RSACONFERENCE2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Mind Over Matter: The Pragmatic, Strong, and Smart Approach to Security

SESSION ID: SPO1-T09

Ammar Alkassar
CEO
Sirrix AG security technologies
Saarbrücken, Germany

Dr. Kim Nguyen
Managing Director
D-Trust GmbH
Chief Scientist Security
Bundesdruckerei GmbH
Berlin, Germany

In This Presentation, we will motivate

- That mass application of current IT security approaches will only lead to a hamster wheel
  - We need a smart approach, that fundamentally addresses the threats
  - We need a pragmatic approach as IT security is not expected to change user experience
  - We need a strong approach as threats today are backed by profitable business models
- And thus, IT security is just before an innovation leap

Agenda

- Part 1: Expolit-Protection: Pro-Active Security (Ammar Alkassar, Sirrix)
- Part 2: Authentication and Identity (Kim Nguyen, Bundesdruckerei/D-Trust)

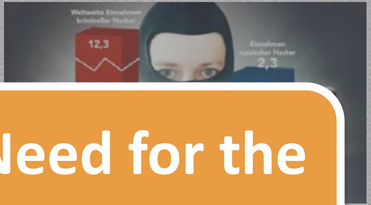
RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Exploit-Protection
Pro-Active Security

Ammar Alkassar
Sirrix AG

Driver of Threats


Weltweite Einnahmen krimineller Hacker
12,3
Einnahmen russischer Hacker
2,3

Cyber-
Crime

Need for the
SMART

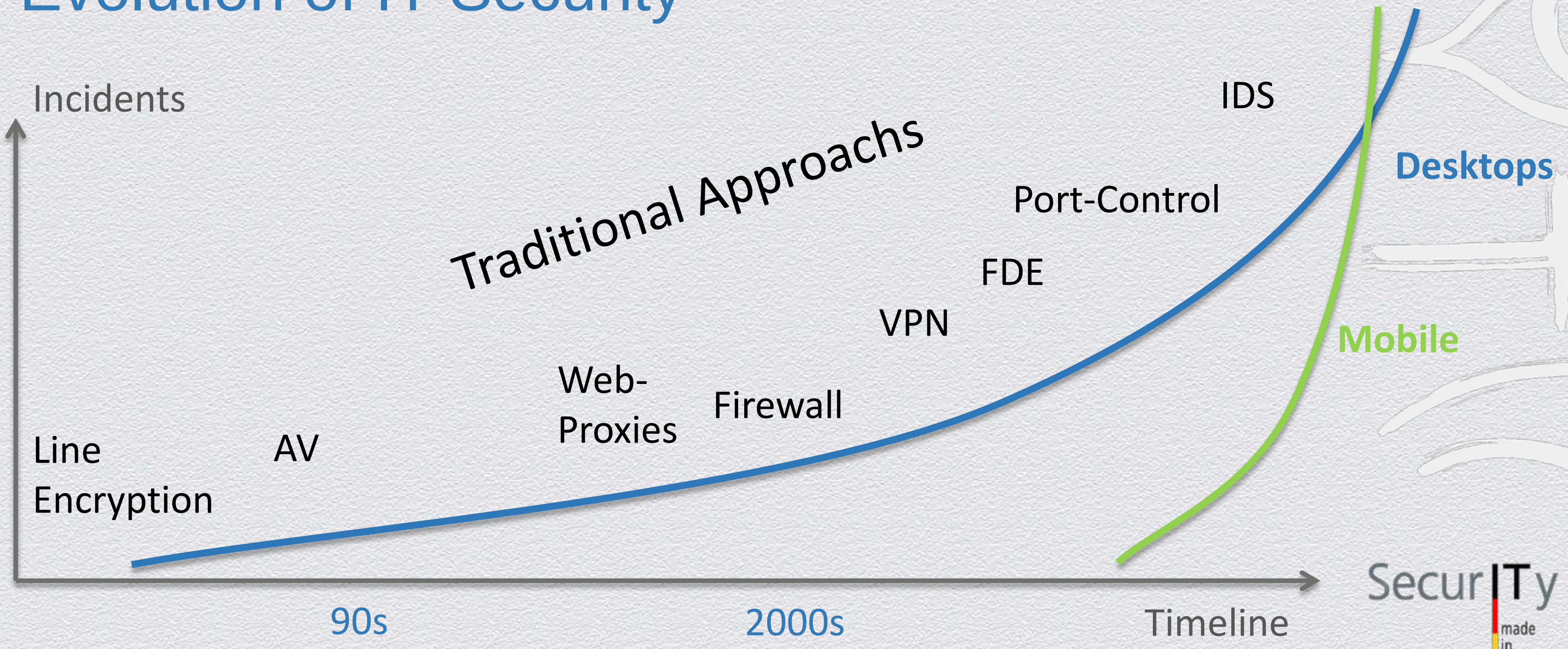
Need for the
STRONG

Advan
Persist
Threa
(APT)

Collateral
Cyber-
ge

Need for the
PRAGMATIC

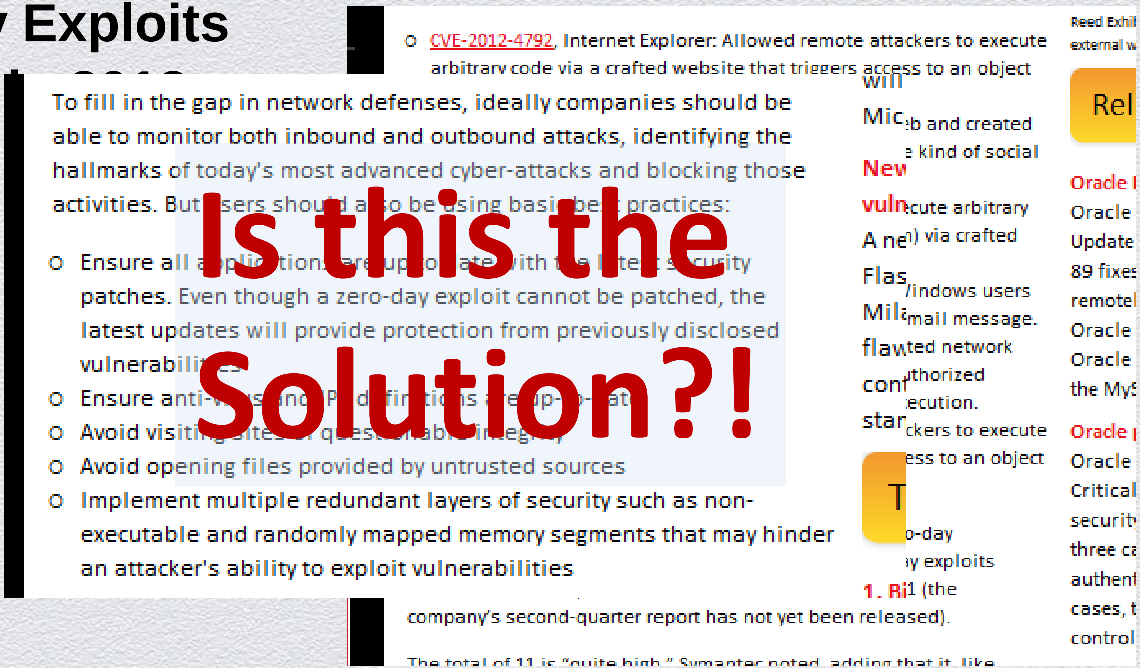
Evolution of IT Security



SecurITy made in Germany
TeleTrusT Quality Seal www.teletrust.de/itsmig

Threat, Dominating the Future

- **Zero-Day Exploits Escalate**



- CVE-2012-4792, Internet Explorer: Allowed remote attackers to execute arbitrary code via a crafted website that triggers access to an object

will

Mic ...b and created

... kind of social

New

vuln ...cute arbitrary

A ne ...) via crafted

Flas

... /indows users

Mil ...mail message.

flaw ...ted network

conf ...uthorized

...ecution.

star ...ckers to execute

...ess to an object

T

...-day

...y exploits

1. Ri ...1 (the

company's second-quarter report has not yet been released).

The total of 11 is "quite high," Symantec noted, adding that it, like

Reed Exhi

external w

Rel

Oracle

Oracle

Update

89 fixes

remotel

Oracle

Oracle

the MyS

Oracle

Oracle

Critical

securit

three c

authent

cases, t

control

To fill in the gap in network defenses, ideally companies should be able to monitor both inbound and outbound attacks, identifying the hallmarks of today's most advanced cyber-attacks and blocking those activities. But users should also be using basic best practices:

- Ensure all applications are up to date with the latest security patches. Even though a zero-day exploit cannot be patched, the latest updates will provide protection from previously disclosed vulnerabilities
- Ensure anti-virus and IPS definitions are up-to-date
- Avoid visiting sites of questionable integrity
- Avoid opening files provided by untrusted sources
- Implement multiple redundant layers of security such as non-executable and randomly mapped memory segments that may hinder an attacker's ability to exploit vulnerabilities

Is this the Solution?!

The Proactive Approach

- Today’s approaches fail in providing sustainable security

Still applied approaches

- „Airbag approach“:
  If it happens, it should hurt less.

Required approach :

- „ESP strategy“:
  Avoid skidding,
  before it happens.

