SECURITY IMPLICATIONS OF NFC IN AUTHENTICATION AND IDENTITY MANAGEMENT

Security in knowledge

Dmitry Barinov

SecureKey Technologies Inc.

Session ID: MBS-W09

Session Classification: Advanced

RSA CONFERENCE EUROPE 2013

Session goals

- Appreciate the superior security achieved using Multi Factor Authentication (MFA)
- Understand the difficulties with existing approaches
- Recognize the benefits of using NFC to achieve MFA
- Explore security implications of using existing NFC devices with credentials that customers already have
- Learn of open standard authentication protocols between NFC devices, Credential Service Providers and Relying Parties.

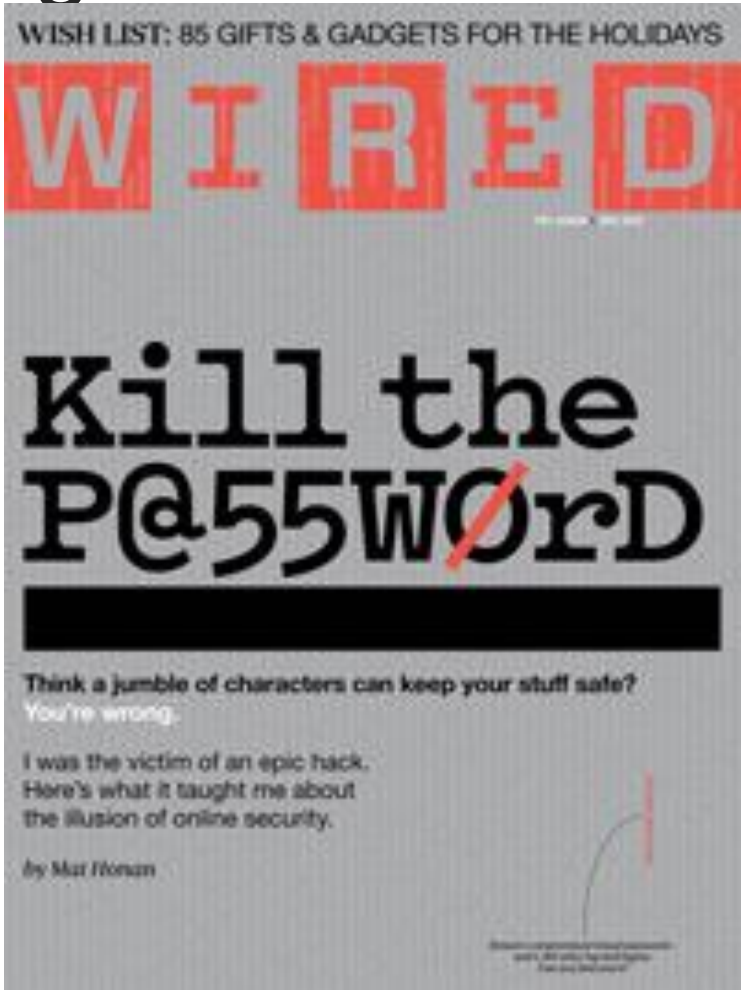
Session Outline

- Authentication problem
- MFA and its benefits, risks, implementations
- Levels of assurance and Strong Consumer Credentials
- Demos
- NFC – technology, deployments, risks and benefits
- NFC credentials in Authentication schemas
- Credential Brokering
- Compliancy and Conclusions

MFA concepts

Multifactor vs. Strong Auth

- “Strong authentication“ definitions are controversial.
- Is soliciting multiple answers to challenge questions = strong authentication?
- **Kill the Password: Why a String of Characters Can’t Protect Us Anymore by** Mat Honan, 11.15.12



WISH LIST: 85 GIFTS & GADGETS FOR THE HOLIDAYS

WIRED

Kill the P@55WØrD

Think a jumble of characters can keep your stuff safe? You're wrong.

I was the victim of an epic hack. Here's what it taught me about the illusion of online security.

by Mat Honan

MFA Drivers

- “The U.S. FFIEC (Federal Financial Institutions Examination Council):

"By definition true multifactor authentication requires the use of solutions from two or more of the three categories of factors. Using multiple solutions from the same category ... would not constitute multifactor authentication.“

White House releases plan for an Internet ‘identity ecosystem’

The White House released the National Strategy for Trusted Identities in Cyberspace (.pdf) April 15, a government-coordinated effort to create a digital "identity ecosystem," executed by the private sector.

