New Generation of Online Authentication Strategies

- Don Malloy – NagraID Security
- Johan Rydell – Technology Nexus AB

- September 21st, 2012

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

2011 – 285 million consumer records were breached – resulting in almost $1Trillion in losses

15+ Million Americans were victims of fraud last year

This amounts to over $500M 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.

History of OATH

- Created 6 years ago to provide open source strong authentication.
- It is an industry-wide collaboration that…..
- Leverages existing standards and creates an open reference architecture for strong authentication which users and service providers can rely upon, and leverage to interoperate.
- Reduces the cost and complexity of adopting strong authentication solutions.

OATH Membership (Partial)

ACTIVIDENTITY
AniCa ANIMATING THE WORLD
Authenex
BR TOKEN
CRYPTOMATHIC
DS3
Entrust
gemalto security to be free
EZMCOM
FEITIAN WE BUILD SECURITY
ireth
i-sprint INNOVATIONS
LIEBERMANSOFTWARE
mobilegov THE DIGITAL DNA
movilok FOCUSED ON MOBILE INNOVATION
nagraID SECURITY
nordic edge
nexus
PointSharp
Symantec.
THALES e-SECURITY
SmartDisplayer
yubico

Authentication Algorithms

- Open and royalty free specifications
- Proven security: reviewed by industry experts
- Choice: one size does not fit all

HOTP	TOTP	OCRA
-Event-based OTP	-Time-based OTP	-Based on HOTP and TOTP
-Based on HMAC, SHA-1	-Standard completed 2011	-Challenge-response authentication
-IETF RFC 4226	-HMAC with SHA-1, SHA-256, SHA-512	-Short digital signatures
	-IETF RFC 6238	-IETF RFC 6287

Token Innovation

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

HOTP

oath

50+ products shipping

Soft OTP Token

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

What is a Display Card?

Signature Panel

Magnetic Stripe

Holographic Stamp

Printable Surface for In-House personalization

High Speed Display Panel With Scrolling Character Capacity

Custom Graphics & Branding

Laser Engraving

EMV Contact Chip

Multiple Touch Button Option

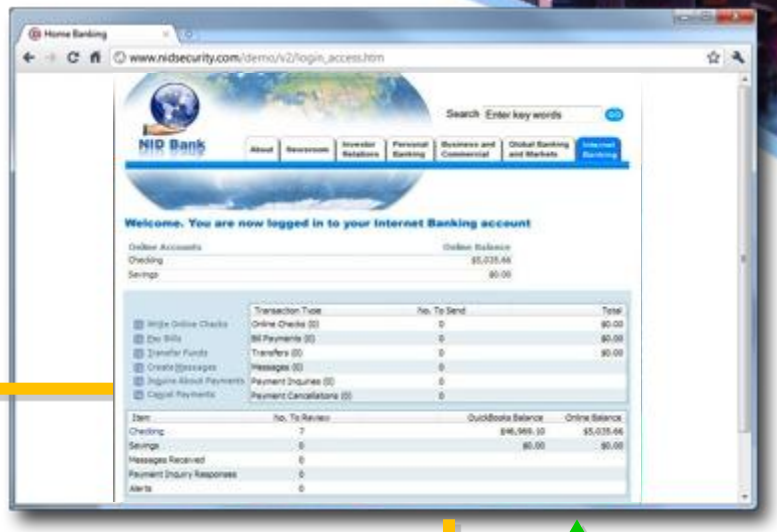
Wireless Interface For Contactless Physical Access or Payment Applications (ISO14443A/B, LEGIC, MIFARE, HID, PAYPASS)

