

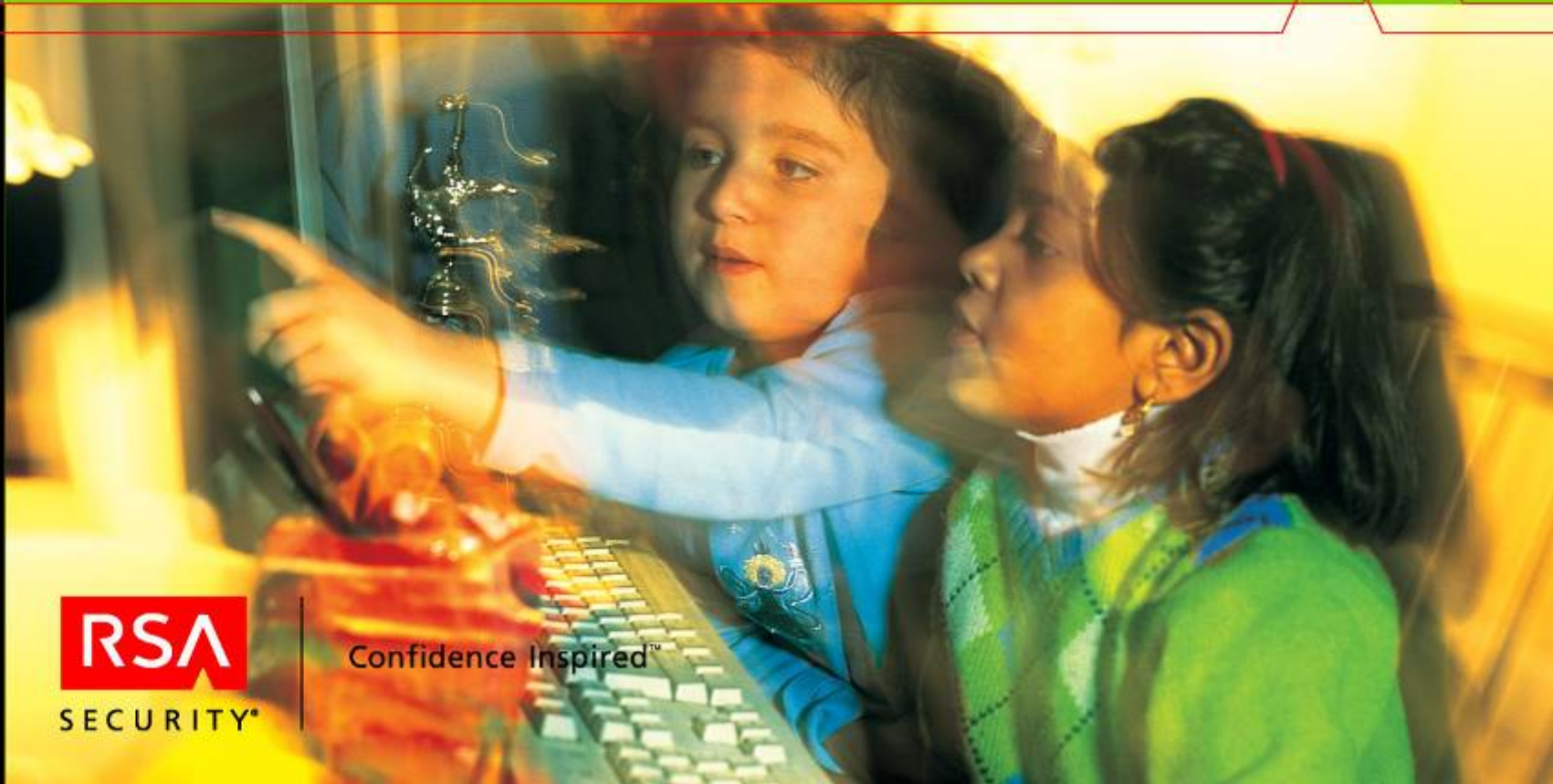
Adaptive Authentication from RSA

Consumer Authentication in a Changing World

Version 5.4

Andrew Moloney,
November 10/ 11, 2005

Budapest/ Praha CIP Roundtable Events



Confidence Inspired™

RSA – A trusted partner in the Banking Community

- 86% of the Top 50 World Banks Use RSA Security
- 92% of the Top 25 World Banks Use RSA Security
- ~2M tokens, in Customer facing Applications
- Finance Customers in Europe include:

Strong authentication since 1987

Drop rolling SecureID out to ~500k customers

Adding 50k new Internet banking customers per month

Logos visible in the collage: CREDIT SUISSE, ABN-AMRO, UBS, BARCLAYS, Deutsche Bank, UniCredit, Volkswagen Bank, VISA, Rabobank, Banca Popolare di Sondrio (suisse), BOUTTS, ADP, Förenings Sparbanken, BTV 3 Banken Gruppe, Landsbanki, PROBANKA, BANCA POPOLARE DI VERONA - BANCO S.GEMINIANO E S.PROSPERO, MasterCard, RSA SECURITY, Julius Bär.

Consumers under attack and “Losing the Faith”



Lack of confidence in online transactions

Of online consumers, identity theft concerns have convinced...

- **35%** to not enroll or use online banking or bill payment
- **41%** to not apply online for a financial product
- **33%** to not shop online with a credit card

(Source: Forrester Research)

Phishing attacks proliferate

- 2,870 active phishing sites were reported in March '05 alone—an **increase of 28% a month**
(Source: Anti-Phishing Working Group)
- Nearly **1 million U.S. consumers were defrauded** via phishing between May '03 – '04
- This cost banks and card issuers more **\$1.2 billion** in direct losses

(Source: Gartner)

Card fraudsters target the Web: 08/11/2005

- **Card-not-present (CNP) fraud jumped 29% to £90.6m in the first half of the year, mainly due to increasing levels of Internet fraud,** according to the latest stats from the UK's Association for Payment Clearing Services (Apacs). Apacs says the introduction of chip and PIN in the UK helped cut overall card fraud by 13% in the six months to the end of June 2005 to £219.4m, compared to £252.6m last year. The technology has also helped reduce counterfeit card fraud, which fell 31% to £45.6m.
- **But the roll out of chip and PIN has led to fraudsters committing more Internet, phone and mail order fraud.** CNP rose to £90.6m in the first six months of this year, compared to £70.2m last year. **Online card fraud accounted for the largest part of CNP fraud, increasing five per cent to £58m in H1.** The research also shows that **online banking fraud losses more than trebled** in the first half to £14.5 m, compared with £4m last year...

Business Drivers are Growing



Increase consumer confidence

- Increase customer satisfaction and retention
- Drive consumer transactions from offline outlets to online
- Provide differentiated solutions
- Enhance security offerings
- Increase market share

Meet compliance requirements

- Audit trail can be critical
 - BASEL II, Sarbanes Oxley Compliance
 - Trail only as good as authentication
- EU regulatory organizations are now recommending stronger methods of authentication
- Prevent account takeovers and reduce online fraud

The Goal Posts are moving for Online Banking...

