

IS YOUR ONLINE BANK REALLY SAFE?



Zoltan Szalai

eBanking Solution Manager

It all starts with trust.



Gemalto for You

ONE THIRD OF THE WORLD'S POPULATION

USE OUR SOLUTIONS EVERYDAY



- BANKS & RETAIL
- TELECOM
- TRANSPORT
- GOVERNMENT
- ENTERPRISE

About Gemalto



Over €2 BILLION in Revenue in 2011

€250+ MILLION Software and Value Added Services

BILLION Intelligent Cards Produced and

Personalized on a Yearly Basis

14 R&D Centers

1,400 Scientists

15 Production Sites

28 Personalization Centers

74 Sales & Marketing Offices

10,000+ Employees

100 Nationalities

43 Countries

Gemalto eBanking



The acquisition of Xiring and Todos positioned Gemalto as the leader in the eBanking World.

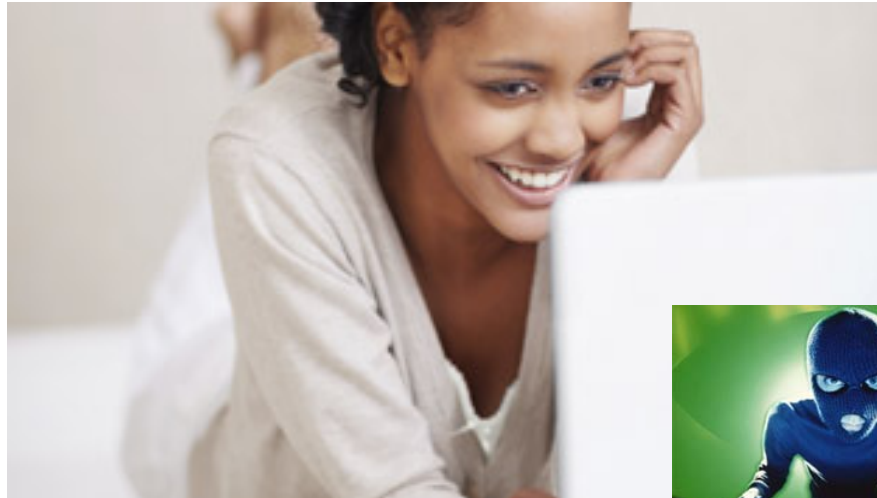
~ **150** CUSTOMER BANKS

50+ MILLION USERS

40+ MILLION DEVICES

120 EMPLOYEES

EZIO LIFE



eBANKING ATTACKS - STILL EVOLVING

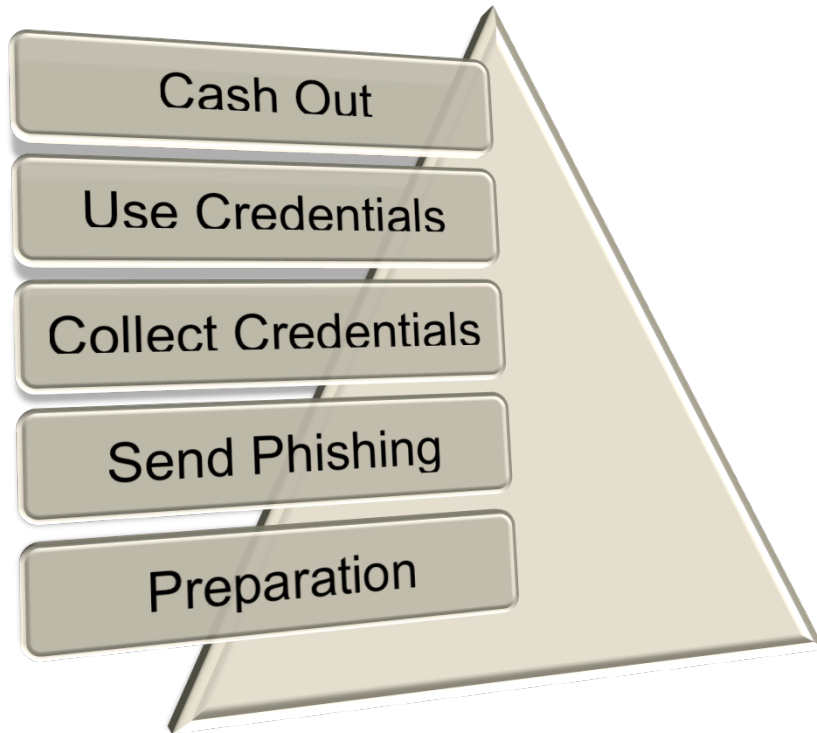
1 2 3 4 5 6

Password 1

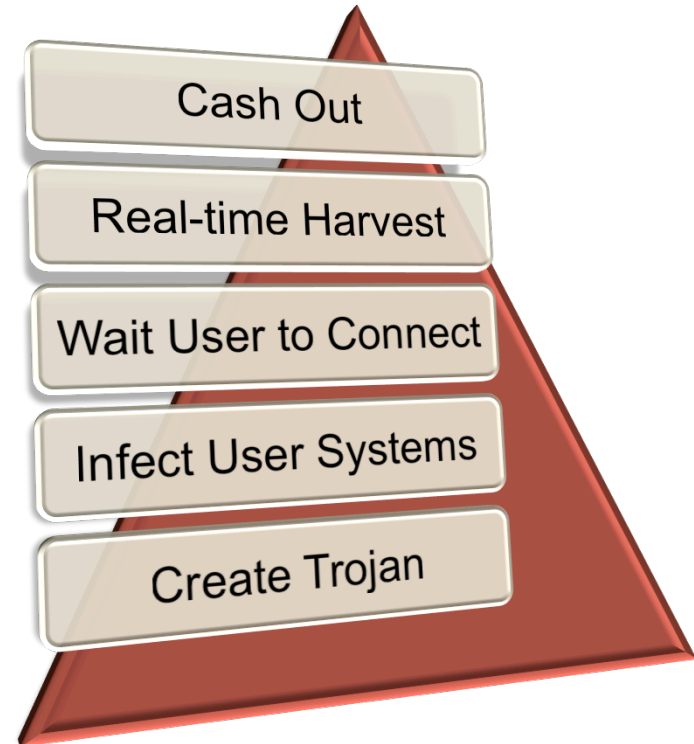
eBanking Fraud is Changing

SIMPLE PHISHING >>> SOPHISTICATED MALWARE

“OLD” Type of Attack



“NEW” Type of Attack



31% of EU internet users were infected by worm or Trojan in 2010

eFraud Attacks Become Smarter

THE eBANKING THREAT IS ADAPTING



Dear valued customer of TrustedBank,

We have received notice that you have authorized the following amount from your checking account to be debited from your account. As a safety measure, please verify your personal information:

<http://www.trustedbank.com/gen>

Once you have done so, our fraud department will be happy to help you with any discrepancy.

Thank you,
TrustedBank



Zeus Trojan hits TrustedBank hard

Published: 08 Sep 2009