SecurITy made in Germany
TeleTrusT Quality Seal
www.teletrust.de/itsmig

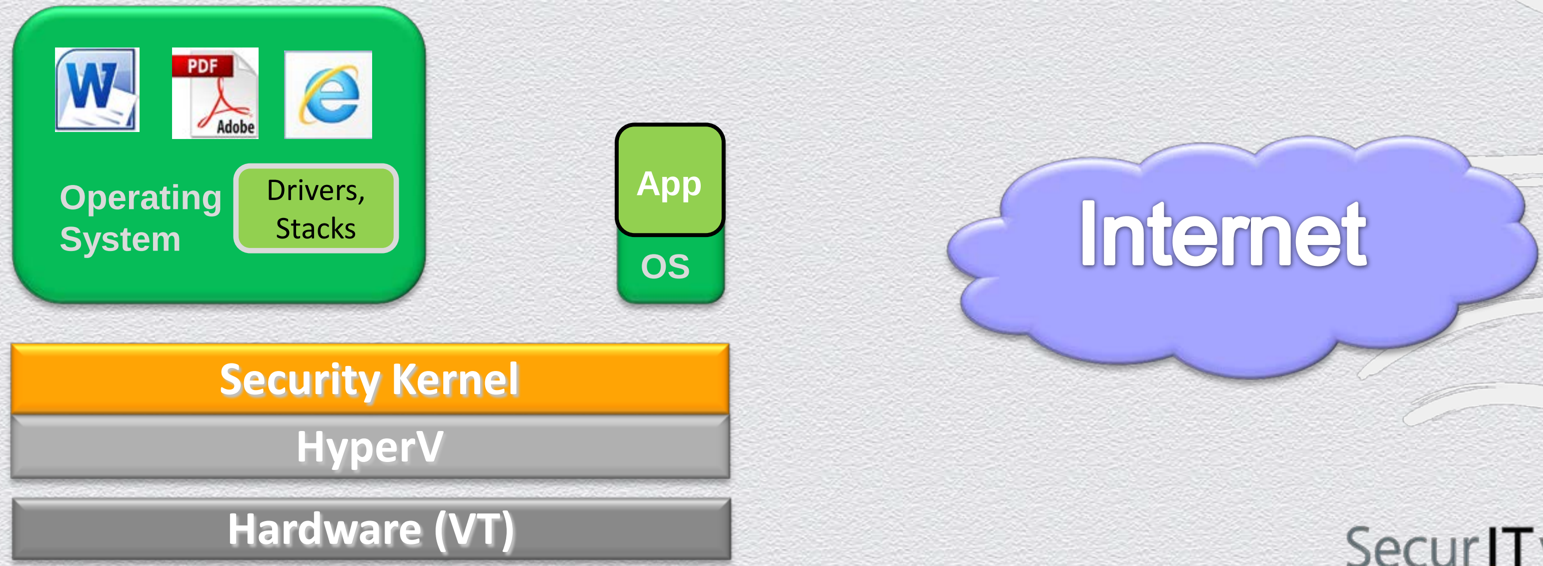
Approaches to Next Generation

- Sandboxing-Techniques
  - App-Level, e.g., as Adobe Reader, Google Chrome
  - OS-Level, e.g., Invincea, Sandboxie, Trustware Bufferzone, ZeroVulnerabilityLabs
- (Execution on Remote Server)
- Full Desktop-Virtualization with Security Kernel
  - E.g., SINA VW, GeneralDynamics TVE, TrustedDesktop
- Game-changer: Micro-Virtualization with Security Kernel

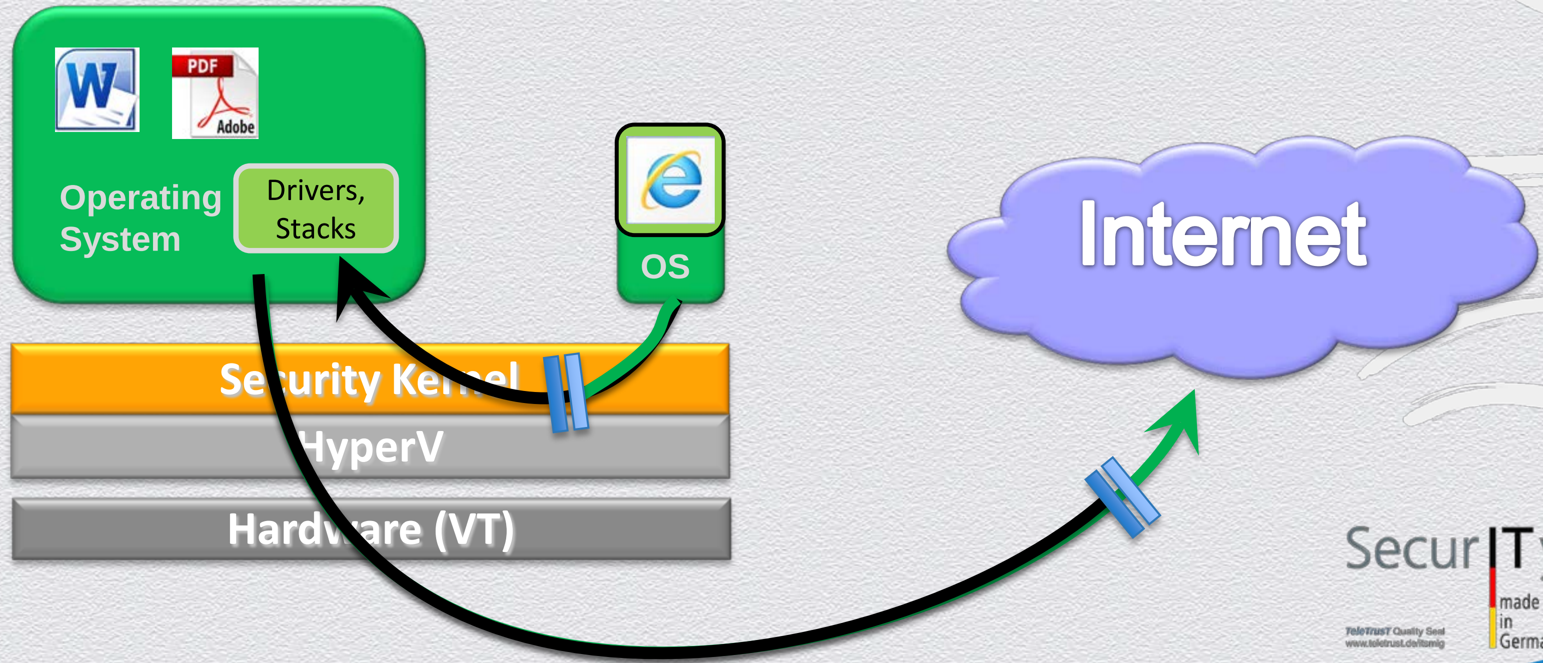
Requirements

- Don´t change the user‘s experience (Pragmatic)
- Provide pro-active protection (Strong)
- Keep the solution lightweight (Smart)

