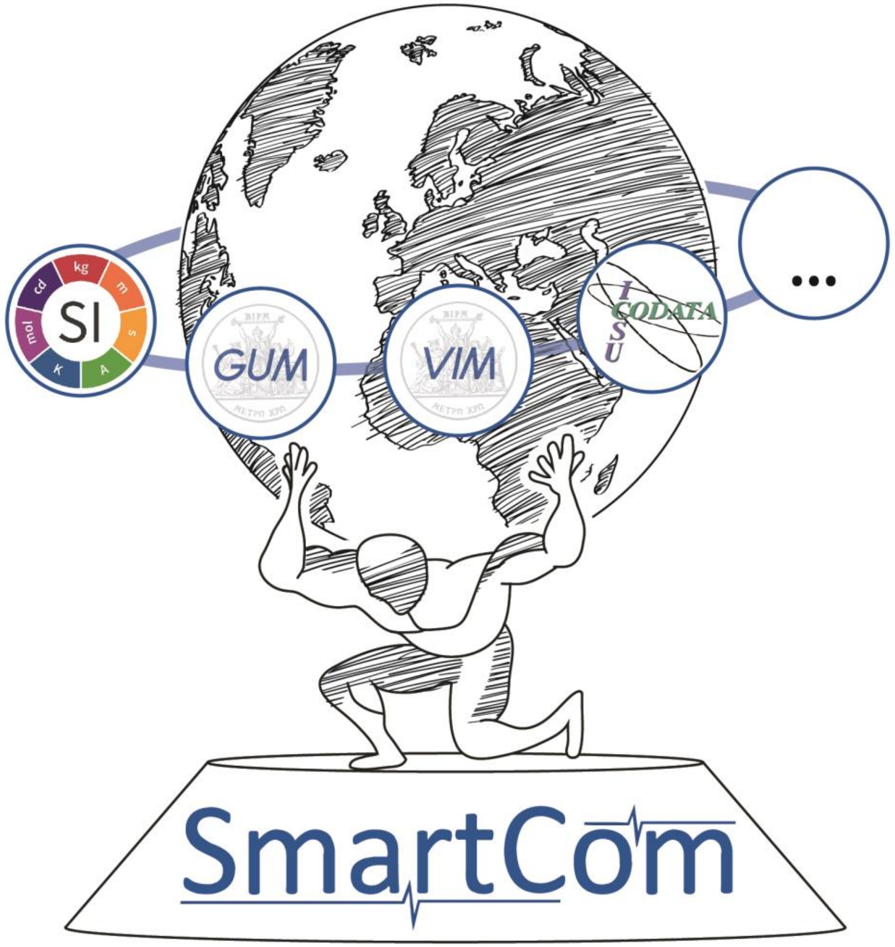


Showcase Cryptography for DCCs

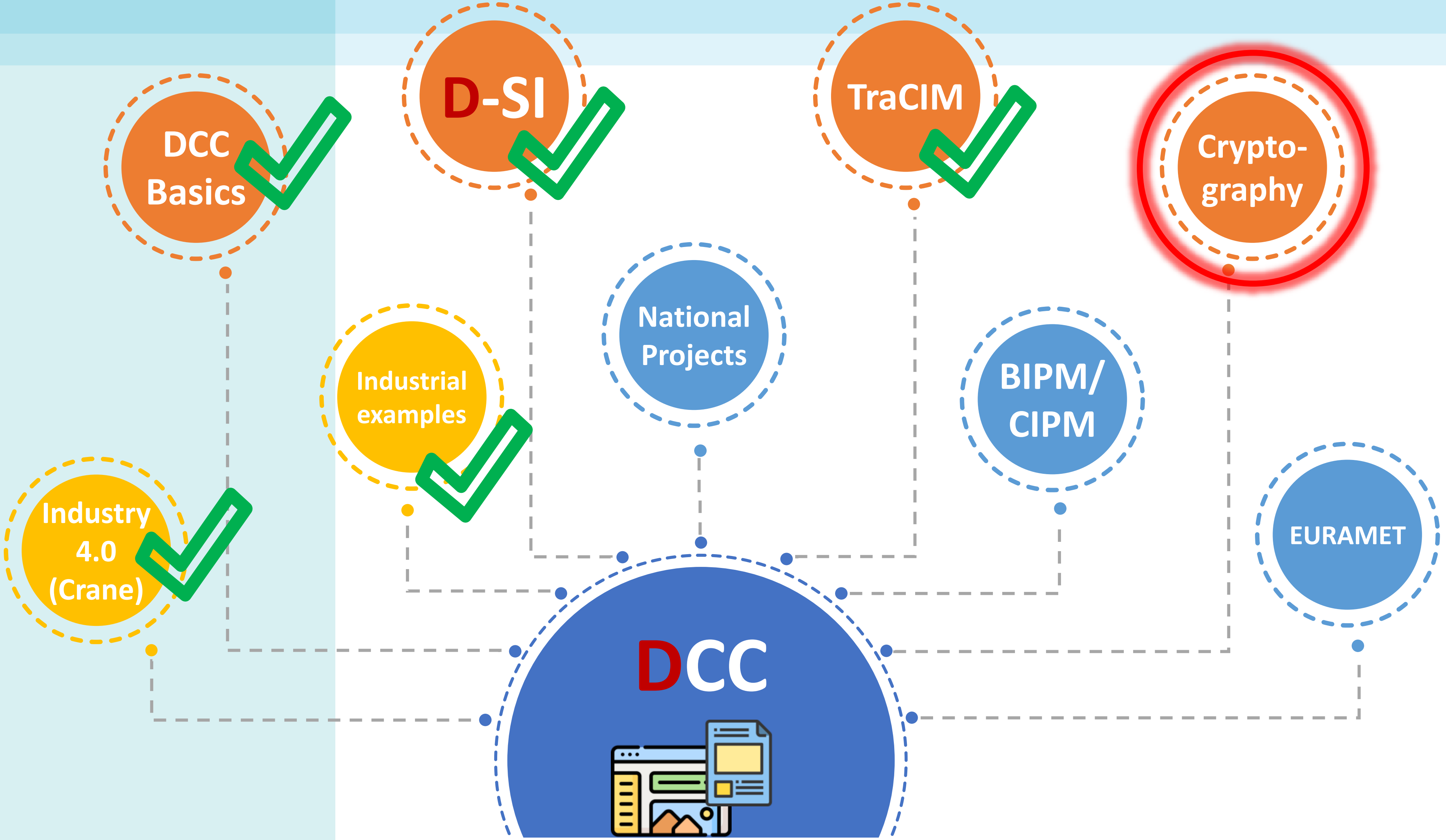
SmartCom

M4DT – Online Session III

29-Sep-21

Daniel Hutzschenreuter

DCC – Showcases



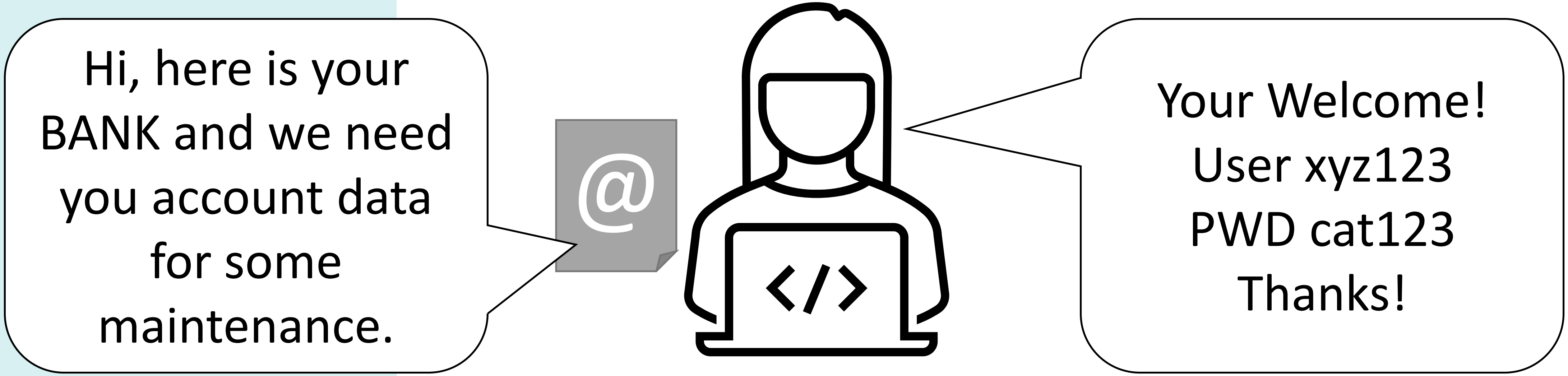
Why cryptography?

Postal service trusted infrastructure for paper certificate today

