

# CA Compliance Info-Day

## eIDAS and Trust Service Provider Conformity Assessment

Organizer: Bundesdruckerei, TÜVIT, ETSI STF 458  
 Date: Tuesday, 04.11.2014 from 10:00 AM to 05:00 PM  
 Venue: Bundesdruckerei, Berlin-Mitte, Conference Center, Kommandantenstraße 15 (**new entrance**)  
 Website: [http://www.bundesdruckerei.de/de/kontakt/kontakt\\_anfahrt/index.html](http://www.bundesdruckerei.de/de/kontakt/kontakt_anfahrt/index.html)

### Proposed Program: (Status 03.11.2014)

10:00	Welcome by Bundesdruckerei	Kim Nguyen, Bundesdruckerei, Chief Scientist Security, Managing Director, D-Trust	1
	<b>Implementing eIDAS</b>		
	eIDAS Regulation: State of play	Gerard Galler, EC	2
	First experiences with eIDAS	Riccardo Genghini, SNG	3
	Overview CEN/ETSI eSignature Standardisation	Nick Pope, Thales UK	4
	Role of accreditation in the Conformity Assessment Process	Kevin Belson, UKAS	5
	Implementing Conformity Assessment under eIDAS	Christoph Sutter, TÜVIT	6
	<b>Q+A to speaker roundtable</b>		
12:30	<i>Lunch</i>		
13:30	<b>The CA-View on eIDAS Regulation and other relevant policies</b>		
	CA/Browser Forum Developments	Ben Wilson, DigiCert	7
	Implementing Certificate Transparency:	Inigo Bareira, Izenpe	8
	New directions for signing: FIDO and beyond	Kim Nguyen, D-TRUST	9
	View from a Commercial CA	Robin Alden, Comodo	10
	Digital ID Challenges	Conny Enke, SwissSign	11
	A 10000 foot view on eIDAS from the outer edge of EU	Mads Henriksveen, BUYPASS	12
<b>16:15</b>	<b>Q+A to speaker roundtable and panel discussion</b>		
	Lessons learned, “paper-policies” and the actual threads? eIDAS: New business for TSP?	Moderator: Arno Fiedler ETSI STF 458 with Atilla Biler, TÜRKTRUST and Danilo Cattaneo, InfoCert	13
			14
17:00- 18:00	<i>Get together</i>		

# Update on the Work of the CA / Browser Forum

Ben Wilson  
Chair Emeritus



Report Prepared for ETSI CA Day  
Berlin, Tuesday, 4 November 2014

# Outline

- Internal CA / Browser Forum Developments of 2014
- Newsworthy Events of 2014
- Key Discussions that have occurred within the Forum
- Update on CA/B Forum Working Groups
  - Code Signing Working Group
  - Policy Review Working Group
  - Security Information Sharing Working Group
- Current Discussions
- Future Developments

# Forum Developments

- New CA/Browser Forum Website plus Bugzilla Tracking
- Membership has grown substantially
- New Chair (Dean Coclin) and Vice Chair (Kirk Hall)
- We've revisited / discussed scope of CA/B Forum activity
- CA/B Forum Baseline Requirements Implementation by CAs, Auditors, and Browsers (with Network Security)
- More gTLDs have been added to the registry by ICANN

# News of 2014

- Implementation of Certificate Transparency (CT) in 2015
- SHA-1 Deprecation and Transition Away from It by 2017
- Heartbleed vulnerability in OpenSSL and lack of advanced warning that CAs might need to reissue
- Indian Sub CA Compromised raising concern about audit and oversight of government-run CAs
- Elimination of SSL v.3 and move toward full TLS in response to POODLE

# 2014 Discussions

- What is an SSL Certificate for purposes of applying the Baseline Requirements?
  - Does use of the id-kp-serverAuth EKU determine?
  - Is a poison certificate extension a way to exempt?
- How can subordinate CAs be technically constrained?
- How fresh or stale should information be to renew?
- Should CAs issuing EV certificates carry insurance?
- Browsers programmatically screen for violations, leave procedural and management controls to auditors

# Working Groups

- Code Signing Baseline Requirements
- Extended Validation Review – revised definitions and tightened up language used to describe vetting processes
- Certificate Policy Review
- Security Information Sharing Working Group
- SSL Performance Working Group (disbanded)

# Code Signing Baseline Requirements

- Better Key Protection
  - Threat: Key Compromise, Takeover Attack
  - Section 16.3 Levels– 1- TPM, 2-FIPS Level 2/EAL4, 3-USB
  - Sec. 11.7 - strike 1: no USB, strike 2: Audit, 3: Permission
  - Unique, Registration-based Identifier or non-sequential unique ID generated by CA > 20 bits of entropy
- Better Communication about Malware w/ AV Vendors
  - High-Risk Regions (Geographic Locations) - Blank
  - Database / Blacklist -> Security Info Sharing W.G.
- Signing Service Platforms



# Policy and Info Sharing WGs

- Policy Review Working Group
  - Review CA/B Forum guideline documents with an eye toward conformity, coordination and consistency
  - Identifying gaps in CA/Browser Forum policies by
    - Reviewing NIST IR 7924 and Network Security Requirements
    - Mapping ETSI and WebTrust audit criteria
- Security Information Sharing Working Group
  - Structure a system that minimizes potential for legal liability (e.g. libel, unfairness/lack of due process, etc.) when reporting or maintaining data or listings

# Current Discussions

- Policy Object Identifiers (OIDs) and OID processing
  - Should standard OIDs identify publicly trusted SSL?
- 72-Hour Certificates without Revocation Pointers
  - Who blinks first? Can't browsers build a work-around?
- Omitting S= and L= in Subject DNs where C is small
  - Taiwan, BVI, Vatican, Singapore, Bermuda, etc.
- Scope of SHA1 Deprecation (e.g. private PKIs, OCSP)
- Financial responsibility requirements for CAs
  - Current Assets greater than Current Liabilities, etc.

# The More Things Change ...

- Certificate Authority (CAA) Records – April 15, 2015
- OCSP Stapling – Working on Must-Staple OID
- Better planning coordination
- Advance communication of plans
- Better notification of threats in the future (Heartbleed)
- Browser processing and UI display
- SHA1 Deprecation -- Microsoft, Mozilla and Google



**Thanks!**

**Ben Wilson**

**[ben.wilson@digicert.com](mailto:ben.wilson@digicert.com)**

# CERTIFICATE TRANSPARENCY: ANOTHER NEW CHALLENGE FOR CAs



QTSP from the Basque Country

# CONTENT



- [CT AT A GLANCE](#)
- [VISION FROM THE CA](#)
- [VISION FROM THE CT LOG SERVER OPERATOR](#)



# CT at a glance

Some history...

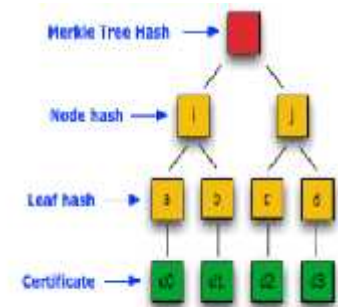
# Introduction

- Google idea
- This idea was mentioned in CABF F2F at NYC in Sept. 2012
- CT was described by Google (B. Laurie, A. Langley, E. Kasper) in June 2013 at the IETF as "Experimental Request for Comments 6962" is an experimental RFC (and now with 6962-bis), that will soon be supported in Google Chrome (February 2015). Initially only for EV certificates
- Goal: to improve transparency around TLS certificates. How?
  - Increase hurdles for a CA to issue a TLS/SSL certificate for a domain
  - Become an open auditing and monitoring system that can be used by any domain owner or CA to check whether a certificate has been issued by mistake or with malicious intent
  - Protect users as far as possible from harm which originates from certificates that have been issued by mistake or with malicious intent



# What and how CT does and try to solve?

- **What CT does?**
  - Addresses vulnerabilities in current trust model
  - The detection of certificates (SSL up to now) wrongly issued or misissued
- **How CT does it**
  - Using the Merkle tree which has 2 proofs mainly:
    - Consistency proof: verifies that a later log contains all certificates in previous log in same sequence
    - Audit proof: any chosen certificate has been included in the log
- **How will CT solve the issue?**
  - Make all end-entity TLS certificates public knowledge
  - Hold CAs publicly accountable for all certificates they issue



# Pros and cons

## **PROS**

- Compatible with current PKI implementations
- Supported by Google and some CAs
- Uses current specifications
- Expands the existing system with logging and log-checking
- Public logs enhance security
- Early detection leads to better/faster mitigation
- leading to a greater public trust

## **CONS**

- CT is only useful if every publicly trusted certificate is logged and admitted by all browsers
- Browsers must reject TSL/SSL connections with certificates that are not publicly logged

# IN SUMMARY: OUR VISION AS A TSP





Vision from a CA  
perspective

How we do it

# How a CA sees it

- A CA has to prove that issues certificates rightly
- A CA has to ask “permission” to issue EV certificates to a CT log operator (need to be included in at least 3 CT log servers)
- The reputation of a CA for issuing EV certs is based on the CT log servers
- Are OCSP responses less important?

# HOW IZENPE IMPLEMENTS CT

- Izenpe CA: New Add-in “Certificate Transparency”
  - Configuration
    - Activate and configure the CT per Certificate Policy
      - “Embedded” or “Later publication”
      - Number of SCT needed
    - Management of CT Log Servers
    - Precertificates signing key
  - Issuance of certificates
    - “Embedded”: Generation of PreCertificates and sending to the Log Server during the issuance process
    - “Later Publication”: Later to the issuance, automatic sending of the certificate to the CT Log servers
  - Operational
    - Browsing of received SCTs
    - Publication of certificates issued without CT
- Izenpe VA: Incorporation of the SCTs in the OCSP responses



# Vision from a CT Log Server operator

How we do it

# How a CT log server sees it

- The CT log server operator decides which CA to admit as “trusted”
- The CT log server operator shall work for the 3 options the CA can choose according to RFC
- The CT log server operator shall offer a reliable response.



# THE IZENPE CT LOG SERVER



➤ <https://ct.izenpe.com>

➤ **Additional urls:**

➤ [https://ct.izenpe.com/ca\\_list.py](https://ct.izenpe.com/ca_list.py)

➤ <https://ct.izenpe.com/certificates.py>

# IZENPE SOLUTION FOR A CT LOGS SERVER

- Different phases in the implementation of this project
- Use of Google's provided code with some additional modifications. Implement and test run.
- Once the tests were running, isolated the process to start the CT:
  - Parameters: private key (to sign the SCT), a port, a DB and a list of authorized CAs.
  - To register the certificates or precertificates:
    - Call the service <https://ct.izenpe.com/ct/v1/add-chain>
    - You can check which certificates admits a CT with this url: <https://ct.izenpe.com/ct/v1/get-roots>
- **Issues with the private key.** Google CT code only work with elliptic curves (RFC 6962 allows you to use also RSA SHA-2)

# DIFFERENT POINT OF VIEWS

- Google is focused on CT.
- Microsoft is going with the smart filters.
- Mozilla, Opera, Safari, etc. are “waiting”.
- Other approaches like CAA, OCSP Stapling, CRLSets and OneCRL, etc. are also on the way.
- Where are the TSPs going?



# CONCLUSIONS



- Realize that it affects all of us: TSPs, browsers, relying parties, auditing bodies, standard bodies, end users, etc.
- Today is for EVs only and in Chrome, tomorrow ...
- Enhancing security is a must, but getting consensus is also a must and it's not good making own wars.

# IS THERE SOMETHING ELSE TO CHANGE?

- Who has to deal with this?
- Why all the changes affect the TSPs?
- Is this enough?





IZENPE  
Iñigo Barreira  
[www.izenpe.com](http://www.izenpe.com)



