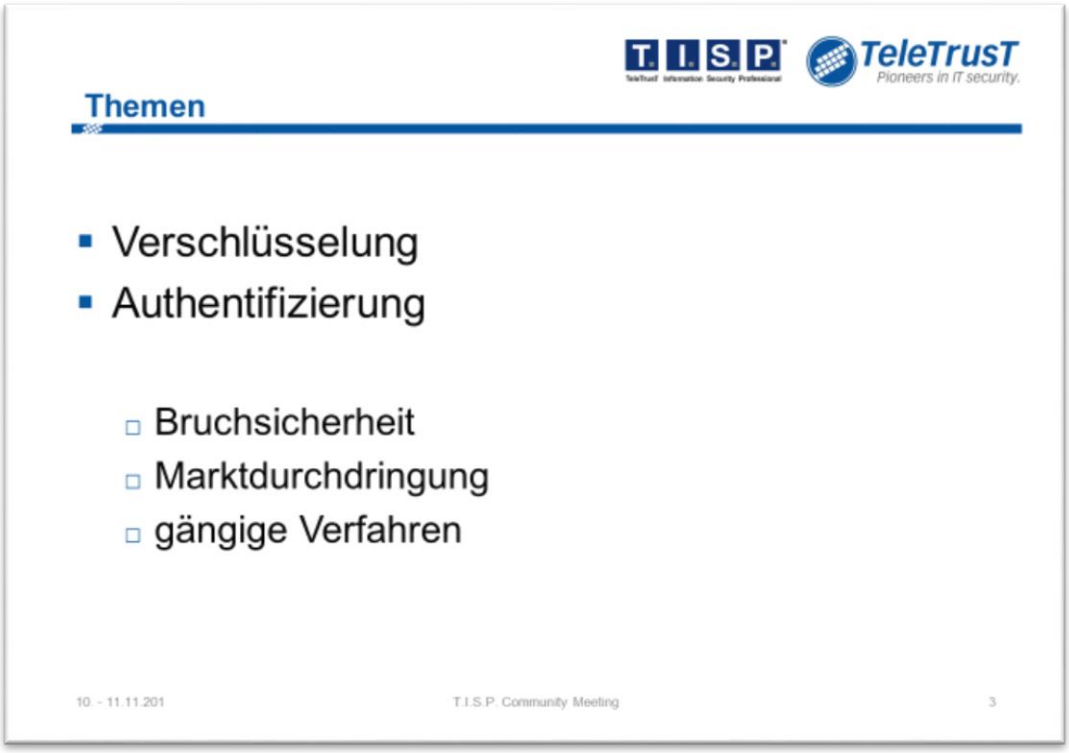
Handout mit Quellen

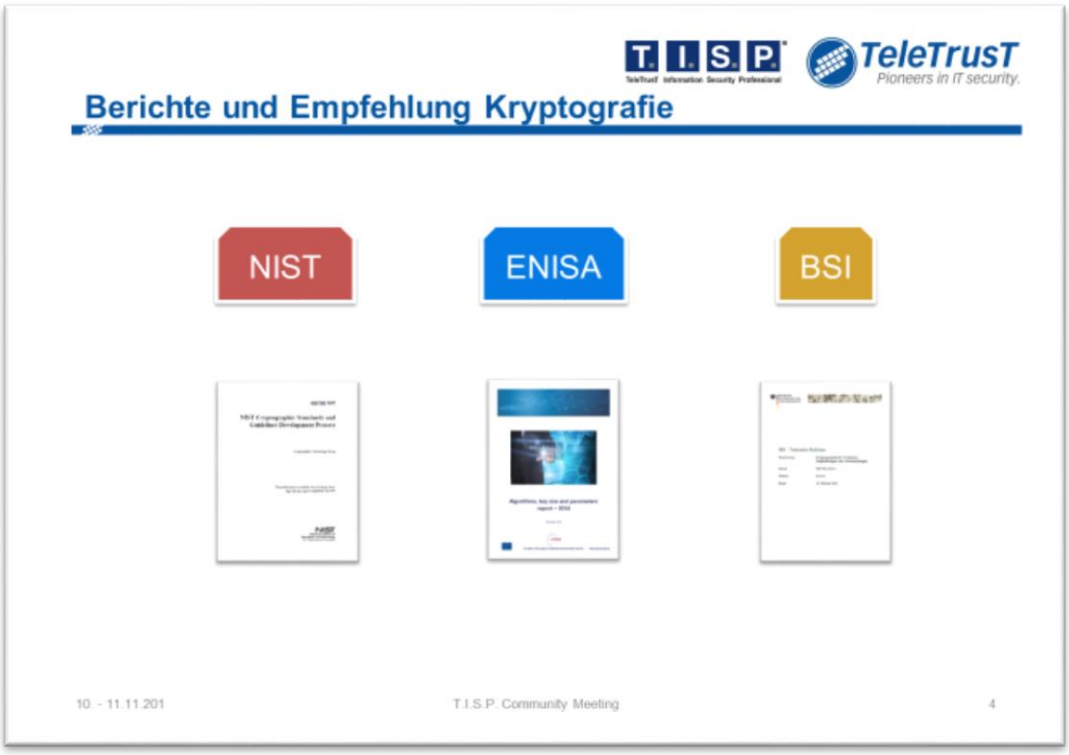
State-of-the-Art-Sicherheitsmaßnahmen bei Verschlüsselung und Authentifizierung

