XXVI Congreso de Seguridad Bancaria
CELAES 2011

Solving Online Fraud with Strong Authentication

Don Malloy
Johan Rydell
September 16th, 2011

Agenda

Industry Trends
Need for Strong Authentication
How OATH combats Fraud
Types of Strong Authentication solutions
Securing online transactions
Summary
Demo

Growth in Fraud

Fraud continues to grow world-wide

2010 – 285 million consumer records were breached – resulting in almost $1Trillion in losses

10 Million Americans were victims of fraud last year

This amounts to over $300M of online fraud last year alone

Hacking into web sites and stealing passwords continue to be a main focus of fraudsters

Static Passwords are not secure: 80% hacked

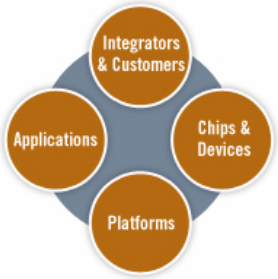
Need for Strong Authentication

Networked entities face three major challenges today.

- Theft of or unauthorized access to confidential data.
- The inability to share data over a network without an increased security risk limits organizations.
- The lack of a viable single sign-on framework inhibits the growth of electronic commerce and networked operations.

Justification for Strong Authentication

- The Initiative for Open Authentication (OATH) addresses these challenges with standard, open technology that is available to all.
- OATH is taking an all-encompassing approach, delivering solutions that allow for strong authentication of all users on all devices, across all networks.
- The use of Multi-factor authentication products with an OATH application will protect against The ATM hacks mentioned previously.



OATH Membership (Partial)

nagra ID SECURITY · ENFORCE · nexus

ACTIVIDENTITY · Aladdin · AniCa ANIMATING THE WORLD · aradiom the phone reborn · Authenex · BIO-key INTERNATIONAL

BR TOKEN · Clareity Security · COMARCH INFORMATION TECHNOLOGY · CRYPTOMATHIC · DS³ · DIVERSID AUTENTICACIÓN · DEEPNET SECURITY

Diversinet · DynamiCode Revolution for Your eAccess · Entrust · EZMCOM · FEITIAN WE BUILD SECURITY · fireID

gemalto security to be free · iretH · InfoSERVER · Giesecke & Devrient · i-sprint INNOVATIONS

IRONKEY · LIEBERMANSOFTWARE · mobilegov THE DIGITAL DNA · movilok FOCUSED ON MOBILE INNOVATION · nagra ID SECURITY

nordic edge · nexus · PhonoClick · PointSharp · SmartDisplayer

Symantec · THALES e-SECURITY · TOPPAN FORMS · yubico

Authentication Algorithms

-Open and royalty free specifications

-Proven security: reviewed by industry experts

-Choice: one size does not fit all

HOTP	OCRA	T-HOTP
-Event-based OTP	-Based on HOTP	-Time-based HOTP
-Based on HMAC, SHA-1	-Challenge-response authentication	-Submitted to IETF
-IETF RFC 4226	-Short digital signatures	-Standard completed 2011
		-IETF RFC 6238

Token Innovation and Choice

OTP embedded in credit card

OTP soft token on mobile phones

HOTP applets on SIM cards and smart-cards

OTP embedded in flash devices

OTP Token

Soft OTP Token

HOTP

oath

50+ products shipping

Multi-Function Token (OTP & USB Smart Card)

One Time Password Devices

Initial Applications

- Financial – Most Governments have demanded more than static passwords
- Online Authentication
- Physical Access

One Time Password Devices

Subsequent Applications

- Contactless Payment
- Secure Network Access
- E-wallet application
- Mobile Banking

Layered Approach to Security

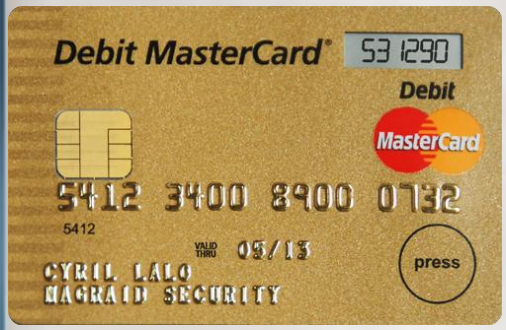
Applications

- OTP
- Pin Activation
- Challenge/Response
- Physical Access
- Contactless Payment
- Secure Network Access

Cards will be used for:

- EMV Payment
- Debit Cards
- Single sign on and multi apps

Payment and Authentication



- Recent certification by MasterCard announced at their Debit Conference in Budapest last summer.
- Announced WW promotion at RSA Conference last month
- VISA trialing a PinPad OTP card in Europe at 9 different banks
- EMV for secure payment application
- OATH authentication device as well

Information Display Card uses Existing Infrastructure

Standard EMV chip technology updates the information every time the card is authorized online.

1. Customers insert the payment card in the POS terminal and input their PIN to pay for their purchases.

2. Merchant(acquirer) terminal requests the payment authorization from the issuer through the MasterCard payment network.

4. Acquirer terminal receives approval code and executes the EMV script to update information on the cardholder's display card.