Why cryptography?

Postal service trusted infrastructure for paper certificate today

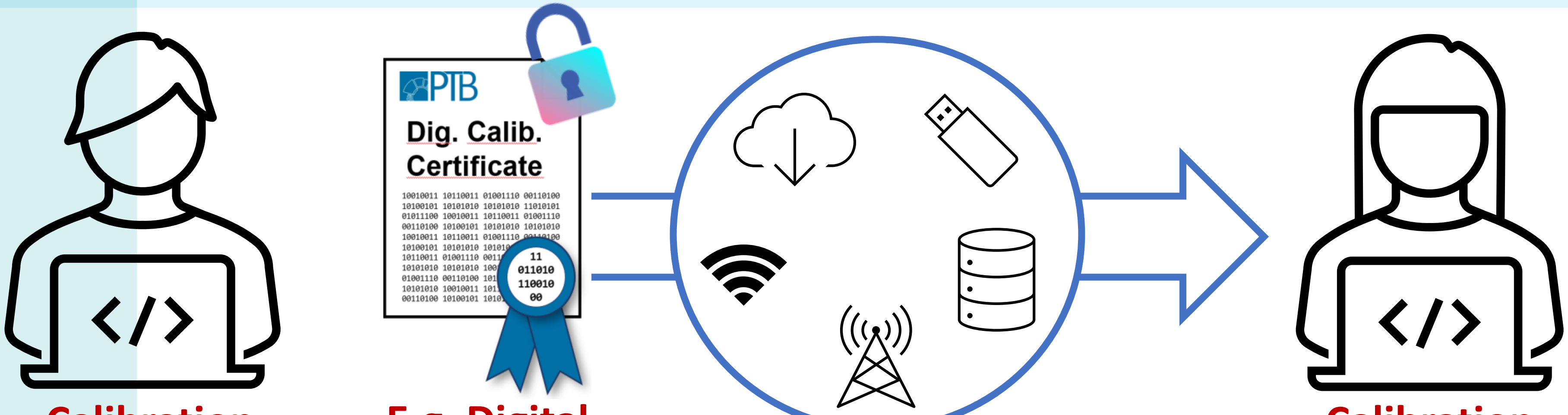
Need of trusted infrastructure for certificates in a digital world



Hi, here is your BANK and we need you account data for some maintenance.

Your Welcome!
User xyz123
PWD cat123
Thanks!

