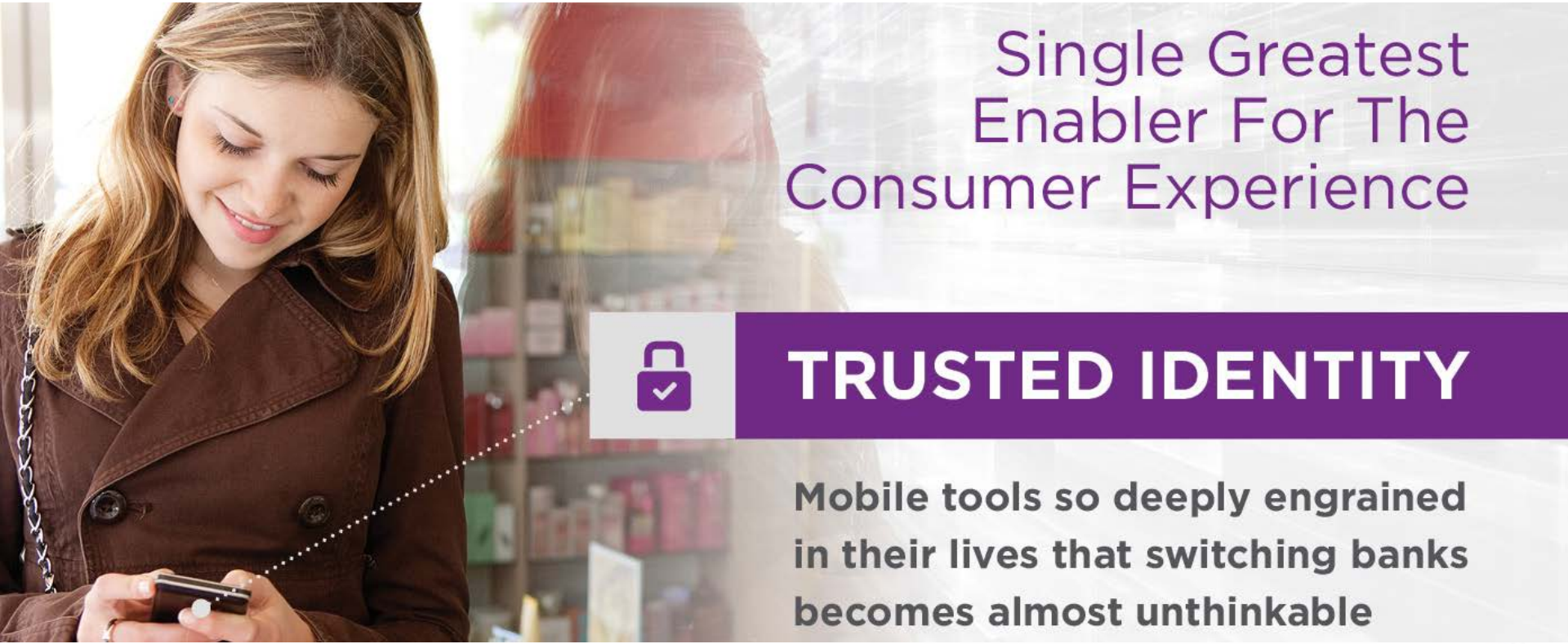
Solving the core issue

BUILDING A TRUSTED DIGITAL IDENTITY & EMPOWERING MOBILITY

Achieving Usability & Security

SO HOW DO WE MOVE TOWARDS TRUSTED IDENTITES?