Marcia S. ...
Informat...

A Trojan that steals online banking information is a successful piece of malware, according to a report from SearchFire.

Zeus is the "biggest banking Trojan" found during a recent company webcast. It's a money-stealing machine that has been used for a long time.

Also called Zbot, Zeus and its variants are among the most common malware attacks on computers at a steady clip this spring, said Ben Greenbaum, senior manager in the security response unit at Symantec Corp. The malware is easy to configure and widely available on the Internet, with prices ranging from a couple hundred dollars to free, he added.

Member FDIC © 2005 TrustedBank, Inc.



5 April 2011, 17:13

Attacks on German mTAN banking

Anti-virus software vendor F-Secure is reporting that a new malware, SpyEye, uses sophisticated methods to intercept mobile phone numbers. Its brother Zeus[2], SpyEye appears to have its own methods of user authentication employed by financial institutions.

The mTAN[3] procedure, introduced by many German banks, involves the bank sending a text message to the user's mobile phone number. An online banking transaction is left with no opportunity to interfere with this data.

Consequently, Zeus and SpyEye have learned to circumvent the mTAN procedure by sending a text message to the user's mobile phone. The user is asked to enter their mobile phone number and IMEI. A little later, they receive a message containing what purports to be an installer for the new certificate. If they launch the installer, the following message (in German) is displayed: "Die Seriennummer des Zertifikats: 88689-1299F" (The serial number of the certificate: 88689-1299F).