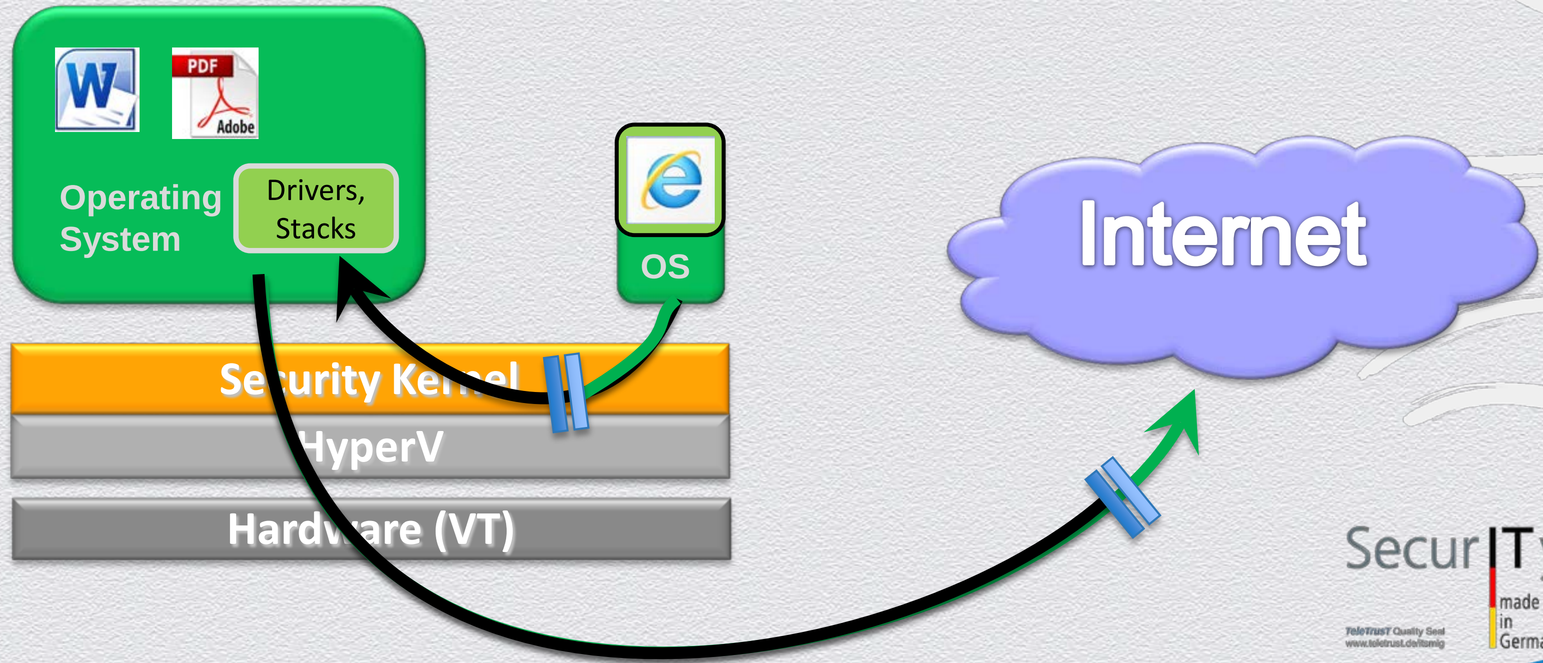
Web-Access Protection



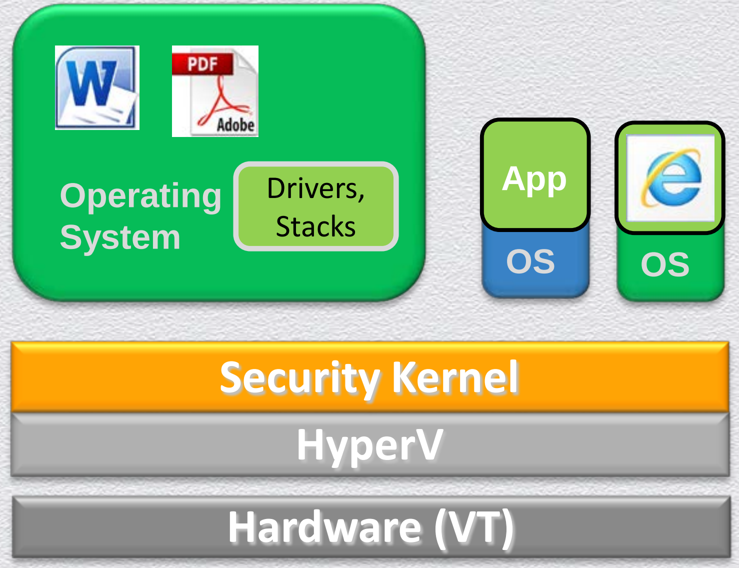
Web-Access Protection



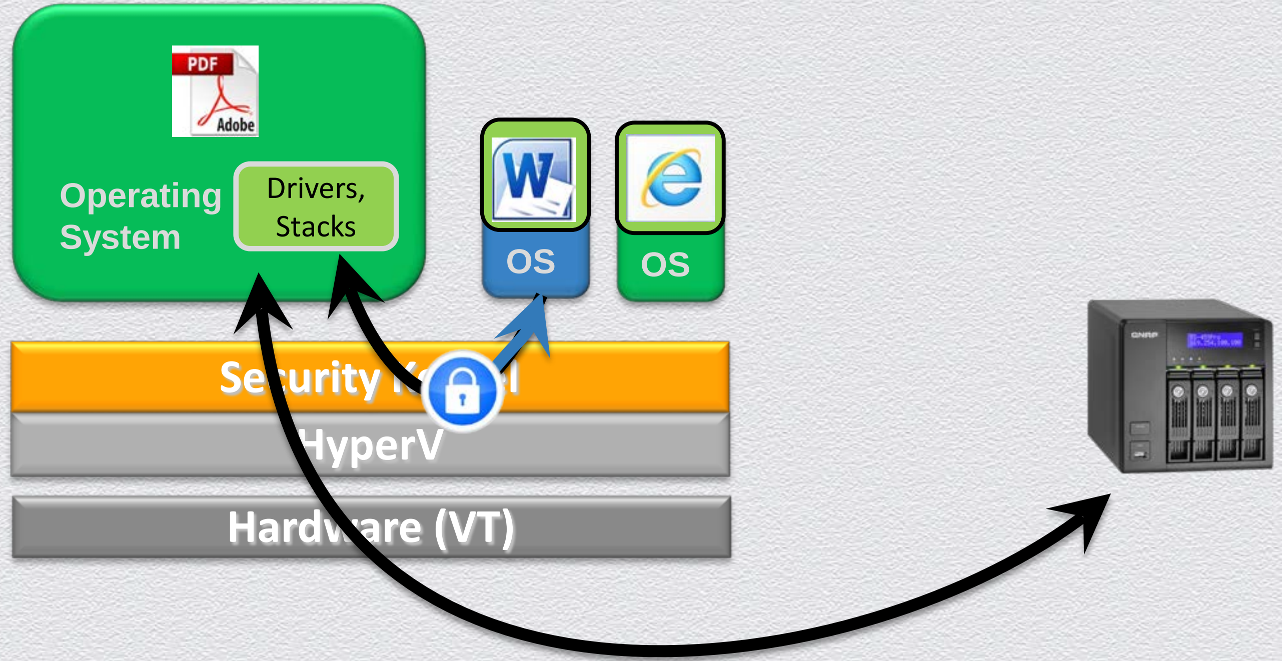
Internet-Access



Micro-Virtualization



Micro-Virtualization



SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig

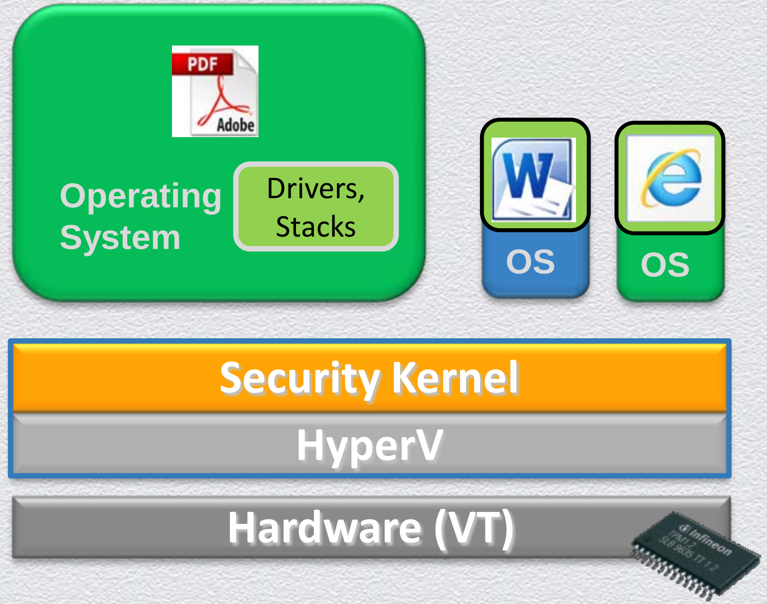
Sirrix AG
security technologies

BUNDESDRUCKEREI

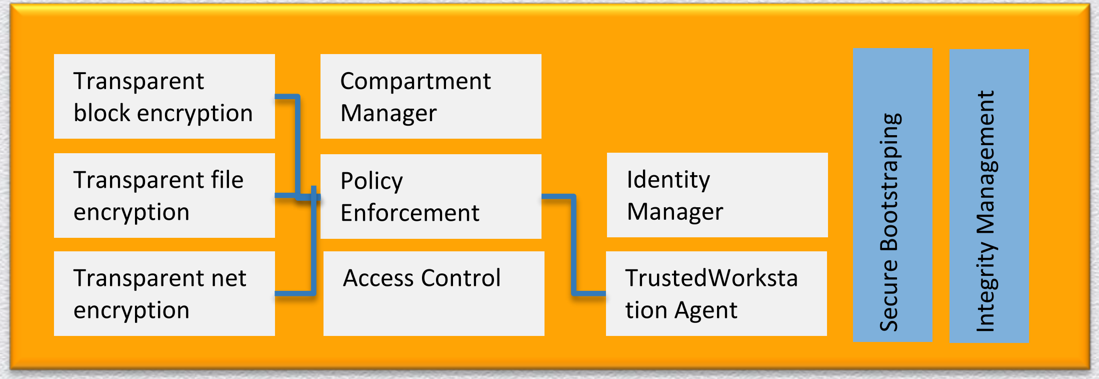
#RSAC

RSACONFERENCE2014

Micro-Virtualization



Security Kernel



Challenges, Exemplary

- Lightweight, secure and dynamic full-virtualization (including Kernel)
- Defining and preserving the integrity of OS and Apps
  - Throw-Away Write-Cache
- Efficient separation lines and labeling
  - Trusted Virtual Domains (TVDs, EU FP7-TClouds)
- Trusted Computing Based is significantly reduced
  - But still "doors" need to be evaluated

Increasing Number of Vendors

- Desktop Full-Virtualization:
  Secunet SINA Virtual Workstation, Sirrix TrustedDesktop, GD TVE, …

- Sandboxing and Micro-Virtualization
  Bromium (vSentry), Invincea (Containment), Sirrix (BitBox, TrustedApp)

Approach works for Mobiles

- E.g., BizzTrust
  - Enables strict separation between business and personal apps and data
  - Prevents from malware infection and APT attacks , even in the presence of exploits in android framework or in any app.
  - Provides information-flow control and includes strong encryption for stored data and communication data.
  - Uses TURAYA™ Type-Enforcement Security Kernel
  - Fully manageable with TOM

SecurITy made in Germany
TeleTrusT Quality Seal www.teletrust.de/itsmig

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Authentication and Identity made easy

Kim Nguyen
Bundesdruckerei GmbH
D-Trust GmbH

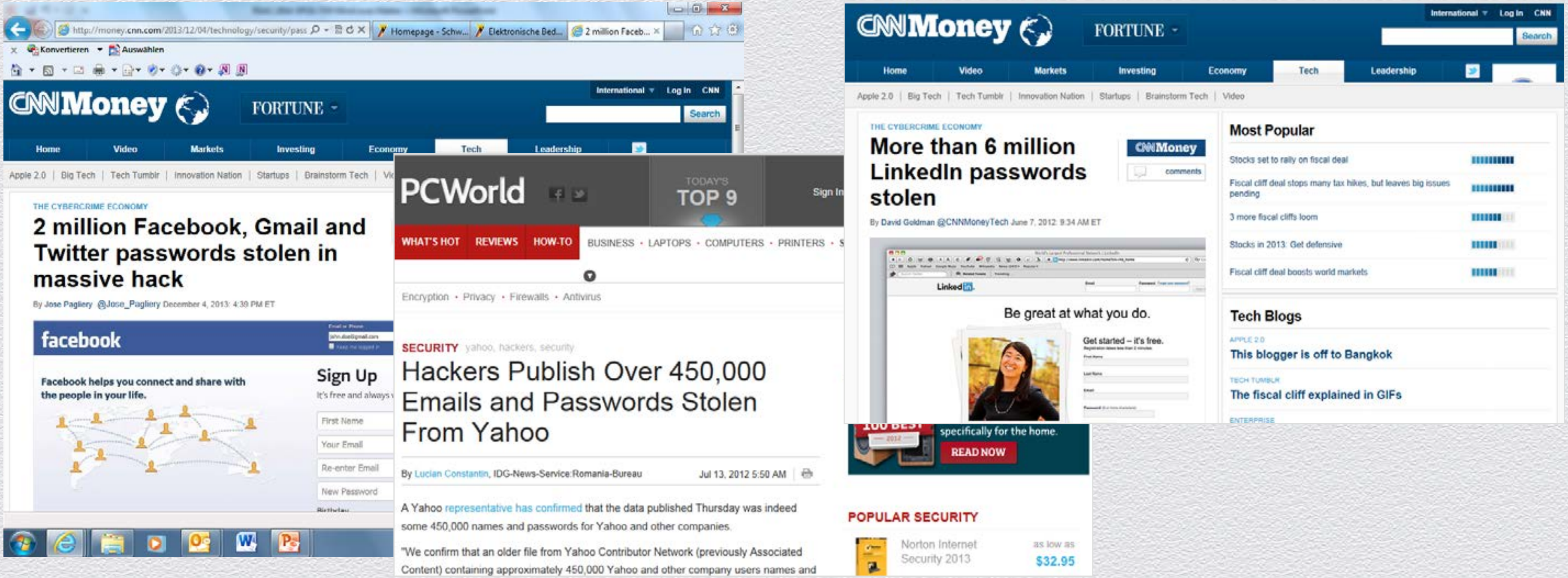
Agenda

- Authentication, security and user experience
- FIDO Alliance approach
- A layered authentication and identification model
- Bridging the gap between different worlds:
  private and governmental ID