Single Greatest Enabler For The Consumer Experience

TRUSTED IDENTITY

Mobile tools so deeply engrained in their lives that switching banks becomes almost unthinkable

Benefits of a Mobile-Based Trusted Identity

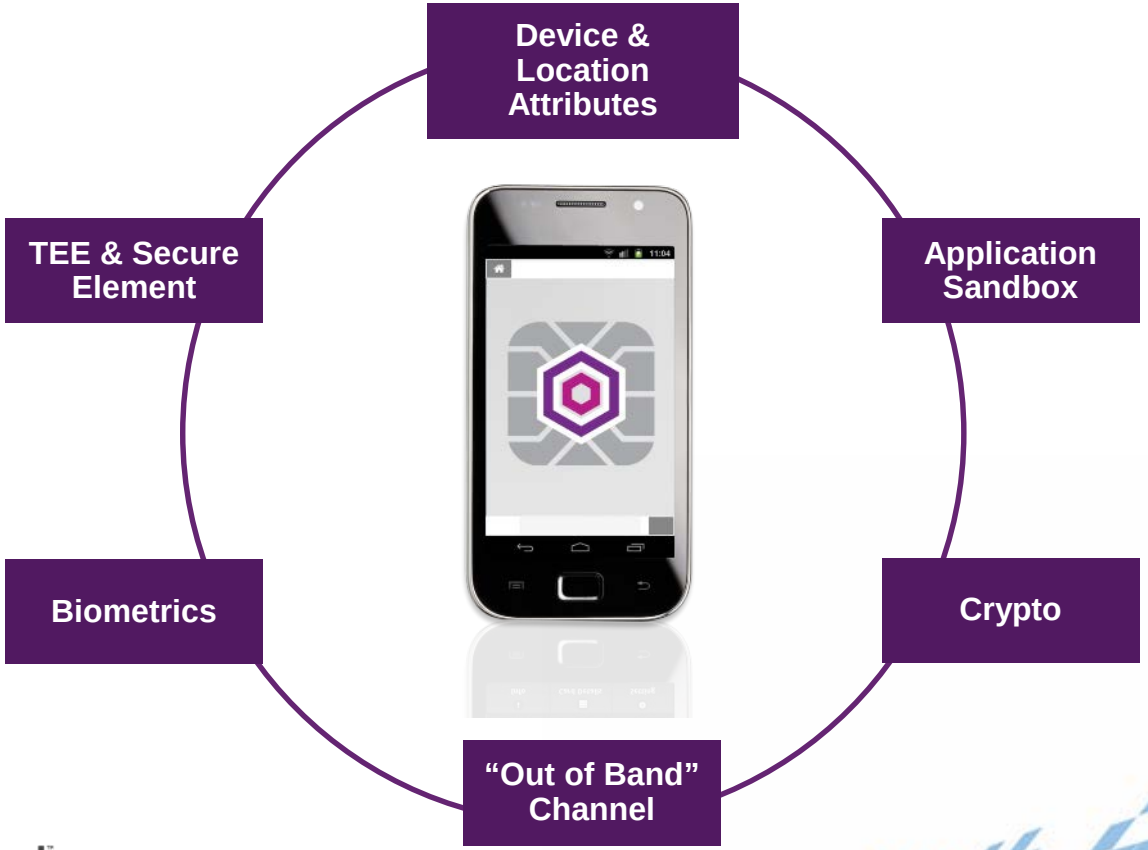
Protect the business & our customers

New Services / better processes

Improve productivity & UX

Reduce IT cost and complexity

Powerful Native Features Enhance Security



Transparent/Low friction security that adapts to risk

RISK VECTORS

Jail broken phones
Lost/stolen phones
Rogue applications
Breached credentials
Impersonating devices
Banking trojans/malware
CNP fraud

SECURITY LAYERS		
OPERATING SYSTEM		Jailbreak detection Sandboxing Malware detection Trusted execution environment (TEE)
DEVICE		Device fingerprinting Geo-location Device ID Protected application access
CHANNEL		Mutual SSL authentication
USER		Adaptive authentication Embedded digital ID Push authentication
TRANSACTION		Push transaction signing Transaction signing tokens