Malware Targets Bank Accounts 'Gameover' Delivered Via Phishing E-Mails

01/06/12

Cybercriminals have found a way to bypass your bank's security. Auto-generated phishing emails from the Federal Reserve Bank of San Francisco are being sent to thousands of recipients. The result is a "game over" for your bank account.

Methods of user authentication employed by financial institutions are being targeted by malware. If you receive a phishing email, it's definitely "game over."

Gameover is a newer variant of the Zeus malware, which targets banking information.

~~Static password~~ ~~TAN, iTAN, other simple OTP~~

eFrauds in the Region

The collage features several overlapping screenshots of banking websites:

- ING BankOnLine**: Shows a navigation menu with options like "Jstavenia", "Bezpečnosť", "Regulácie", "Pomoc", "Drukuj", and "Odšviez".
- CIB BANK**: Shows a login form with fields for "Príhlasenie meno", "Príhlasenie heslo", and "PIN karty" (circled in red). It also includes a language selection dropdown.
- ERSTE BANK**: A large white box on the right contains a Hungarian notice titled "Kedves számlatulajdonos!" (Dear account holder!). The text discusses a system update on December 1, 2006, and asks customers to verify their account information. It includes a link: <http://www.erstebank.hu/verification>.
- Other screenshots**: Show various parts of banking interfaces, including "Pharming/Phishing 'Pozor na útoky'" (Warning of attacks) and "Maximálna informáciok" (Maximum information).

Local Situation

Successful criminal prosecutions

Russian bank fraud case

Group #1

- stole 600 000\$ in a single transaction
- case in court
- used phishing sites (hosted on Gogax)



Group #2

- stole 832 000\$ (over 1 month)
- case in court
- used phishing sites (hosted on Gogax)

Interesting facts about



**Cybercriminals in Russian Speaking Countries:
\$ 2.5 Billion (~36% of Total)
20,400,000,000 Grivnas!!!**



Phishing Sites are in the Corner

TOP 10 COUNTRIES THAT HOST PHISHING SITES JAN-MAY 2011

©2011 Websense, Inc. All Rights Reserved.



Regarding Targets?
Regarding Users & Their Devices?
Regarding Attack(er)s?

LEARNINGS FROM eBANKING ATTACKS & eFRAUD

Learnings from eBanking

- ✘ Weakest eBanking solution is attacked and hit the most
- ✘ Bank Brand popularity attracts attackers online fraud also

Learnings from eBanking

- ✘ There are always some eBanking customers who fall into some trap
- ✘ User device popularity attracts attackers (at first)
- ✘ Customers systems ~~cannot~~ mustn't be expected to be secure

Learnings from eBanking

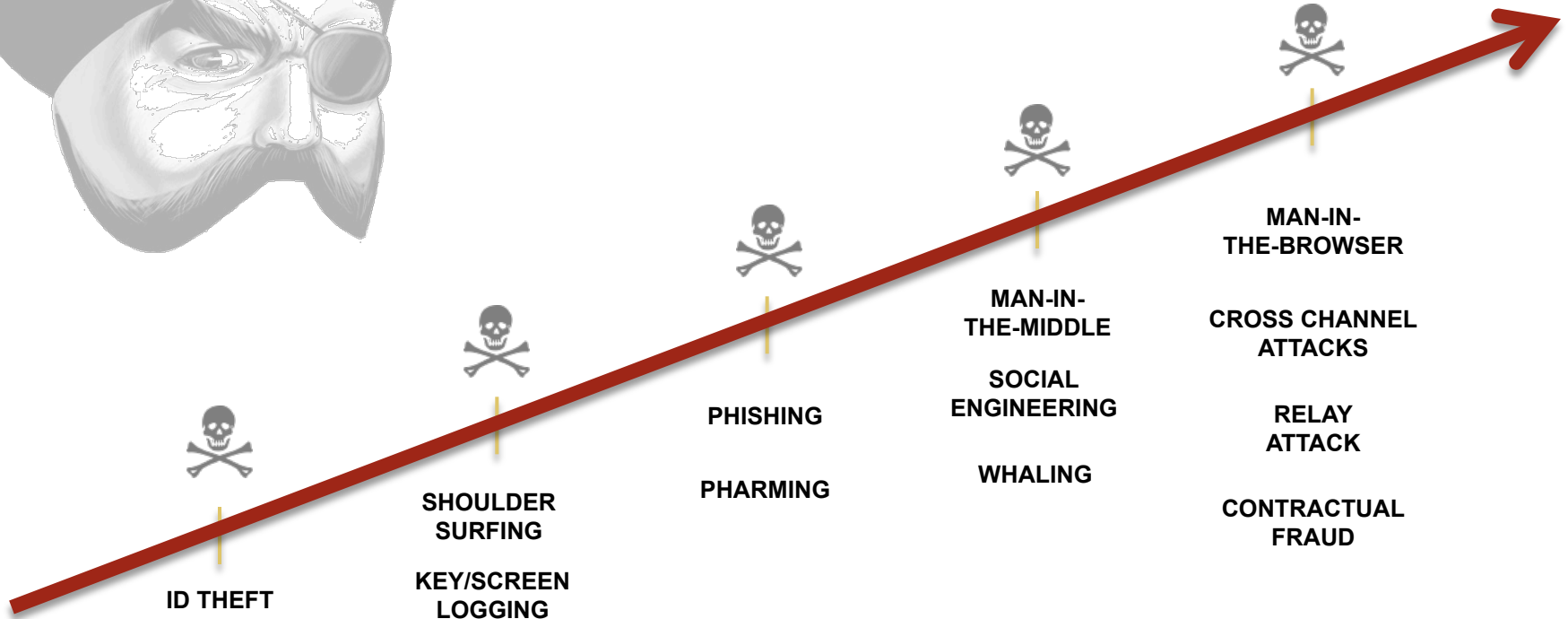
- ✘ Attackers are persistent if they find a profitable victim
- ✘ Attackers are adapting to increasing eBanking security measures (over time)