Image: © iStockPhoto/porcorex

MFA examples

- At ATM:
  - physical ATM card ("something the user has")
  - PIN ("something the user knows")
- Logging in to the corporate network:
  - password ("something the user knows")
  - physical token ("something the user has").
- Crossing the border:
  - biometric input (“something you are”)
  - an electronic passport (“something you have”)

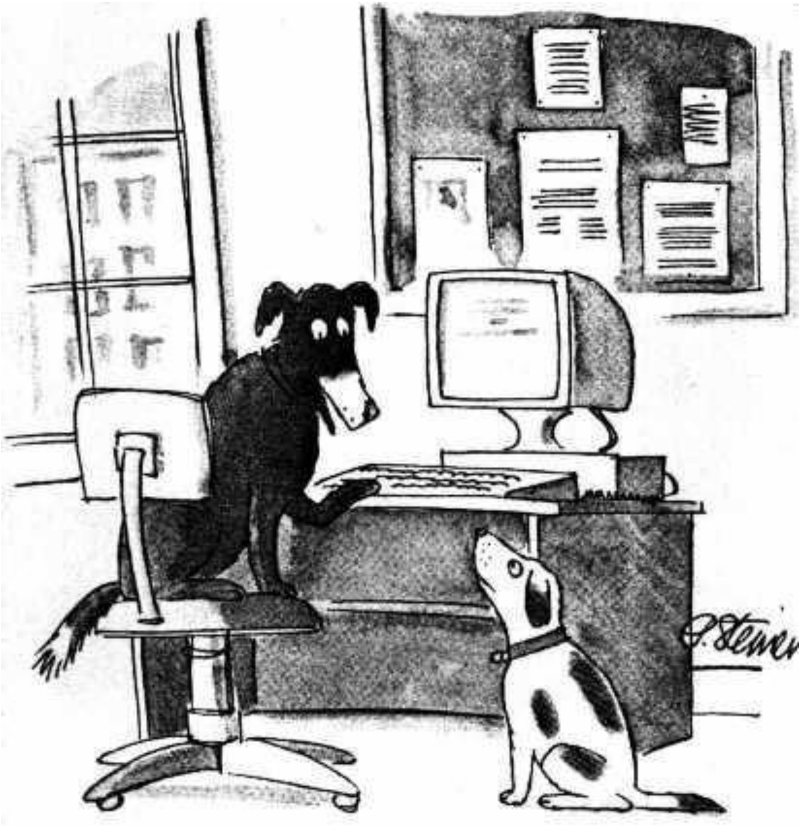
Levels of Assurance

- NIST has issued a Levels of Assurance “Code of Laws” - Special Publication (SP) 800-63, *Electronic Authentication Guideline*, by William E. Burr, Donna F. Dodson, and W. Timothy Polk
- Similar international guidelines
  - Canadian ITSG-31
  - EU eID
- Technical guidance on existing and widely implemented methods for remote authentication

LoA1

- Level 1 requires little or no confidence in the asserted identity
  - No identity proofing is required at this level
  - A wide range of available authentication technologies can be employed
  - To be authenticated, the claimant must prove control of the secret (aka token) through a secure authentication protocol
- Plaintext passwords or secrets are not transmitted across a network at Level 1. However, this level does not require cryptographic methods that block offline attacks by an eavesdropper
- **Example**: simple password challenge-response protocols are allowed

LoA1: On the Internet, nobody knows you’re a dog



"On the Internet, nobody knows you're a dog."

- cartoon by Peter Streiner published by The New Yorker on July 5, 1993

LoA2

- Requires confidence that the asserted identity is accurate.
- Provides for single-factor remote network authentication, including identity-proofing requirements
- A wide range of available authentication technologies can be employed, including passwords.
- Claimant must prove through a secure authentication protocol that the he controls the secret (aka token).
- Eavesdropper, replay, and online guessing attacks are prevented.

LoA3

- Level 3 provides multifactor remote network auth
- Identity-proofing procedures require verification of identifying materials and information
- Authentication is based on proof of possession of a key or password through a cryptographic protocol
- Cryptographic strength mechanisms protect the primary authentication token against compromise by the protocol threats, including eavesdropper, replay, online guessing, verifier impersonation, and man-in-the-middle attacks.
- A minimum of two authentication factors is required

LoA4

- The highest practical assurance of remote network authentication.
- This level is similar to Level 3 except:
  - that only “hard” cryptographic tokens are allowed,
  - cryptographic module validation requirements are strengthened,
  - subsequent critical data transfers must be authenticated via a key that is bound to the authentication process.