Cryptography means for Trust



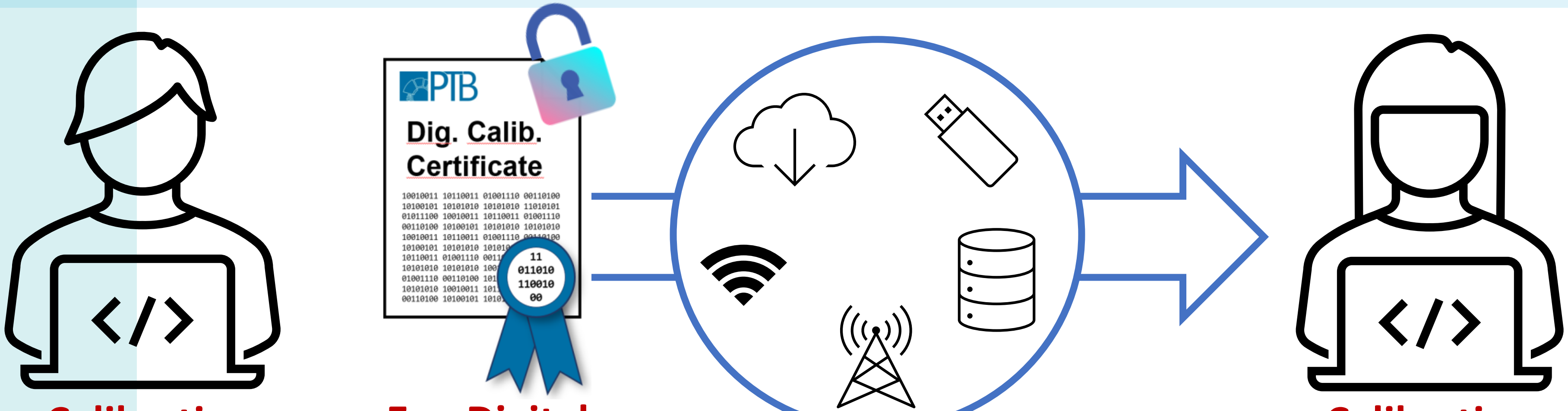
Calibration Laboratory

E.g. Digital Signature

DCC Exchange

Calibration Customer

Cryptography means for Trust



Calibration Laboratory

E.g. Digital Signature

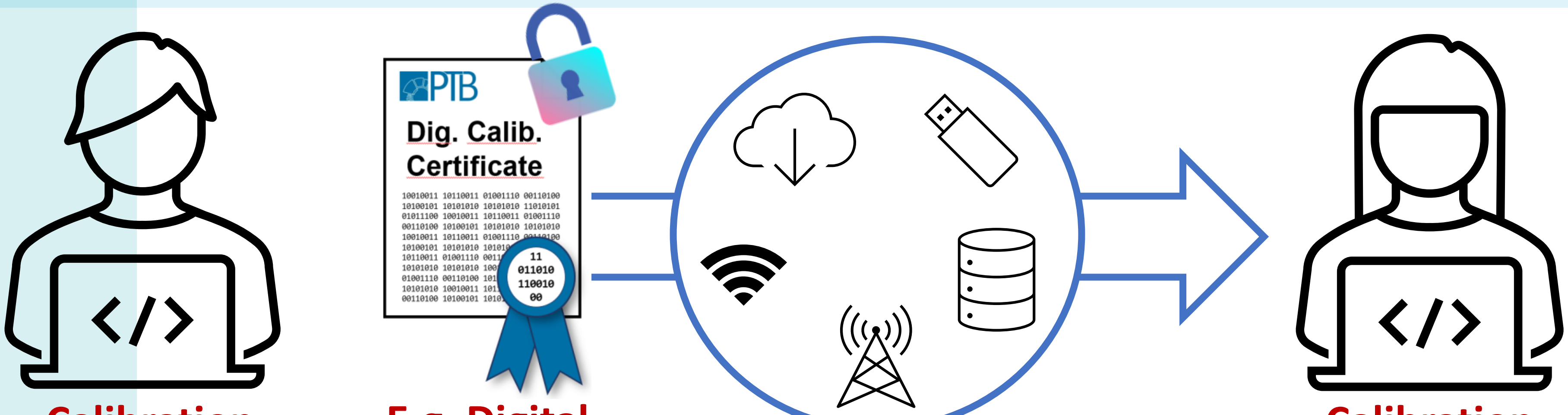
DCC Exchange

Calibration Customer

Providing DCC Integrity
(no modifications)

Providing DCC Authenticity
(from our "lab")

Cryptography means for Trust



Calibration Laboratory

E.g. Digital Signature

DCC Exchange

Calibration Customer

Providing DCC Integrity
(no modifications)

Providing DCC Authenticity
(from our "lab")

Correct DCC from the Calibration Laboratory

Confidential transmission
(encryption)

Data security is essential for a successful transition to digitalised data exchange

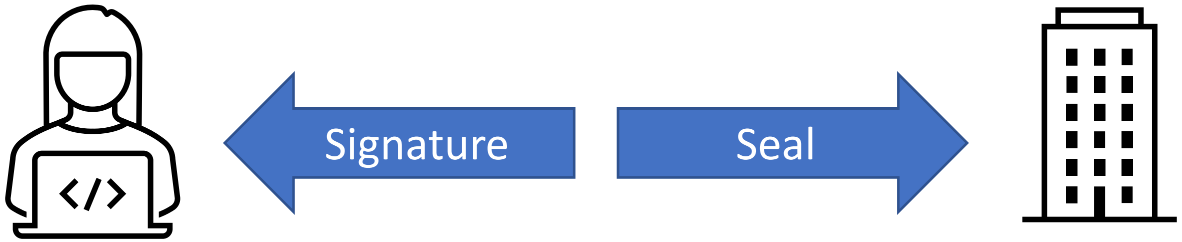
The DCC needs to have…

- **A signature or seal of the issuer to validate the authenticity and integrity of the document**
- **A possibility to protect confidential information**
- **A possibility for a withdrawal**
- **A capability for long time storage**
- **A capability to prove existence**
- **…**