MOVING TOWARDS THE PASSWORD-LESS ENTERPRISE

Use Cases


APPROVALS
& SIGNING
x 010
PHYSICAL
ACCESS
TRANSACTION
VERIFICATION
11:04
LOGICAL
ACCESS
FEDERATE
TO SAAS
VPN

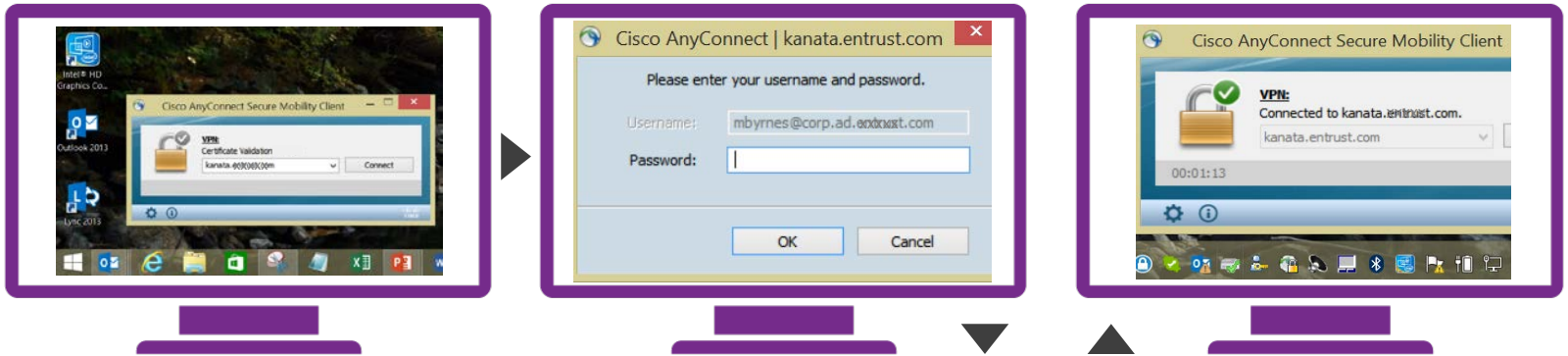
VPN Authentication

PROBLEM:

- Hardware tokens are secure but not user friendly
- IT provisioning and logistics is complex
- Expensive, limited use technology

- Mobile Push Authentication simplifies 2FA for users and IT

Mobile Push for VPN authentication



- No hardware tokens to carry
- Better user experience
- Easy user provisioning
- Certificate approach is password-less

Physical / logical access

PROBLEM:

- Passwords are painful to use and insecure
- Smart cards are expensive and complex to deploy
- Building access cards are insecure

SOLUTION:

- Transform mobile devices into multi-purpose virtual smart cards

Windows SCLO

Traditional Smart Card

Windows SCLO

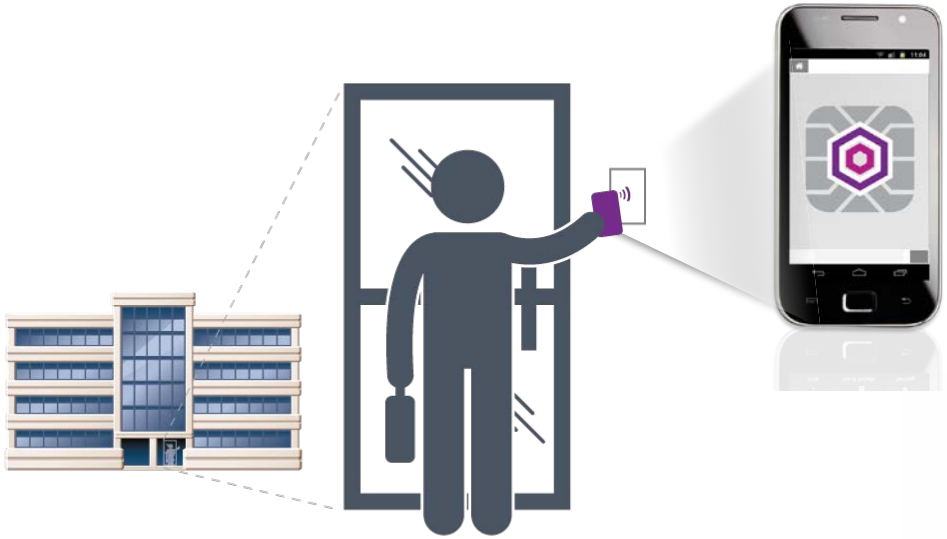
Traditional Smart Card

***Mobile* Virtual Smart Card** → **Virtual smart card reader**

Convenient “auto-detect”

Secure “auto-logout”

Physical access



NFC-based communication to PACs

Convenient / always in hand

Strong Authentication

- Can’t be “skimmed”
- PKI certificate-based
- Biometrics
- PIV / Derived Credential compliant

On-the-go approvals

PROBLEM:

- Constant need to improve business process (employees and customers)
- Many processes require formal approvals / signatures
- Traditional digital signing is complex to deploy and have a poor UX

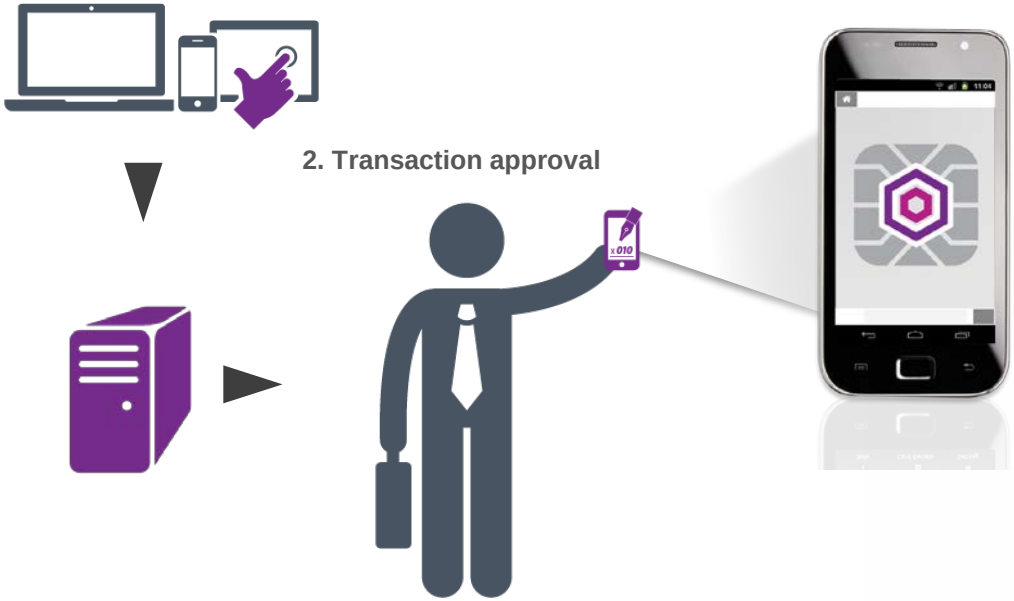
SOLUTION:

- Use mobile for anywhere, anytime digital signing

Digital Signature Using Mobile

1. Transaction origination

- Doctor writing a prescription
- Banker offering a loan
- Employee submitting a requisition



Enable Business Transformation

- Convenient / user friendly process
- Improve internal efficiency
- Improve consumer experience