Strong Credential – a key to high Assurance Level

- Typical token challenges:
  - Credential Distribution
  - Credential management
  - Credential lifecycle
  - Additional costs
- Customers don’t want “another thing”, they want less!
- Proprietary solutions are risky

- On the other hand Users
  - Love to use own devices
  - Love to leverage credentials they already have
  - May already have strong credentials
  - Don’t want “another thing”
  - Want less!

NFC Credentials

- Strong security
- Are in the hands of customers
- Are actively managed – I will be worried if I can't find my phone or credit card
- Are convenient to use – just tap and go
- Can be federated – use one credential for many uses
- Allow enhanced privacy – your identity does not have to be on Credential

Demos

#RSAC

Use Cases and Demos

- Lets see some demos and videos
  - Authenticate with EMV NFC card to Gov office
  - Authenticate with NFC credential to commercial online system
  - Authenticate with NFC credential to government online system
  - …

NFC security

#RSAC

RSACONFERENCE EUROPE 2013

NFC

Set of standards to establish radio communication by bringing devices into close proximity, defined by the NFC Forum

- Present and anticipated applications include contactless transactions, data exchange
- Communication is also possible between an NFC device and an unpowered NFC chip, called a "tag"
- NFC standards cover communications protocols and data exchange formats, and are based on existing RFID standards including ISO/IEC 14443
- The Forum promotes NFC and certifies device compliance

NFC Security

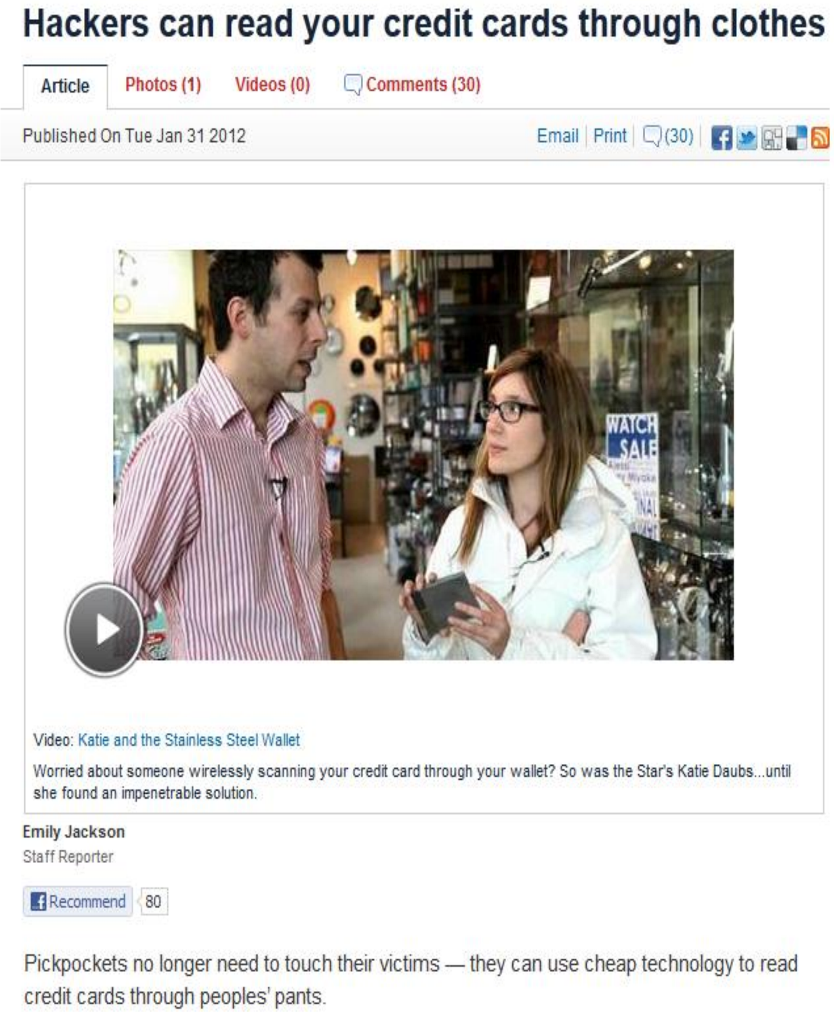
- Great White Paper by Ernst Haselsteiner and Klemens Breitfuß
- In short: NFC requires additional controls to be fully secure such as
  - Application providers must use higher-layer cryptography to establish secure communication channel.
  - Device providers need to safeguard NFC-enabled devices with strong cryptography and authentication protocols;
  - Transaction parties need to deploy security solutions to prevent spyware and malware from infecting systems.