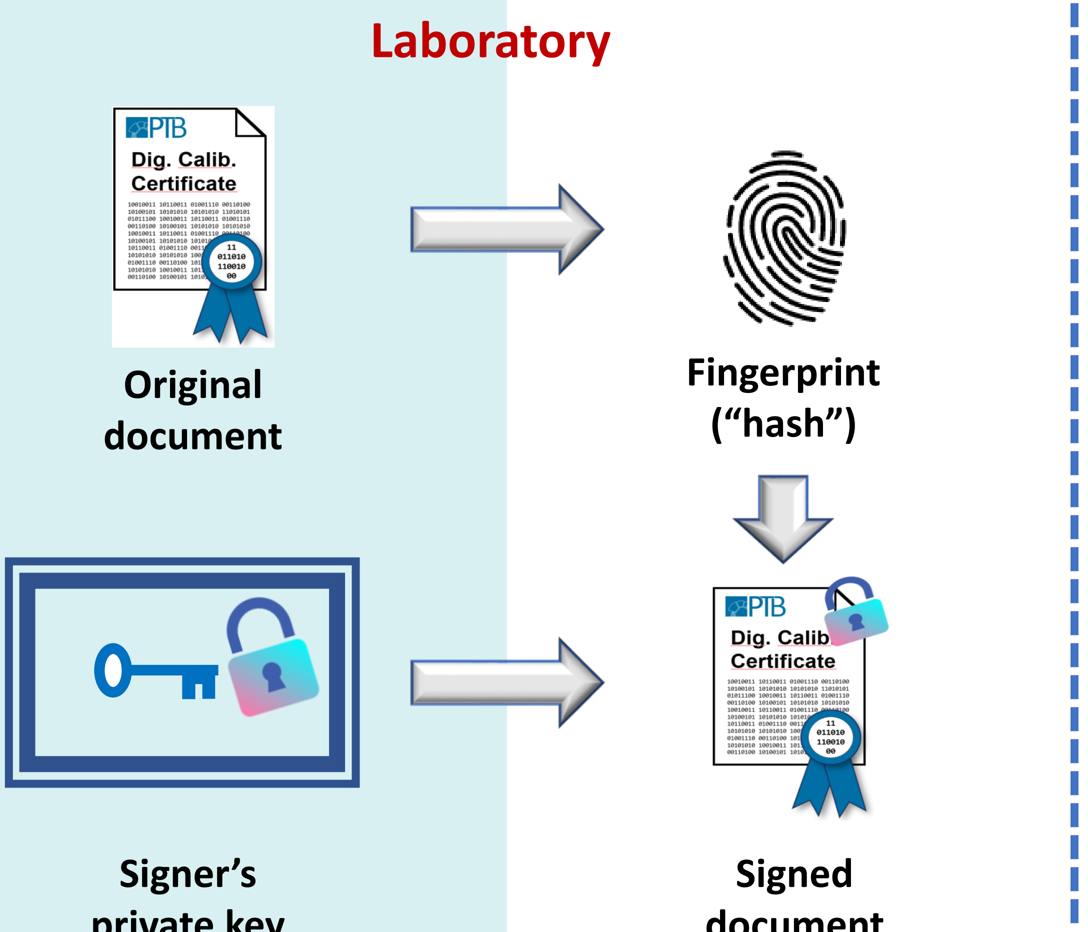
AUTHENTICITY

CONFIDENTIALITY

INTEGRITY



How do digital signatures work?



Calibration Laboratory

Original document

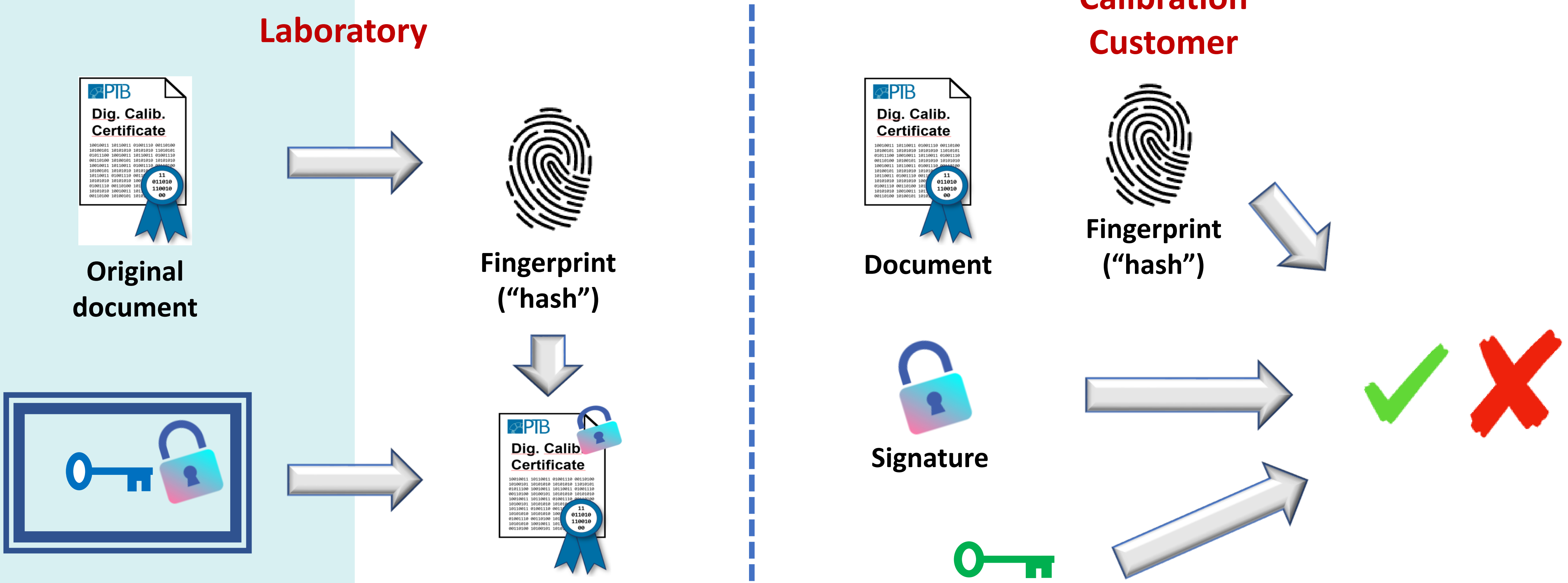
Fingerprint (“hash”)

Signer’s private key

Signed document

Calibration Customer

How do digital signatures work?



Calibration Laboratory

Original document

Fingerprint ("hash")