FRAUDS & MITIGATION

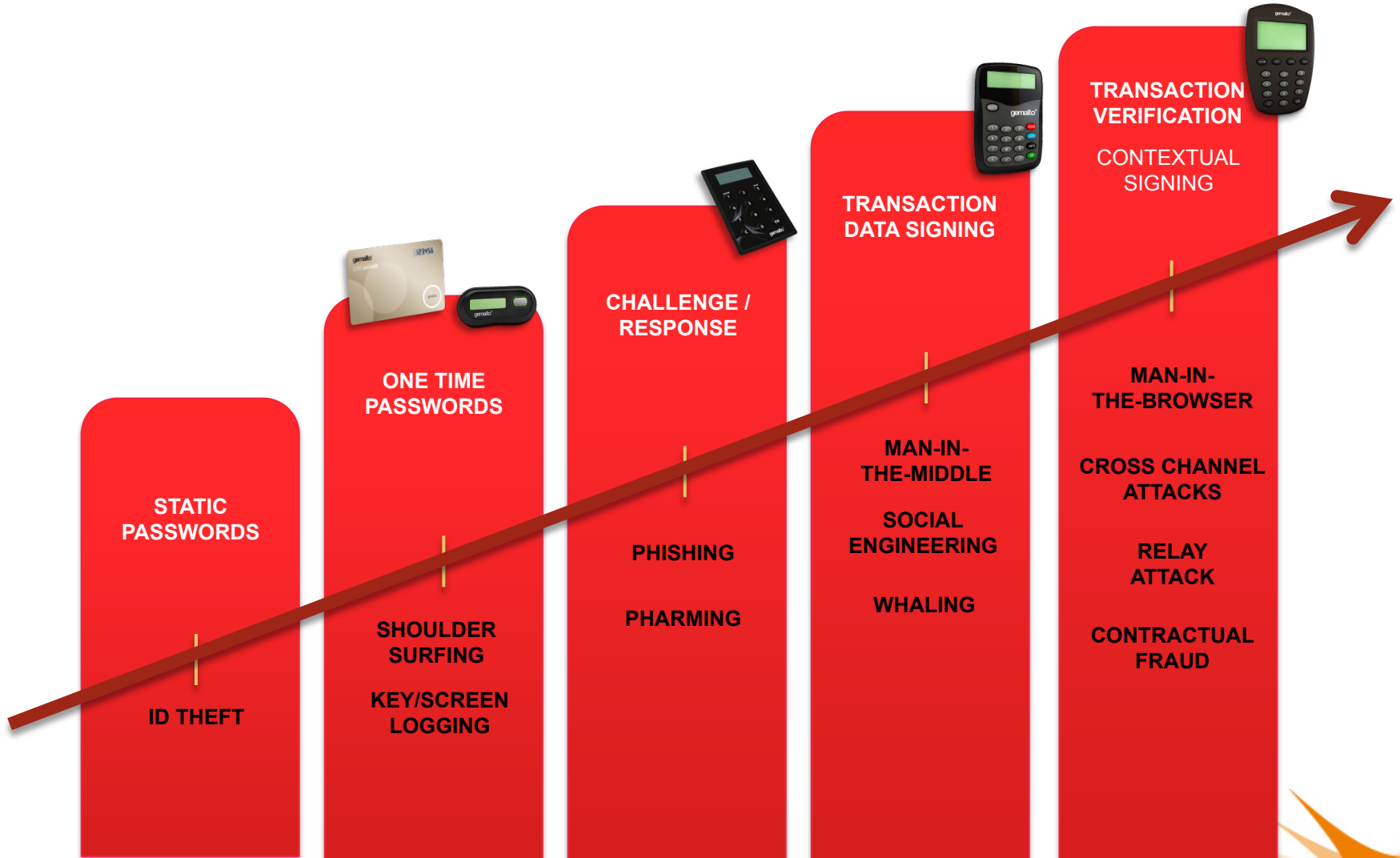
Identifying Business Needs...