# New directions for authentication&signing: FIDO, PKI and beyond

4th of November, 2014, Berlin

Dr. Kim Nguyen, Chief Scientist Security, Technology,  
Bundesdruckerei GmbH

Managing Director, D-Trust GmbH

1

- FIDO: Next generation authentication

2

- FIDO and beyond
- Adding identification to authentication

3

- Post Issuance and usage of certificates on a FIDO token



# FIDO: Fast Identification Online



## INTERNET SERVICES



## COMPONENT & DEVICE VENDORS



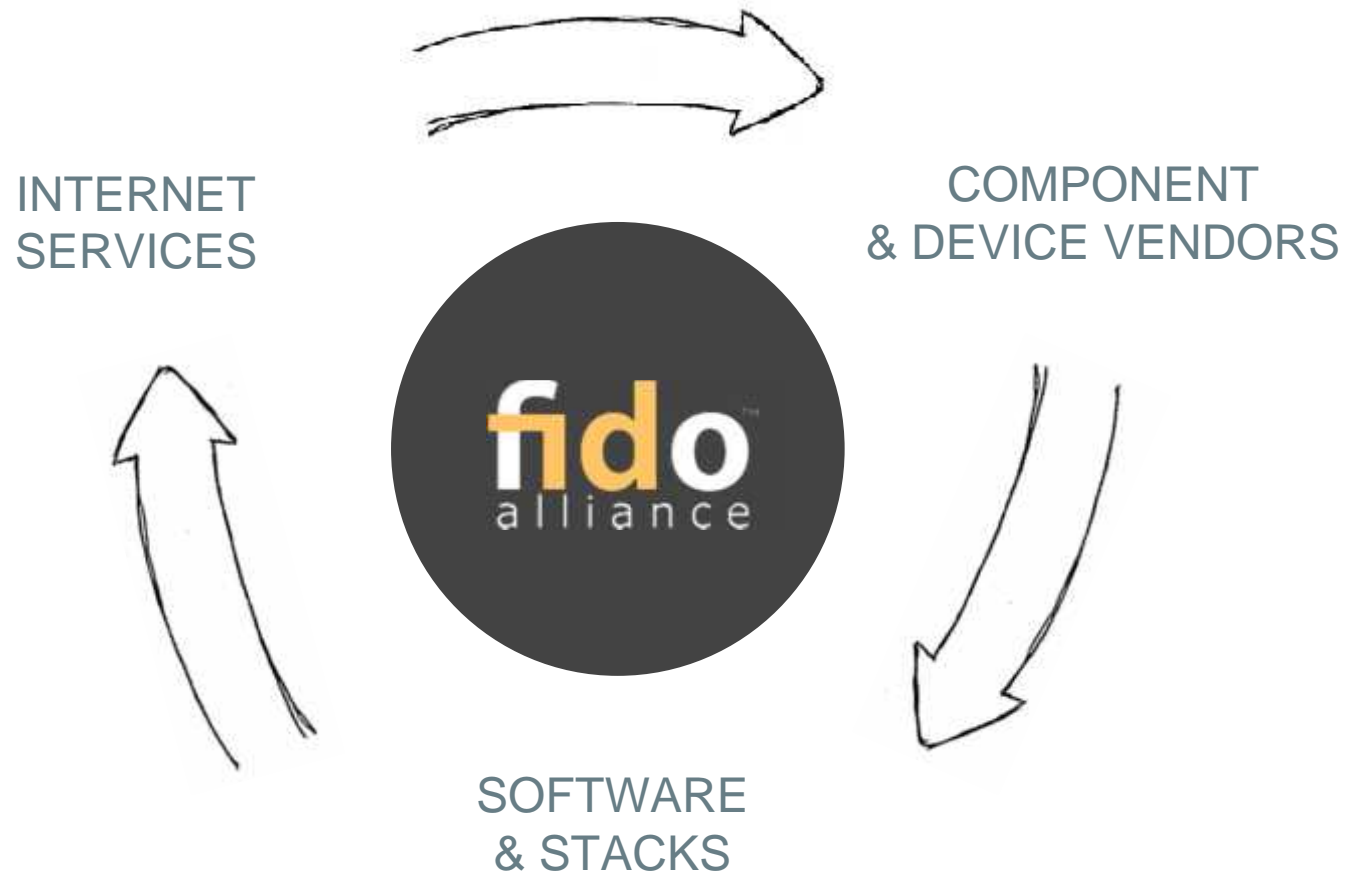
## SOFTWARE & STACKS



# FIDO: Next generation authentication

---

Building a trusted ecosystem



## FIDO Experiences

USER ONLINE APPROVAL

LOCAL DEVICE AUTH

SUCCESS

NO PASSWORDS



Transaction Detail



Show a biometric



Done

TWO FACTOR



Login & Password

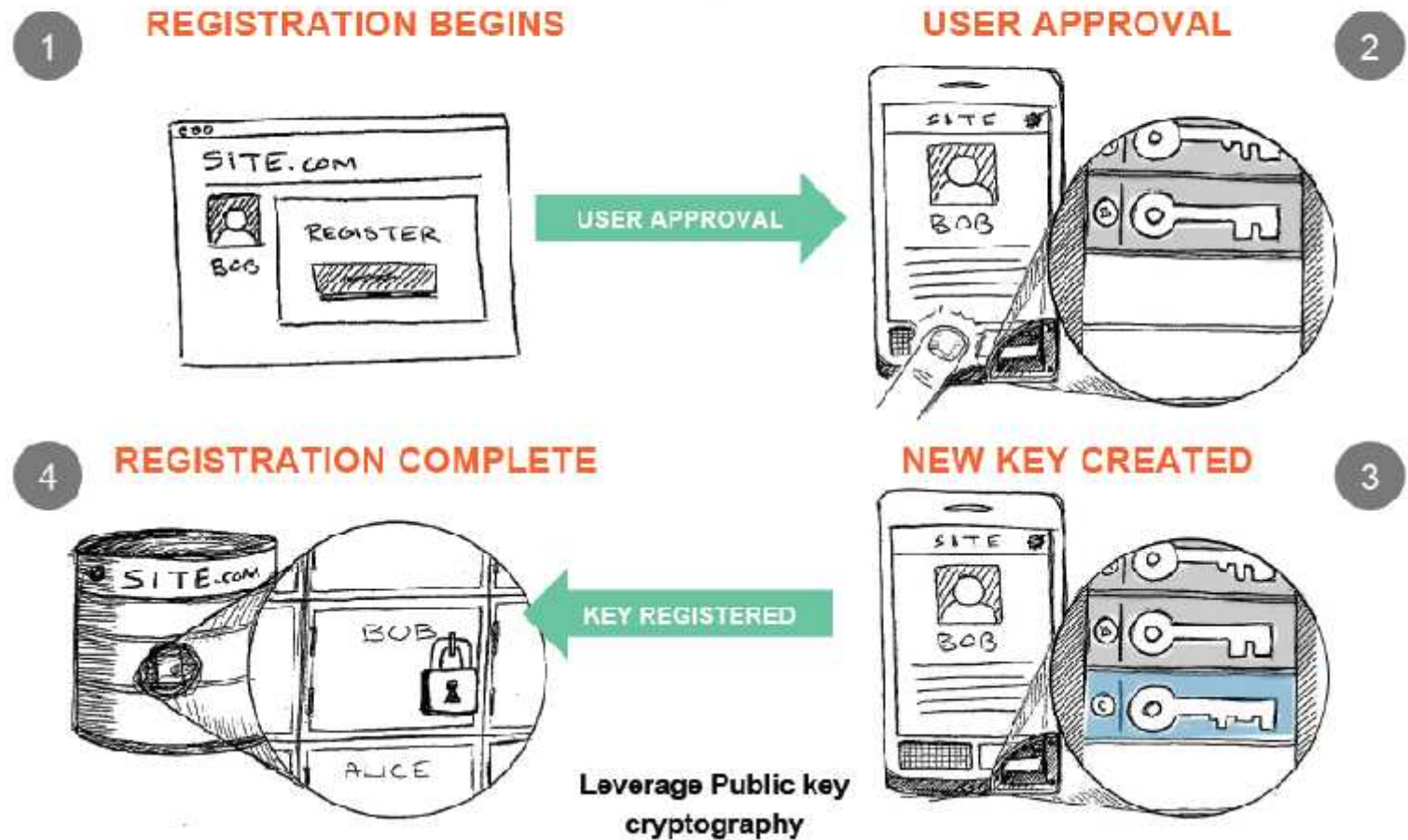


Insert Dongle, Press button

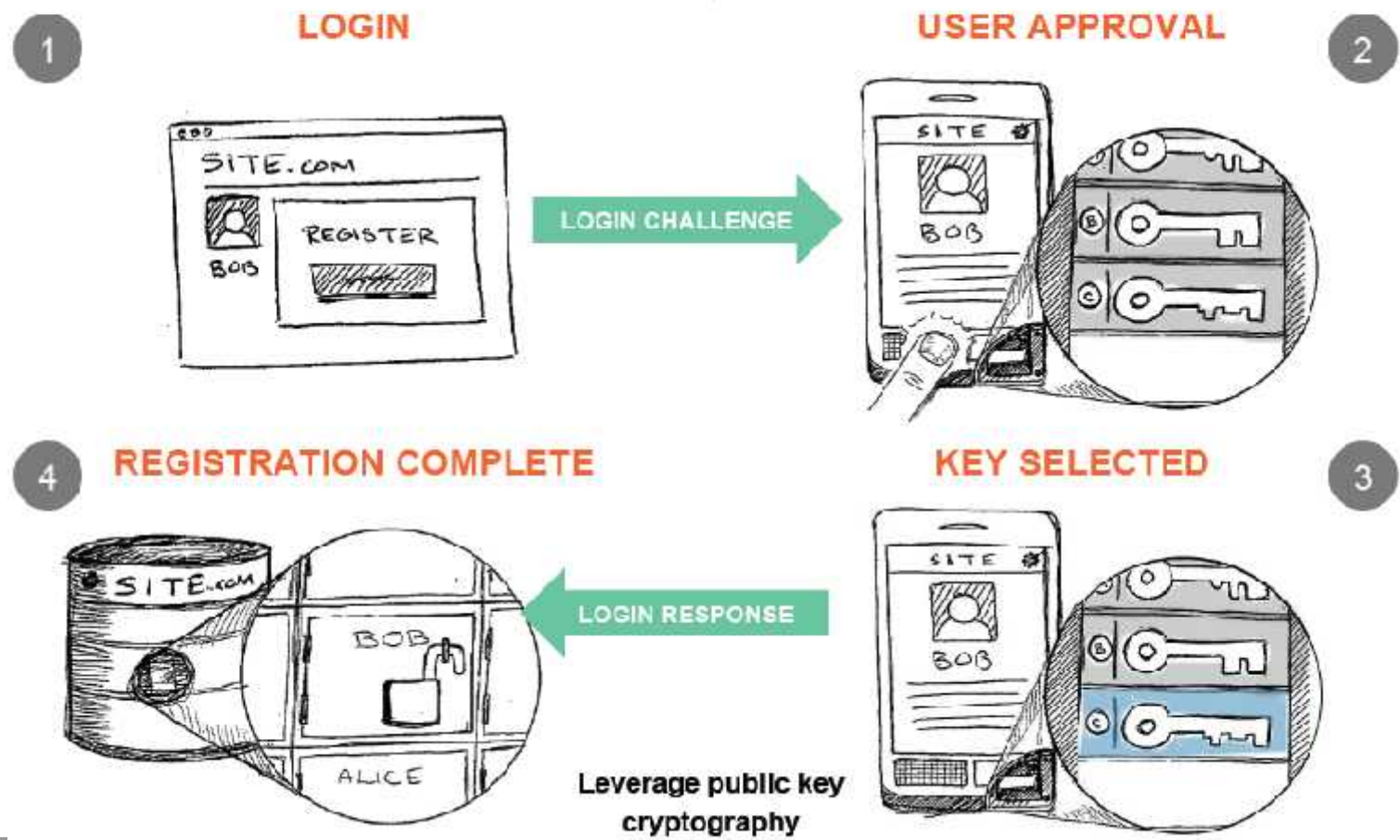


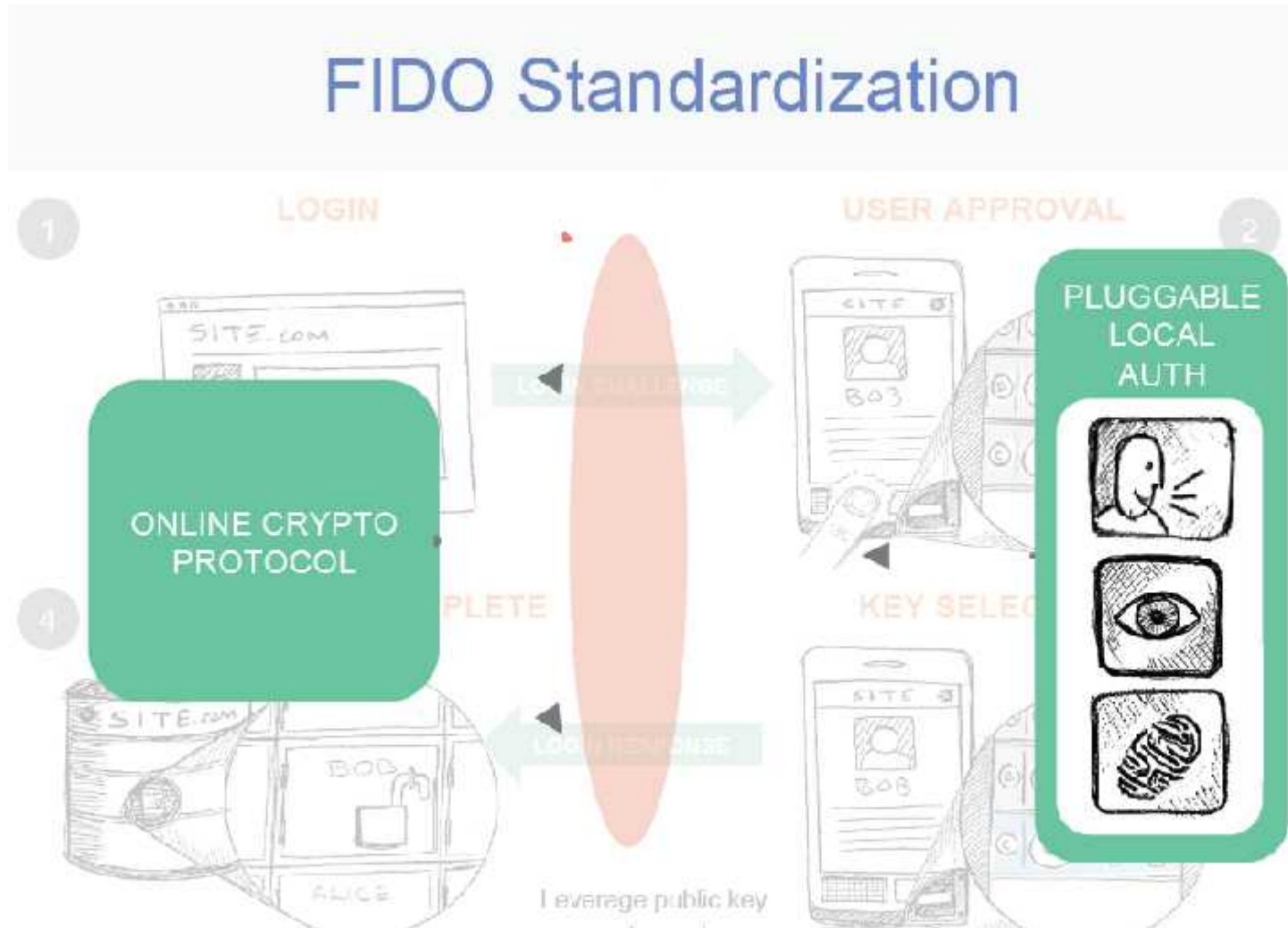
Done

## FIDO Registration

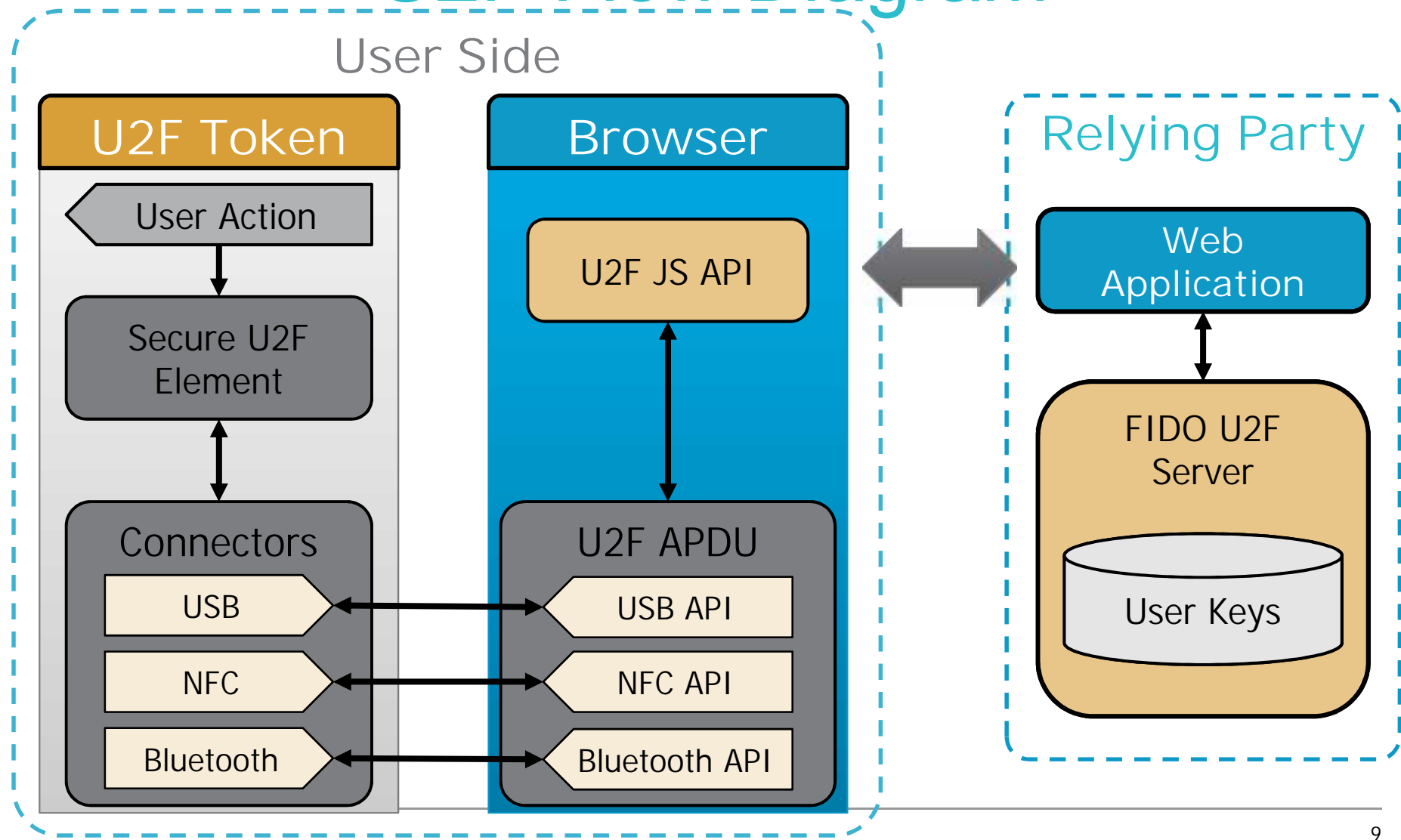


## FIDO Login





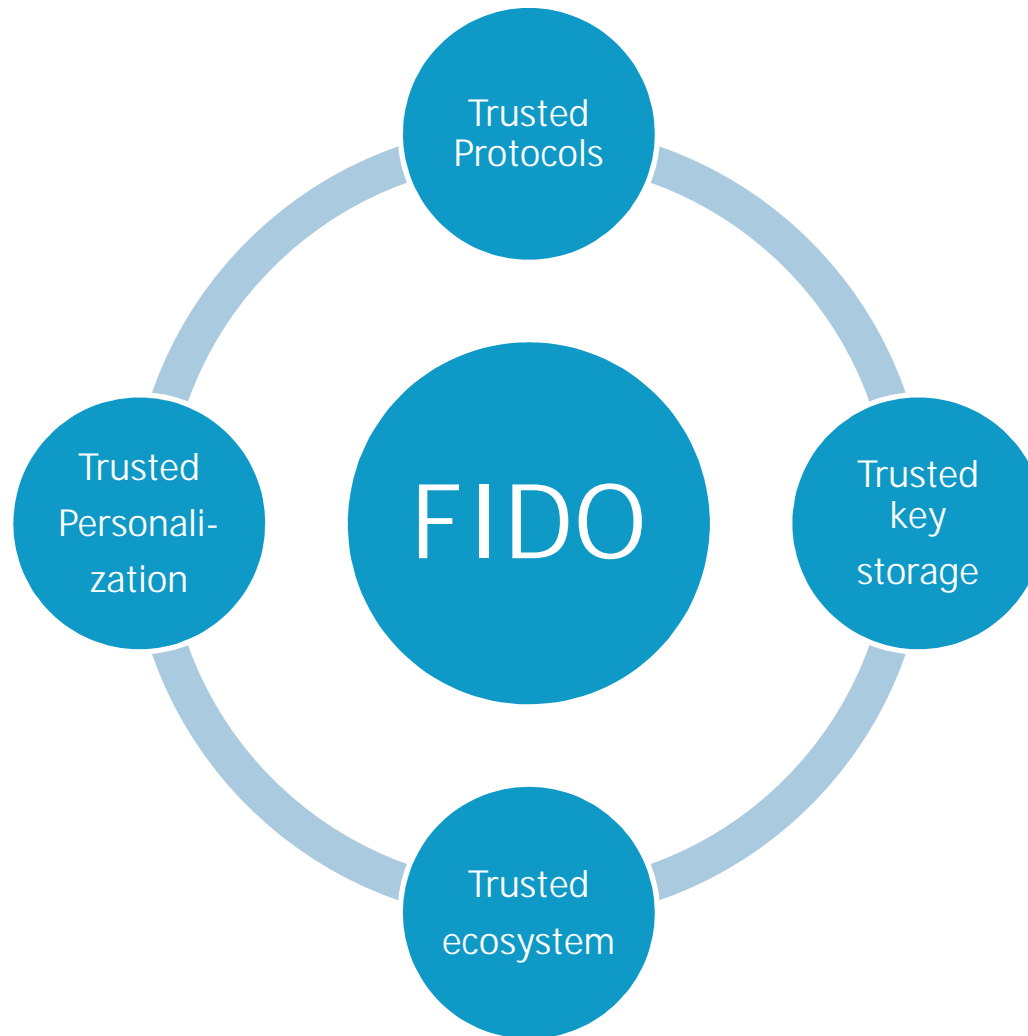
## U2F Flow Diagram



- FIDO is an authentication system based on asymmetric cryptography without the typical PKI directory services on end user level
- An ecosystem will be needed to establish trust in FIDO tokens for relying parties nevertheless.
- Elements of this ecosystem could be modelled closely after mechanisms successfully established in classical PKI systems



# Establishing trust - Four dimensions



## Reliability

- Availability of trusted metadata will be necessary to establish trust in FIDO token by relying parties
- Integrity and authenticity of this meta data needs to be secured -> classical PKI topic

## Transparency

- Publication of organizational and technical processes for backend mechanisms
- Modelled after already widely accepted scenarios (e.g. SSL / ETSI/ CABF)

## Certification

- Certification is a good way to prove the compliance by independent audit bodies
- Again, widely accepted scenarios already exist in the PKI world (ETSI/CABF/ISO 27001)

# FIDO and beyond - Joining authentication and identification

- Classical PKI based mechanisms typically mix elements of authentication and identification
- FIDO mechanisms allow a clear differentiation between authentication and identification
- Positive aspects both for the relying party as well as the user (data protection, provide only the minimum amount of data required)

# AUTHENTICATION AND IDENTIFICATION WORLDS



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

Governmental  
eID Solutions  
With officially verified ID



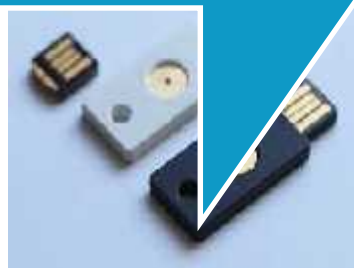
Typically, no interaction between these worlds exist

# BRIDGING THE WORLDS



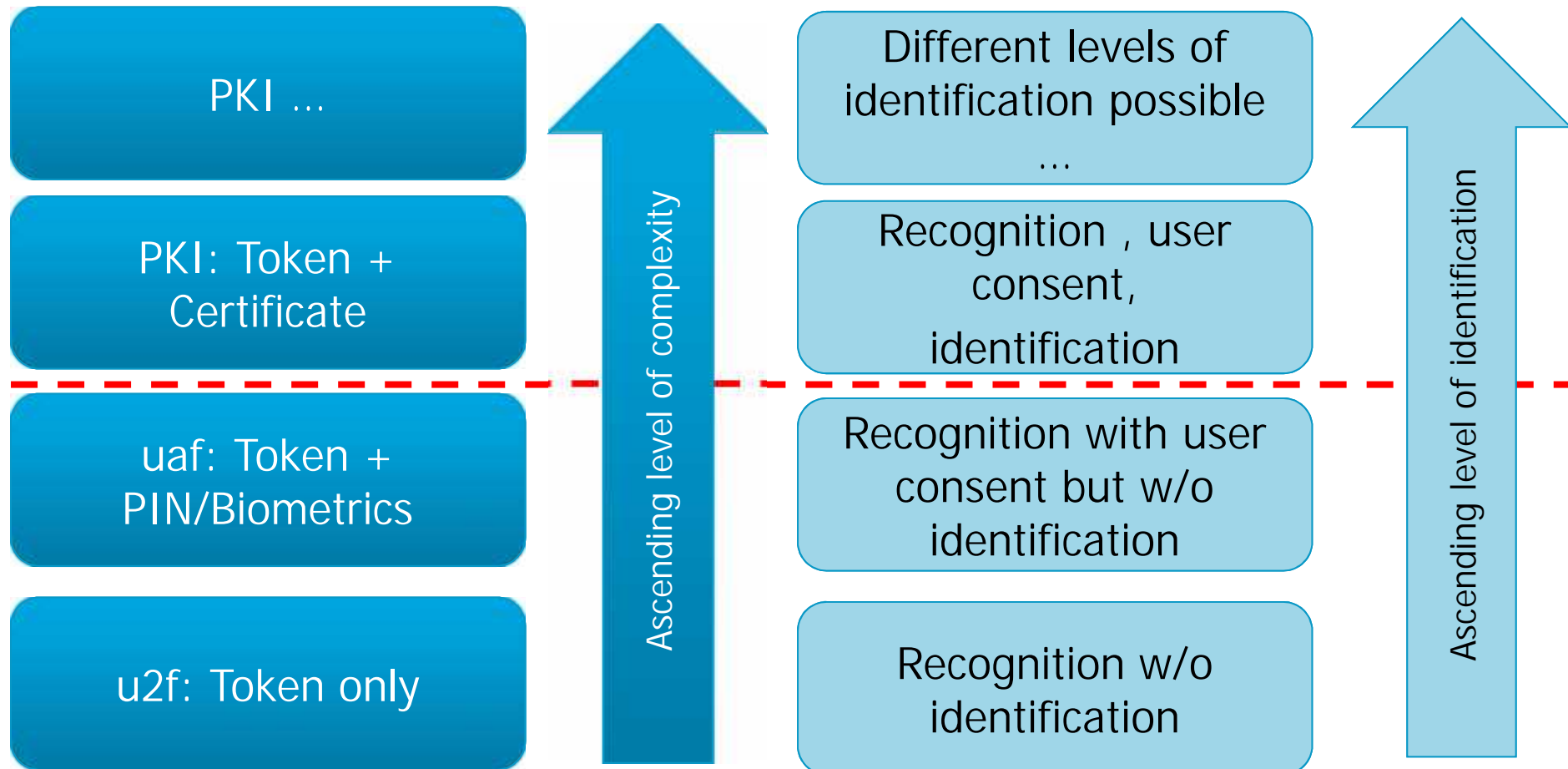
„Proprietary“  
authentication systems,  
e.g. username/  
password, AppleID,  
token ...

