

New Directions for Authentication & Identification

FIDO, PKI and beyond

11th of May 2015,
FIDO Seminar, Dublin
Dr. Kim Nguyen | Managing Director, D-TRUST GmbH

1

FIDO Next Generation Authentication

2

FIDO and beyond
Adding Identification to Authentication



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.



1
TRUSTED
Protocols

2
TRUSTED
Key Storage

3
TRUSTED
Ecosystem

4
TRUSTED
Personalization

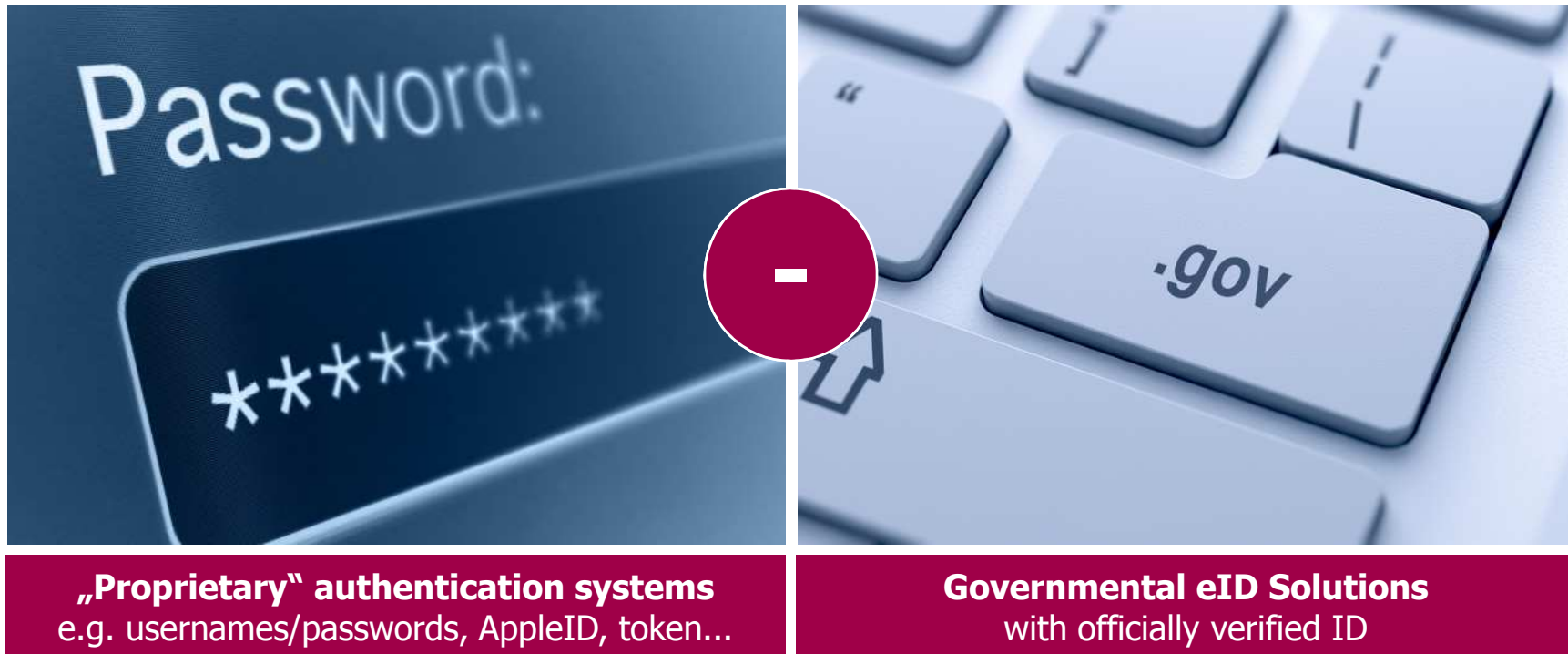
FIDO



Classical PKI based mechanisms typically **mix** elements of **authentication** and **identification**.

FIDO mechanisms allow a clear **differentiation** between **authentication** and **identification**.