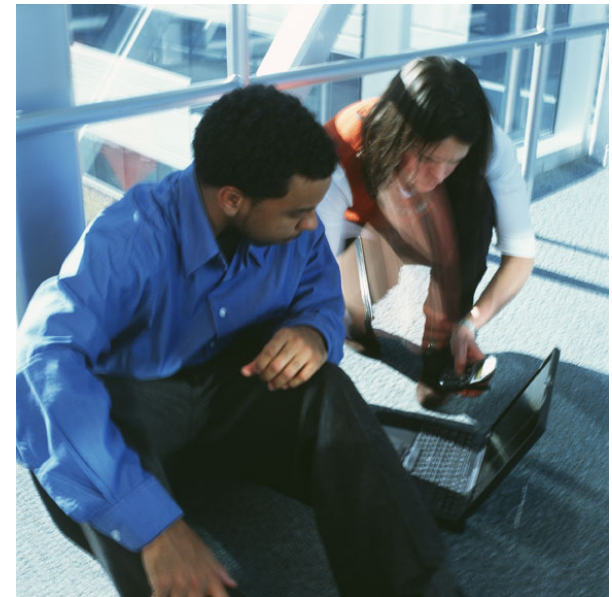


- Move from “silo’ed” online presence, to integrated service delivery mechanism
 - But more channels to the customer must be supported
- Phishing attacks on the increase and now targeting European banks*
- Desire to use online banking as a revenue generation rather than merely cost saving tool

How can this be achieved if Consumers are losing faith?

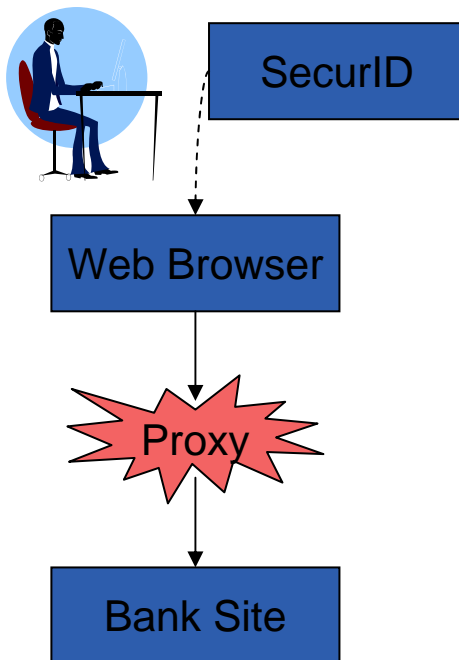
...and threats will continue to evolve

- Today's threats are simple, but future ones are more complex
- Phishing is a business. Attacks today are only as complex as is needed to be successful
 - Future threats will grow more sophisticated, pulling on multiple techniques to achieve goals
- Online banking fraud losses generally not substantive as yet, but risks and trends are clear



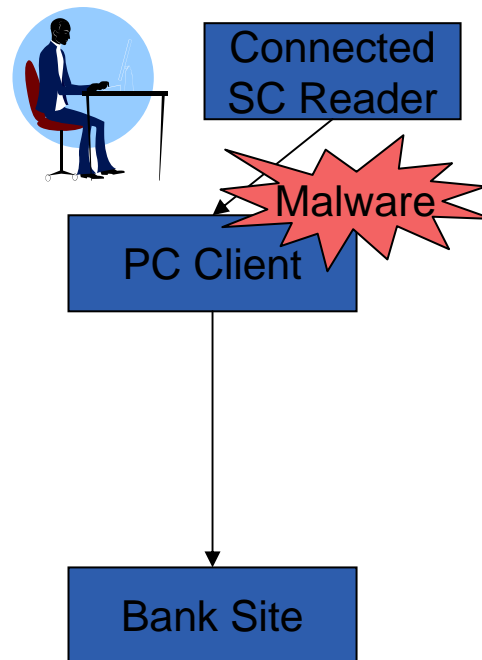
The “Near” Future in Online Fraud...

Online MITM



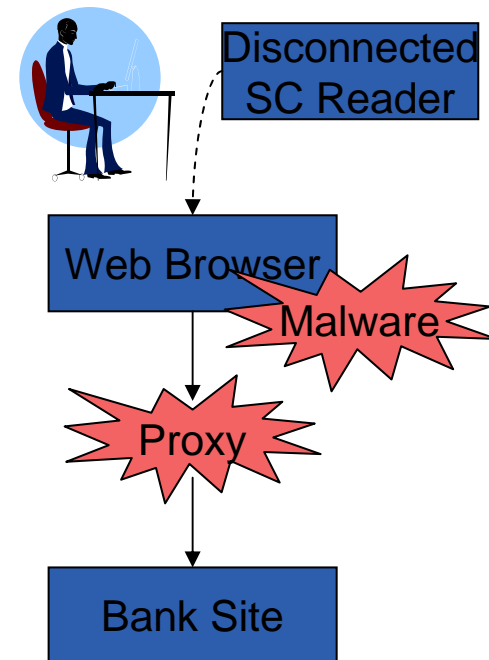
User lured to a fake web site sitting between the user and the real site. Thief intercepts the flow of information and replaces a/c no.s, values, etc.