eBANKING FRAUD IS GETTING MORE AND MORE SOPHISTICATED



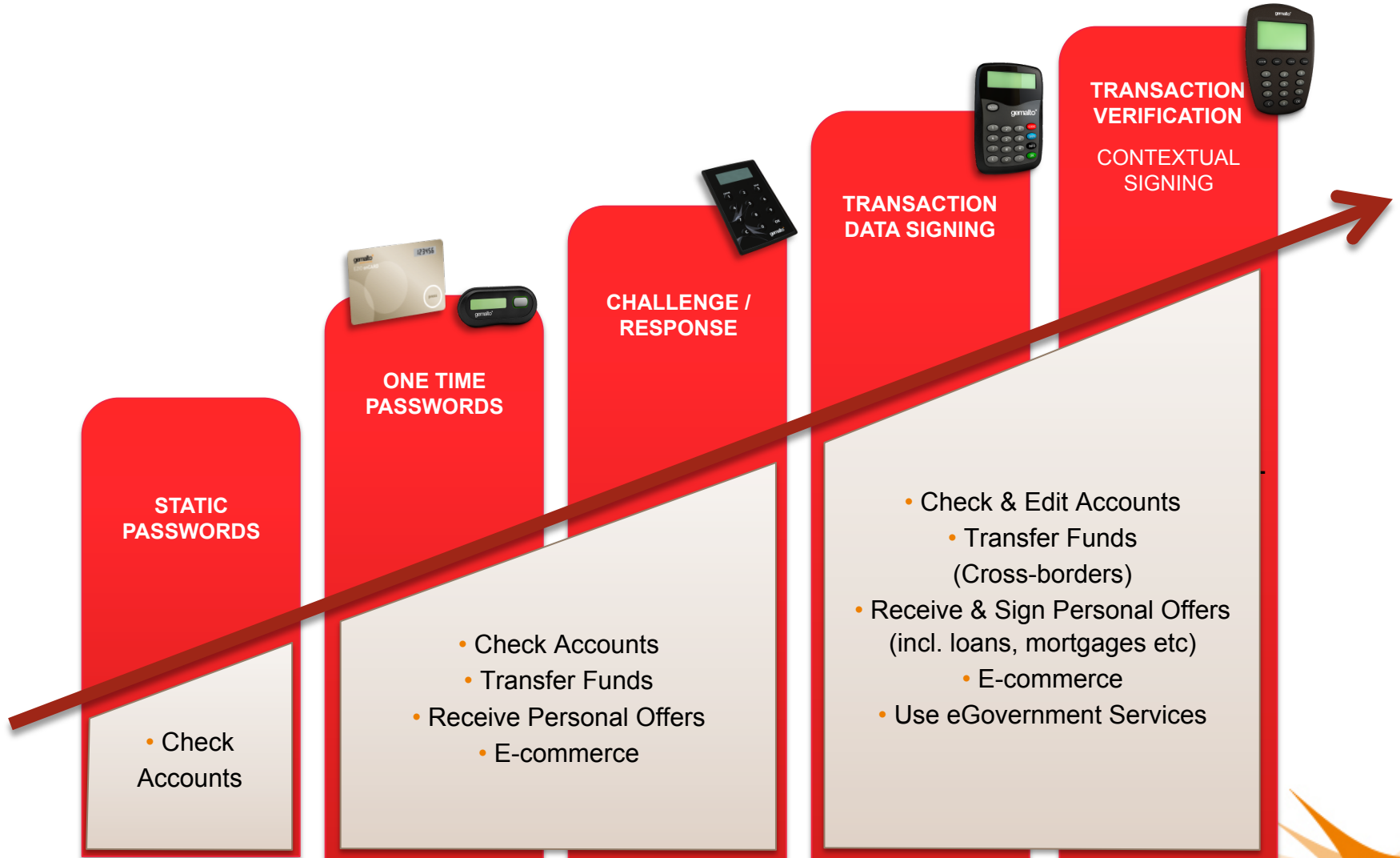
...and Showing How we Meet the Needs

USER-FRIENDLY MITIGATION OF ALL CURRENT AND FUTURE THREATS



...and What Services Banks Can Offer

TO GROW THEIR BUSINESS ACROSS ALL DIGITAL CHANNELS





GEMALTO'S SOLUTION

All Banks Follow the Same eBanking Path

...WE LIKE TO CALL IT THE EZIO WAY



VISIT WWW.EZIOWAY.COM



eBankingSecurity.net

THE 9 STEPS OF SUCCESSFUL E-BANKING SECURITY DEPLOYMENTS

Ezio Highlight: Segmentation

EVERY E-BANKING USER IS THE SAME. **HIGHLY INDIVIDUAL.**



Ezio Highlight: Segmentation

LEVERAGE THE **INDIVIDUALITY** OF YOUR CUSTOMER BASE



Ezio Suite



PIN PAD CARD READERS (CAP/EMV)



EZIO EDGE



EZIO CLUB



EZIO THIN



EZIO THIN OPTIC



CONNECTABLE PIN PAD CARD READERS (EMV/CAP/ PKI)



EZIO SHIELD PRO



EZIO SHIELD TALK



PKI CLIENT-SIDE SOLUTIONS