Governmental  
eID Solutions  
With officially verified ID



Bridging the world offers advantages for both users and relying parties

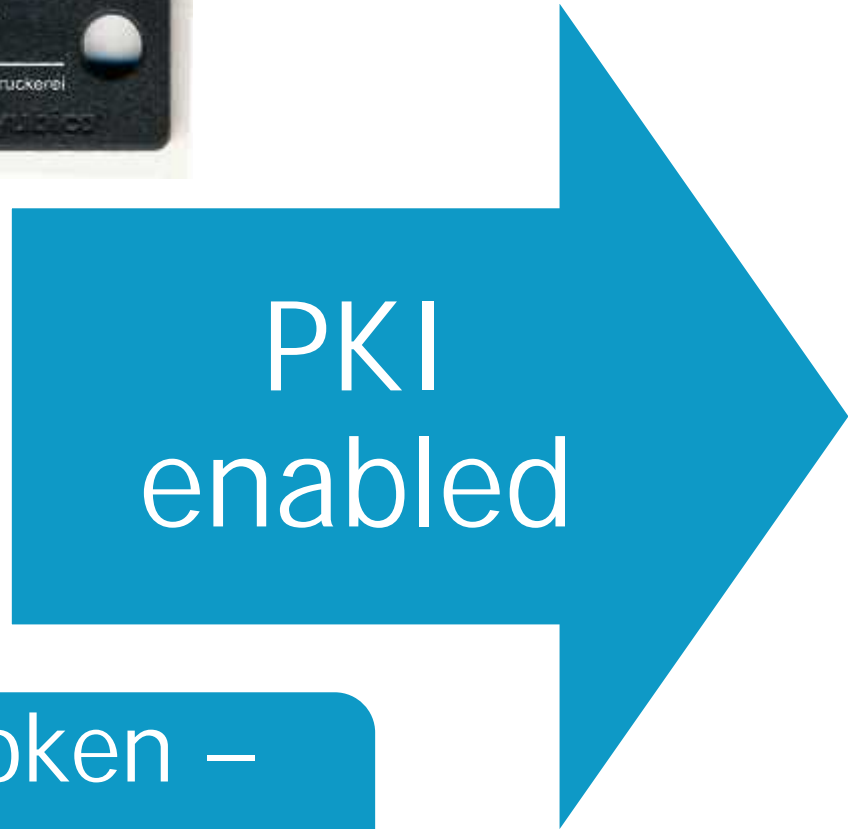
# Layered Authentication/Identification model for FIDO and PKI





# THE SOLUTION: THE TOKEN

---



One token –  
Two worlds

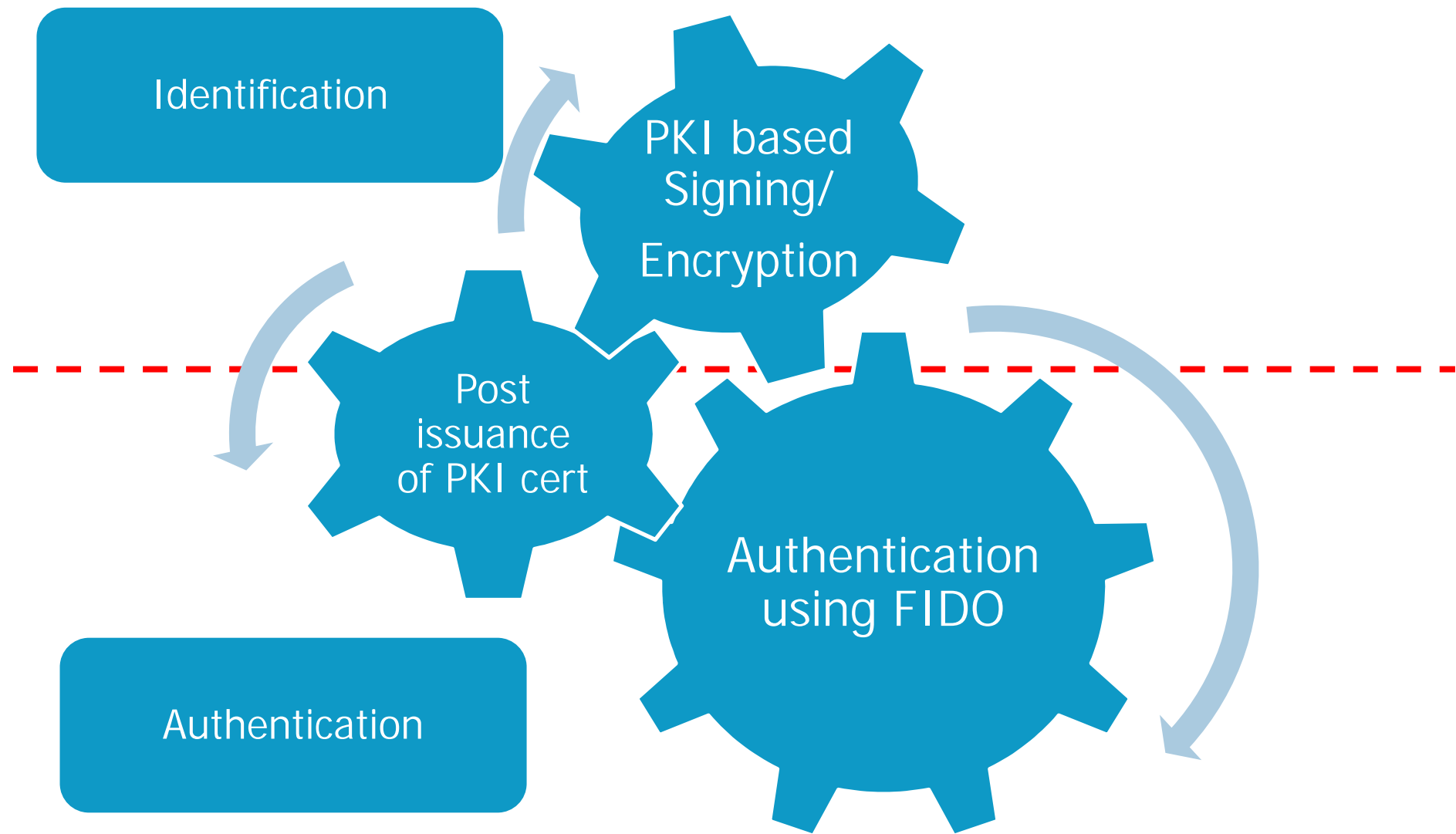
# THE SOLUTION: THE TOKEN

---

- 1 CC Certified chip hardware and chip operating system (CC EAL4+)
- 2 FIDO ready certified application,  
PKI application pre-installed using CV ePasslet suite
- 3 PKI application certified according to European standards for Secure signature creation devices, i.e. eIDAS ready!

# USE CASES

---



# TWO INTERESTING MIGRATION SCENARIOS

---

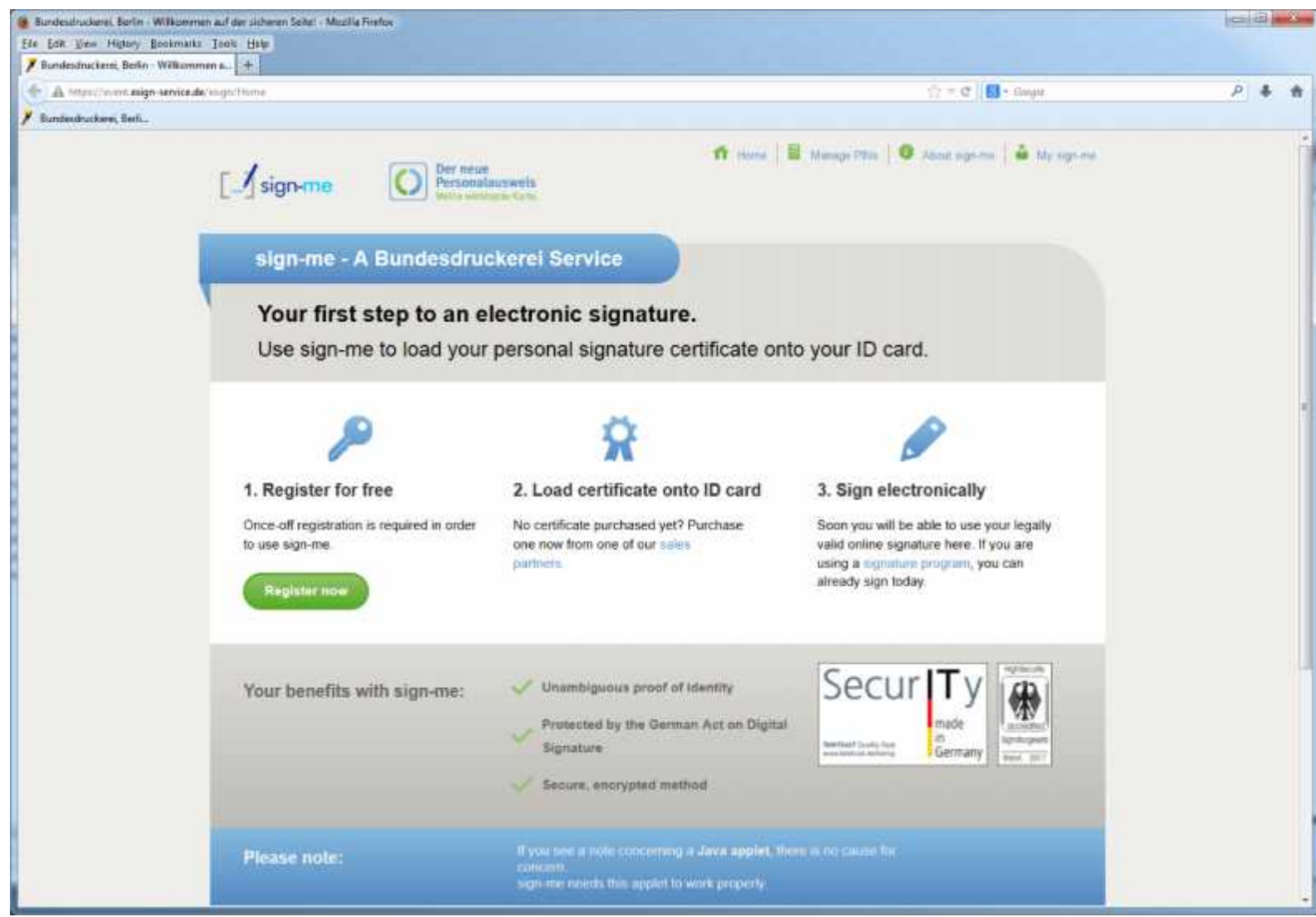


Move an existing PKI ecosystem to a PKI+FIDO ecosystem



Move an existing FIDO ecosystem to a FIDO+PKI ecosystem

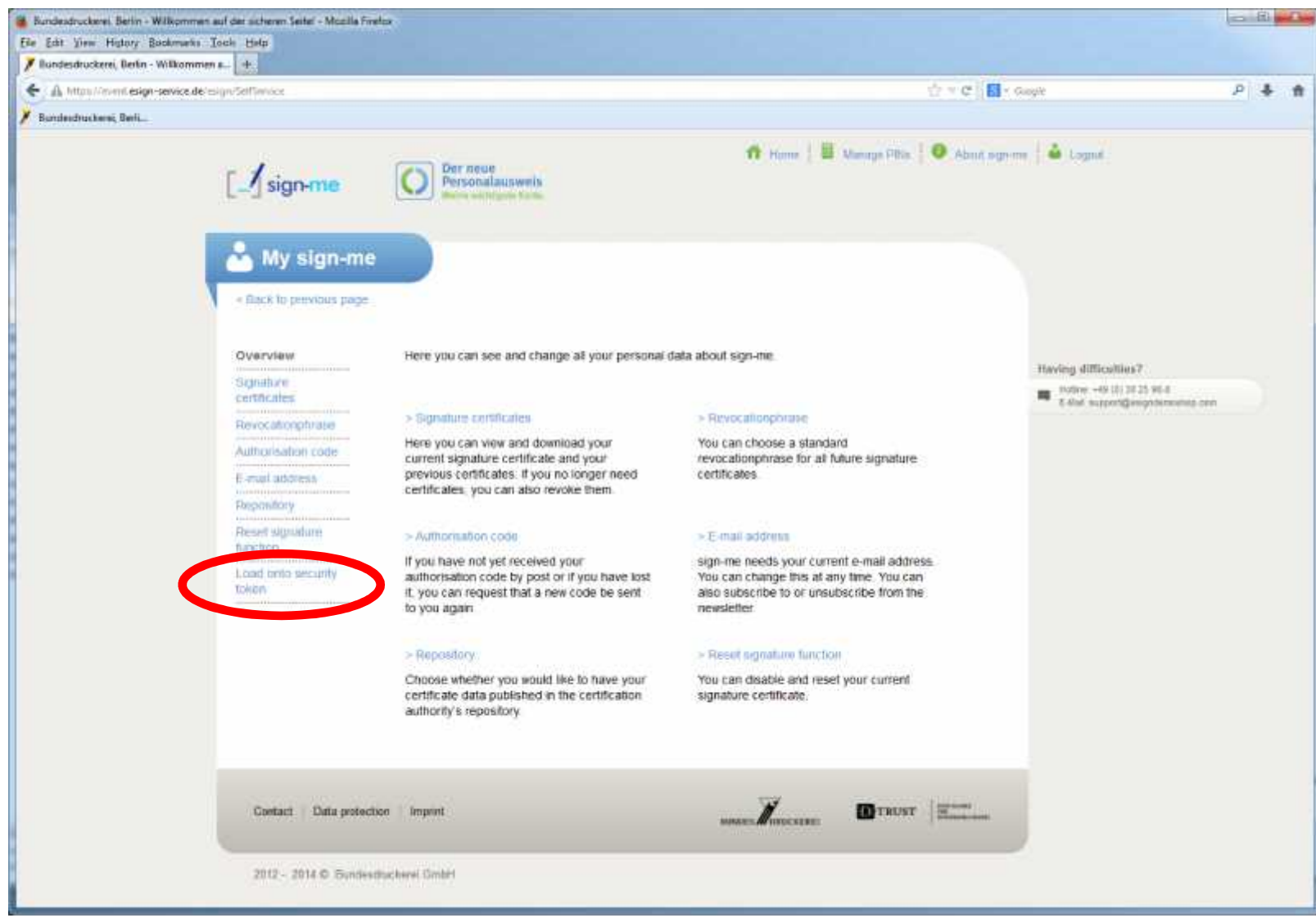
# Post-Issuance scenario

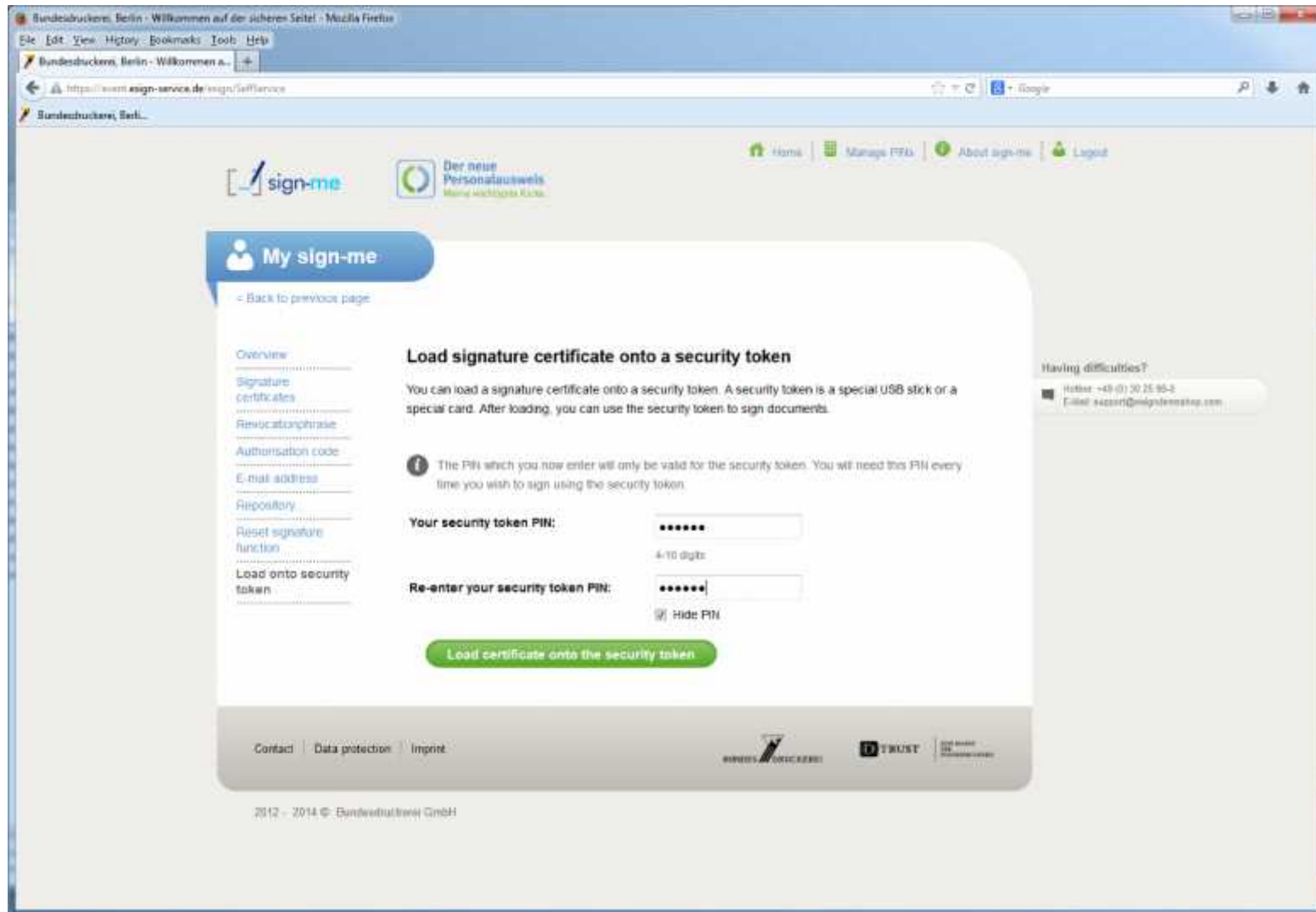


The screenshot shows a web browser window with the following content:

- Browser Title:** Bundesdruckerei, Berlin - Willkommen auf der sicheren Seite! - Mozilla Firefox
- Address Bar:** https://event.sign-service.de/sign/Hello
- Navigation:** Home, Manage PIDs, About sign-me, My sign-me
- Logo:** sign-me
- Text:** Der neue Personalausweis mit dem neuen Chip
- Section Header:** sign-me - A Bundesdruckerei Service
- Main Text:** Your first step to an electronic signature. Use sign-me to load your personal signature certificate onto your ID card.
- Three Steps:**
  - 1. Register for free:** Once-off registration is required in order to use sign-me. [Register now](#)
  - 2. Load certificate onto ID card:** No certificate purchased yet? Purchase one now from one of our [sales partners](#).
  - 3. Sign electronically:** Soon you will be able to use your legally valid online signature here. If you are using a [signature program](#), you can already sign today.
- Your benefits with sign-me:**
  - ✓ Unambiguous proof of identity
  - ✓ Protected by the German Act on Digital Signature
  - ✓ Secure, encrypted method
- Security Logos:** SecurITy made in Germany, and a logo for the German Federal Government.
- Please note:** If you see a note concerning a Java applet, there is no cause for concern. sign-me needs this applet to work properly.

# Post-Issuance scenario





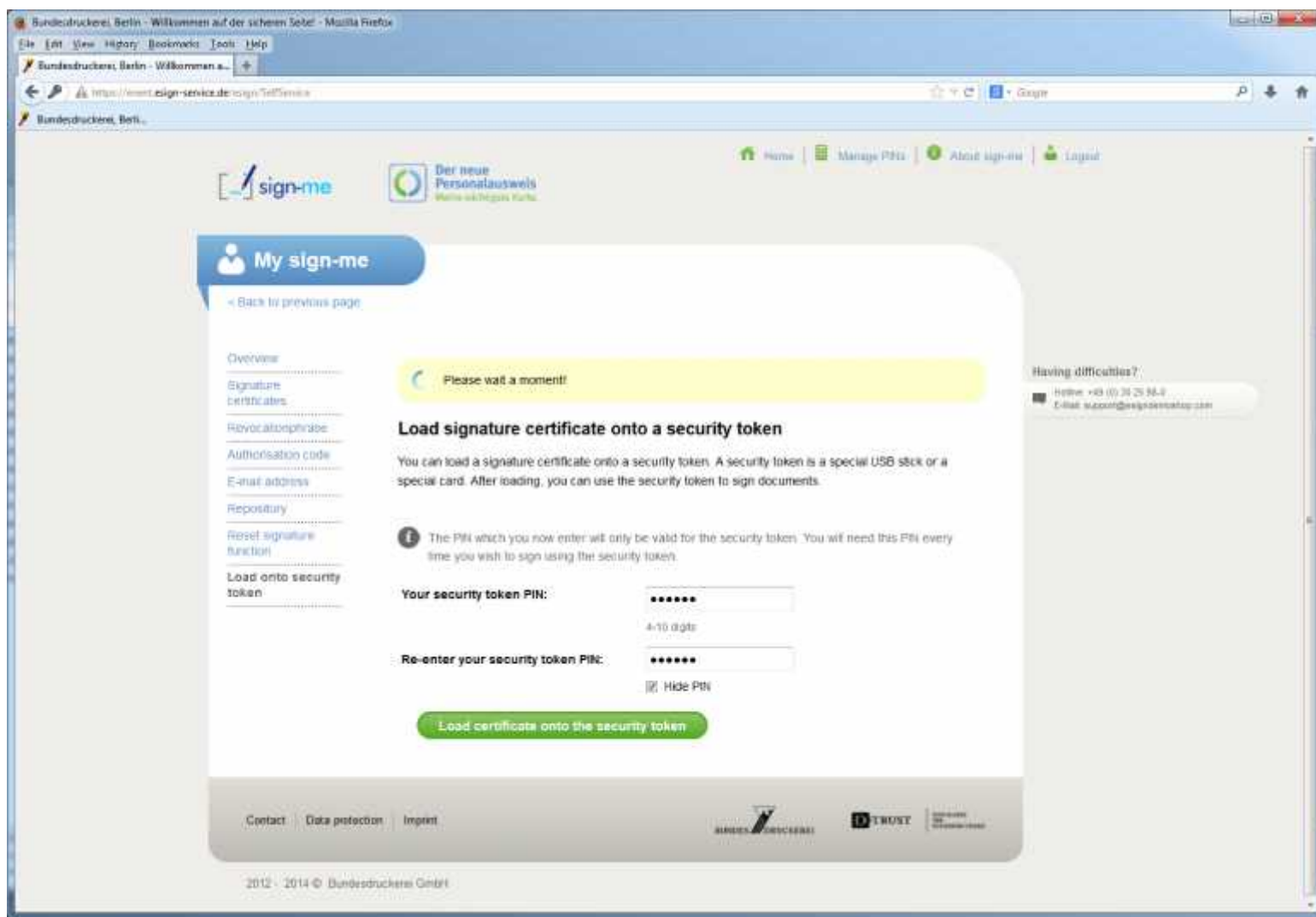
The screenshot shows a web browser window with the URL <http://www.sign-service.de/sign/Service>. The page title is "Bundesdruckerei, Berlin - Willkommen auf der sicheren Seite! - Mozilla Firefox". The browser's address bar shows the URL and a search engine icon.

The main content area is titled "My sign-me" and includes a navigation menu on the left with links: Overview, Signature certificates, Revocation phrase, Authorisation code, E-mail address, Repository, Reset signature function, and Load onto security token. The central section is titled "Load signature certificate onto a security token" and contains the following text: "You can load a signature certificate onto a security token. A security token is a special USB stick or a special card. After loading, you can use the security token to sign documents." Below this is an information icon and text: "The PIN which you now enter will only be valid for the security token. You will need this PIN every time you wish to sign using the security token." There are two input fields for "Your security token PIN:" and "Re-enter your security token PIN:", both masked with dots. A "Hide PIN" checkbox is present below the second field. A green button labeled "Load certificate onto the security token" is at the bottom of the form.

On the right side, there is a "Having difficulties?" section with contact information: "Hotline: +49 (0) 30 25 95-3" and "E-mail: [support@bundesdruckerei.com](mailto:support@bundesdruckerei.com)".

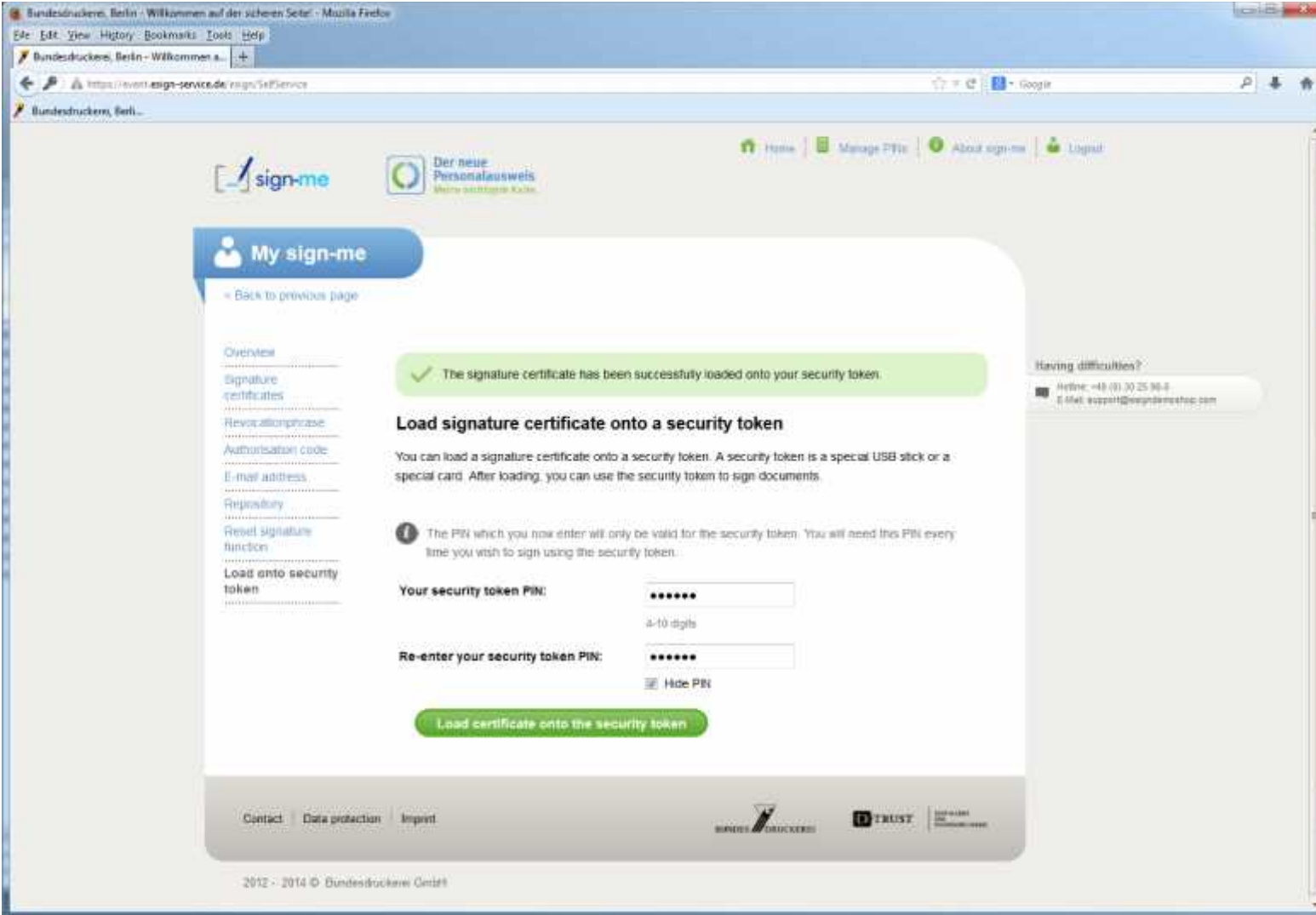
The footer contains links for "Contact", "Data protection", and "Imprint", along with logos for "BUNDES DRUCKEREI", "TRUST", and "cert made in Germany". The copyright notice at the bottom reads "2012 - 2014 © Bundesdruckerei GmbH".