Malware



Malware on users desktop, sitting between the PC and the smart card. It sends false transactions to the smart card to be signed without the users' knowledge.

Pharming



Malware modifies the PC's configuration to direct traffic to a fake site. The fake site modifies information and executes illegitimate transactions.

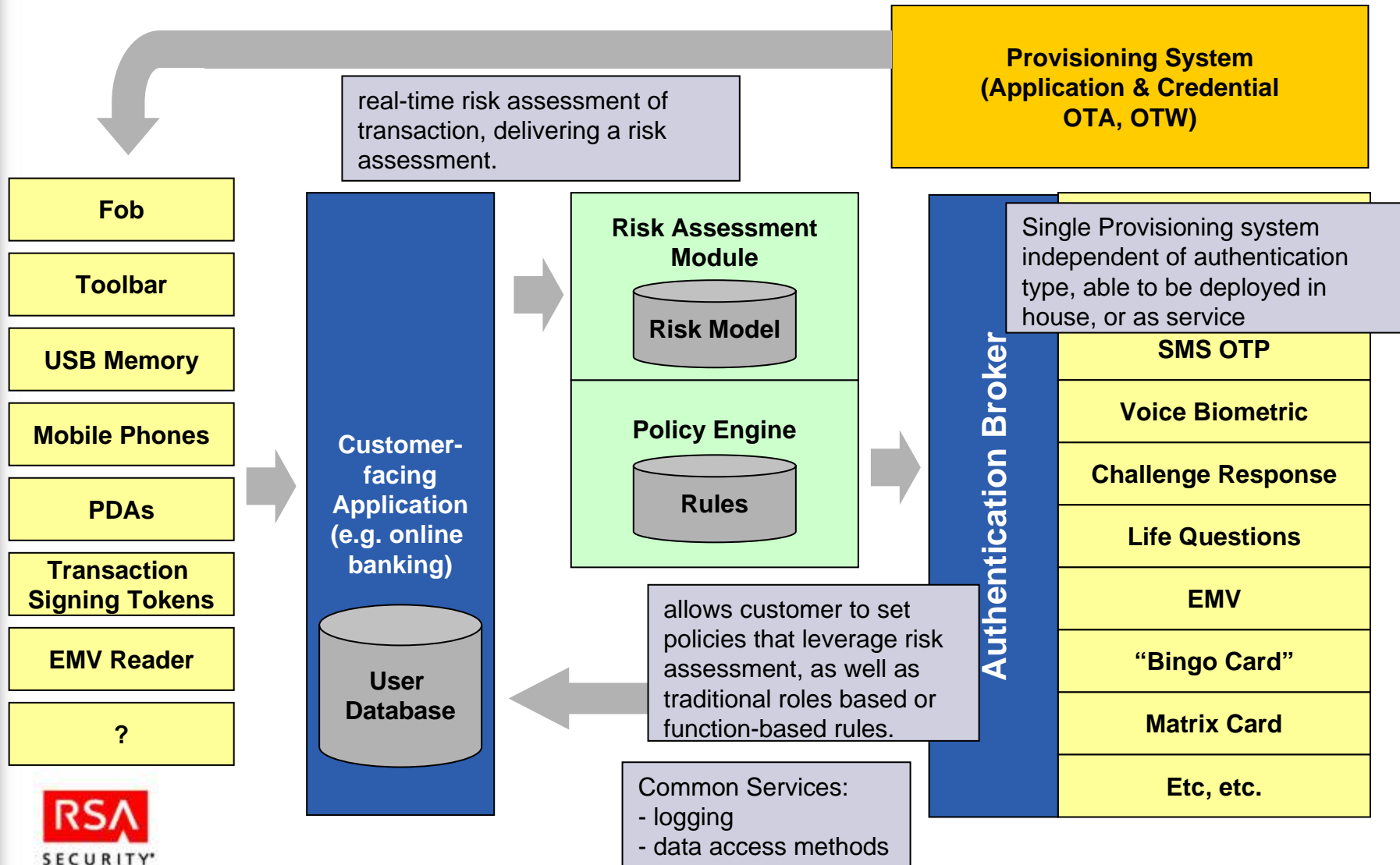
Time to Act...