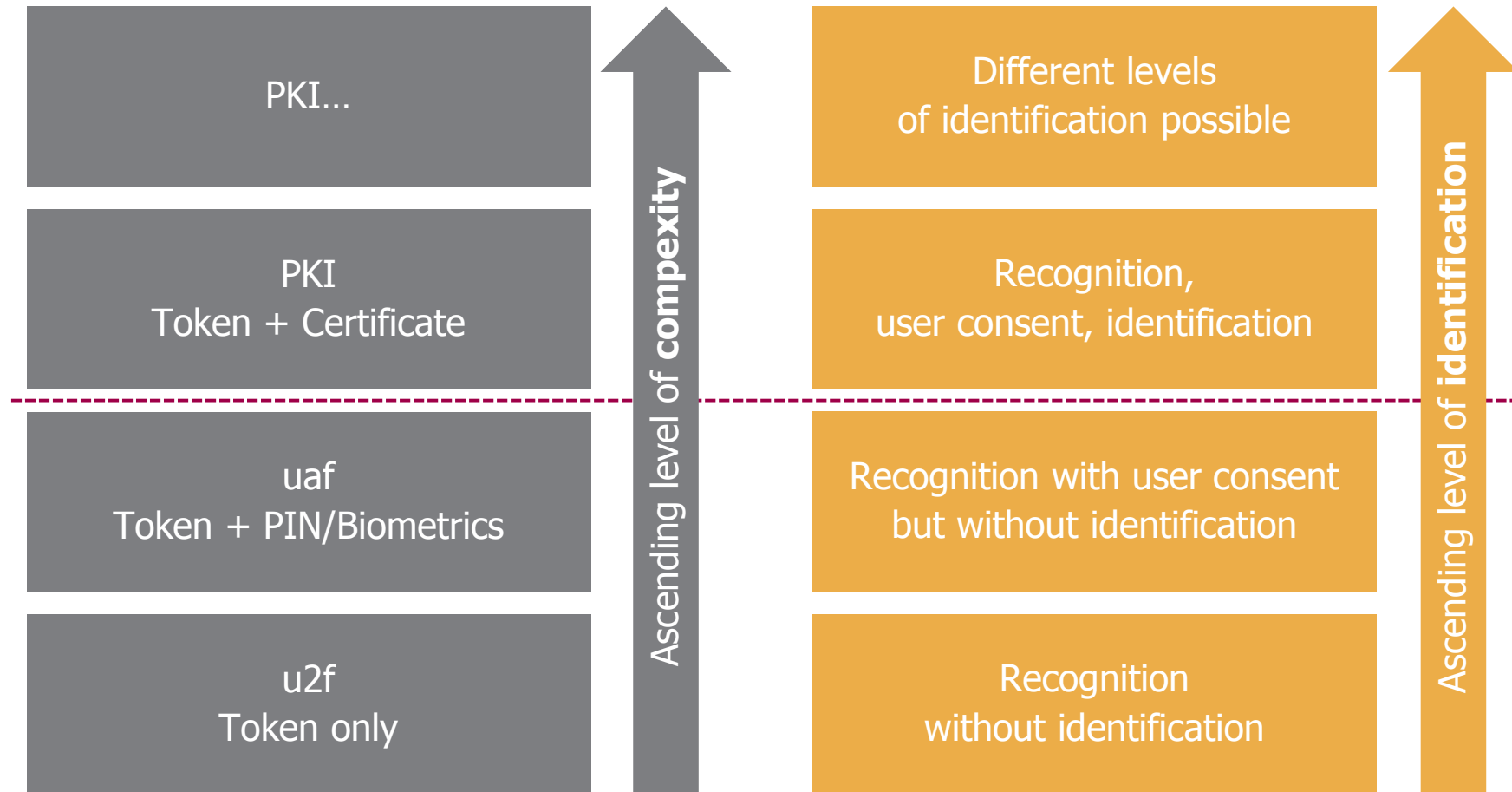
Positive aspects both for the **relying party** as well as the **user** (data protection, provide only the minimum amount of data required).



Typically, **no interaction** between these **two worlds**.



Bridging the world offers **advantages** for users and relying parties.