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

© The New Yorker

Identity in the Internet … is a hot and critical topic!


http://money.cnn.com/2013/12/04/technology/security/pass
Homepage - Schw...
Elektronische Bed...
2 million Faceb...
Konvertieren
Auswählen
CNNMoney
FORTUNE
International
Log In
CNN
Search
Home
Video
Markets
Investing
Economy
Tech
Leadership
Apple 2.0 | Big Tech | Tech Tumblr | Innovation Nation | Startups | Brainstorm Tech | Video
facebook
Facebook helps you connect and share with the people in your life.
Sign Up
It's free and always
First Name
Your Email
Re-enter Email
New Password
Birthday
PCWorld
TODAY'S TOP 9
Sign In
WHAT'S HOT
REVIEWS
HOW-TO
BUSINESS • LAPTOPS • COMPUTERS • PRINTERS
Encryption • Privacy • Firewalls • Antivirus
yahoo, hackers, security
specifically for the home.
READ NOW
POPULAR SECURITY
Norton Internet Security 2013
as low as $32.95
comments
Linked in
Be great at what you do.
Get started – it's free.
Most Popular
Stocks set to rally on fiscal deal
Fiscal cliff deal stops many tax hikes, but leaves big issues pending
3 more fiscal cliffs loom
Stocks in 2013: Get defensive
Fiscal cliff deal boosts world markets
Tech Blogs
APPLE 2.0
This blogger is off to Bangkok
TECH TUMBLR
The fiscal cliff explained in GIFs
ENTERPRISE

THE CYBERCRIME ECONOMY

2 million Facebook, Gmail and Twitter passwords stolen in massive hack

By Jose Pagliery @Jose_Pagliery December 4, 2013: 4:39 PM ET

SECURITY

Hackers Publish Over 450,000 Emails and Passwords Stolen From Yahoo

By Lucian Constantin, IDG-News-Service:Romania-Bureau Jul 13, 2012 5:50 AM

A Yahoo representative has confirmed that the data published Thursday was indeed some 450,000 names and passwords for Yahoo and other companies.

"We confirm that an older file from Yahoo Contributor Network (previously Associated Content) containing approximately 450,000 Yahoo and other company users names and

THE CYBERCRIME ECONOMY

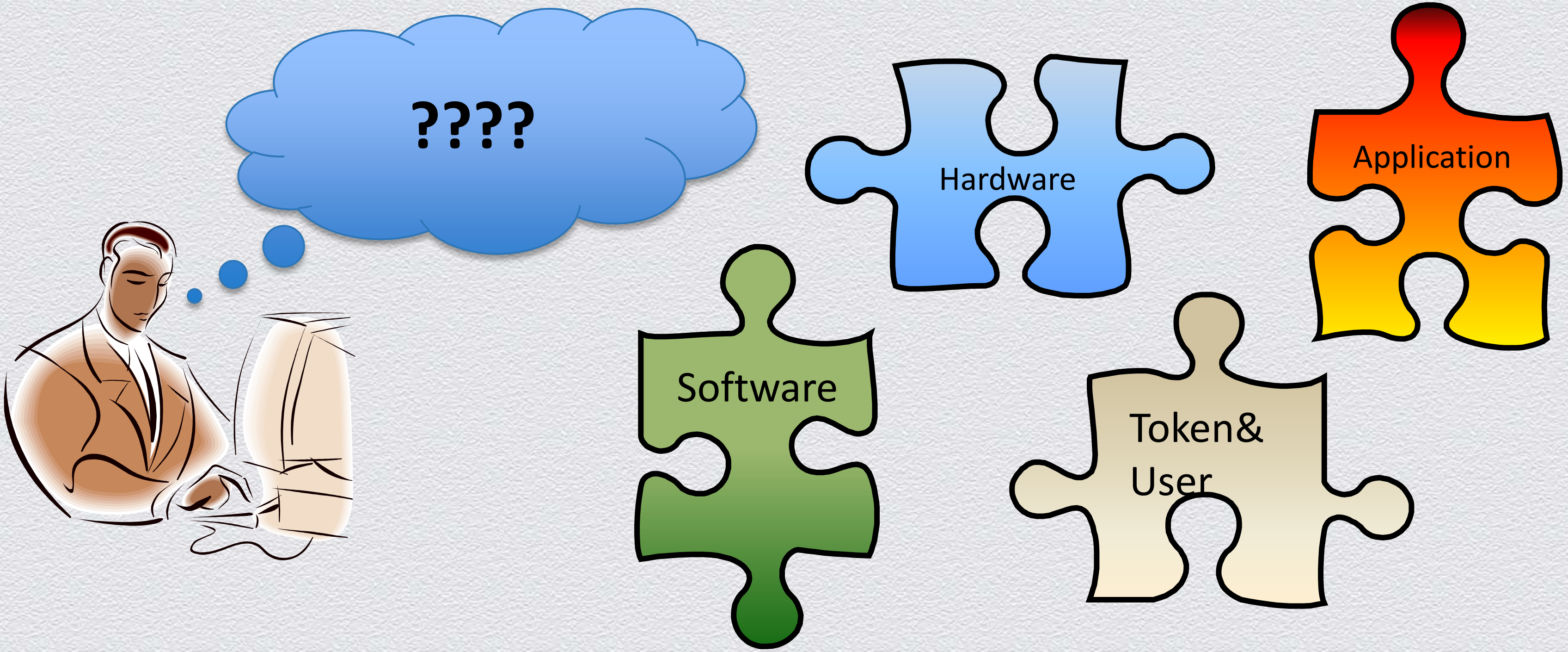
More than 6 million LinkedIn passwords stolen

By David Goldman @CNNMoneyTech June 7, 2012: 9:34 AM ET

Do we need to make things more secure …? Yes we do!

SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig



????

Hardware

Application

Software

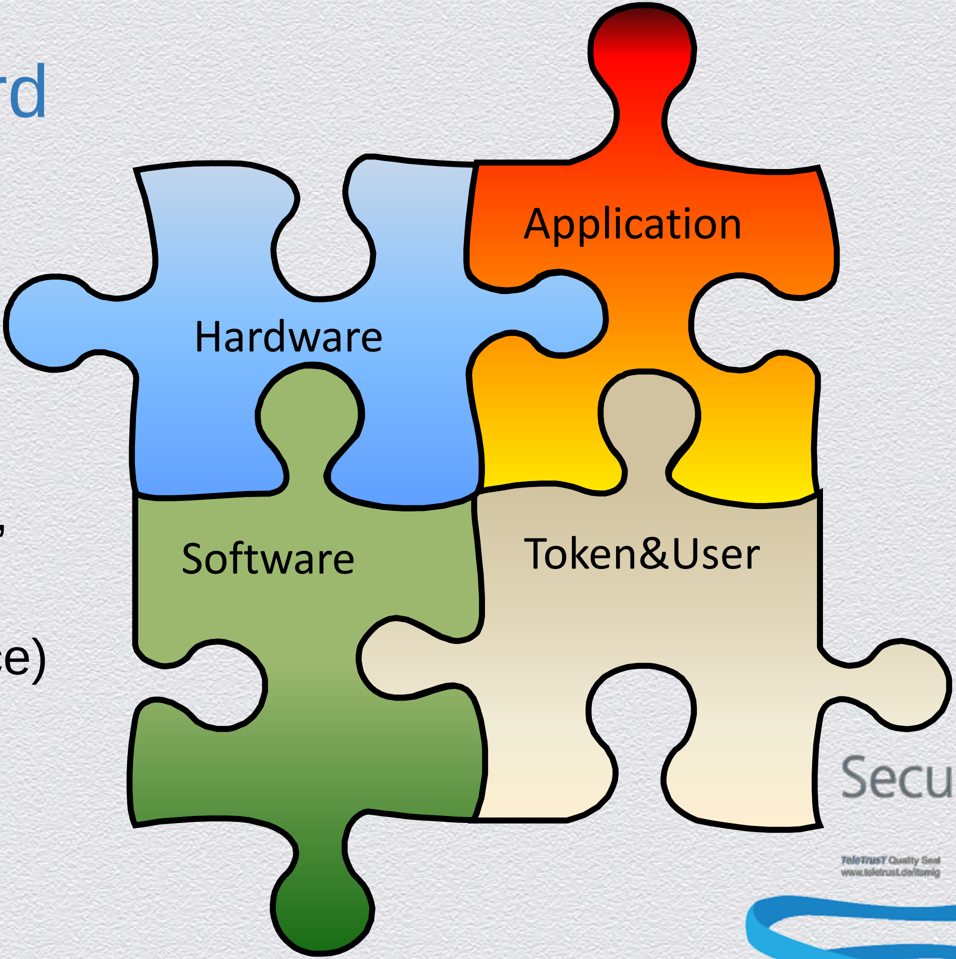
Token&
User

Why are existing technologies not easily adopted?