Embossing

Single Button/Switch

OTP token authentication workflow

1. Input **userID** and Password on VPN, eCommerce, online banking site ….



2. Generate dynamic password **(OTPa)** with the display card and use it for authentication

3. Authentication information is sent to the application server (webserver, database server, vpn etc…)

4. UserID and **OTPa** is sent to secure authentication server

5. Authentication server uses the **userID** to retrieve the corresponding display card information (seed).

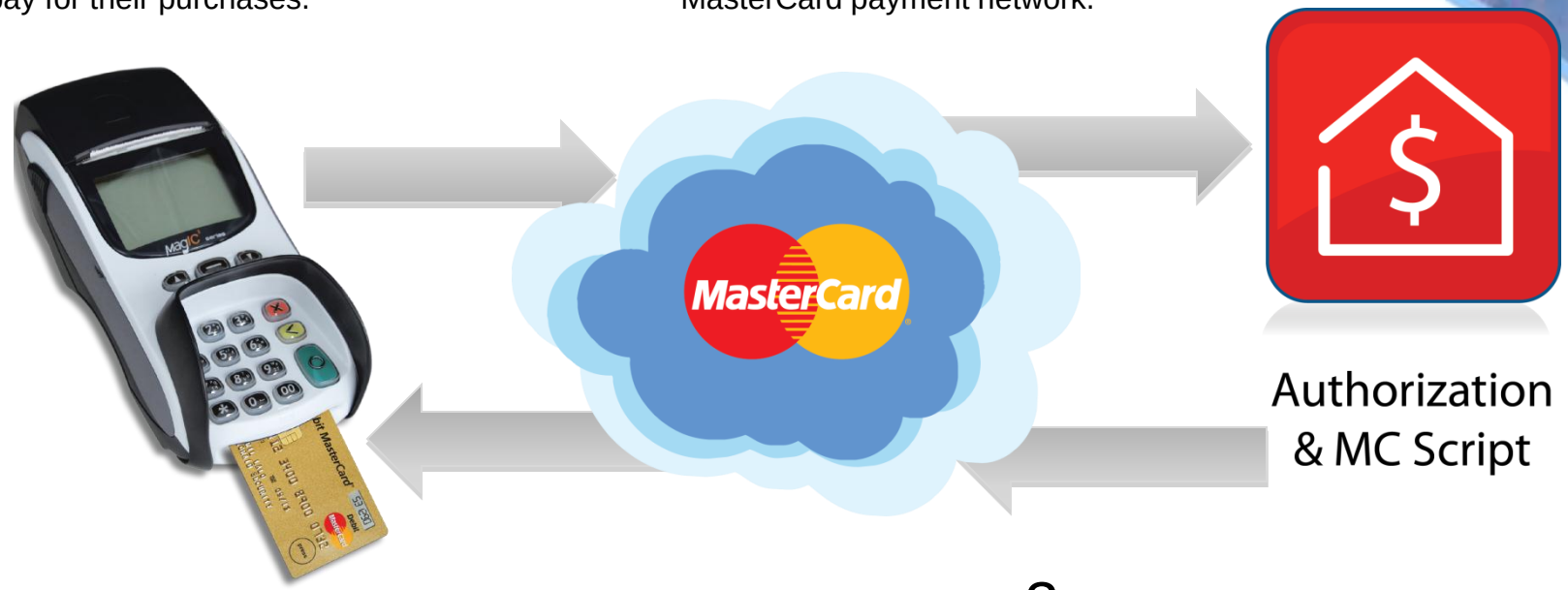
The seed is used to generate **OTPb**, and compares if **OTPa** = **OTPb**