NFC – Myths and Scares

- What’s mentioned in these articles is “factually” true – you can scan cards and get PAN and expiry date and one time CVC/CVV.

What’s implied in the articles is not true – you cannot manufacture or “clone” cards based on this information.

- Online CNP requirements are not met by PAN and expiry date



Hackers can read your credit cards through clothes

Published On Tue Jan 31 2012

Video: Katie and the Stainless Steel Wallet

Worried about someone wirelessly scanning your credit card through your wallet? So was the Star's Katie Daubs...until she found an impenetrable solution.

Emily Jackson
Staff Reporter

Pickpockets no longer need to touch their victims — they can use cheap technology to read credit cards through peoples’ pants.

Tapper myth

- Current generation of RFID-chip enabled cards contain a credit-card number, an expiration date and a dynamically generated CVV/ CVC3 – different from the one on the magstripe and one printed on the card.
- This information is sent to the terminal along with a cryptogram that verifies the card's authenticity.
- Good solutions are not threatened by fraudsters ability to scan the NFC interface due to the following protecting controls:
  - Dynamic CVC (CVC3)
  - Terminal Random number validated at the server
  - Cryptogram based on the EMV standards and strong encryption
  - Fraudster would have to clone an EMV card to submit the transaction

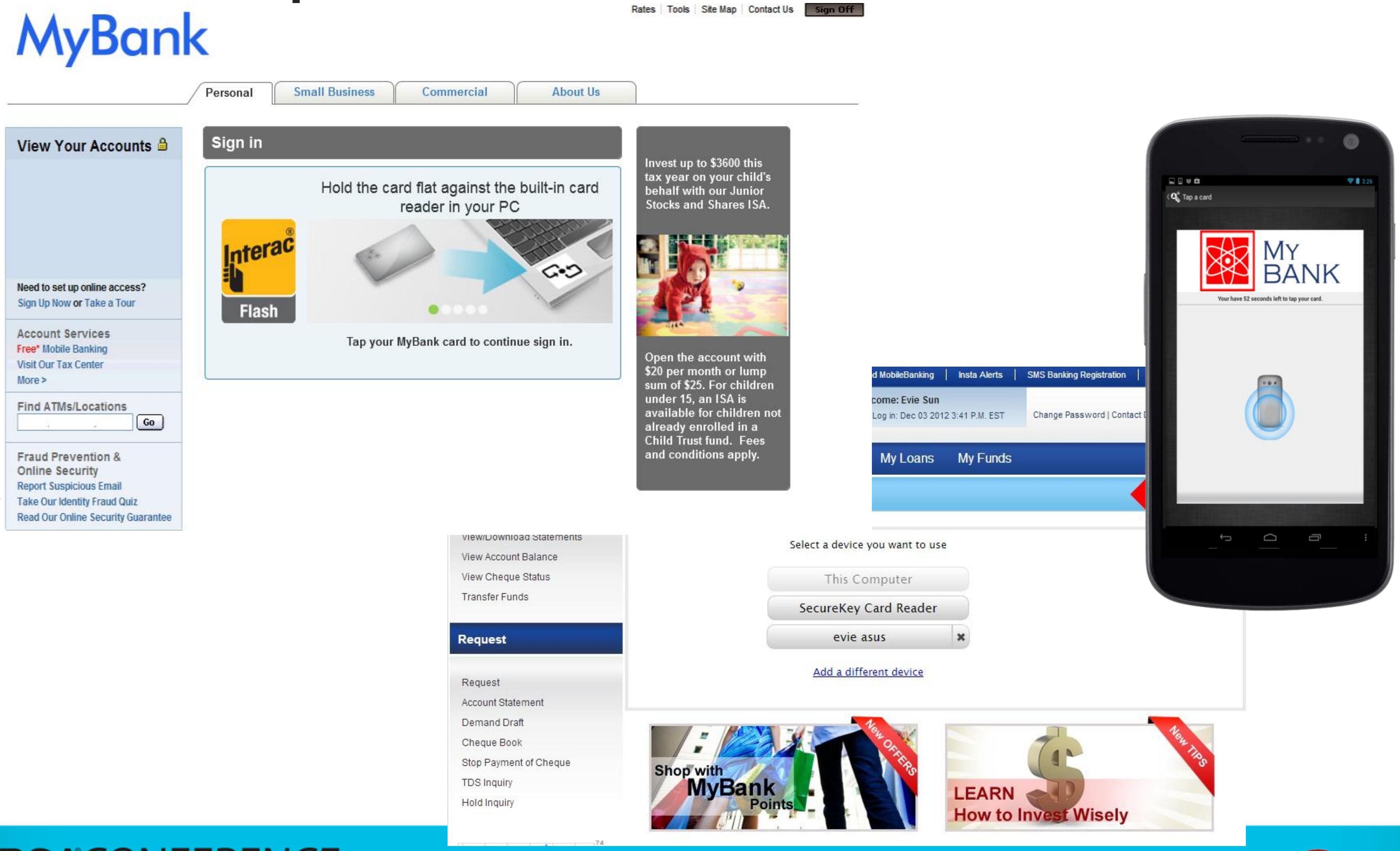
NFC vs. Bluetooth