Our technology, your problem!!! The pieces of the puzzle do not fit together…

A possible way forward

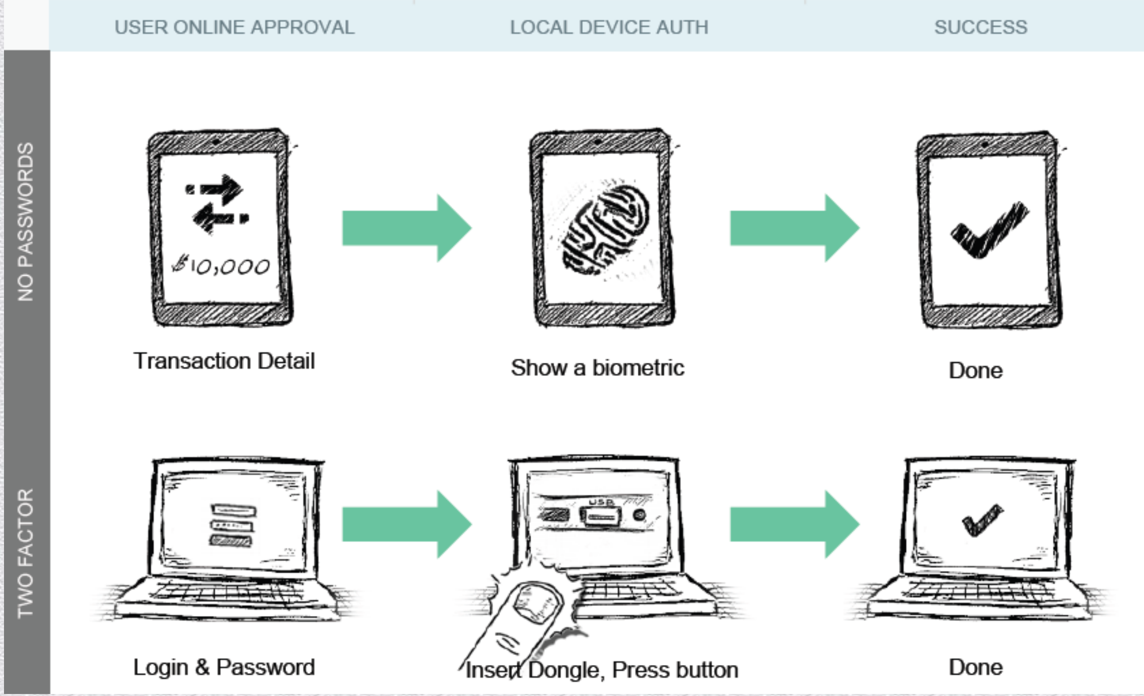
- Bringing together the pieces of the puzzle
- Deep integration in hardware, software and solutions
- PRAGMATIC (user experience)
- SMART (application)
- STRONG (HW, SW, crypto)