# Post-Issuance scenario

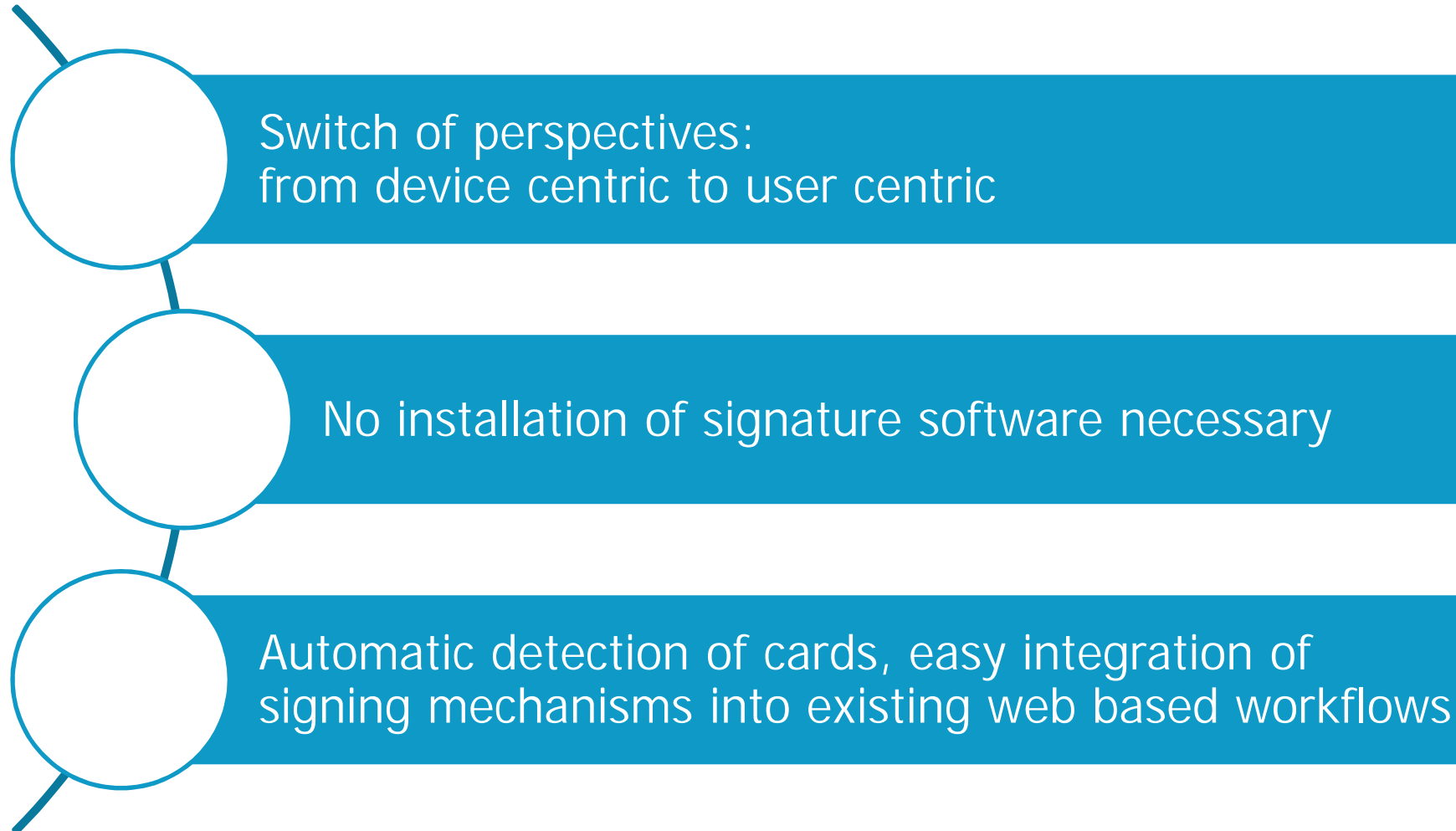




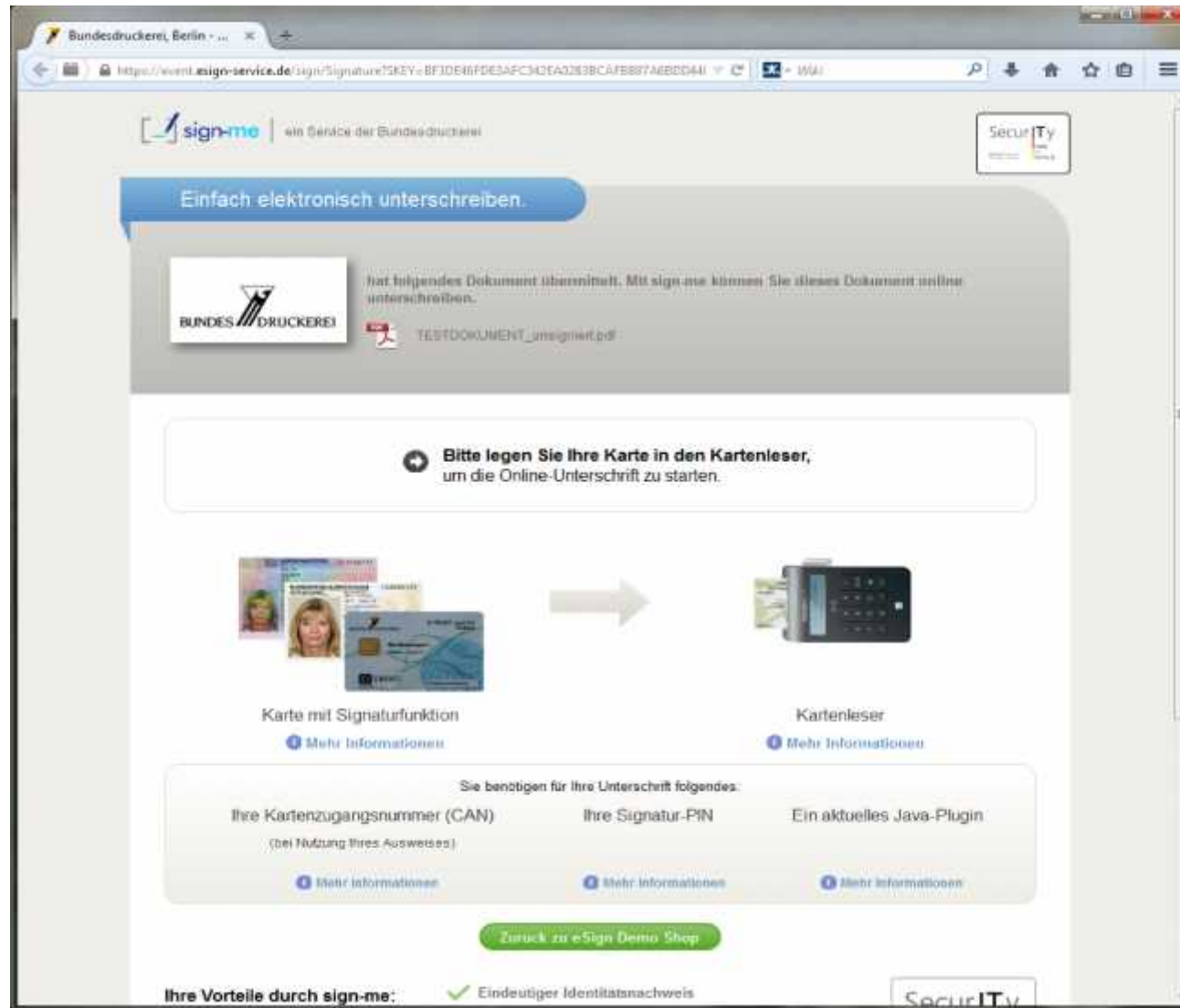
# Post-Issuance scenario



The screenshot shows a web browser window displaying the 'sign-me' service interface. The browser's address bar shows the URL 'https://event.sign-service.de/sign/Service'. The page features a navigation menu with links for 'Home', 'Manage PINs', 'About sign-me', and 'Logout'. A 'My sign-me' section contains a sidebar with links for 'Overview', 'Signature certificates', 'Reset activation phrase', 'Authorization code', 'E-mail address', 'Repository', 'Reset signature function', and 'Load onto security token'. The main content area displays a green success message: 'The signature certificate has been successfully loaded onto your security token.' Below this, the heading 'Load signature certificate onto a security token' is followed by an explanatory paragraph. An information icon and text state: 'The PIN which you now enter will only be valid for the security token. You will need this PIN every time you wish to sign using the security token.' The form includes two input fields for 'Your security token PIN:' and 'Re-enter your security token PIN:', both masked with dots. A 'Hide PIN' checkbox is located below the second field. A green button labeled 'Load certificate onto the security token' is positioned at the bottom of the form. The footer contains links for 'Contact', 'Data protection', and 'Imprint', along with logos for 'BUNDES DRUCKEREI', 'TRUST', and 'CERTIFIED SIGNATURE SERVICE'. The copyright notice at the bottom reads '2012 - 2014 © Bundesdruckerei GmbH'.

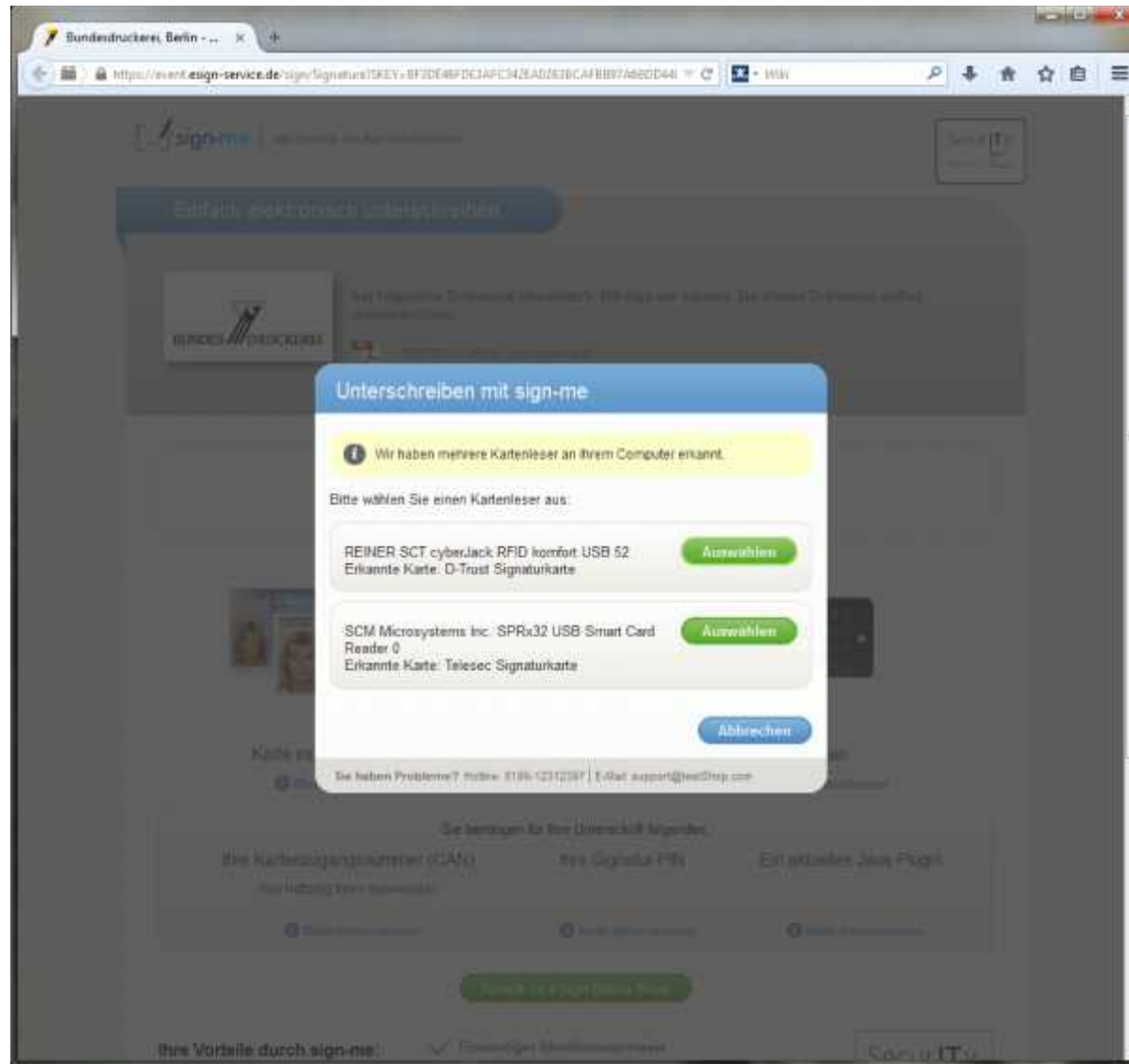


# Usage of certificates

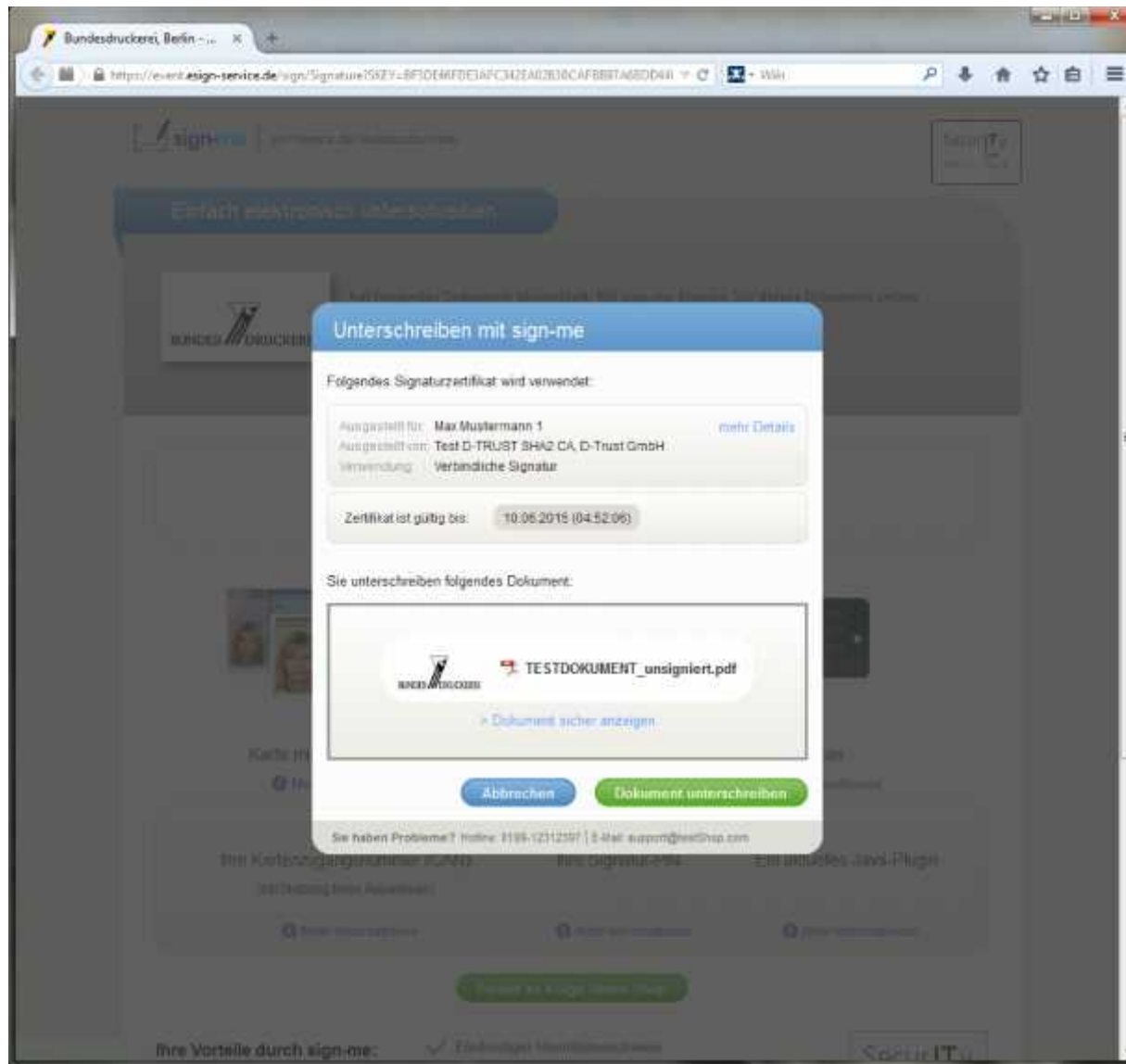


The screenshot shows a web browser window with the URL <https://event.sign-service.de/sign/Signature?KEY=BF1DE6FDE3AFC343EA0283BCAFCB87A6BDD44>. The page header includes the 'sign-me' logo and a 'Security' badge. A blue banner at the top reads 'Einfach elektronisch unterschreiben.' Below this, a document titled 'TESTDOKUMENT\_unsigniert.pdf' is shown with the Bundesdruckerei logo. A central instruction box says: 'Bitte legen Sie Ihre Karte in den Kartenleser, um die Online-Unterschrift zu starten.' Below this, an illustration shows a 'Karte mit Signaturfunktion' (signature card) being inserted into a 'Kartenleser' (card reader). A list of requirements for signing is provided: 'Ihre Kartenzugangsnummer (CAN) (bei Nutzung Ihres Ausweises)', 'Ihre Signatur-PIN', and 'Ein aktuelles Java-Plugin'. Each requirement has a 'Mehr Informationen' link. A green button at the bottom says 'Zurück zur e-Sign Demo-Shop'. At the very bottom, it lists 'Ihre Vorteile durch sign-me: Eindeutiger Identitätsnachweis'.

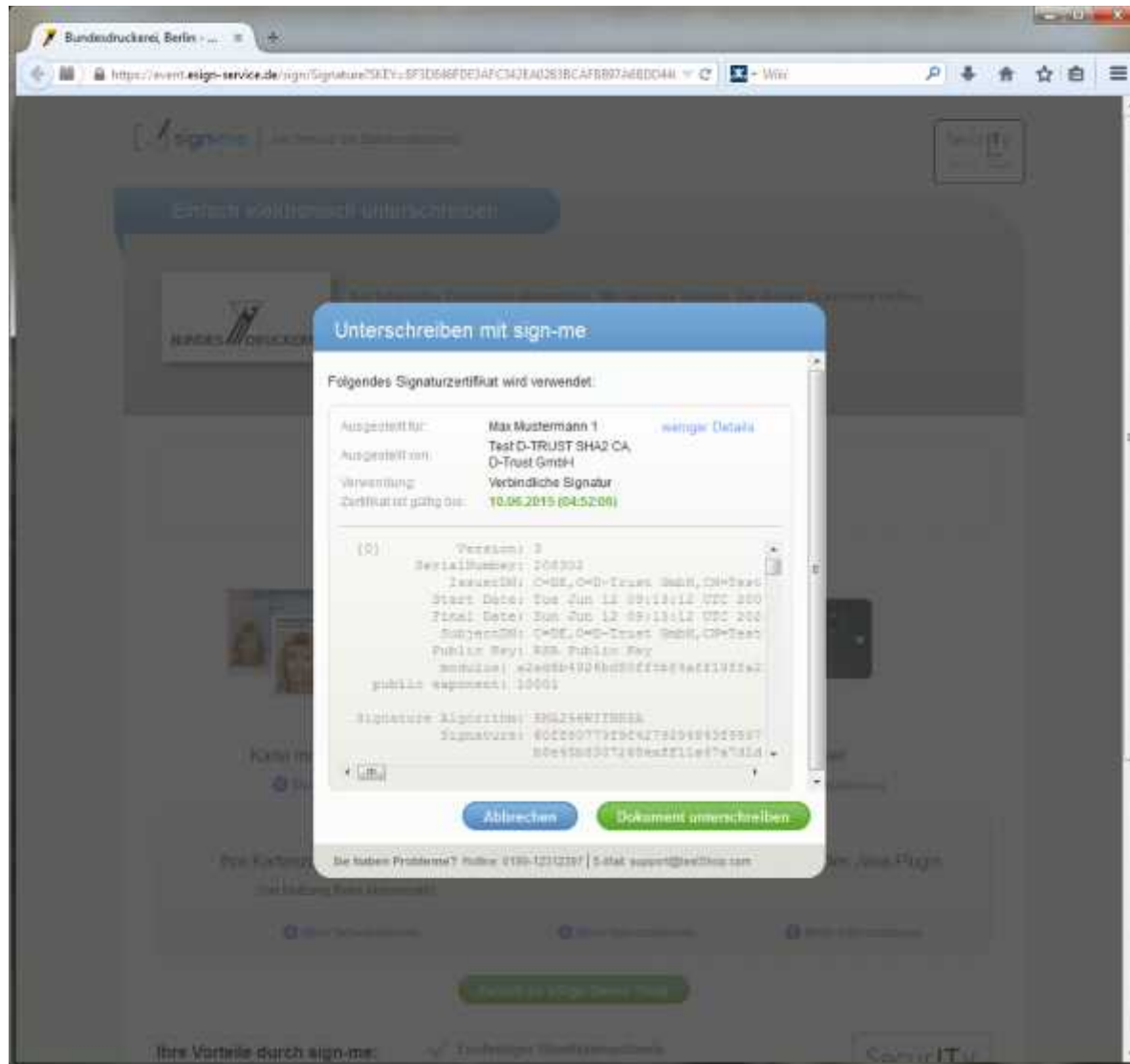
# Usage of certificates



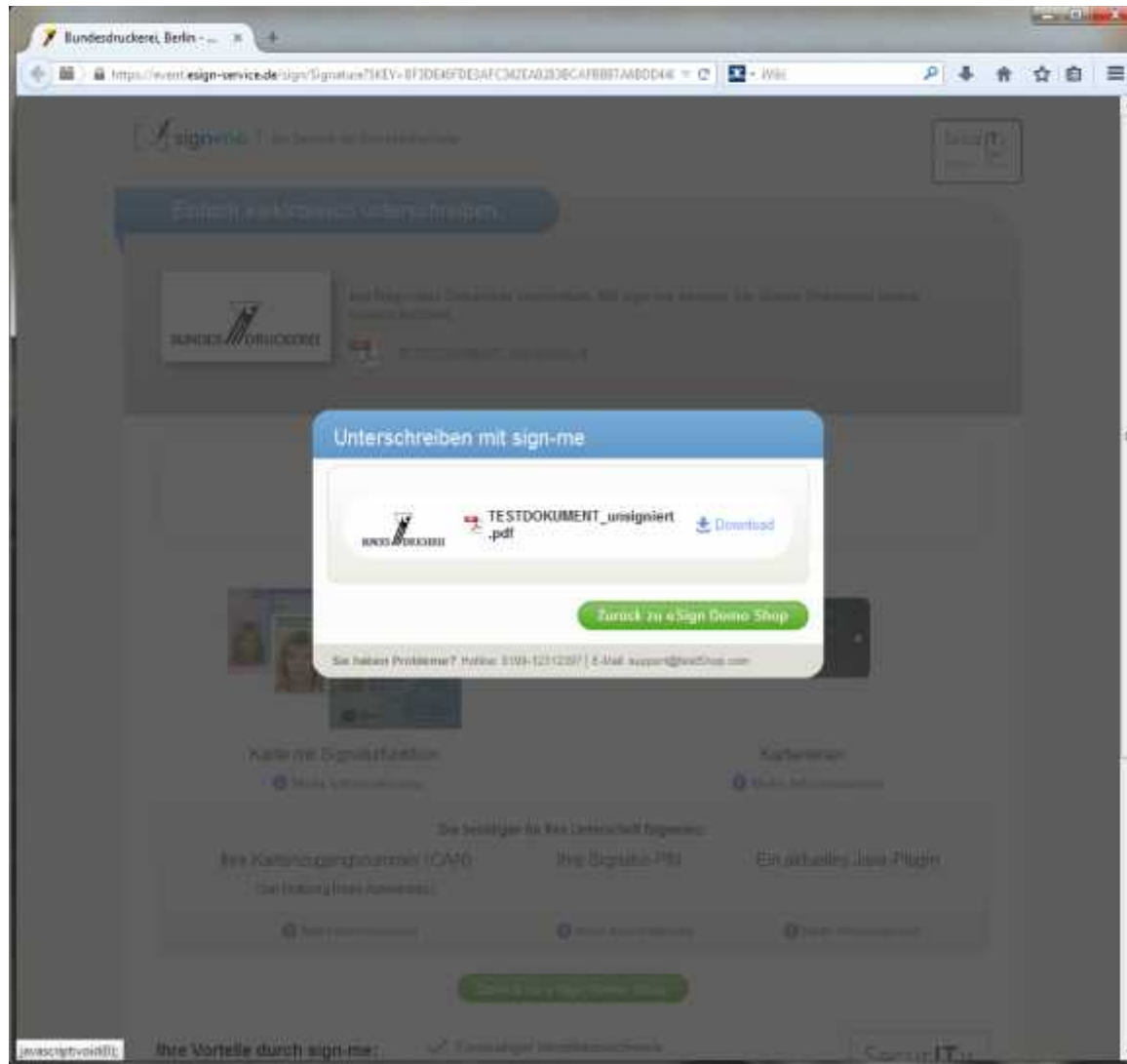
# Usage of certificates



# Usage of certificates



# Usage of certificates



- FIDO offers a new userfriendly approach to authentication – FIDO is the future
- Trust in FIDO mechanism will rely both on trust into the token as well as in the ecosystem
- FIDO can be combined easily with (PKI based) identification mechanisms – bridging two worlds
- Switch from device centric to user centric approach is vital – the success of eIDAS will largely depend on this!