Summary

Identity is critical to today's connected enterprise

Dated authentication methods fall short

- Security
- Usability
- Cost / IT management

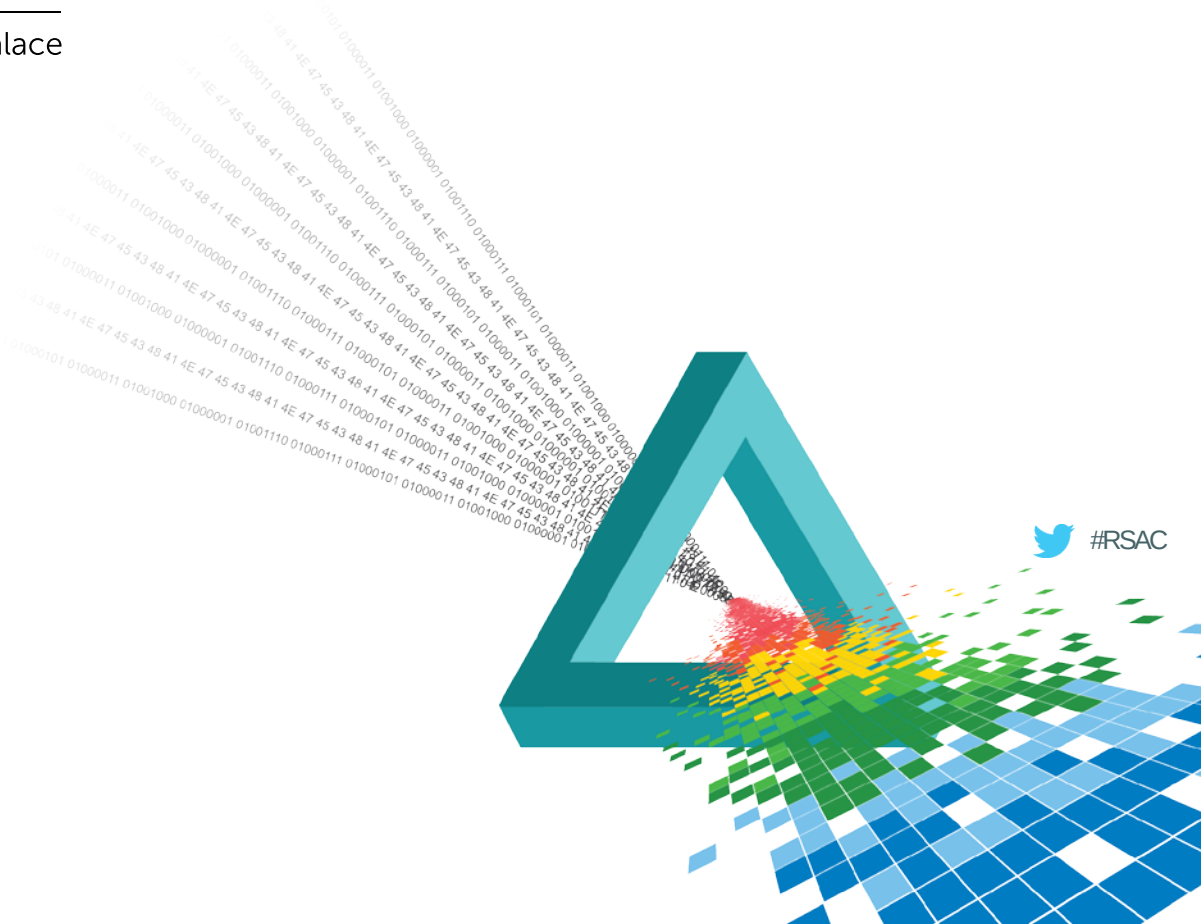
Mobile trusted identities transform business and the password-less enterprise

- More secure
- More convenient
- Truly multi-purpose

Apply what you have learned today

- Next week you should:
  - Identify opportunities and use cases in your organization whereby trusted identities on mobile devices can be leveraged
- In the first three months following this presentation you should:
  - Assess the critical qualities that would be used in the vendor qualification process
  - Begin vendor selection
- Within size months you should:
  - Select a vendor's solution and conduct a pilot with your first use case
  - Plan the implementation for supporting all use cases