SecurITy made in Germany

TeleTrusT Quality Seal www.teletrust.de/itsmig

FIDO Experiences



USER ONLINE APPROVAL | LOCAL DEVICE AUTH | SUCCESS

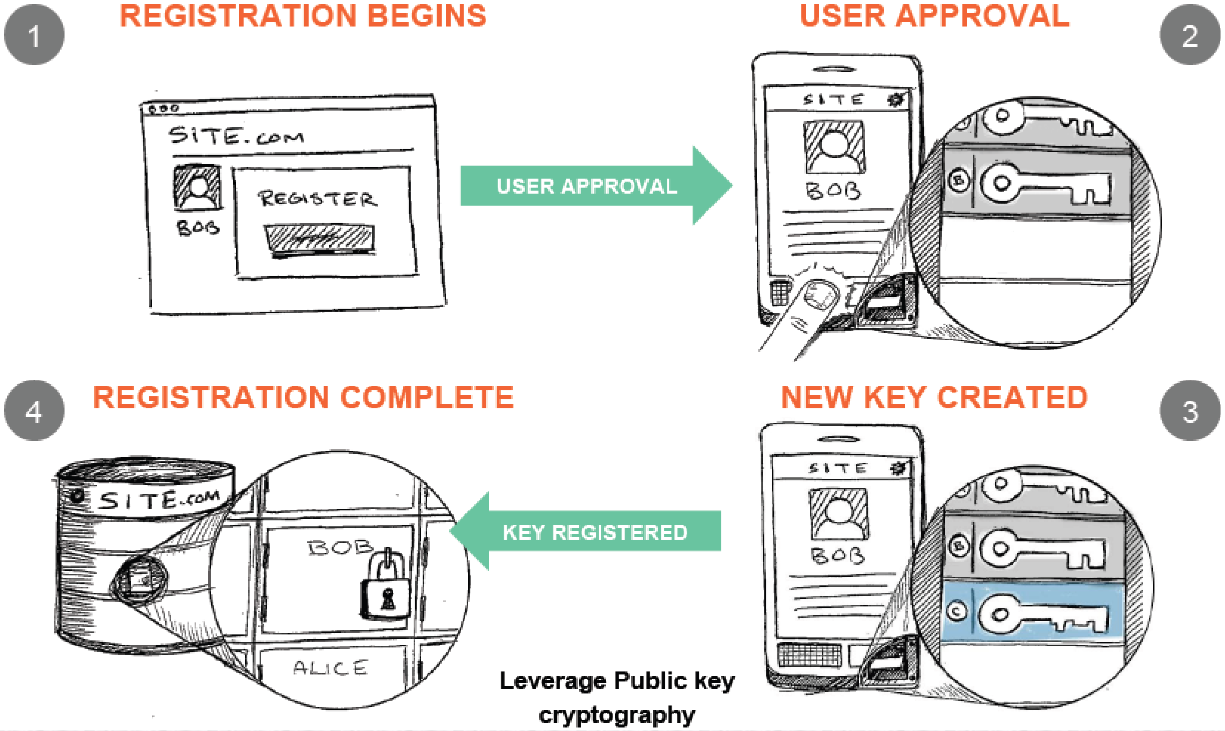
NO PASSWORDS

Transaction Detail → Show a biometric → Done

TWO FACTOR

Login & Password → Insert Dongle, Press button → Done

FIDO Registration



1 REGISTRATION BEGINS

USER APPROVAL

2 USER APPROVAL

3 NEW KEY CREATED

KEY REGISTERED

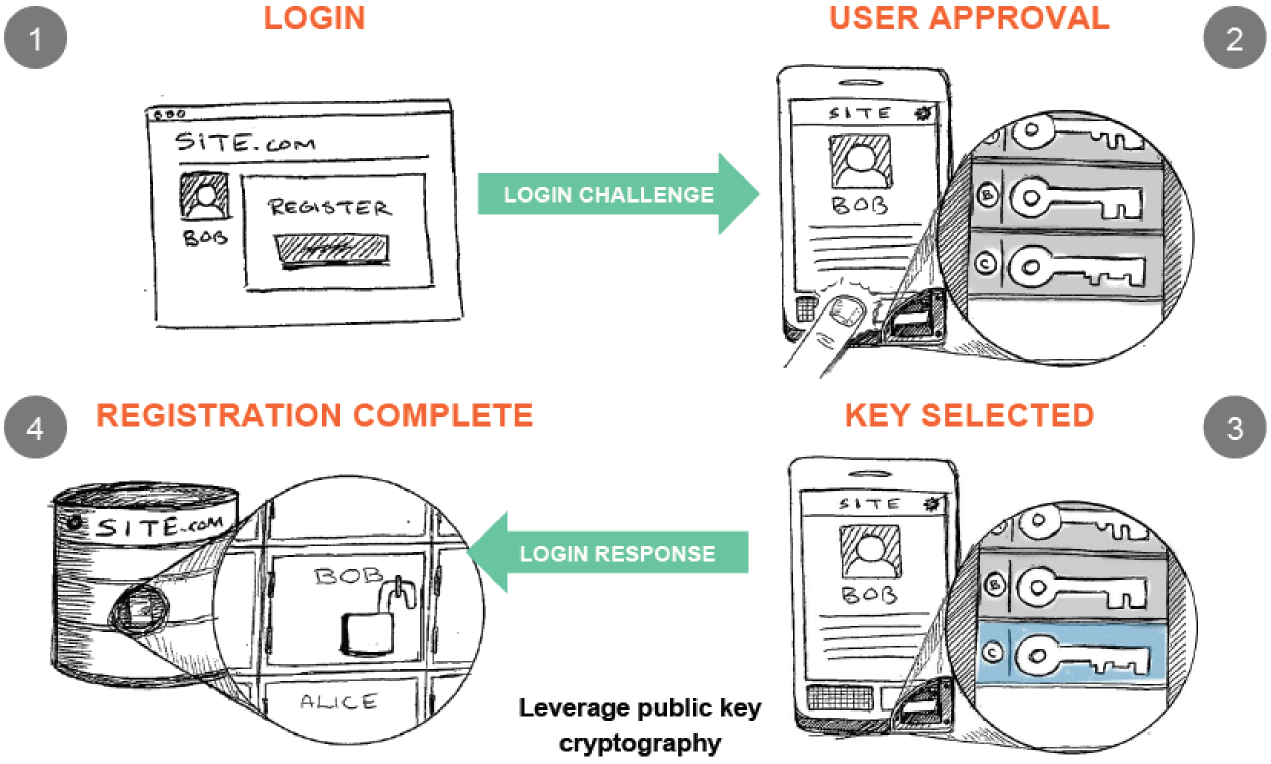
4 REGISTRATION COMPLETE

Leverage Public key cryptography

SecurITy made in Germany

TeleTrusT Quality Seal www.teletrust.de/itsmig

FIDO Login



1 LOGIN

2 USER APPROVAL

3 KEY SELECTED

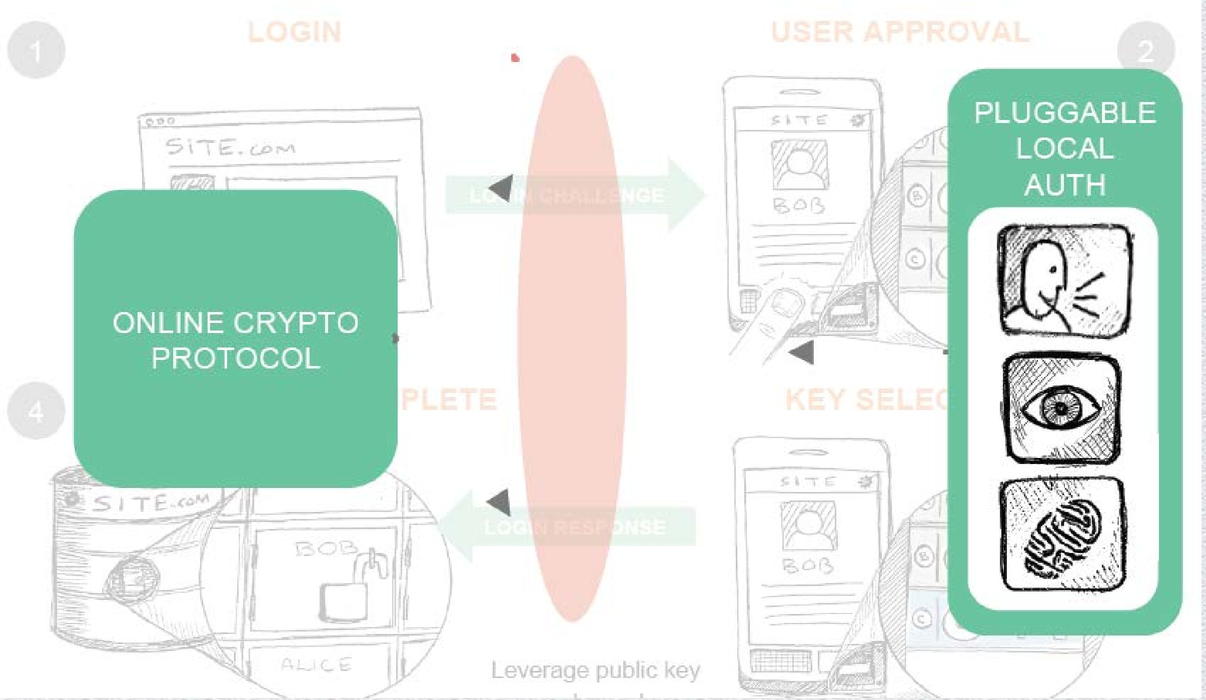
4 REGISTRATION COMPLETE

LOGIN CHALLENGE

LOGIN RESPONSE

Leverage public key cryptography

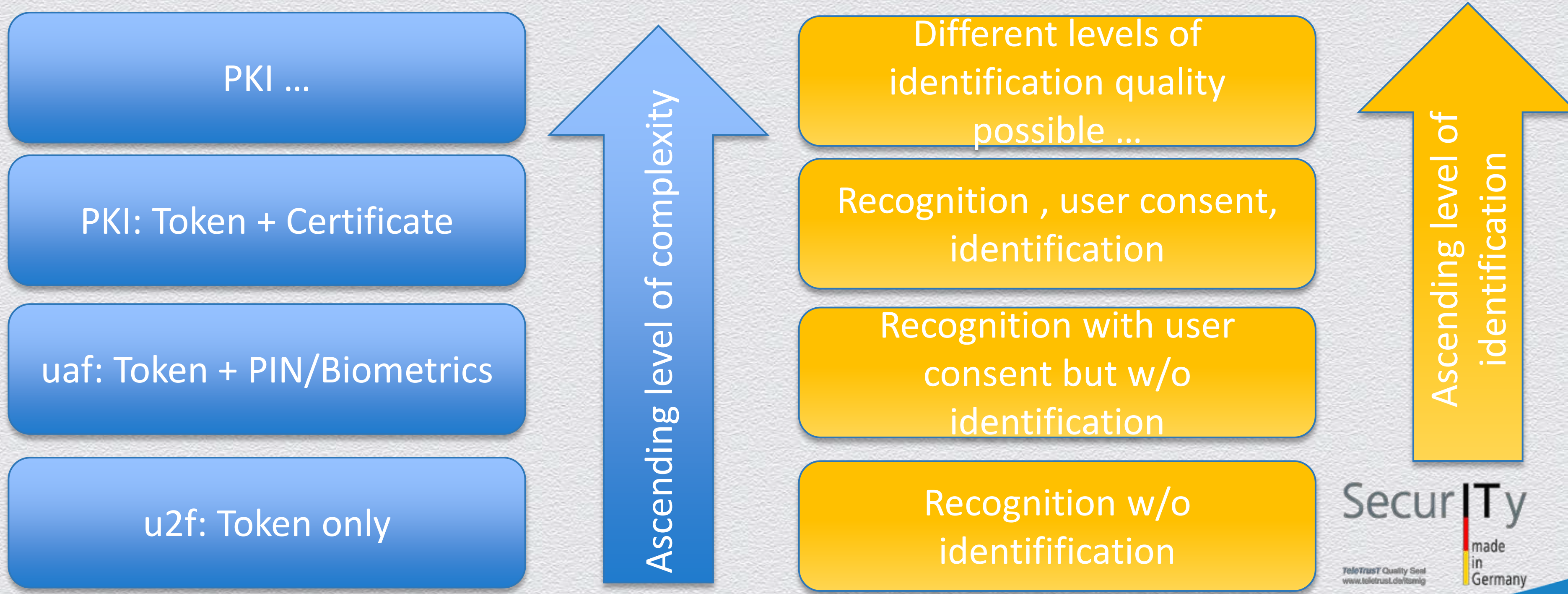
FIDO Standardization



ONLINE CRYPTO PROTOCOL

PLUGGABLE LOCAL AUTH

Layered Authentication/identification model



PKI …

PKI: Token + Certificate

uaf: Token + PIN/Biometrics

u2f: Token only

Ascending level of complexity

Different levels of identification quality possible …

Recognition , user consent, identification

Recognition with user consent but w/o identification

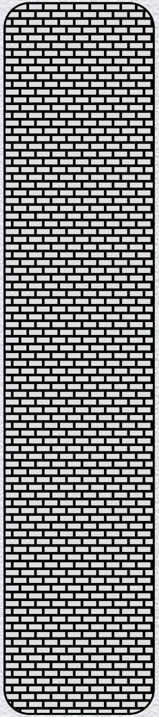
Recognition w/o identifification

Ascending level of identification

SecurITy made in Germany

TeleTrusT Quality Seal www.teletrust.de/itsmig

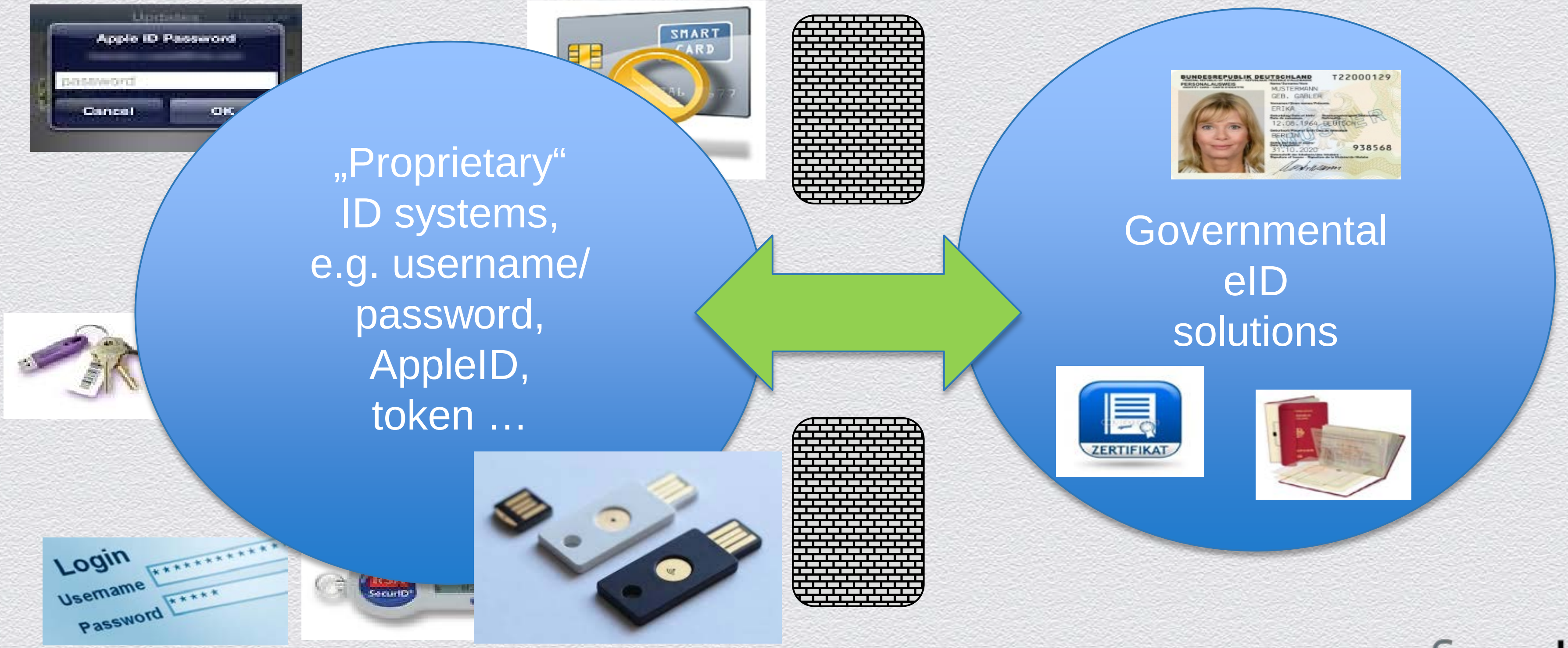
„Proprietary“
ID systems,
e.g. username/
password,
AppleID,
token …



Governmental
eID
solutions

Bridging the ID worlds

Typically, NO interaction between these two worlds exist for the user…



„Proprietary“
ID systems,
e.g. username/
password,
AppleID,
token …

Governmental
eID
solutions

Bridging the ID worlds

The future of eID lies within the controlled interaction of both ID worlds

Transformation of token in the field

- User experience today:
  access functionality/app in the moment you need it (PRAGMATIC)
- Consequence for token:
  update of functionality/increase of reliability is also needed instantaneous, not on basis of complicated paper based processes (PRAGMATIC)
- Therefore:
  Post-personalization of token in the field is necessary (SMART)

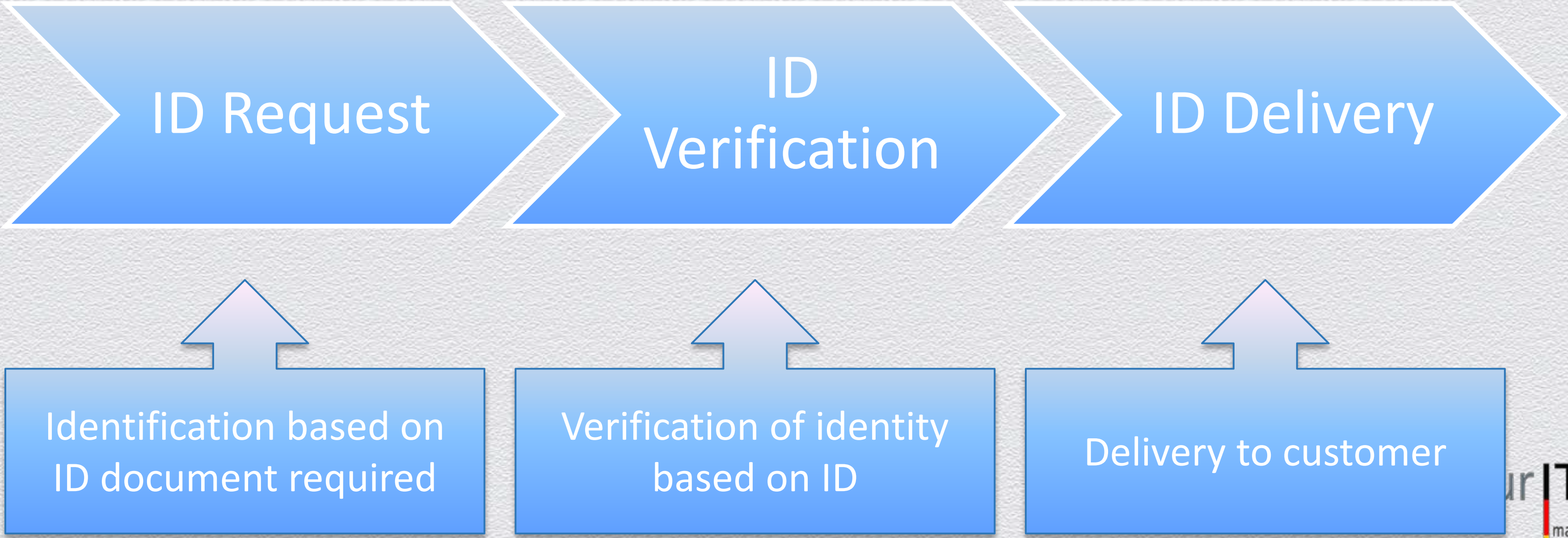
SecurITy made in Germany
TeleTrusT Quality Seal
www.teletrust.de/itsmig