Signer's private key

Signed document

Calibration Customer

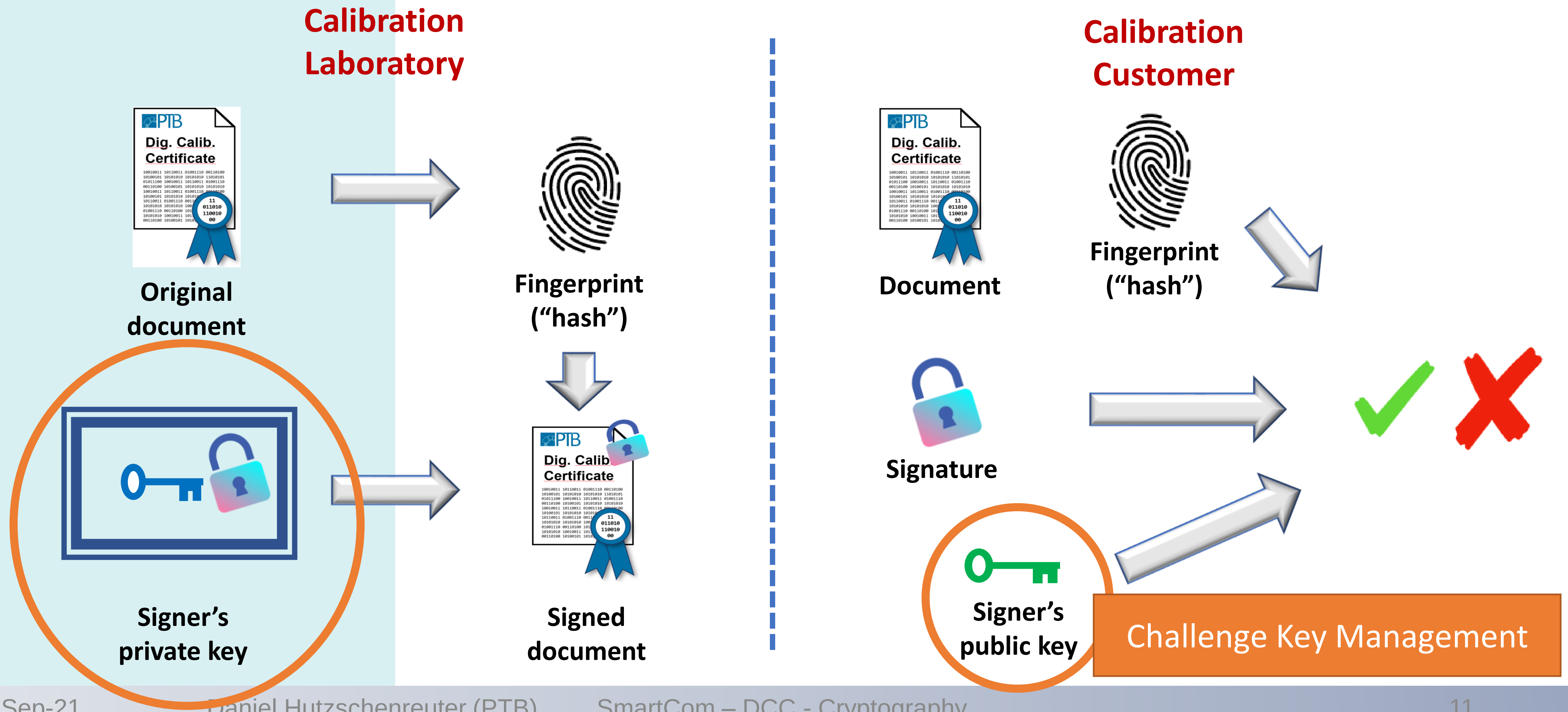
Document

Fingerprint ("hash")

Signature

Signer's public key

How do digital signatures work?



Calibration Laboratory

Original document

Fingerprint (“hash”)

Signer’s private key

Signed document

Calibration Customer

Document

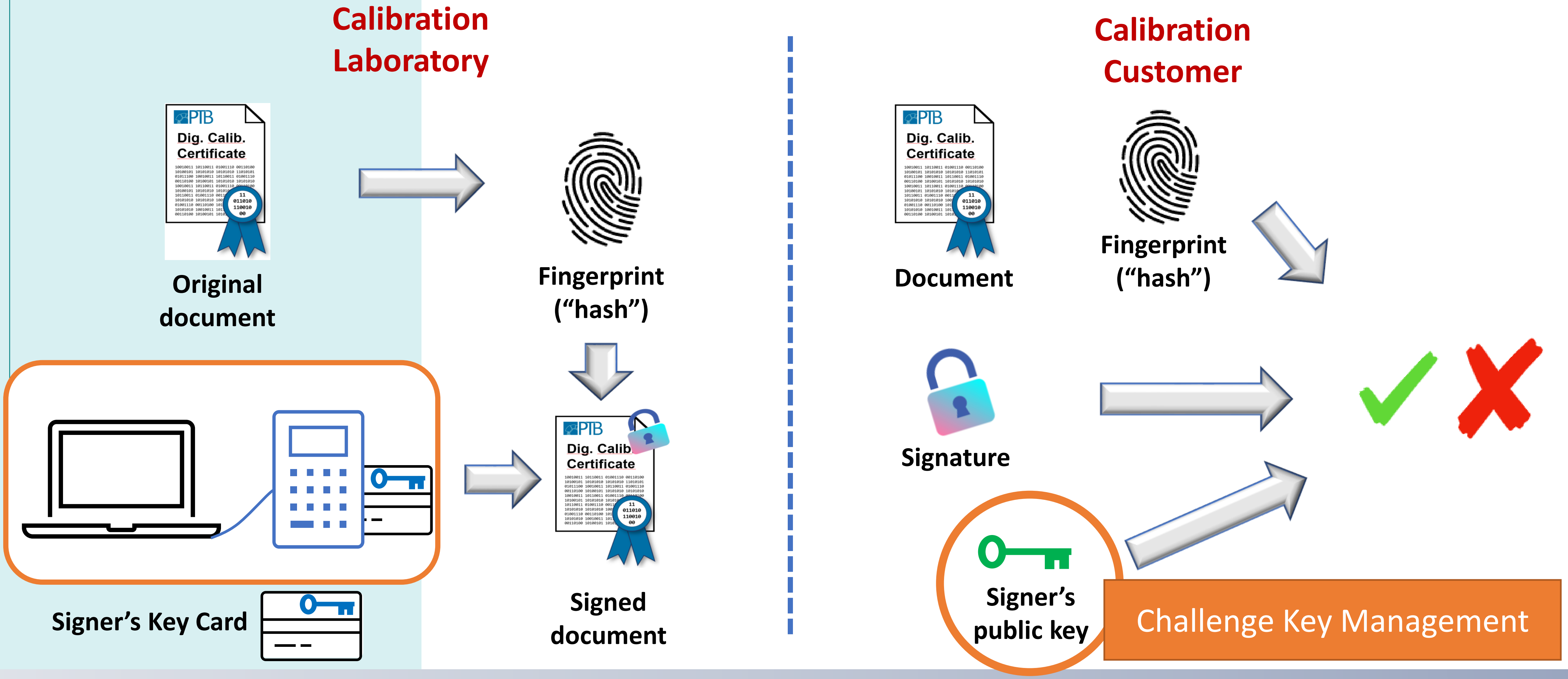
Fingerprint (“hash”)

Signature

Signer’s public key

Challenge Key Management

How do digital signatures work?