- Both are short-range communication technologies, integrated into various devices.
- NFC consumes far less power
- NFC pairing is automatically established in less than a tenth of a second.
- NFC has a maximum working distance of less then 20 cm, (shorter range then Bluetooth)
- NFC is compatible with existing passive RFID (ISO/IEC 18000-3) infrastructures , illuminating the passive tag
- Bluetooth LE closes the gap

Derived and Federated credentials

- Does one need to use NFC card all the time?
- Pair an NFC phone to the service
- Vet the NFC phone with an EMV card tap
- Could device cryptogram be as trusted now as your credit card's cryptogram?
  - Yes, it can be

Example of NFC authentication



MyBank
Rates | Tools | Site Map | Contact Us | Sign Off
Personal | Small Business | Commercial | About Us

View Your Accounts

Need to set up online access?
Sign Up Now or Take a Tour

Account Services
Free* Mobile Banking
Visit Our Tax Center
More >

Find ATMs/Locations
Go

Fraud Prevention & Online Security
Report Suspicious Email
Take Our Identity Fraud Quiz
Read Our Online Security Guarantee

Sign in

Hold the card flat against the built-in card reader in your PC

Tap your MyBank card to continue sign in.

Invest up to $3600 this tax year on your child's behalf with our Junior Stocks and Shares ISA.

Open the account with $20 per month or lump sum of $25. For children under 15, an ISA is available for children not already enrolled in a Child Trust fund. Fees and conditions apply.