Sirrix AG security technologies

BUNDESDRUCKEREI

#RSAC

Trust Service Provider



ID Request

ID Verification

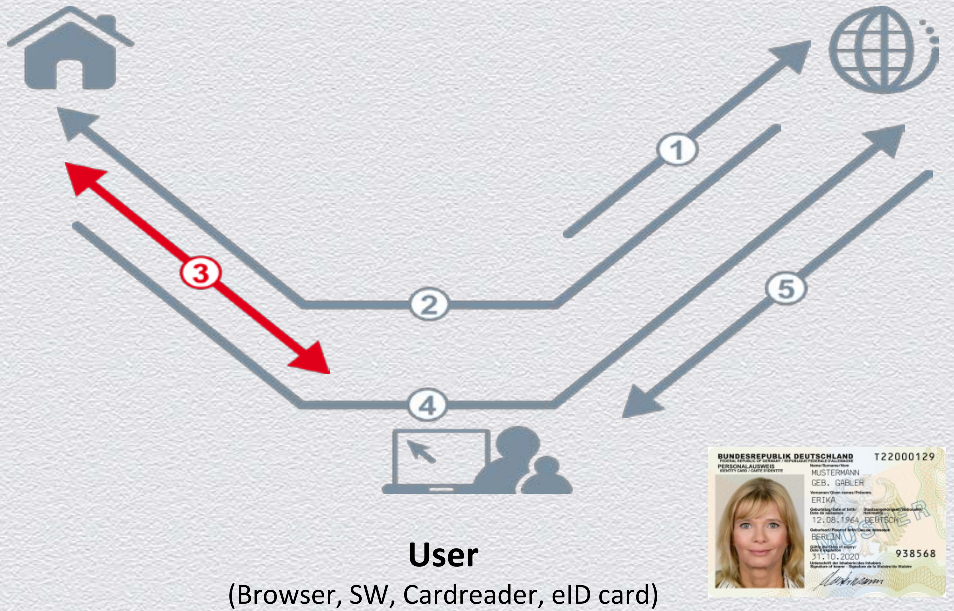
ID Delivery

Identification based on ID document required

Verification of identity based on ID

Delivery to customer

1: User requests Service
2: ID request redirected to eID-Service
3: Mutual strong authentication and access to data
4: Requested ID returned
5: Service provided



eID-Service

Serviceprovider
(Web-Application using eID-Connector)

User
(Browser, SW, Cardreader, eID card)

Example: Identification using German eID

SecurITy made in Germany
TeleTrusT Quality Seal
www.teletrust.de/itsmig

1: User requests Certificate based on eID identification

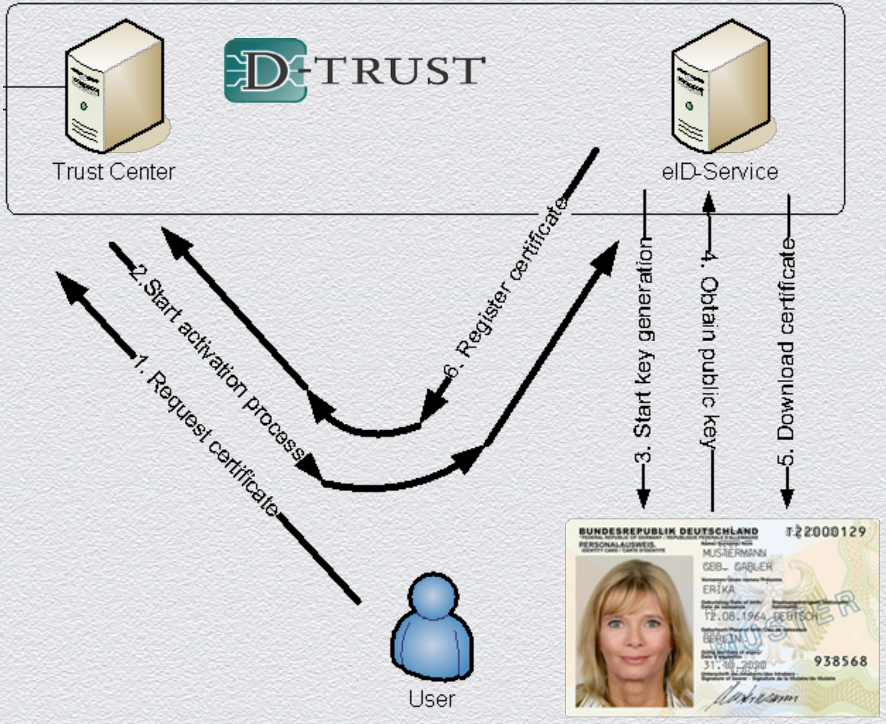
2: activiation process startes

3: Key generation on the eID card

4: Public key send to CA

5: Load certificate on eID card

6: certificate registered with CA

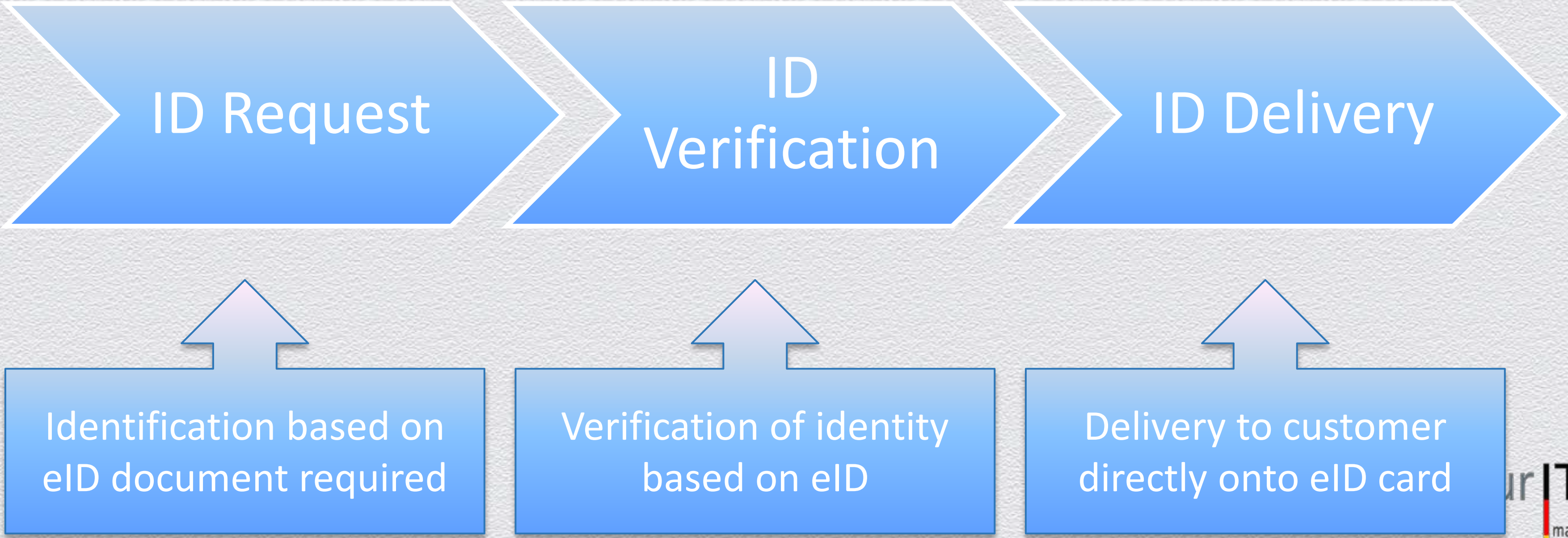


sign-me

Postissuance of certificates based on eID identification

German eID card is basis of identification as well as carrier of key and certificate