Thank you very much for your  
attention!

Dr. Kim Nguyen

[k.nguyen@d-trust.net](mailto:k.nguyen@d-trust.net)

# CA Compliance Info-Day

## 4<sup>th</sup> November 2014

Policy requirements from different fora.

Robin Alden

Chief technical Officer

**COMODO**

Creating Trust Online®



- Comodo is one of the largest commercial CAs.
- We have been issuing SSL certificates since 2002.
- We are audited by WebTrust licenced auditors who are based in the US.

# Policy requirements from different fora

Across the world, policy is pushed down to CAs from several different places.

- National Requirements
- (intra) Governmental Requirements
- Commercial Requirements

# Commercial Trust Programmes

- Microsoft Windows and Windows Mobile
- Apple operating systems
- Mozilla browsers and operating systems
- Google browsers and operating systems

# Commercial Trust Programmes

- Microsoft Windows and Windows Mobile, including Microsoft Internet Explorer.
- Apple operating systems, Desktop & Phone, including the Safari browser
- Mozilla browsers and operating systems, including the FireFox browser
- Google browsers and operating systems, including Android & Chrome

# Audit for Commercial Trust Stores

- Browsers/Platforms require audit
- Browsers/Platforms are free to specify their own audit criteria.
- They are not all the same..!

# Audit for Commercial Trust Stores

- Browsers/Platforms require audit
- Browsers/Platforms are free to specify their own audit criteria.
- They are not all the same..!
- Fortunately they have sets of criteria in common, and WebTrust audits are acceptable, as are audits to ETSI TS 102 042



# WebTrust

from <http://www.webtrust.org/item64428.aspx>

- Principles and Criteria for Certification Authorities 2.0

Can be done stand-alone

- SSL Baseline with Network Security – Version 2.0  
(usually done with P&C for CAs)
- Extended Validation SSL – Version 1.4.5  
(usually done with P&C for CAs or ETSI TS102 042)
- Extended Validation Code Signing  
(usually done with P&C for CAs or ETSI TS102 042)

# WebTrust

from <http://www.webtrust.org/item64428.aspx>

- Principles and Criteria for Certification Authorities 2.0

Can be done stand-alone

- **SSL Baseline with Network Security – Version 2.0**

(usually done with P&C for CAs)

- Extended Validation SSL – Version 1.4.5

(usually done with P&C for CAs or ETSI TS102 042)

- Extended Validation Code Signing

(usually done with P&C for CAs or ETSI TS102 042)

# WebTrust

from <http://www.webtrust.org/item64428.aspx>

- Principles and Criteria for Certification Authorities 2.0

Can be done stand-alone

- SSL Baseline with Network Security – Version 2.0  
(usually done with P&C for CAs)

- Extended Validation SSL – Version 1.4.5

- (usually done with P&C for CAs or ETSI TS102 042)

- Extended Validation Code Signing

- (usually done with P&C for CAs or ETSI TS102 042)

# WebTrust

from <http://www.webtrust.org/item64428.aspx>

- Principles and Criteria for Certification Authorities 2.0

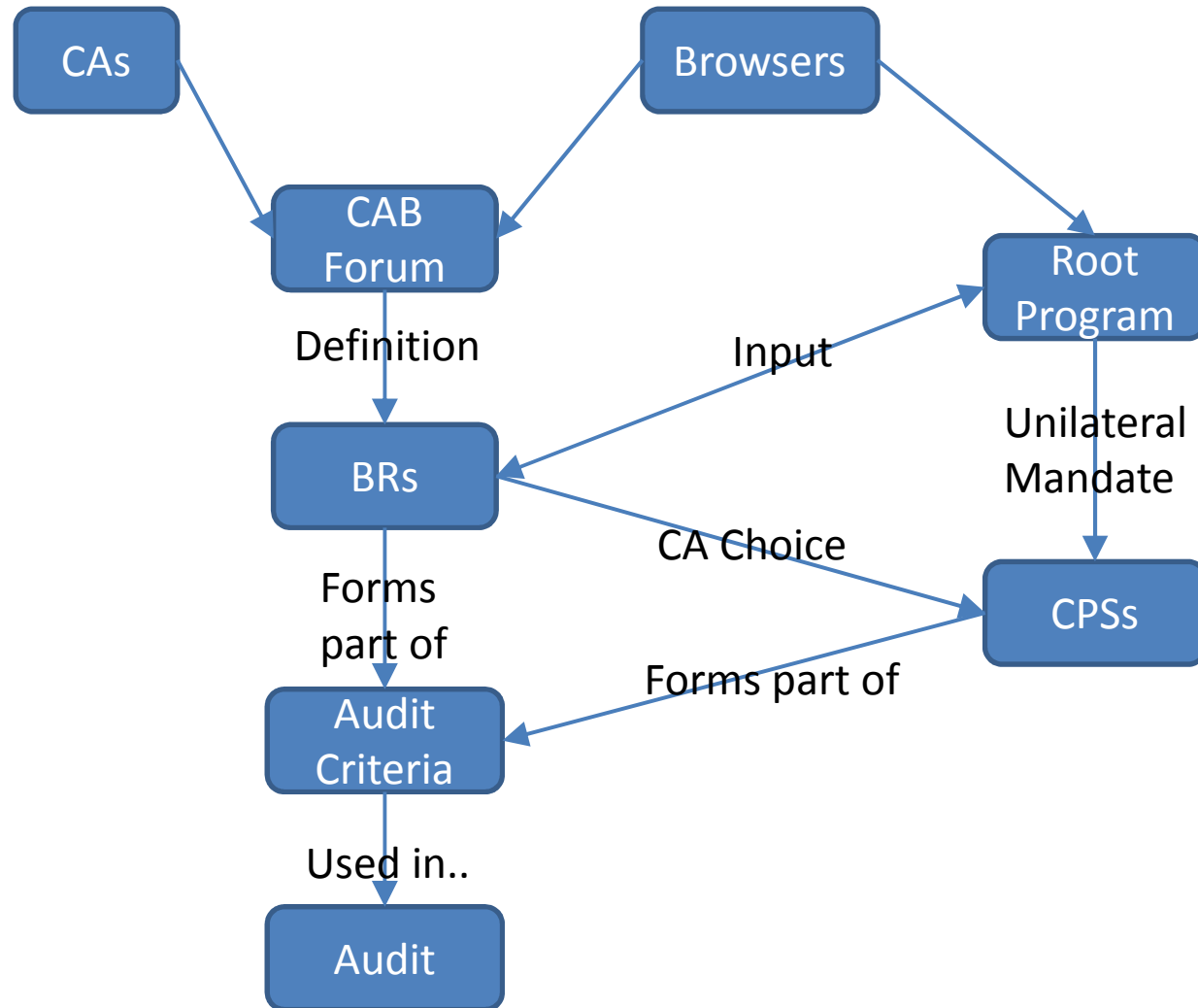
Can be done stand-alone

- SSL Baseline with Network Security – Version 2.0  
(usually done with P&C for CAs)
- Extended Validation SSL – Version 1.4.5  
(usually done with P&C for CAs or ETSI TS102 042)
- **Extended Validation Code Signing**  
(usually done with P&C for CAs or ETSI TS102 042)

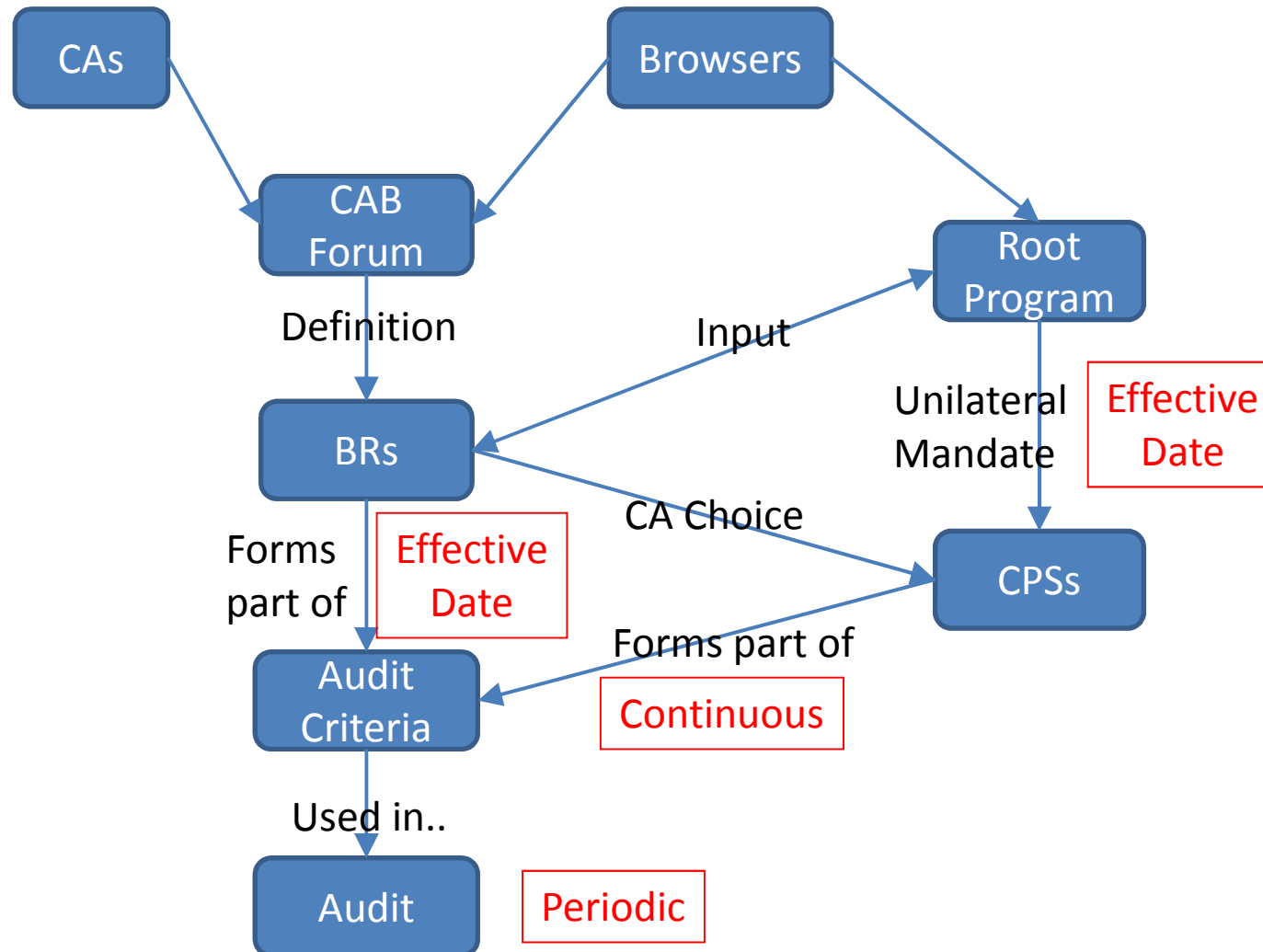
# US Federal PKI

- The FBCA have their own CP.
- The CA CP/CPS is mapped to the FBCA CP.
- Requires a 3rd party audit to cover all mapped parts of the CPS.
- WebTrust for CAs or ETSI audits alone are not sufficient.

# Flow-down of Policy requirements



# Timing of Policy requirements



# NIST IR 7924

- In response to the DigiNotar breach in 2011 and other attacks on CAs, NIST published a draft 'Reference' CP.
- It is not yet clear how this mixes with everything else.



# Mapping Requirements

- DigiCert have contributed to the CAB Forum an initial mapping between the policy requirements of RFC3647 (as the nearest to a common format) and..
- TS 102 042
- EN 319 411-1
- NIST's CP
- CAB Forum Baseline Requirements

# RFC 3647 + TS 102 042 + EN 319 411-1 + NIST CP + CABF BR

RFC 3647 section	TS 102 042	EN 319 411-1	NISTIR 7924 4/2013	BR 1.1.6
1 INTRODUCTION				
1.1 Overview	5.1	5.1	1.1	8.2, 8.3
1.2 Document name and identification	5.2	5.2	1.2	9.3
1.3 PKI participants	4.2, 4.3	4.2, 4.3	1.3	8.1, 8.4
1.4 Certificate usage	5.3	5.3	1.4	7.1, 7.2, 8.1
1.5 Policy administration	Cover pages	Cover pages	1.5	8.2
1.5.1 Organization administering the document	ETSI	ETSI		
1.5.2 Contact person	Cover pages	Cover pages		
1.5.3 Person determining CPS suitability for the policy	-	7.1		
1.5.4 CPS approval procedures	7.1	7.1		
1.6 Definitions and acronyms	3	3	1.6	4, 5
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES				
2.1 Repositories	7.3.5	7.3.5	2.1	13.2
2.2 Publication of certification information	7.3.5, 7.3.6, 7.3.4	7.3.4, 7.3.5, 7.3.6	2.2	8.3, 13.2
2.3 Time or frequency of publication	7.3.5, 7.3.6	7.3.5, 7.3.6	2.3	13.1
2.4 Access controls on repositories	7.4.6	7.4.6	2.4	16.5
3 IDENTIFICATION AND				

3 IDENTIFICATION AND AUTHENTICATION	TS 102 042	EN 319 411-1	NISTIR 7924 4/2013	BR 1.1.6
3.1 Naming	7.3.3	7.3.3	3.1	9.1, 9.2, 9.4, 9.6, 11.2, 12
3.2 Initial identity validation	7.3.1	7.3.1	3.2	9.2, 9.5, 11.1, 11.2, 14.1, 15.3
3.3 Identification and authentication for re-key requests	7.3.2	7.3.2	3.3	
3.4 Identification and authentication for revocation request	7.3.6	7.3.6	3.4	13.1, 13.2
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS				
4.1 Certificate Application	7.3.1	7.3.1	4.1	10.1, 10.2
4.2 Certificate application processing	7.3.3	7.3.3	4.2	10.2
4.3 Certificate issuance	7.3.3	7.3.3	4.3	9, 10
4.4 Certificate acceptance	7.3.1	7.3.1	4.4	10.3
4.5 Key pair and certificate usage	6.2, 6.3	6.2, 6.3	4.5	10.2
4.6 Certificate renewal	7.3.2	7.3.2	4.6	15.2
4.7 Certificate re-key	7.3.2	7.3.2	4.7	15.2
4.8 Certificate modification	7.3.2	7.3.2	4.8	
4.9 Certificate revocation and suspension	7.3.6	7.3.6	4.9	13.1, 13.2

# Where next..?

- How to unify the requirements without creating a single all-powerful root of trust for all purposes?
- Probably not quite that bad..
- The requirements will converge
- .. Even if there remain multiple sets of audit criteria.

# The End

- Thank you for listening!

Robin Alden

[robin@comodo.com](mailto:robin@comodo.com)

**COMODO**  
Creating Trust Online®



swiss made  
software

swiss  
sign **>**  
TRUSTED  
IDENTITY

# Digital ID Challenges

SwissSign – Trusted Identity  
Made in Switzerland

Cornelia Enke  
Security & Compliance



# › Agenda

- › **About SwissSign**
- › SuisseID
- › SuisseID Concept
- › Status Today
- › Digital ID Challenges



# About SwissSign

- › Founded in 2001, about 30 employees
- › A Swiss Post Company since 2005
- › Internationally accredited Certificate Services Provider (CSP)
- › Certificates of any type: machines, individuals, organizations
- › Compliant with international standards (Webtrust, ETSI, CA/Browser Forum, ISO 27001)
- › Compliant with Swiss Law ZertES, EIDI-V, GeBüV
- › Audited by KPMG





## ➤ Agenda

- About SwissSign
- **SuisseID**
- SuisseID Concept
- Status Today
- Digital ID Challenges



# Purpose of SuisseID



## User's needs:

- Simple and secure
- User-friendly
- Master key
- Data confidentiality



## Companies's needs:

- Focus on core processes
- Legal compliant
- Optimized access security
- Simple integration
- Outsourcing:
  - Identity Management
  - Authentication

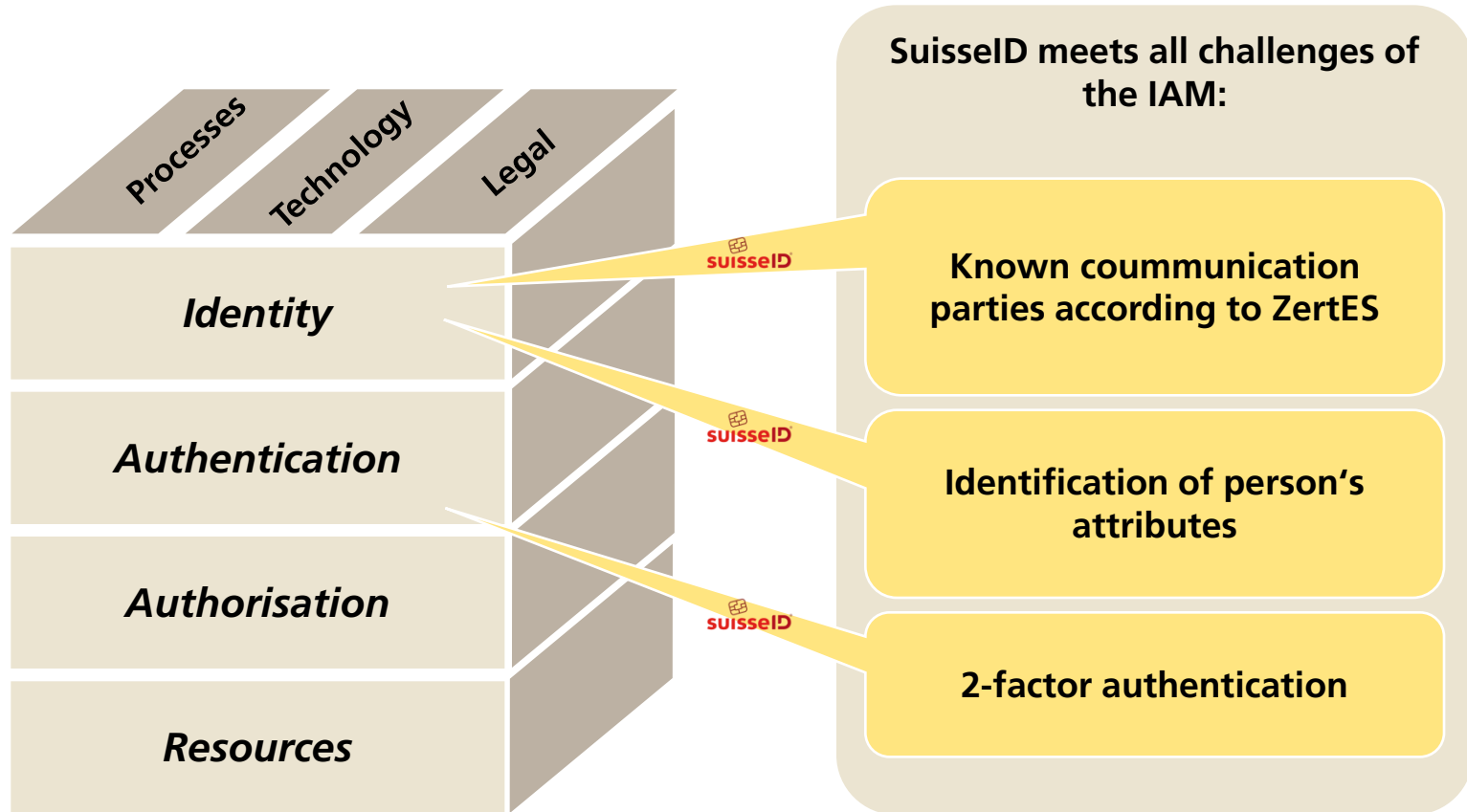


## Statutory requirements

- OR Art. 14 Para 2bis  
Swiss Code of Obligations
- ZertES  
Swiss legislation on electronic signatures
- EIDI-V  
Ordinance of the Swiss FDF  
on electronic data and information



# SuisseID – Identity and Access Management



## ➤ Agenda

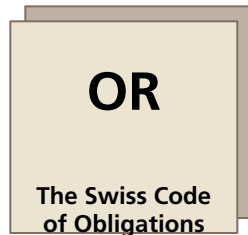
- About SwissSign
- SuisseID
- **SuisseID Concept**
- Status Today
- Digital ID Challenges



# SuisseID Concept



- SuisseID is Switzerland's standardised electronic proof of identity : **legally valid electronic signature** and **secure authentication**.