Challenge Key Management

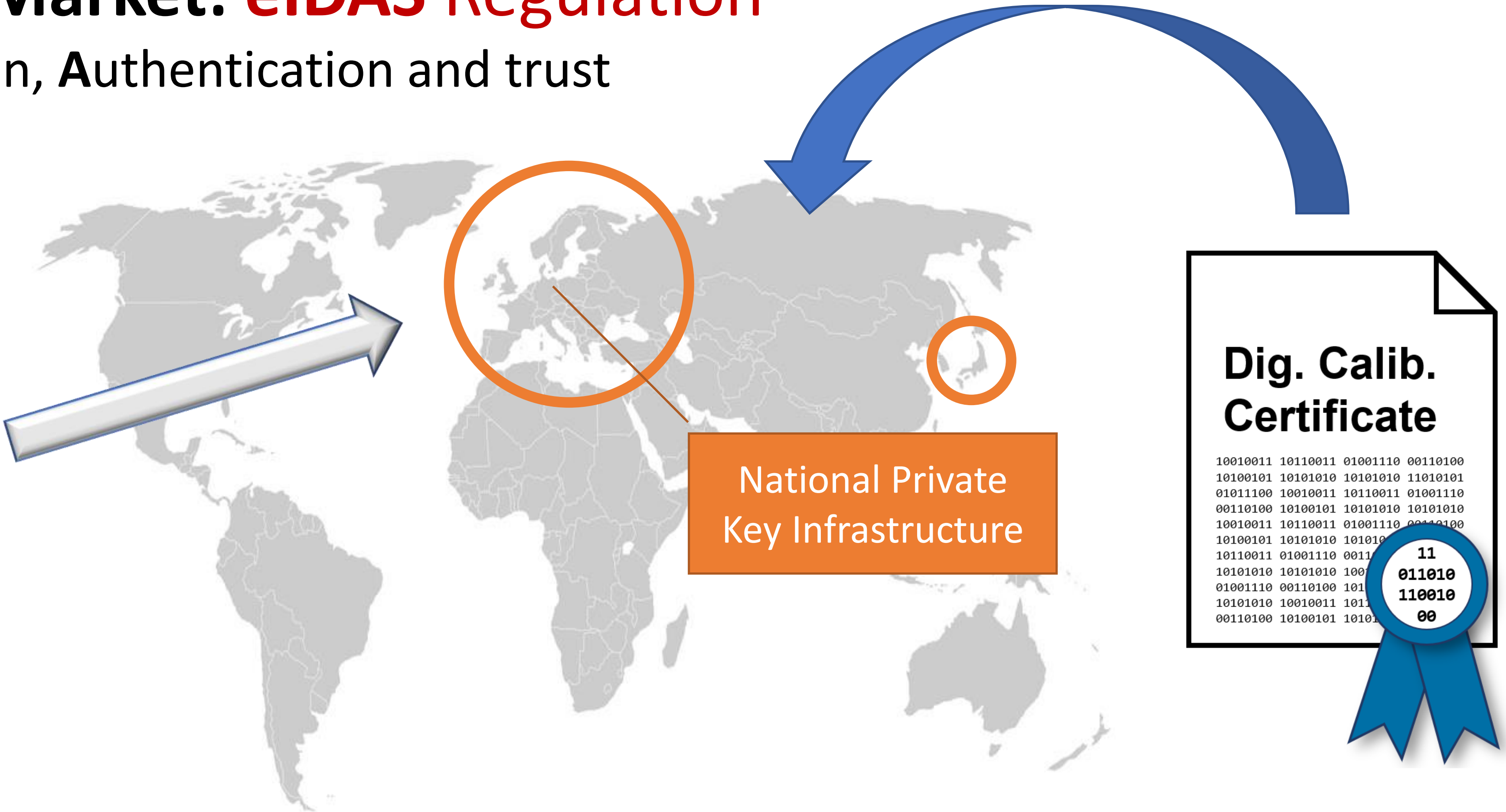
Trusted exchange: regional and global?

European Single Market: eIDAS Regulation

(**e**lectronic **ID**entification, **A**uthentication and trust **S**ervices)

EU Trust Mark (Wikipedia)

EU Trusted Lists



National Private Key Infrastructure

Dig. Calib. Certificate

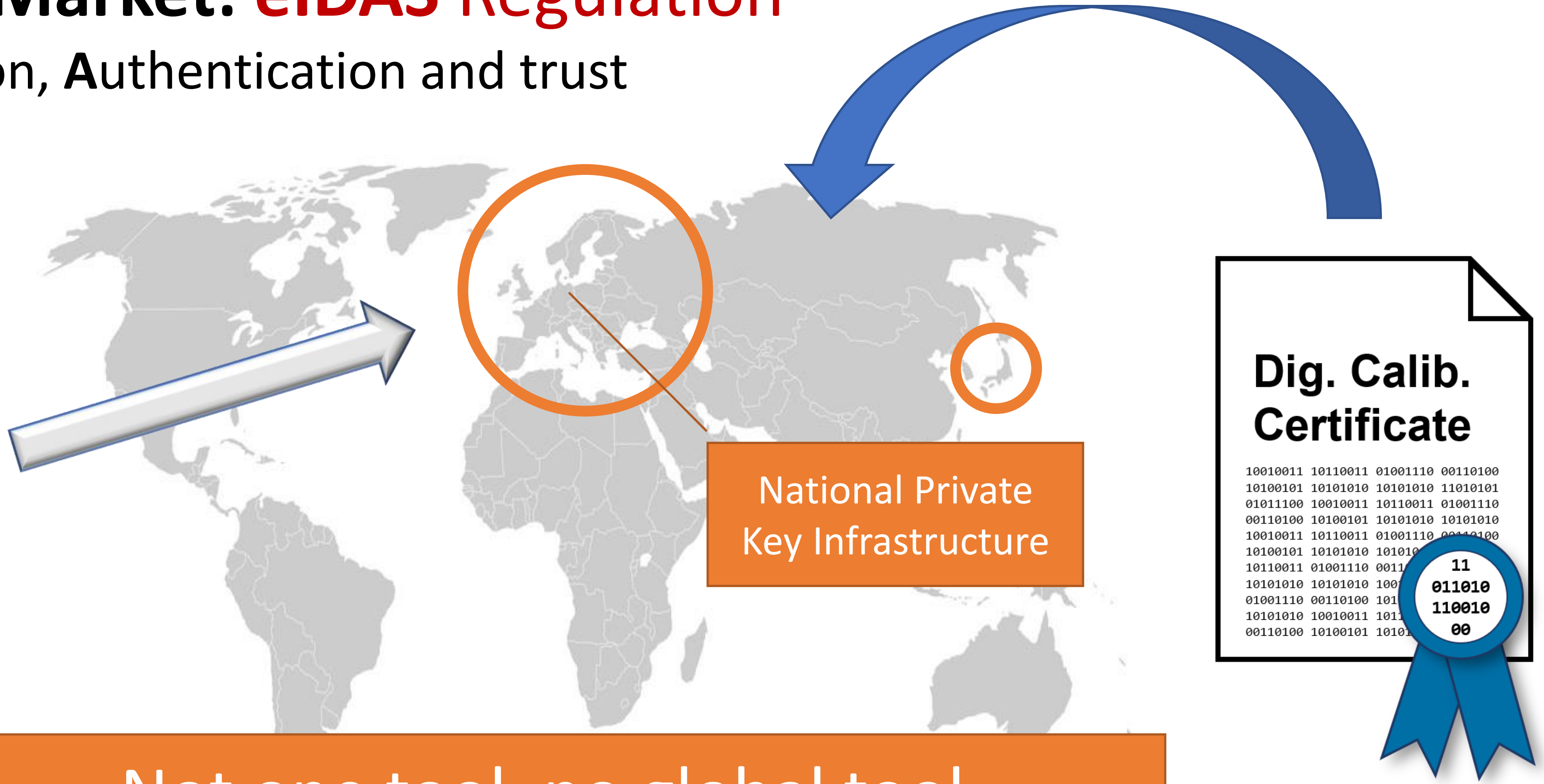
Trusted exchange: regional and global?