EZIO PC USB-TR



EZIO PKI CARD



EZIO CLASSIC CLIENT



MOBILE SOLUTIONS



EZIO bySMS



EZIO MOBILE SDK



EZIO MOBILE TOKEN



TOKENS



EZIO LAVA



EZIO PICO
NEW !



EZIO onCARD



EZIO onCARD PAD



SERVER & LIBRARY



EZIO SERVER



EZIO LIBRARY
NEW !

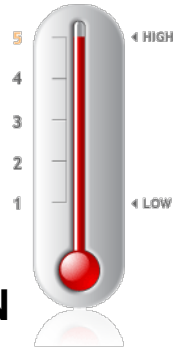


Product planned to be released end 2012

User-friendly Technology

DYNAMIC SIGNATURES

ASK THE RIGHT QUESTIONS AT THE RIGHT TIME



LOW RISK TRANSACTION

- Challenge:
986 523
- Enter PIN:

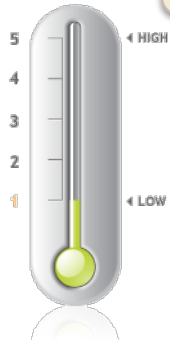
- Response:
567 890



HIGH RISK TRANSACTION

- Challenge:
635 265
- Currency:
1) EUR 2) USD 3) GBP...
- Amount:
5 000,00
- Enter PIN:

- Response:
723 905



DS

Why Gemalto Solution?

Ezio Suite is the market's most **versatile** and **easy-to-implement** eBanking security solution with a **proven track-record** of customers.