- Swiss legal qualified signatur (ZertES), audited by KPMG.
- Base on European ETSI standards.
- In Switzerland: like handwritten signature (Art. 14 Abs 2bis OR).



- SuisseID utilises internationally recognised standards such as SAML 2.0 (see STORK Project).
- SuisseID : efficient in the areas of e-government and e-economy.



- Continuity guaranteed.
- Continous development sponsored by Swiss Post.



# SuisseID Technical Concept

## **Unique / distinctive**

Holder verification via the distinctive SuisseID number

## **Lifelong**

The SuisseID number is assigned to the individual (lifelong)

## **Permanent**

The SuisseID number is retained if there is a change in certificate/smartcard

## **Issuer-independent**

If supplier changes – the SuisseID number stays the same

## **Linking element**

The SuisseID number links the elements of the standardised authentication certificates (IAC), qualified certificate (QC) and the data in the SuisseID Identity Provider (IDP), the central data storage

## SuisseID within the EU region

- › SuisseID is EU-compatible:
- › Technical standards implemented
- › EU-compatible in organisational terms

**The technical conditions should be in place in the Stork Project as a minimum requirement for success: the technology used for SuisseID, the so-called Security-Assertion-Markup-Language (SAML), will also be used by Stork. In addition, SuisseID is based on the European Telecommunication Standard ETSI. This means that from both the technical and organisational aspects SuisseID is EU-compatible, as Weber says. A conscious decision was taken not to use any proprietary solution in Switzerland, although there was a leaning towards developing a separate “Swiss solution”.**

Source: Netzwoche / Christian Weber (Seco)



## ➤ Agenda

- About SwissSign
- SuisseID
- SuisseID Concept
- **Status Today**
- Digital ID Challenges





## eIDAS Related Legal Situation Switzerland

- › No need for further changes on ZertES caused by eIDAS
- › New eID technical proposal planned for Q3/2015
- › The new law proposal will be worked out after March 2016
- › Legal proposal of Electronic delivery platform: November 2016
- › E-Invoice 2016 (Project)



## ➤ Agenda

- About SwissSign
- SuisseID
- SuisseID Concept
- Status Today
- **Digital ID Challenges**



## Digital ID Challenges

- We have to cope with
  - National (Swiss) Law: ZertES, EIDI-V
  - eIDAS regulations
  - ETSI standards
  - CA/Browser Forum Baseline Requirements and EV Guidelines
  - Application and operation system supplier guidelines
- Sometimes overlapping, sometimes additional ....
- In focus: trustful certificates ready for cross-border use

WWW instead of EUW



 Thanks!

 Cornelia Enke

 [cornelia.enke@swisssign.com](mailto:cornelia.enke@swisssign.com)



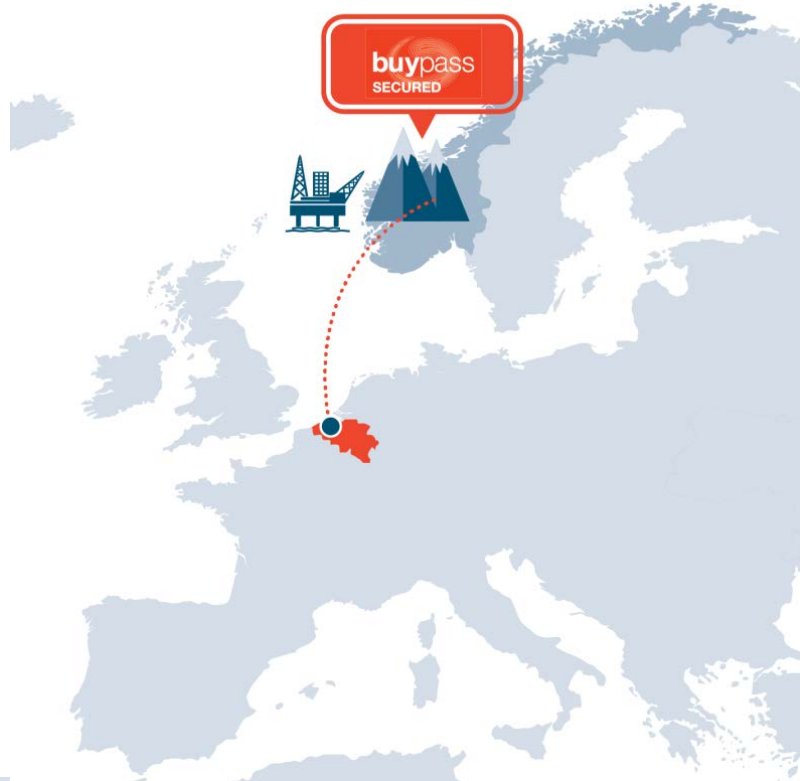
# A 1000 foot view on eIDAS from the outer edge of EU

Mads Henriksveen, Buypass

*Berlin*  
Nov 4<sup>th</sup> 2014

eIDAS

## A 1000 foot view on eIDAS from the outer edge of EU



	Norway	EU
Population	5,136,700	507,416,607
Area (km <sup>2</sup> )	385,178	4,381,376
Density	15,5/km <sup>2</sup>	115,8/km <sup>2</sup>
GDP pr capita	\$55,398	\$33,084
HDI	0,944	0, 876
Internet users	96,1%	76,5%

eIDAS

# Norway and EU

## European Free Trade Association





Map of Europe with EFTA members highlighted in green.

## European Economic Area



The EEA in 2014:

-  EFTA member countries (excluding Switzerland)
-  European Union member states (excluding Croatia)

# eID and eSignature in Norway

## eSignature Act (2001)

- Implementing Directive 1999/93/EC

## Self-declaration procedure

- Based on a requirements specification for PKI based eID to be utilised for electronic communication with and within the public sector

## Specification for PKI in the public sector

- Covers PKI based eID (and eSignature) for both legal and natural persons
  - Enterprise certificate
  - Person-High (QC)
  - Person-Standard



# eID and eSignature in Norway

## Framework for authentication and non-repudiation in electronic communication with and within the public sector (2008)

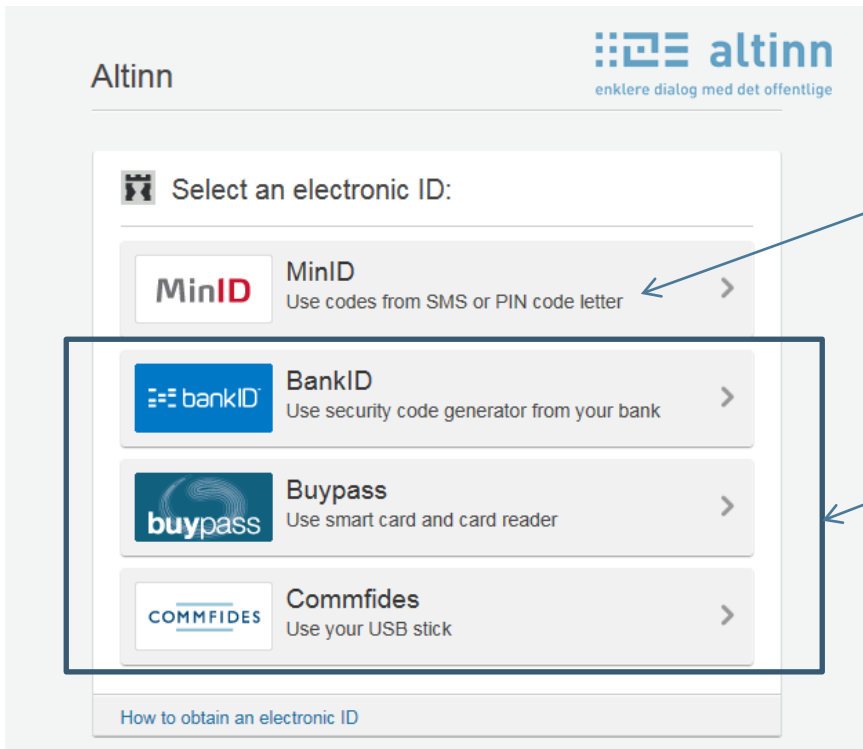
- Defines four security levels and requirements for these
  - Level 4: PKI is mandatory => corresponds to *Person-High* (QC)
  - Level 3: PKI is optional => if PKI, corresponds to *Person-Standard*

## Implementation in Norway

- Private sector distributes level 4 eID to Norwegians
  - PKI based => must comply with the PKI specification
- Public sector distributes level 3 eID to Norwegians
  - Not PKI based => not covered by the PKI specification

eIDAS

# eID and eSignature in Norway



Level 3 eID – public sector

Level 4 eID (PKI) – private sector

# About Buypass

- Jointly owned by Evry and Norsk Tipping
- Leading Trust and Payment Service Provider
  - In house developed technology based on international standards
- Payment Services
  - 2,5 mill end users with e-cash accounts
  - 13 billion NOK in mediated turnover 2013
- **eID and eSignature**
  - **More than 2,5 million end users in Norway**
  - **30 million transactions with Buypass eID per month 2013**
  - **Supplier to all major Norwegian eGovernment projects**
- **SSL/TLS**
  - **Issues SSL/TLS-certificates in the Norwegian market**
  - **Member of CA/Browser Forum**
- Certified information security and quality
  - ISO/IEC 27001 and ISO/IEC 9001
  - ETSI 102 042
  - PCI DSS
- 158 mill NOK in revenue (2013)



eIDAS

# Buypass CA – certs regulated by national legislation



**Buypass CA**



QC person



Enterprise certificate

eIDAS

# Buypass CA – certs regulated by international industry



**Buypass CA**



SSL/TLS certificate



eIDAS

## Buypass' view on eIDAS



eIDAS

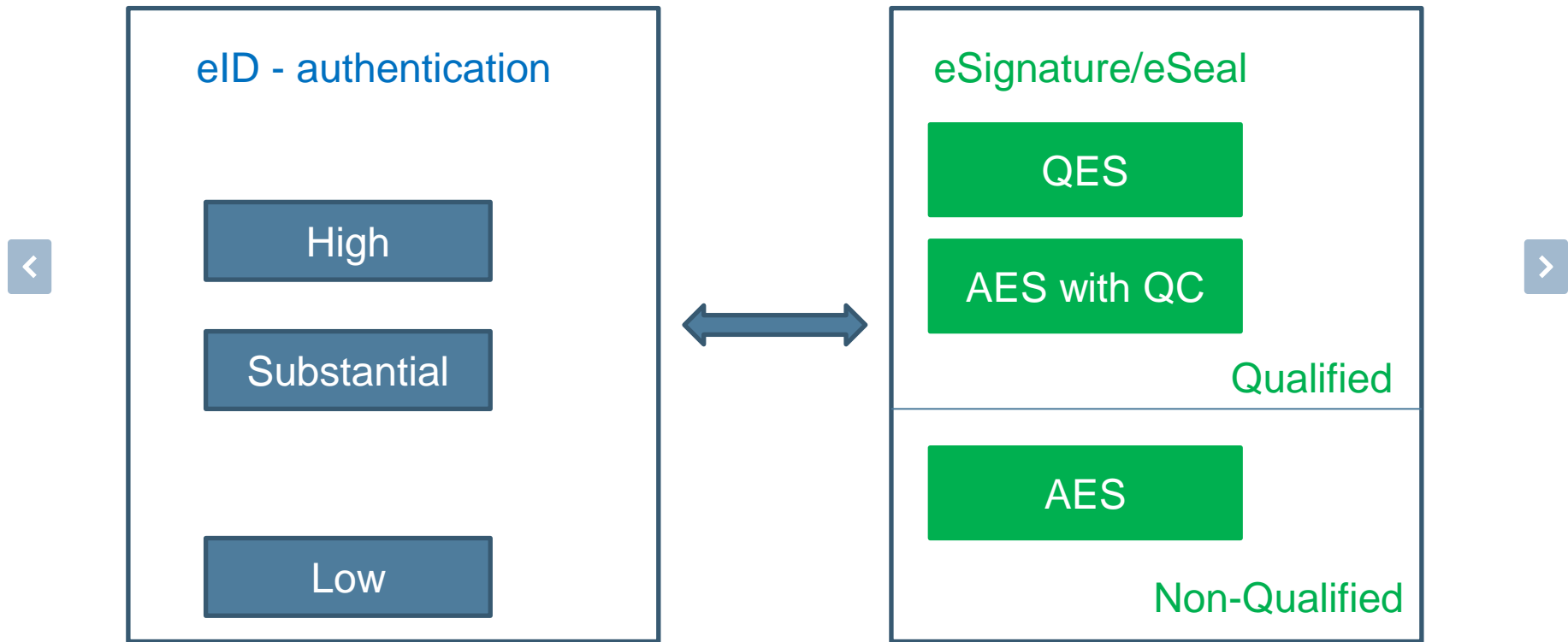
## eIDAS highlights

- aiming at an adequate level of security*
- high level of security*
- open to innovation*
- regulation should be technology-neutral*
- involve the private sector*
- website authentication services*
- remote electronic signatures*
- assurance levels low, substantial and high*
- electronic seals*
- trust service providers*



eIDAS

## eID vs Trust service



eIDAS

# Buypass CA – certs (to be) regulated by eIDAS



**Buypass CA**



QC eSignature



QC eSeal



QC website

eIDAS

Thank you for the attention!

•••••

## Mads Henriksveen

Senior rådgiver / Senior advisor

*m:* +47 952 25 672

*e:* [mads.henriksveen@buypass.no](mailto:mads.henriksveen@buypass.no)

## Buypass AS

Hans Mustads gate 31  
N-2821 Gjøvik, Norway

*t:* +47 22 70 13 00

*w:* [buypass.no](http://buypass.no)





# Trust Services and Applications in Turkey

CA Compliance Info-Day  
eIDAS and Trust Service Provider Conformity Assessment  
Bundesdruckerei, Berlin/Germany – November 4, 2014 Tuesday

**N. ATILLA BILER**  
TÜRKRTRUST Business Development Manager

# Content

- Turkish E–signature Legislation
- Electronic Certification Services and Composition of Turkish Market
- E–signature Usage and Applications in Turkey
- SSL Services and CA/Browser Forum Contribution from Turkey
- Evolving Trust Services in Turkey Based on PKI
- Turkish National e–ID scheme