BACK UP



All industries are at risk

EMPLOYEE IDENTITIES ARE BECOMING A WEAK LINK

Mitigating the risk of fraud

USE CASE 3

PROBLEM:

- Fraud attacks are increasing in scope and sophistication
- Customer data, enterprise systems, intellectual property & money are at risk
- Malware can “ride” on authenticated user sessions

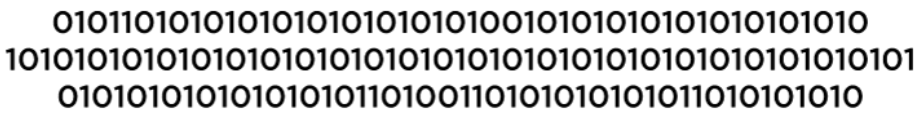
SOLUTION:

- Use mobile to verify transactions “out of band” defeating account takeovers

Mitigating the risk of fraud

USE CASE 3

Compromised with desktop Malware?



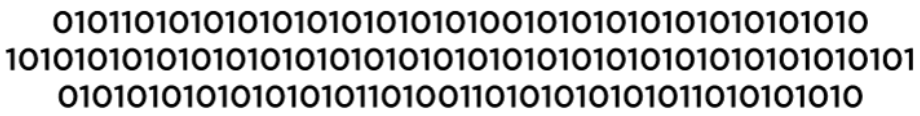
Let's say you want to execute a $5000 bank transfer…

How can you be sure your PC is not infected with malware?

Mobile for Transaction Verification

USE CASE 3

Compromised with desktop Malware?



Transaction details retrieved over secure connection

Offline Transaction Verification

QR Code

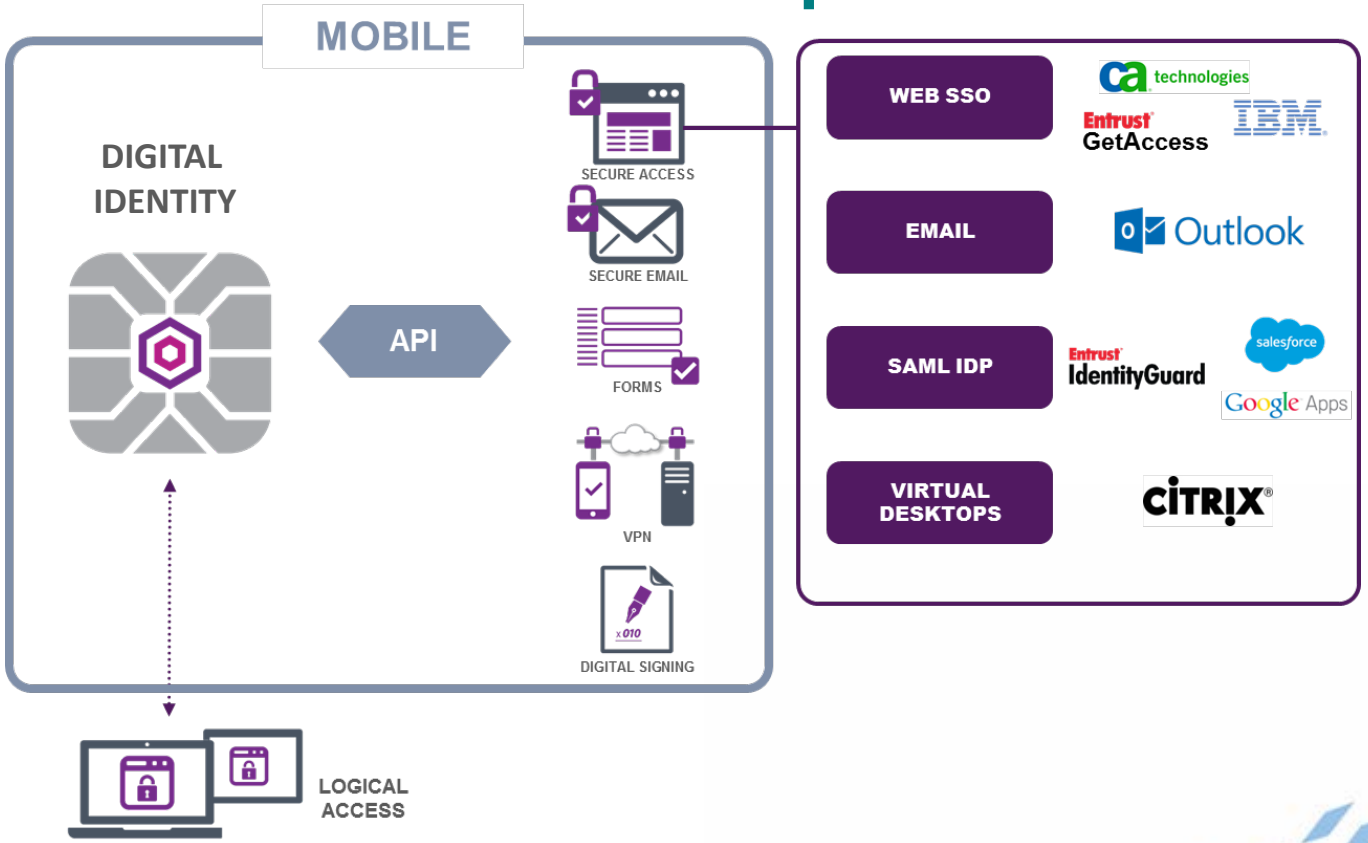
Mobile will become the New Enterprise Desktop