ONE TOKEN

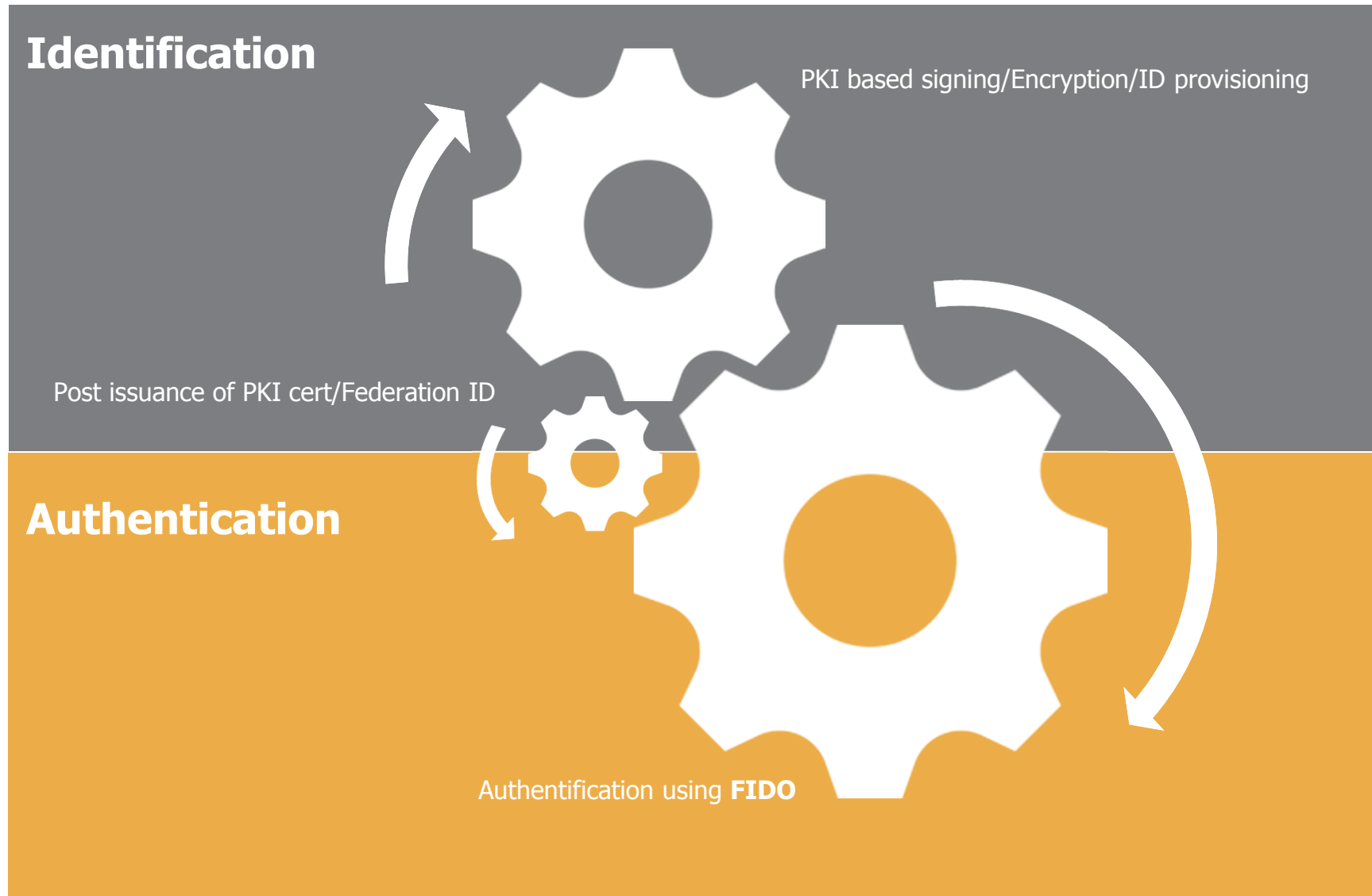


TWO WORLDS

CC Certified chip hardware and chip operating system
(**CC EAL4+**).

FIDO ready certified application,
PKI application pre-installed using CV ePasslet suite.

PKI application certified according to European standards for
Secure signature creation devices, i.e. **eIDAS** ready!



Two interesting migration scenarios



Move an **existing PKI** ecosystem to a **PKI/ID + FIDO** ecosystem. →



Move an **existing FIDO** ecosystem to a **FIDO + PKI/ID** ecosystem. →

1

FIDO offers a new userfriendly approach to authentication – **FIDO** is the future.

2

Trust in **FIDO** mechanism will rely both on trust into the token as well as in the ecosystem.

3

FIDO can be combined easily with (PKI/ID based) identification mechanisms – bridging two worlds.

4

Switch from device to user centric approach is vital – the success will largely depend on this!

[Thank you very much for your attention.]

Dr. Kim Nguyen
E-Mail: k.nguyen@d-trust.net

Note: This presentation is property of Bundesdruckerei GmbH. All content – including excerpts – may not be reproduced, divulged or published without the permission of Bundesdruckerei.
Copyright 2014 by Bundesdruckerei GmbH.