European Single Market: **eIDAS** Regulation

(**e**lectronic **ID**entification, **A**uthentication and trust **S**ervices)

EU Trust Mark (Wikipedia)

EU Trusted Lists

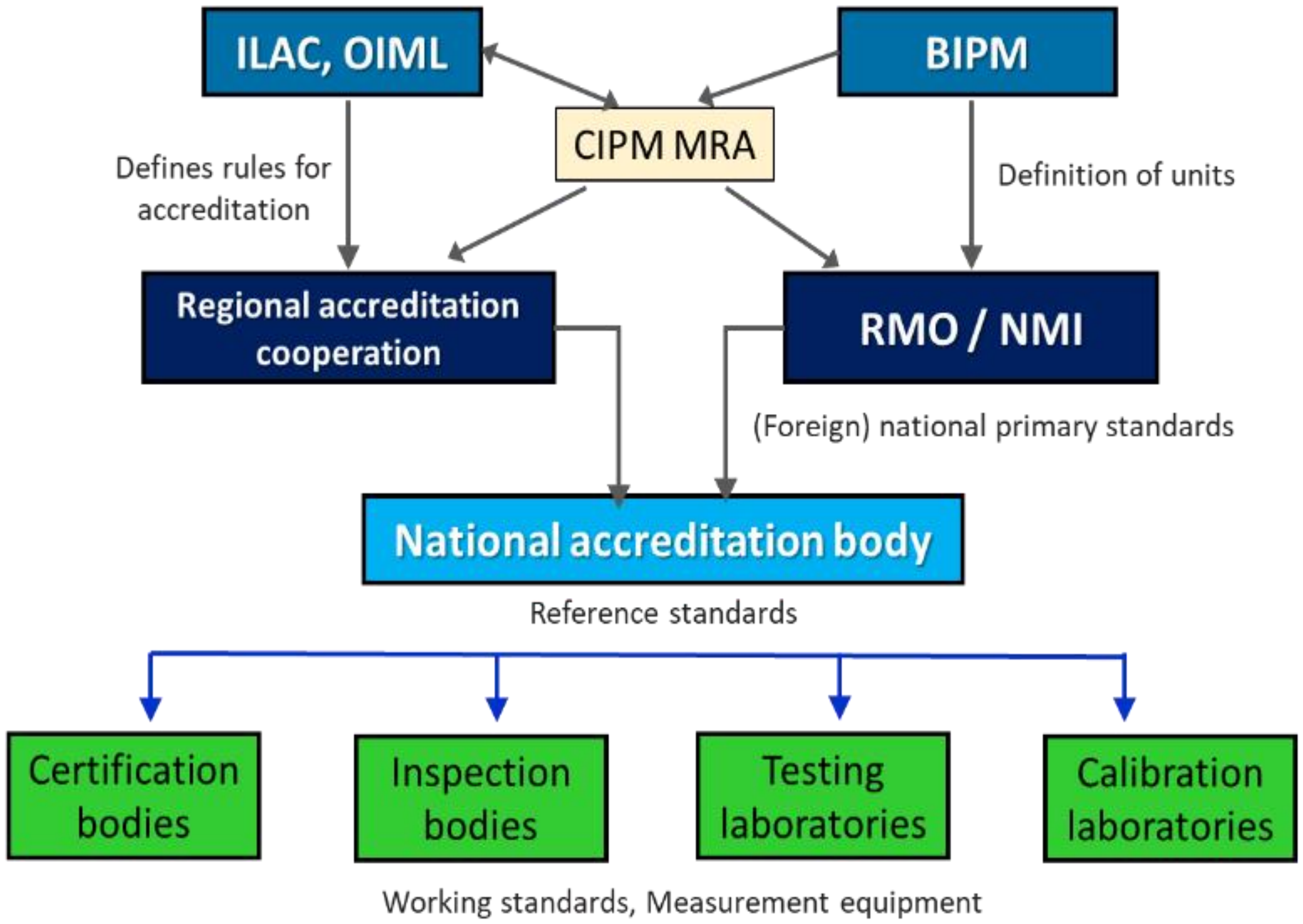


Not one tool, no global tool

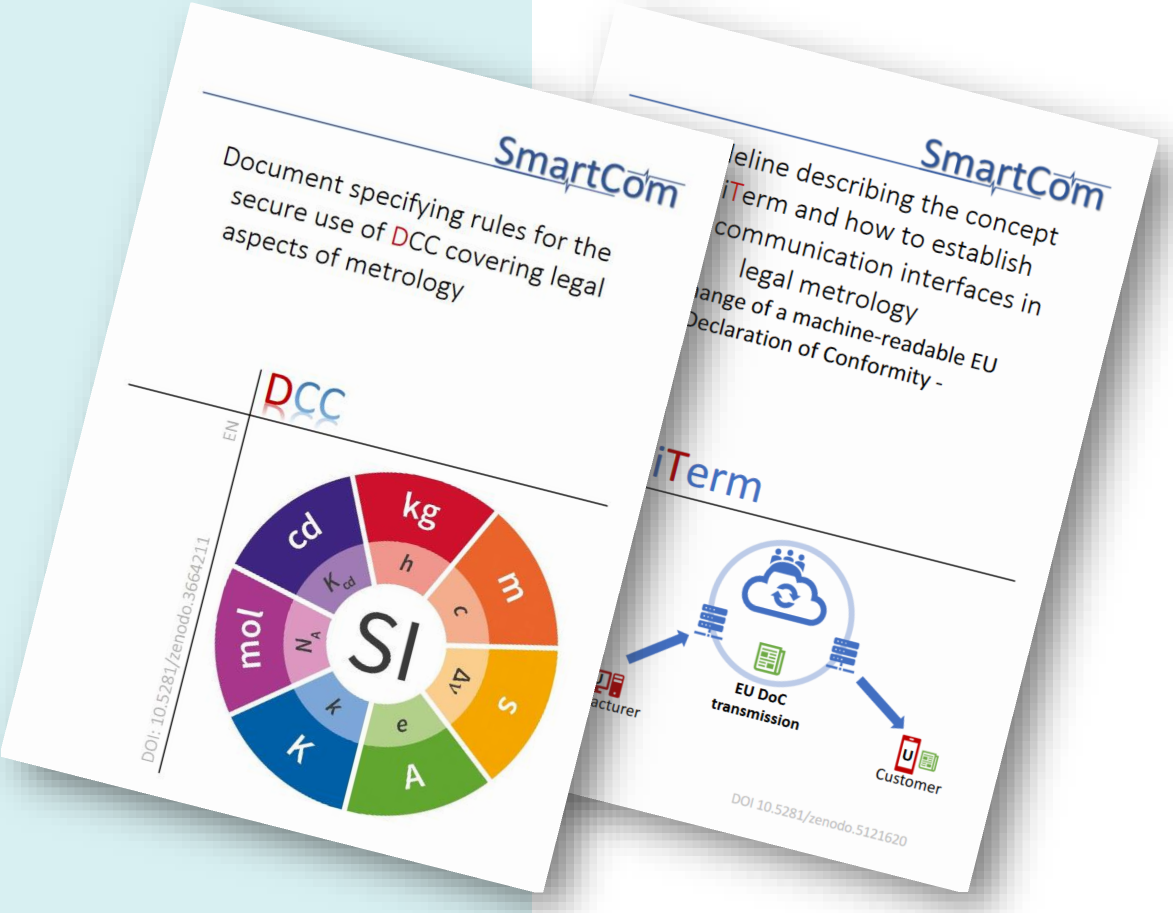
SmartCom vision global DCC security

Mutual recognition for DCC security methods established within the Quality Infrastructure

Such as Private Key Infrastructure
for all Metrology


ILAC, OIML
BIPM
CIPM MRA
Defines rules for accreditation
Definition of units
Regional accreditation cooperation
RMO / NMI
(Foreign) national primary standards
National accreditation body
Reference standards
Certification bodies
Inspection bodies
Testing laboratories
Calibration laboratories
Working standards, Measurement equipment

SmartCom - Documentation



SmartCom

Document specifying rules for the secure use of DCC covering legal aspects of metrology

DCC

EN

DOI: 10.5281/zenodo.3664211

SmartCom

leline describing the concept iTerm and how to establish communication interfaces in legal metrology