6.Result (grant or deny access) is sent to the application server

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

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

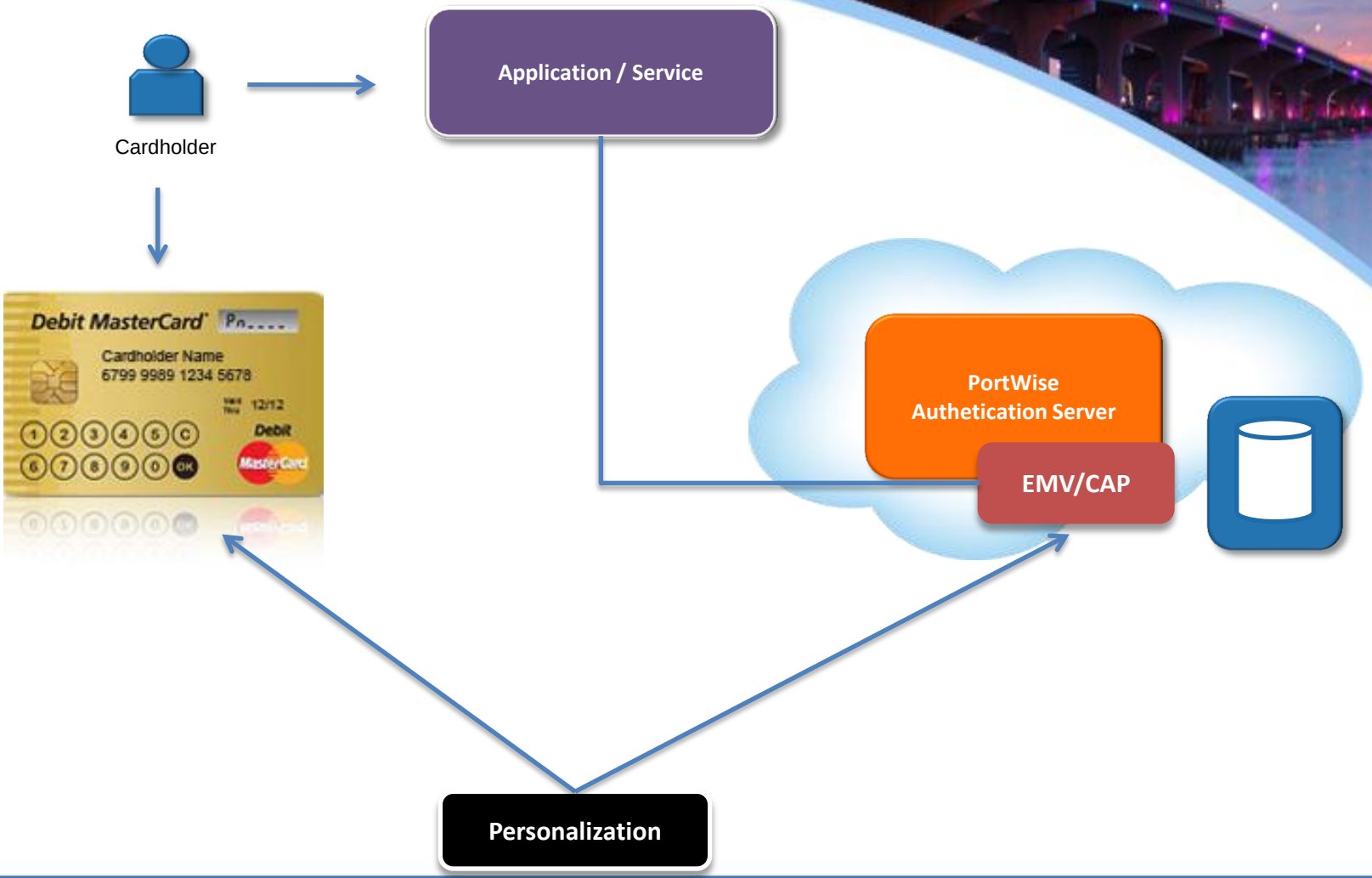
Business

4

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

Support for Multiple Business Functions

One card – multiple purposes


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

Summary

ISSUER BENEFITS:

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

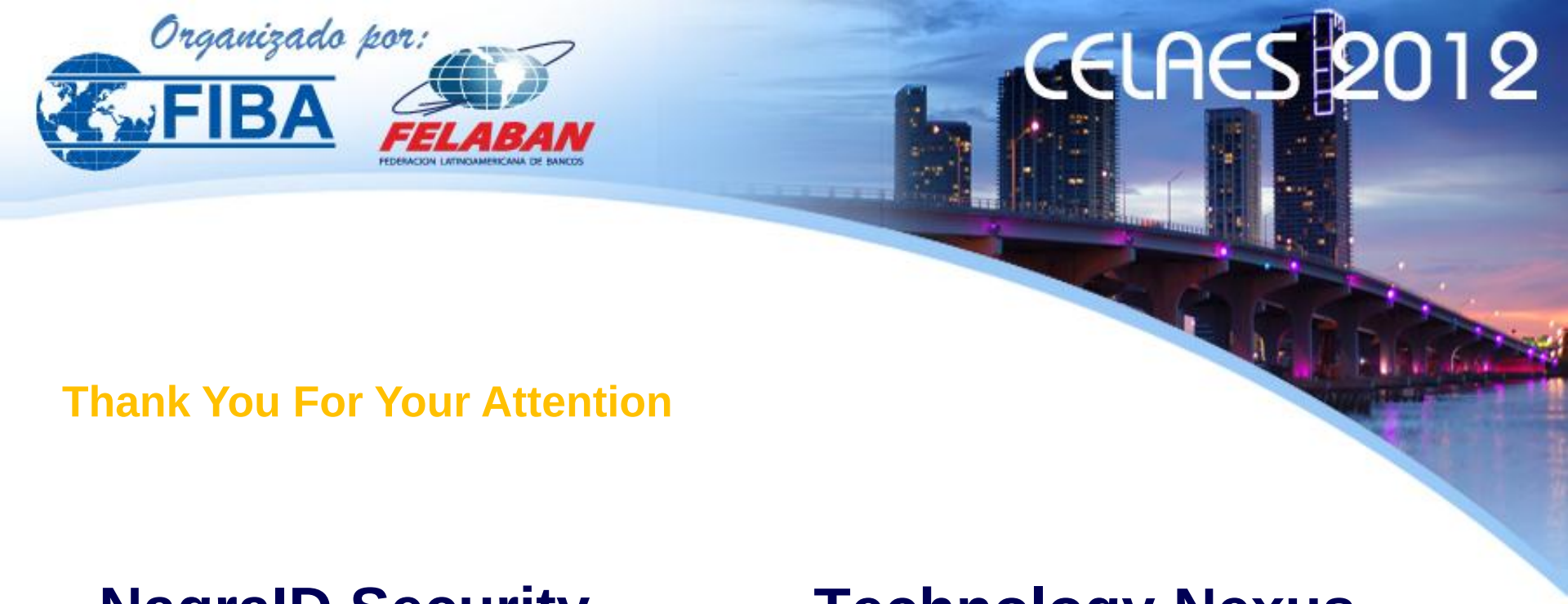
CARDHOLDER BENEFITS

- **Security**
- **Control**
- **Convenience**
- **Peace of mind**

Demonstration

Live Demonstration of Authentication is next……

Introducing – Invisible Token



Thank You For Your Attention

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

Technology Nexus
100 Montgomery street Suite 1080
San Francisco, CA 94109
USA
t: +1 650 515 3569
w: www.nexussafe.com
e: info@nexussafe.com