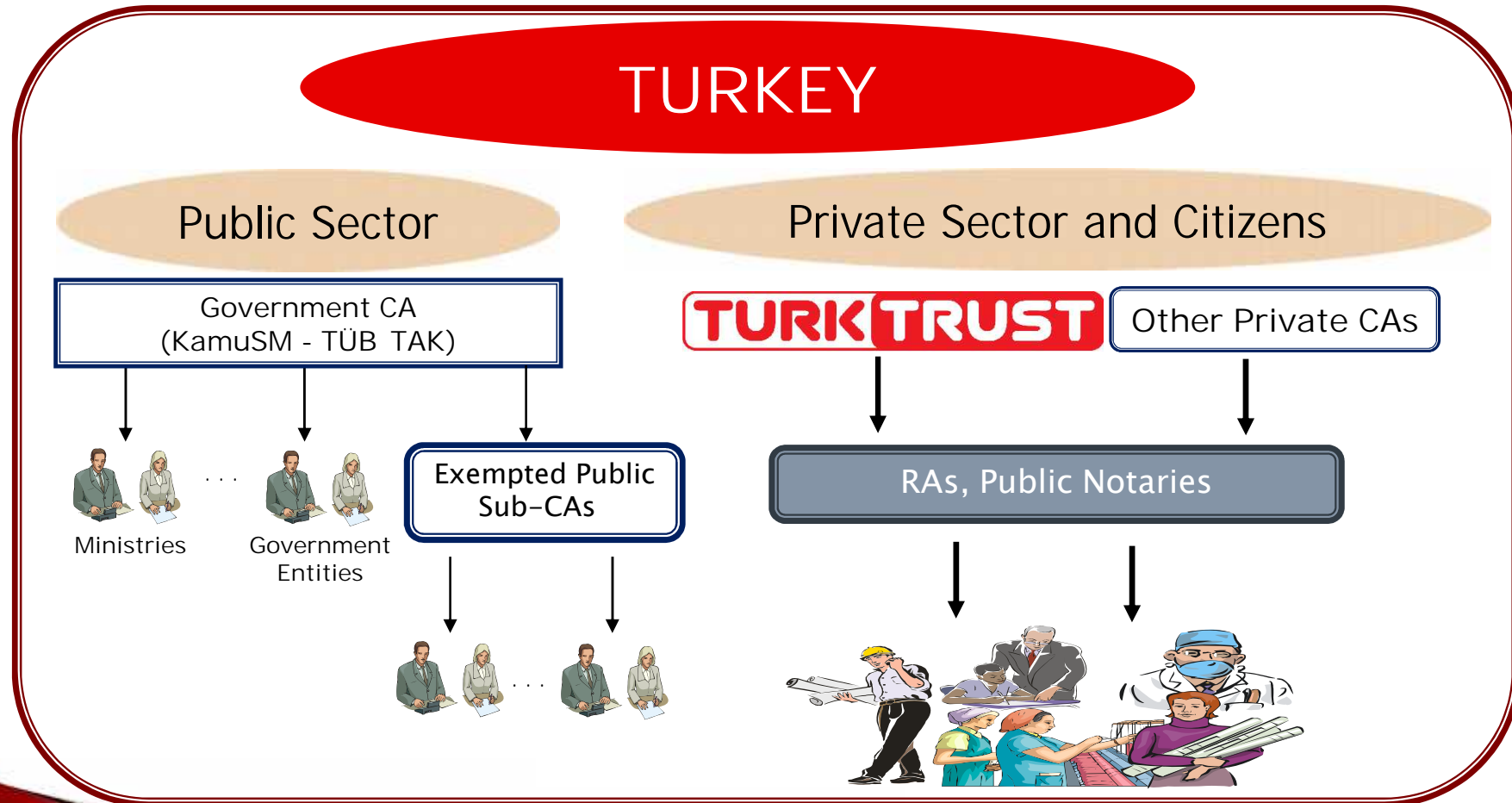
# Turkish E-Signature Legislation

- ▶ Electronic Signature Law (January 15, 2004) – Compliant to related EU Legislation (E-Signature Directive)
- ▶ Ordinance on Procedures and Principles Pertaining to the Implementation of Electronic Signature Law (January 6, 2005)
- ▶ Communiqué on Processes and Technical Criteria Regarding Electronic Signatures (January 6, 2005)
- ▶ Certificate Financial Liability Insurance Regulations (Mandatory for Qualified Electronic Certificate [QEC] issuing Certification Authorities [CAs])
- ▶ Related Prime Ministry Circulars
- ▶ Information and Communications Technologies Authority (ICTA) Board Decisions and Guidelines

# Turkish E-Signature Legislation

- ▶ Only e-signature and time-stamp are regulated by Turkish legislation.
- ▶ SSL and code signing are not regulated in Turkey (for these services, EU regulations, ETSI standards and CA/Browser Forum requirements and guidelines are followed).
- ▶ CAs issuing QECs are regularly audited by the Turkish ICTA.
- ▶ Private sector CAs are not audited by the ICTA for SSL or code signing services. Recently, ICTA performed ETSI based SSL audits only for the Turkish Government CA.

# Electronic Certification Services and Composition of Turkish Market





# Electronic Certification Services and Composition of Turkish Market

- ▶ 1 (one) Government CA  
(KamuSM – TÜBİTAK)
  - 1 (one) Public Sub-CA (Turkish National Police)
  - 1 (one) Public Sub-CA under construction (Turkish Armed Forces)
  
- ▶ 4 (four) Private Sector CAs  
(TÜRKRUST and 3 (three) other authorized private CAs)
  
- \* All CAs have self-signed roots (no single Root CA structure).
- \* Public Sub-CAs have sub-roots signed by the Government CA.

# E-signature Usage in Turkey

- ▶ As of June 2014

E-signature Usage (based on Qualified Electronic Certificates – QECs)	E-Signature	M-Signature	TOTAL
Total Issued QECs	1.088.082	312.631	1.400.713
Revoked QECs	29.323	125.027	154.350
Expired QECs	290.350	171.908	462.258
Suspended QECs	2.905	2.310	5.215
Active QECs (Currently in Use)	765.504	13.386	778.890

- ▶ Over 450.000 (~60%) of the total number of active E-Signature QECs are issued by the Government CA for government users.

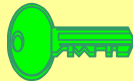
# E-signature Usage in Turkey

## Qualified Electronic Certificates (QEC)

*Secure electronic signature usage*

*(Under the Electronic Signature Law no 5070)*

- Certificate serial number
- ECSP information and country
- QEC notification
- QEC owner identity information
- Authorization information upon request
- Occupation and other personal information upon request
- Possible usage constraints
- Certificate validity period



# E-Signature Applications in Turkey

## ▶ Government Based Applications

Central Registry System for Private Sector Companies (MERSİS)

Free Zone and Import-Export Applications (Ministry of Economy)

E-Invoice Applications (Ministry of Finance)

Warranty Applications for Goods (Ministry of Industry)

Customs Applications (Ministry of Customs and Trade)

Health Registry Applications (Ministry of Health)

Capital Markets and Central Registry Applications (CMB, CRA, BIST)

Ministry of Transport, Ministry of Environment, Ministry of Labor and other government entities' e-signature applications.

## ▶ Private Sector Applications

Banking and Finance Sector

ERPs, DMSs, Corporate Portals etc.

# SSL Services and CA/Browser Forum Contribution from Turkey

- ▶ Currently 3 (three) Turkish CAs are the members of the CA/Browser Forum.
  - 2 (two) Private Sector CAs
  - 1 (one) Government CA
  
- ▶ TÜRKTRUST is contributing to the CA/Browser Forum activities since the beginning of its membership in 2011.
  - Actively attending the Forum Face-to-Face meetings internationally.
  - Hosted Fall 2013 Face-to-Face meeting in Ankara, Turkey.
  - Joining Forum discussions via Forum e-mail lists.
  - ETSI TS 102 042 certified and compliant to the Forum «guidelines» and «baseline requirements».
  - Nominated for the Vice-Chair position of the Forum in the recent election.

# SSL Services and CA/Browser Forum Contribution from Turkey

- ▶ Currently the CA/Browser Forum seems too much Northern America oriented.
- ▶ International contribution for the CA/Browser Forum activities by CAs from all over the world is necessary.
- ▶ More European emphasis is required in the Forum work and decisions.
- ▶ ETSI influence should be increased versus WebTrust dominance.
- ▶ CA and Browser issues should be discussed in more equal terms.

Limited Forum influence on browsers' root recognition schemes so far.

Browsers seem to be driving the changes and forcing the improvements regarding certification services.

More CA contribution and further consensus building are expected in the Forum platform.

# Evolving Trust Services Based on PKI

- ▶ Registered Electronic Mail (REM) in Turkey

  - REM related changes in the Turkish Law of Commerce (January 13, 2011)

  - Ordinance on REM Procedures and Principles (August 25, 2011)

  - Communiqué on REM Processes and Technical Criteria (August 25, 2011)

  - Communique on REM Accounts and REM Address Guide (May 16, 2012)

  - ICTA Board Decision on Interoperability of REM Service Providers (September 9, 2014)

- ▶ 1 (one) Government REMSP (PTT), 2 (two) Private Sector REMSPs

- ▶ 2013 REM Statistics:

REM Accounts	Active (end of 2013)
Personal	5545
Organizational	6873
<b>TOTAL</b>	<b>12418</b>

# Evolving Trust Services Based on PKI

## ▶ E-Invoice and E-Ledger Regulations in Turkey

Currently about 20.000 companies are under the scope of E-Invoice and E-Ledger regulations; the scope will be enlarged gradually.

E-Invoice is mandatory for the above scope since January 1, 2014.

E-Ledger will be mandatory for the above scope after January 1, 2015.

Currently 35 (thirty-five) authorized E-Invoice Service Providers are active.

E-Ledger services are supplied mostly by the same E-Invoice Service Providers.

## ▶ E-Archive Regulation in Turkey

Especially used by telecom operators issuing vast amounts of invoices.

Used for archiving invoices issued for individual users that are not in the scope of e-invoice regulation.

Currently 10 (ten) E-Archive Service Providers are active in Turkey.

- ▶ The above applications utilize «e-signature», «time stamp» and «fiscal seal». E-signature and time stamp services are supplied by the Government CA and private sector CAs. For the time being, the fiscal seal is only supplied by the Government CA.



# Turkish National e-ID scheme

## Technical Features

- ▶ Smart-card based e-ID card with national operating system (AKIS) – EAL4+ Certification
- ▶ Secure card readers (KEC) – National Standard ICS 35.240.15
- ▶ Identity Authentication Server (KDS)
- ▶ Authentication Policy Server (KPS)
- ▶ PKI-based authentication
- ▶ Biometric authentication (3-factor)
- ▶ National identity assertion format and cryptographic protocols

# Turkish National e-ID scheme

## New Requirements in Future Turkish National e-ID

- ▶ Identity management perspective
- ▶ European/International Interoperability
- ▶ Cloud-based identity services
- ▶ Identity-as-a-Service
- ▶ Privacy preserving authentication
- ▶ Privacy preserving credentials/assertions
- ▶ Support multiple identity federation schemes
- ▶ Adoption of new ETSI cryptographic protocol recommendations
- ▶ Support for attributes/roles and authorization
- ▶ Mobile convergence

# Turkish National e-ID scheme

## Interoperability of Turkish National e-ID with European e-ID

- ▶ STORK 2

  - Turkey is participating in STORK 2

  - SAML based interoperability scheme

  - Attribute credentials (identity and role management)

- ▶ e-SENS

  - Architecture under development

  - Aims to provide cross-domain e-ID and e-Signature interoperability

- ▶ Turkish Mobile-ID

  - Based on ETSI standards (under development)

  - Interoperability based on the AdES format

# Turkish National e-ID scheme

## eIDAS Perspective for Turkish National e-ID

- ▶ Turkey is currently not required to comply with the eIDAS regulation (since Turkey is not an EU MS).
- ▶ However Turkey is part of many European large scale pilot (LSP) projects which require e-ID and e-Signature interoperability (Such as PEPPOL, STORK 2, e-CODEX).
- ▶ In the long term the interoperability of Turkish e-ID and e-Signature schemes with European schemes is desired.
- ▶ This interoperability will be shaped by the eIDAS regulation in the long term.
- ▶ In the short term interoperability will be determined by individual domain/LSP project requirements.

# TURKTRUST



## TÜRKTRUST Headquarters:

Hollanda Cad. 696.Sok No:7

Yıldız – 06550 Çankaya / ANKARA

Phone : (+90 312) 439 10 00

Fax : (+90 312) 439 10 01

**Call Center**

**0850 222 444 6**

[www.turktrust.com.tr](http://www.turktrust.com.tr)

[bilgi@turktrust.com.tr](mailto:bilgi@turktrust.com.tr)



# **eIDAS: a new opportunity for digital trust in Europe**

**DTCE point of view**

Danilo Cattaneo DTCE Chairman

November 4th, 2014

# About DTCE

Digital Trust and Compliance Europe

- ▶ Association of ICT Trust and Compliance Vendors.
- ▶ Our Mission is to increase the adoption of trust based services thanks to improvement in both legislation and quality of offered services.
- ▶ We intend to dedicate DTCE efforts to make eIDAS a success, working on SL, participating in standard setting and circulating significant use cases from the Field.

---

## Members



# Digital Identity «Megatrends»

Improving governance and usability of digital identity based services will boost specific trends in different vertical markets

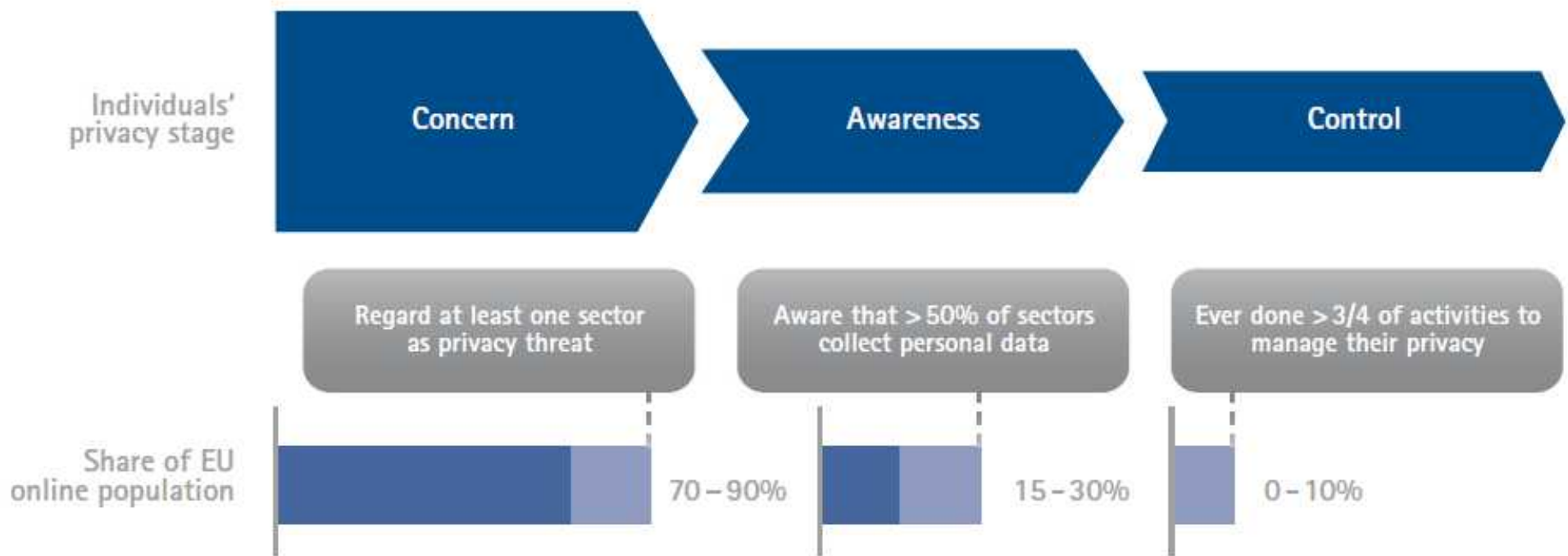


Source: BCG «The Value of our Digital Identity» Nov. 2012



# Digital Identity and user confidence

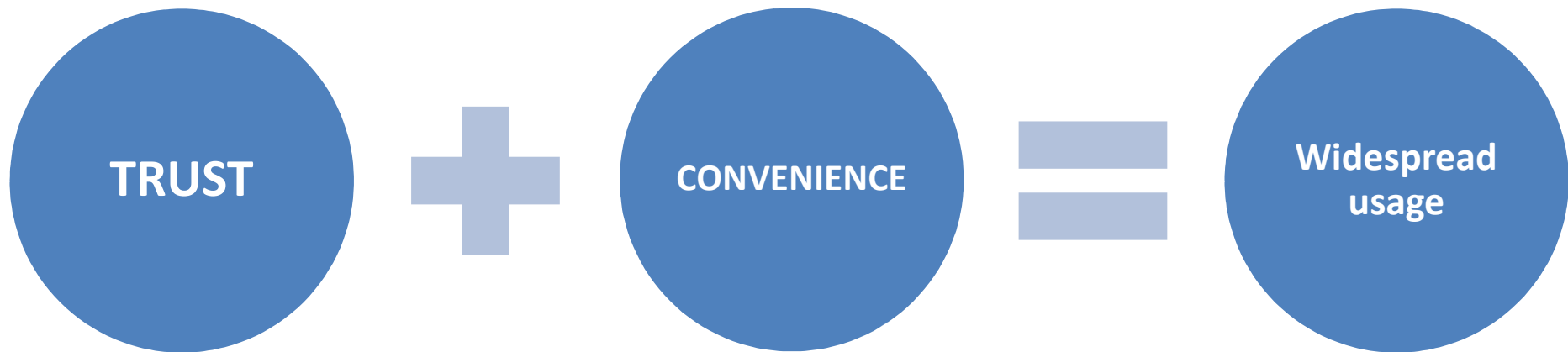
Usage of Personal Data is a concern for most individuals, due to the lack of consciousness of technical and legal aspects and only 10% is aiming to protect privacy



Source: BCG «The Value of our Digital Identity» Nov. 2012  
ENISA «Threat Landscape 2013 - Overview of current and emerging cyber-threat» Dic. 2013

# eIDAS goal

To boost TRUST and CONVENIENCE in secure and seamless cross-border electronic transactions by promoting the widespread use and uptake of electronic identification and trust services (eIDAS services).



# Why is eIDAS improving convenience?

5M certificates @ Italy



50M users @ 188 states



TRUST

VS

CONVENIENCE

# Effect of standards

Which innovation offered the single highest contribution to economic globalization of last decades?

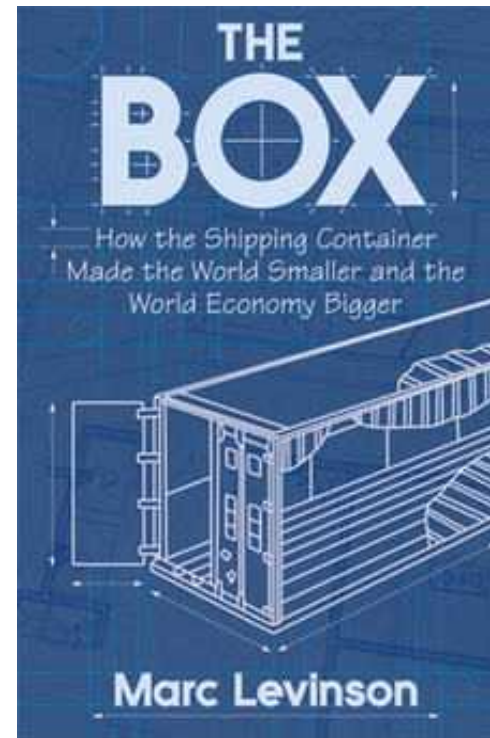
1. TV?
2. Civil Aviation?
3. Internet?



# Future Scenario

Container created a logistic worldwide cloud,  
eIDAS standards can create interoperable  
trusted digital cloud

- Creating a healthy digital ecosystem
  - Standards
  - Interoperability
- Focus on real needs of business and citizens
  - Trust services integrated into the business processes and daily life



# And the potential impact on economy is huge

- Offering improved trust infrastructure to citizens and companies leading to increased volume of electronic transactions
- Enabling new business models and new companies born digital
- Enabling public sector reduce bureaucracy and move processes on digital cloud

# Grazie!

**Danilo Cattaneo**

DTCE Chairman & InfoCert General Manager

[danilo.cattaneo@infocert.it](mailto:danilo.cattaneo@infocert.it)