Trust Service Provider: based on eID



ID Request

ID Verification

ID Delivery

Identification based on eID document required

Verification of identity based on eID

Delivery to customer directly onto eID card

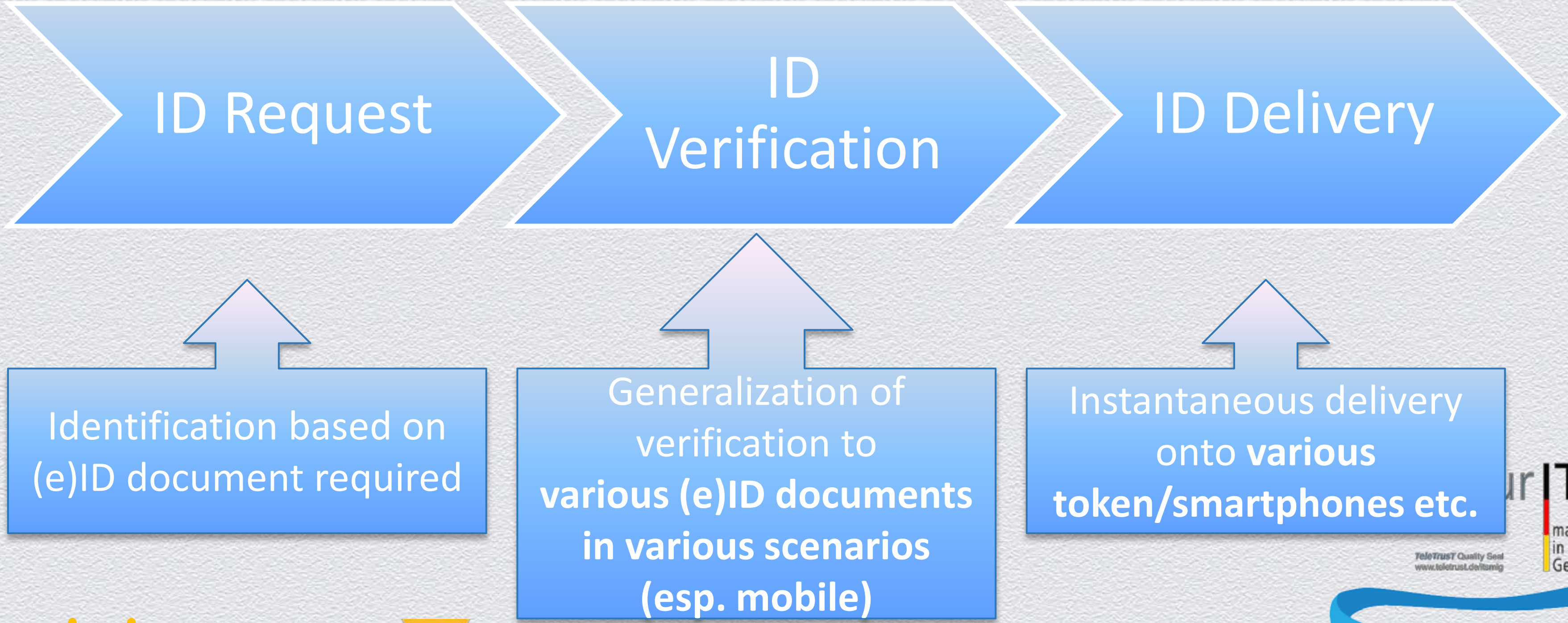
urITy made in Germany

TeleTrusT Quality Seal www.teletrust.de/itsmig

Sirrix AG security technologies

BUNDESDRUCKEREI

Trust Service Provider: generalizations



ID Request

ID Verification

ID Delivery

Identification based on (e)ID document required

Generalization of verification to **various (e)ID documents in various scenarios (esp. mobile)**

Instantaneous delivery onto **various token/smartphones etc.**

The situation

Service Provider

Apple ID Password

password

Cancel

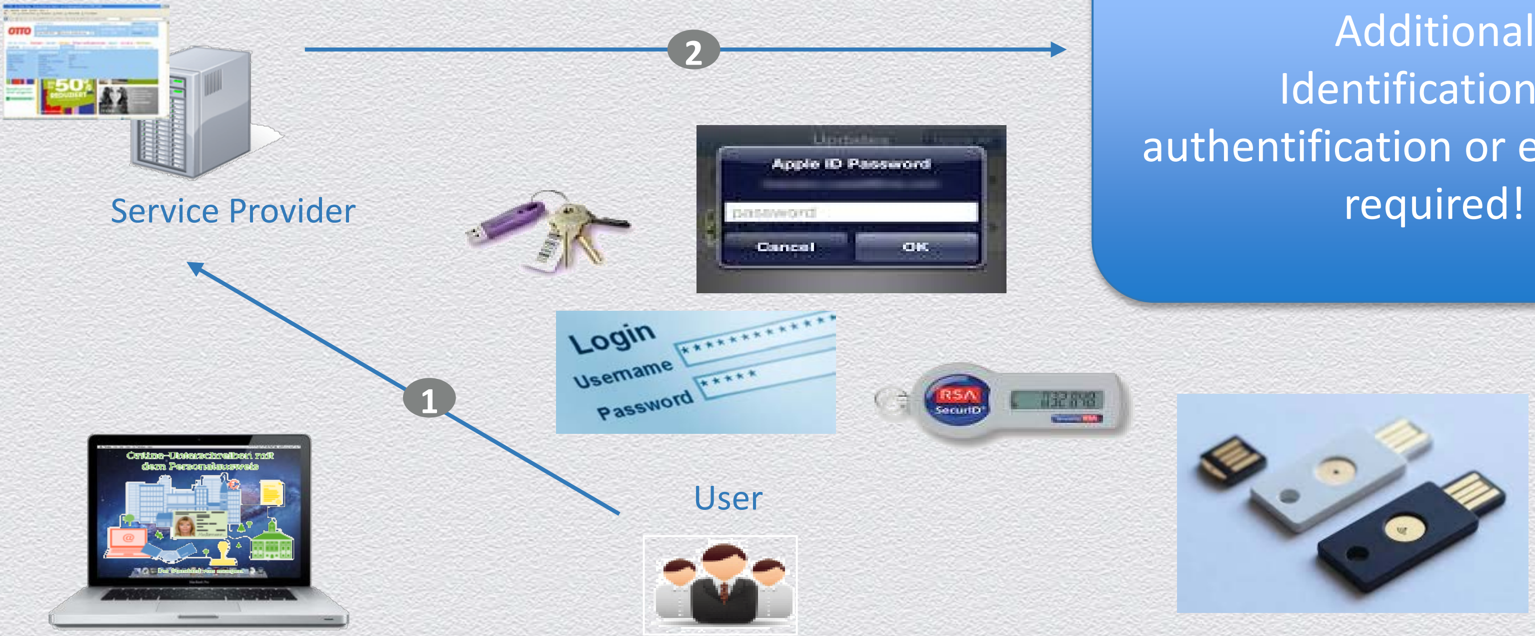
OK

Additional Identification or authentification or encryption required!

USER

1. Service request:
Using conventional authentification methods

The situation



Service Provider

User

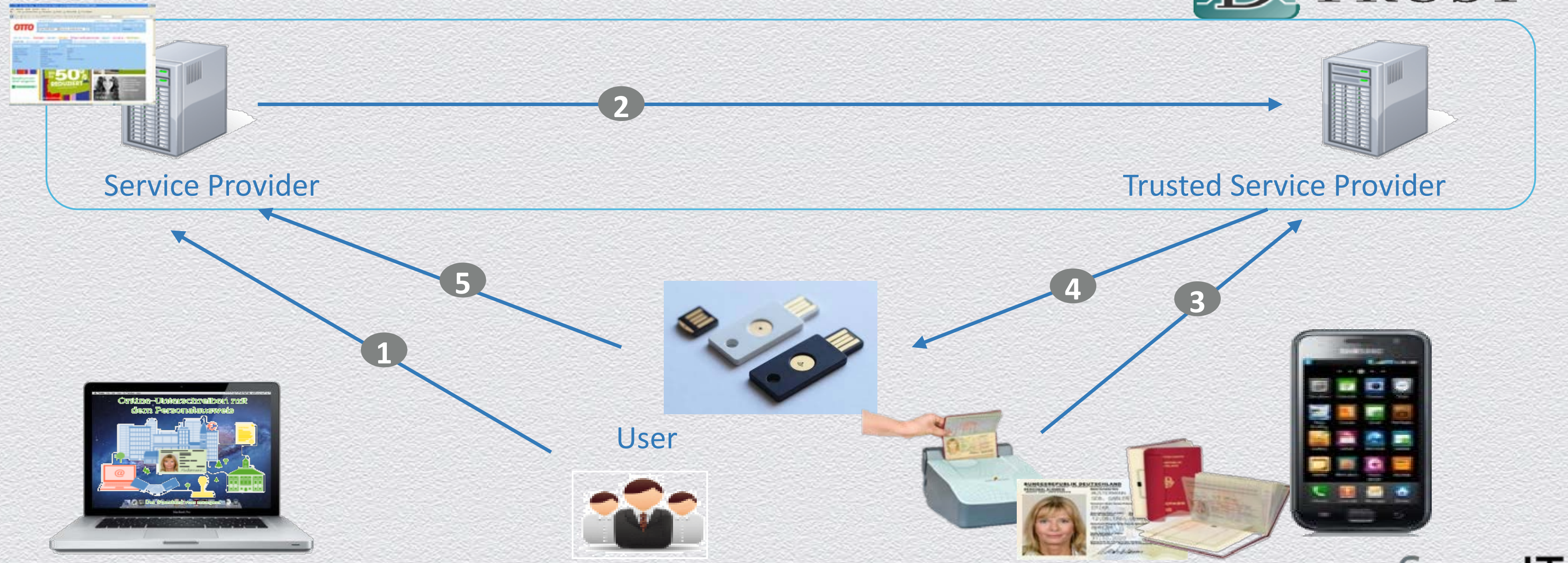
Additional Identification or authentification or encryption required!

1 Service request with conventional login

2 Specific identification needed!

The solution

D-TRUST



Service Provider

Trusted Service Provider

User

1 Service request with conventional login

2 Specific identification request

3 Verify ID (mobile scenario etc)

4 Postissuance of token/vertificate

5 Fulfill aditional request (verified ID)

Secur IT y made in Germany

TeleTrusT Quality Seal www.teletrust.de/itsmig

Sirrix AG security technologies

BUNDESDRUCKEREI

Conclusion

- Reliable and flexible authentication and identification mechanisms are required to enhance security in the web: STRONG
- User requirements need to be stronger taken into account to achieve user acceptance: PRAGMATIC
- A layered approach (as appropriate for different use cases) needs to be taken into account: SMART
- Post-issuance is an important (SMART) mechanism especially if combined with mobile verification and delivery

SecurITy made in Germany
TeleTrusT Quality Seal
www.teletrust.de/itsmig

RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Thank you for your attention!

Visit the German Pavilion…
North Expo
Booth 3421

The partners of the German Pavilion at RSA® Conference 2014

@sec
BUNDESDRUCKEREI
DriveLock
Intelligent Data Protection
itWatch GmbH
ROHDE&SCHWARZ

AUCONET
Business Infrastructure Control
CORISECIO
eco
Association of the German Internet Industry
LINK11
Sirrix AG
security technologies

brainloop
cryptovision
infineon
QGROUP GMBH
TÜViT
TÜV NORD GROUP

www.rsac.german-pavilion.com

The logos and names used herein are the registered trademarks of the respective firms and institutions that own them.

North Expo , Booth 3421