**ONE
SERVER**
ALL
CHANNELS

**MULTIPLE
SECURITY
METHODS**

**A
COMPLETE
SUITE OF
EZIO
DEVICES**

40m
DELIVERED
DEVICES

50m
HAPPY
USERS

150+
BANKS

Local References



Bank	Scope	Status
Delta Bank	100k SMS	In progress
Raiffeisen Aval	100k SMS 5k tokens	Done In progress
BM Bank	5k tokens	In progress





DEMO



SUMMARY

Summary

✧ eBanking Security

- Attackers are very creative in tricking online banking customers
- eBanking fraud is still evolving
- Banks has to learn to adequately improve eBanking security over the years

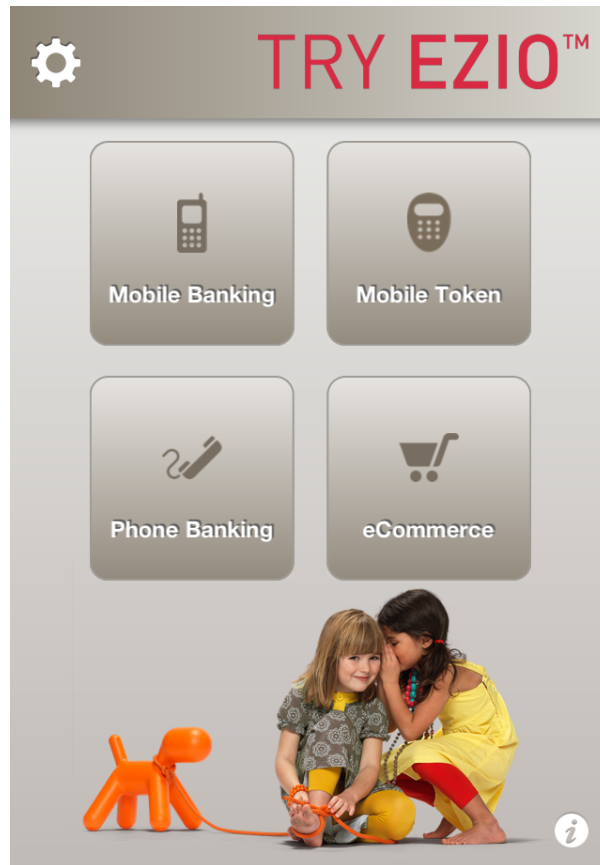


Thank You!

**Building
Value
Together**

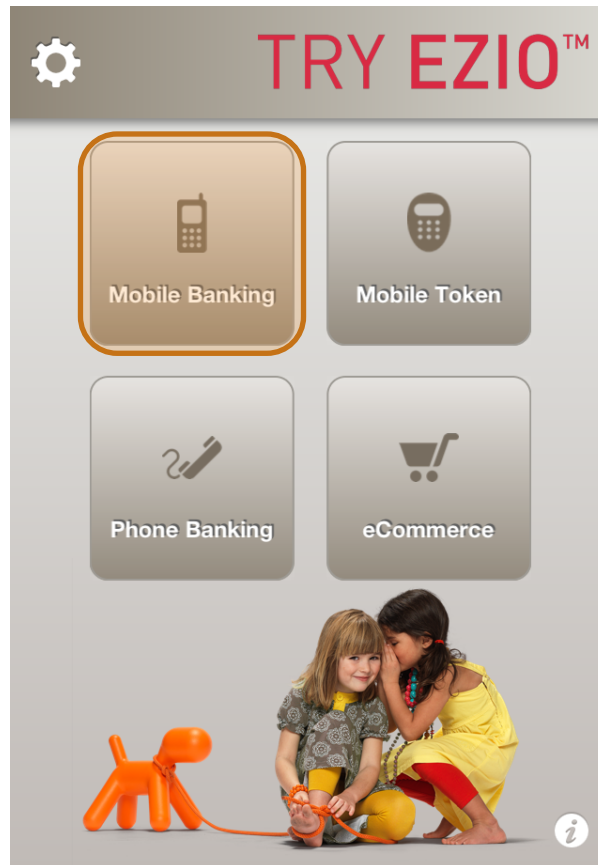
Mobile Bank

Main Menu



Mobile Bank

Mobile Banking



Mobile Bank

Mobile Banking

Cancel TRY EZIO™

User ID
zszalai

Challenge Response
3930 9210

Log in

gemalto

Cancel TRY EZIO™

PIN Code Required
Please enter your PIN code.

●●●●

Cancel OK

Log in

1	2 ABC	3 DEF
4 GHI	5 JKL	6 MNO
7 PQRS	8 TUV	9 WXYZ
	0	✕

gemalto

Logout TRY EZIO™

National payment >

International payment >

Personal account (62 45 38)
1694.30 EUR

Savings account (62 49 78)
8000.00 EUR

Company account (62 91 10)
24837.00 EUR

gemalto