ange of a machine-readable EU Declaration of Conformity -

iTerm

DOI 10.5281/zenodo.5121620

Rules for the secure use of DCCs
DOI: 10.5281/zenodo.3664211

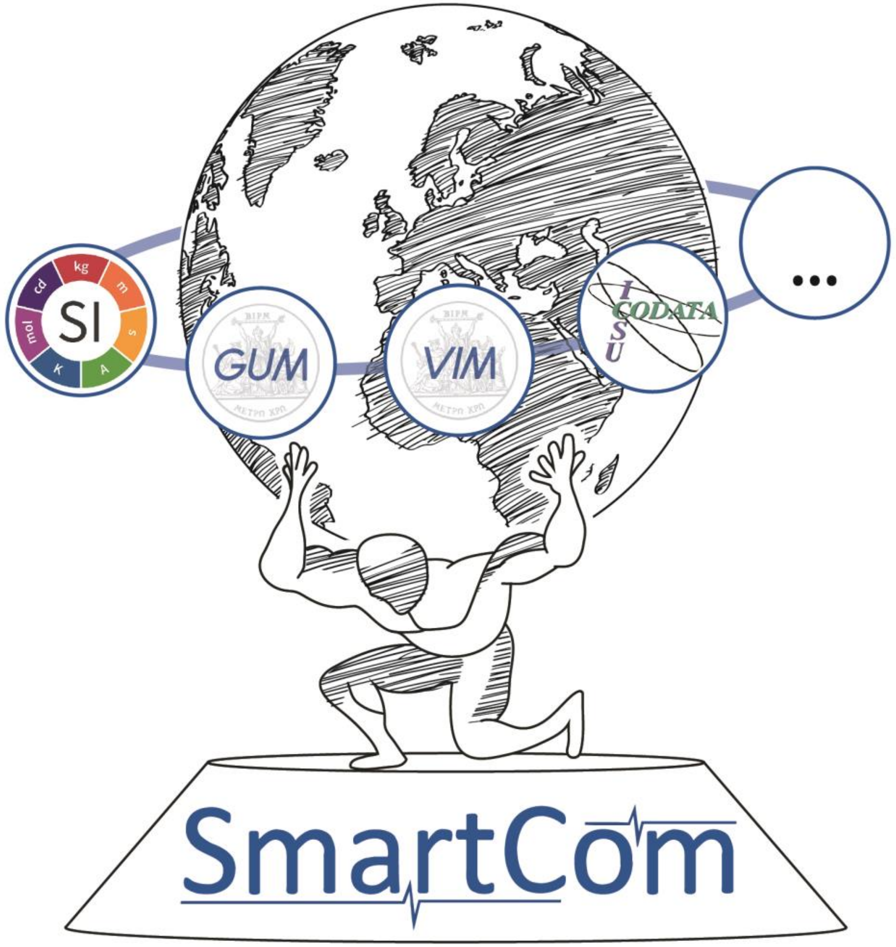
And compact overview in “UniTerm” documentation
DOI: 10.5281/zenodo.5121620

Thank you for your attention!

Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Bundesallee 100
38116 Braunschweig

Daniel Hutzschenreuter
Phone: +49 531 592-9420
E-Mail: daniel.hutzschenreuter@ptb.de
www.ptb.de

Contact: smartcom@ptb.de



Acknowledgements

The authors would like to acknowledge funding of the presented research within **the European Metrology Programme for Innovation and Research (EMPIR)** as well as **the European Association of National Metrology Institutes (Euramet)** in the Joint Research Project **17IND02 SmartCom**.

Further thanks got to Prof. Pekka Nikander and Tuukka Mustapää from Aalto University for input to the slides.

Credit: The presentation uses mind maps from Slidesgo and Freepik