- Not portable
- Secure location
- Work only

- Portable
- Less Secure Locations
- Work & some personal

- Highly portable
- Anywhere anytime access
- BYOD

Mobile as the New Desktop



Entrust Datacard Corporate Overview

Trusted Identities | Secure Transactions

- Privately held, headquartered in Minneapolis, MN, USA
- Founded in 1969
- Approximately $650M in annual revenue
- 2,000+ employees
- 34 worldwide locations
- Sales, service and support covering 150+ countries

So what's the problem?

- Too many identities
- Too many passwords
- Too many password rules / changes
- Lost / forgotten cards / hardware tokens
- More regulatory laws around identities

Mobile- A unique blend of security and usability

Users want to carry them

- Always in hand
- Always connected
- Convenient
- Support work / personal balance

Smart phones are becoming ubiquitous

- Both enterprise and consumer segments

Technology and security allows them to be used for multi-purpose trusted identities

Adaptive Authentication Platform

Entrust® IdentityGuard

RELEASE 11

FRICTIONLESS EXPERIENCE

No passwords

Identify with a simple swipe

Familiar for smartphone users

Highly secure

ENABLING SOLUTION

Adaptive authentication — identifies risks

Layered security — device, identity & behavior analytics

Support for Apple, Samsung & Windows devices

Transaction signing for CNP transaction

Security for Every Vulnerability

MOBILE SECURITY		ONLINE SECURITY
	Phone Jailbreak or Root Detection	
✖	App Access Control — PIN, Biometrics	
✖	Device Authentication — Device Fingerprinting	✖
✖	Adaptive Authentication — External Risk Engines & Contextual Data	✖
✖	User Authentication — Transparent OTP or Certificate-Based	✖
	Transaction Authentication — Mobile Push Notifications	✖
✖	Strong Identity Protection — TEE Storage	✖

AUTHENTICATION

▶ USER

▶ DEVICE

▶ CHANNEL

▶ TRANSACTION

▶ APPLICATION

Stronger controls are not always better

- More complex passwords?
- Hardware tokens for the masses?
- USB security keys?
- Smart cards?

Some offer better security but…

- ☑ Costly
- ☑ Logistics to issues / replace
- ☑ User have to carry them
- ☑ User experience frustrating
- ☑ Not multi-purpose
- ☑ Can you issue them to customers and partners?