come: Evie Sun
Log in: Dec 03 2012 3:41 P.M. EST

Change Password | Contact [

View/Download Statements
View Account Balance
View Cheque Status
Transfer Funds

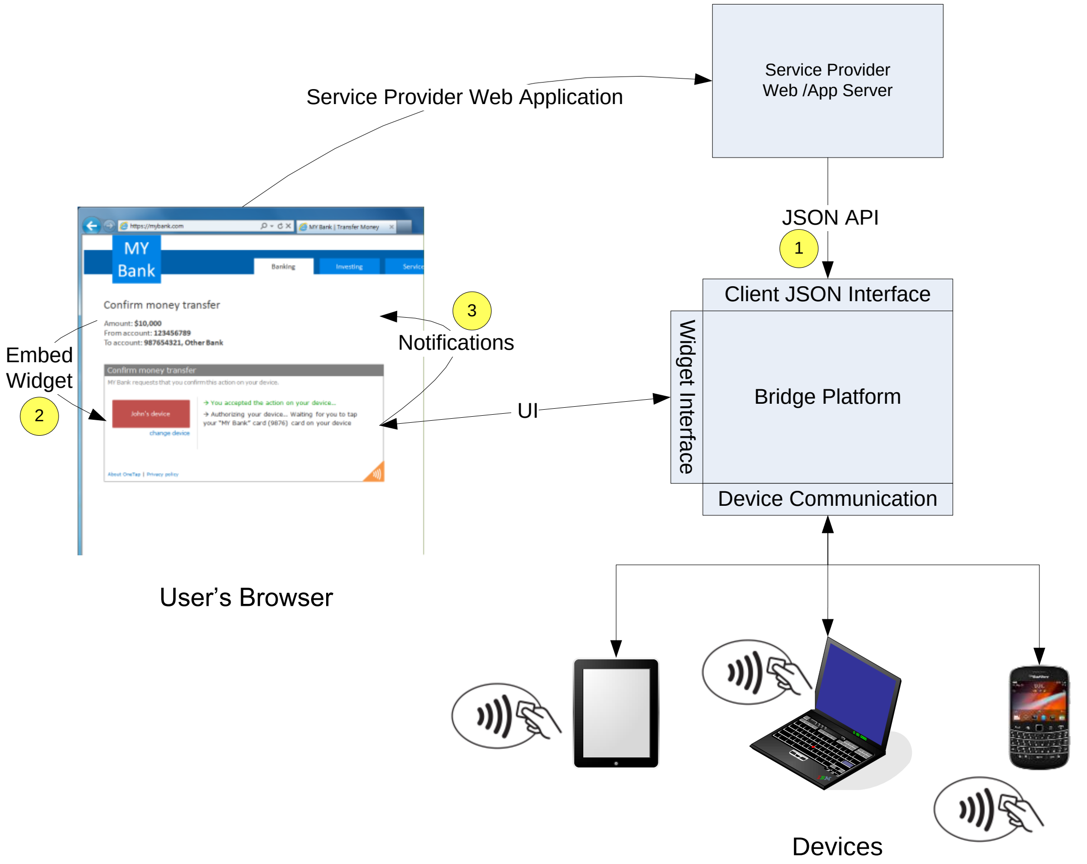
Request

Request
Account Statement
Demand Draft
Cheque Book
Stop Payment of Cheque
TDS Inquiry
Hold Inquiry

Select a device you want to use

Your have 52 seconds left to tap your card.

NFC enabled authentication



Confirm money transfer

Amount: **$10,000**
From account: **123456789**
To account: **987654321, Other Bank**

Confirm money transfer

MY Bank requests that you confirm this action on your device.

John's device

change device

→ You accepted the action on your device...

→ Authorizing your device... Waiting for you to tap your "MY Bank" card (9876) card on your device

About OneTap | Privacy policy

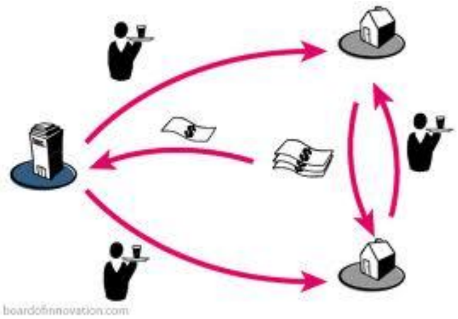
- briidge.net abstracts the communication to the devices from the client
- User Agent does not need to be concerned with the various technologies required to communicate with different devices.

NFC and identity ecosystem

#RSAC

Extending credential and attributes to many RPs

- Use NFC credential to access required Relying Party/Service Provider
- Privacy-enhanced federated authentication lets you using existing login IDs with 3rd parties and across lines of business
- Credential Broker
- Two major methods of brokering
  - SAML 2.0
  - OPEN ID 2.0/ Connect
- Broker MUST enhance privacy
  - Triple Blind concept
  - Consent provisioning
  - Attribute exchange



Federations ecosystem

- Federations of Relying Parties – based on needs, access requirements, geo/org groupings
- Federations of Attribute Providers – based on quality, types of attributes
- Groups of Identity Providers
- Broker that connects the groups
  - Single integration
  - Standard and Policy enforcement
  - Privacy enhancement
  - Ecosystem enabler

NFC, federation and compliance

Strong multifactor authentication is required to comply with a number of compliancy regulations:

- E-Gov Act 2002
- HSPD (Homeland Security Presidential Direction) -12 and related technical FIPS 201 requirements
- FISMA (Federal Information Security Management Act of 2002) and related technical FIPS 200 requirements
- HIPAA (Health Insurance Portability and Accountability Act) and PHI (Protected Health Information)
- EU Data Protection Directive
- PCI
- Others….

In conclusion

- Multi-factor authentication will gather more focus in the future
- Presence of NFC credentials will be growing in authentication and security ecosystems
- Well built authentication solutions based on NFC can meet the strongest security and compliance guidelines
- True value of authentication solutions can be delivered through integration with strong identity ecosystems

Thank you!

Dmitry Barinov

SecureKey Technologies Inc.

dmitry.barinov@securekey.com

www.securekey.com

#RSAC