A Holistic Authentication strategy is required that:

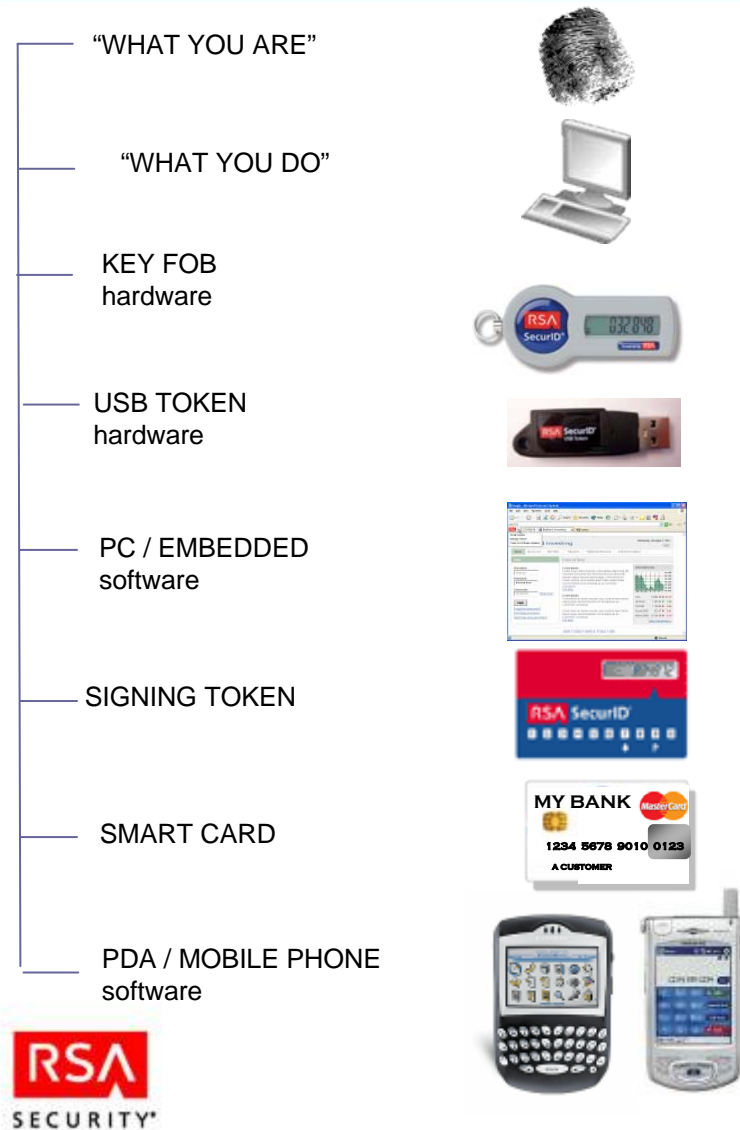
- Optimally addresses the people and processes with the appropriate management policy
- Is part of an integrated strategy which flexes and evolves as threats and organisations change and evolve
- Can be applied equally well to internal and external constituents
- Delivers optimal business results
- Recognises that security is never just a technical, but is a ultimately a business decision

Introducing Adaptive Authentication from RSA Security

Adaptive Authentication Framework



Multiple Authenticators will be required...