3. Card issuer processes the request and replies the acquirer with an approval code + an EMV script

How it Works

Challenge Response

Client

1

The client calls an establishment to make a high valued transaction over the phone

Business

2

The establishment gives the client a verification code (challenge) to enter into the TOUCH Keypad on their card

Client

3

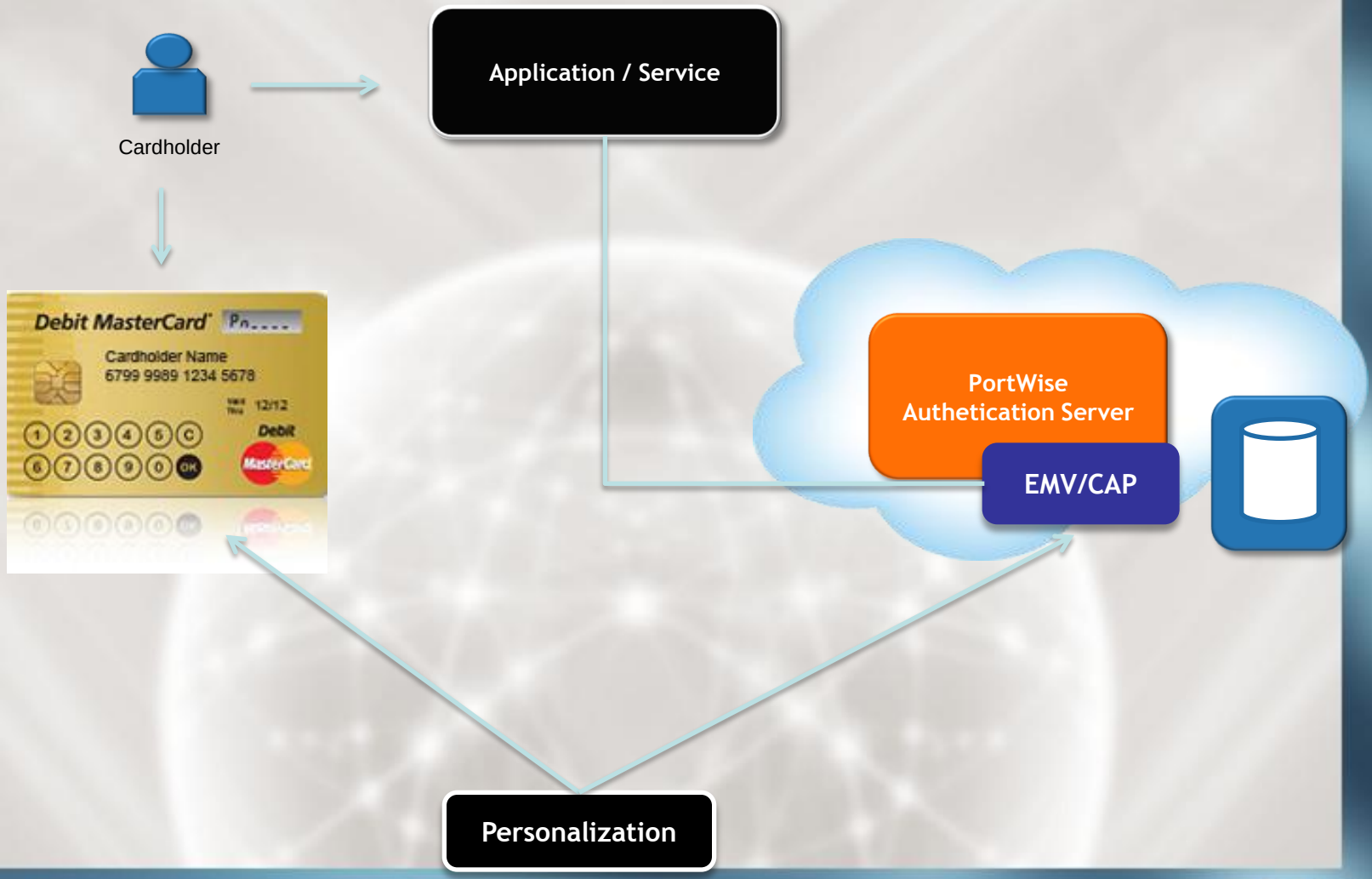
Once the card verifies the challenge code it generates a response code

Business

4

The establishment verifies the clients response code and the request can securely be completed over the phone

Support for Multiple Business Functions


Application / Service
Cardholder
Debit MasterCard
Cardholder Name
6799 9989 1234 5678
12/12
PortWise
Authetication Server
EMV/CAP
Personalization

- Cardholder
  - Ease of use
    - One card
    - No additional hardware
  - Convenient
  - Increased security
- Card Issuer
  - Reduced cost
  - Increased security
  - Market differentiator
  - New applications
  - Adopts to existing card issuing processes

In Summary

ISSUER BENEFITS:

- Increased Revenues
- Reduced Cost
- Greener
- Reduced Fraud
- Many Competitive Advantages

CARDHOLDER BENEFITS

- Security
- Control
- Convenience
- Peace of mind

Demonstration

Live Demonstration of Authentication is next……

End of Presentation

Thank You For Your Attention

Enforce

3 Avenida 12-38 Zona 10
Edificio
Paseo Plaza Business Center
Nivel 6 Oficina 602
T: 786 375-8139
W: www.enforceti.com

Nexus

Arstaangsv. 19 B
SE-100 74 Stockholm
Sweden
T: +46 (8) 655 39 00
W: www.nexussafe.com

NagraID Security

8615 Washington Blvd
Los Angeles, CA 90232
USA
t: (310) 841-2939
w: www.nidsecurity.com
e: info@nidsecurity.com