- Multiple authenticators will grow to be deployed across different channels of access
- Different solutions suitable for different customer segments
 - Accessibility/ Convenience
 - Level of Risk
 - Non-repudiation
- More than one authentication route may be needed

Professional Services Support for Adaptive Authentication



ARCHITECTURE &
STRATEGY
DEVELOPMENT

» Development of secure and scalable technology and process framework for service deployment and management

ON-PREMISE
SOLUTION
INTEGRATION
SUPPORT

» On-premise solution integration and implementation

ON-SITE HELP
DESK TRAINING
WORKSHOPS

» Call center workshops
» Networked-Service or On-Premise solution functions
» Also covers self help training and the escalation process

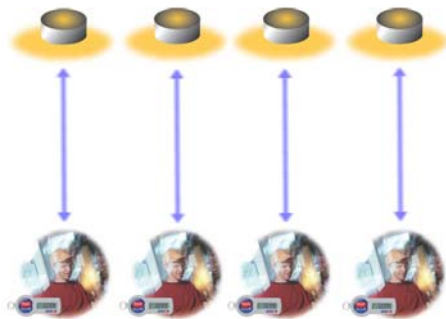
USER INTERFACE
DESIGN AND
DEVELOPMENT

» Design and develop the interfaces for all UIs necessary to implement and manage each function of the solution

Unrivalled Expertise across the Value Chain

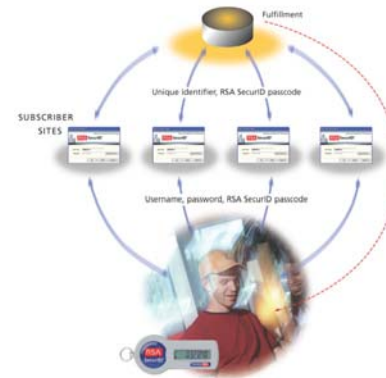
Deployment: On Premise or Managed Service

“On-Premise” Authentication Model



- » Implemented either with Authentication Manager or SecurID Authentication Engines (SAE)
- » Current SecurID authentication occurs on a one-to-one basis between users and sites
- » Different networks would require multiple tokens

“Networked-Service” Authentication Model



- » integrates with RSA’s Service APIs
- » Authentication via single token to any site that subscribes to the RSA Consumer Authentication service
- » Customers benefit from superior economics of shared service, distribution without giving up existing controls

Adaptive Authentication from RSA Security



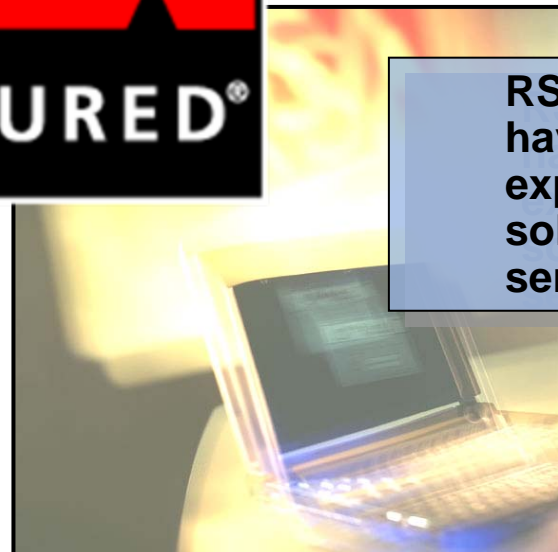
Strong Authentication has come of age in banking



Authentication methods will evolve as new access methods and vectors of threat emerge



Security must extend throughout all elements of the application



RSA Security have the skills, experience, solutions and services to deliver



Next Steps..

We invite you to meet with us over the next few weeks to learn more about our strategy and to evaluate how Adaptive Authentication can meet your business requirements.

- Contact:

Cezary Prokopowicz, Territory Manager

e: cprokopowicz@rsasecurity.com

tel: + 43 699 1941 4028



Confidence Inspired™