T. I. S. P. Community Meeting, Frankfurt 11. November 16

Herr Dennis Scherrer
BLUESITE Beratungsgesellschaft für die Informationstechnologie mbH



Fingerabdrücke in Freizeitparks (Walt Disney World)
https://epic.org/privacy/themepark



Wie die NSA Verschlüsselungen knackt
https://www.welt.de/wirtschaft/article119782731/Wie-die-NSA-Verschluesselungen-knackt.html

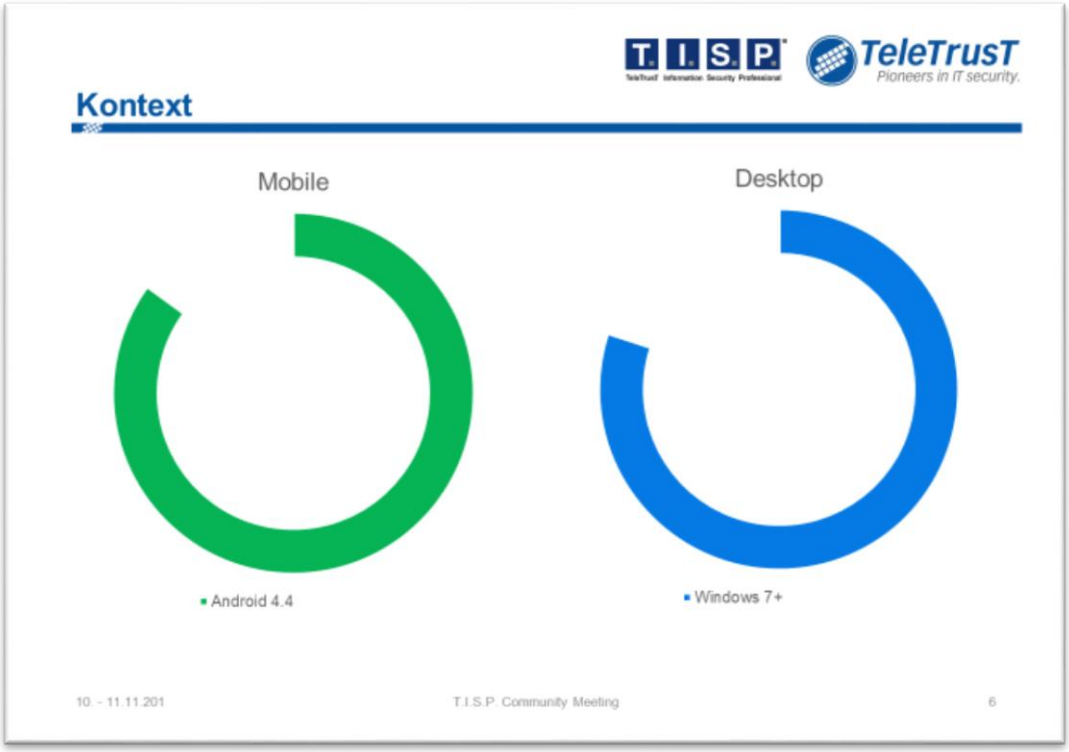
Gemalto ./. NSA zu SIM-Karten
http://arstechnica.com/security/2016/10/how-the-nsa-could-put-undetectable-trapdoors-in-millions-of-crypto-keys
http://www.gemalto.com/press/Pages/Gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-SIM-card-encryption-keys.aspx

National Institute of Standards and Technology, Cryptographic Toolkit
http://csrc.nist.gov/groups/ST/toolkit/index.html

European Union Agency for Network and Information Security (ENISA),
Algorithms, key size and parameters report
https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data/cryptographic-protocols-and-tools

Bundesamt für Sicherheit in der Informationstechnik (BSI), TR-02102-1
"Kryptographische Verfahren: Empfehlungen und Schlüssellängen"
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Signaturbestaetigung/02102_pdf.html

Damien Giry (http://www.uclouvain.be/crypto/people/show/6), https://www.keylength.com



Windows Desktop https://www.netmarketshare.com/operating-system-market-share.aspx Oktober 2016 Windows 7+ 80%+

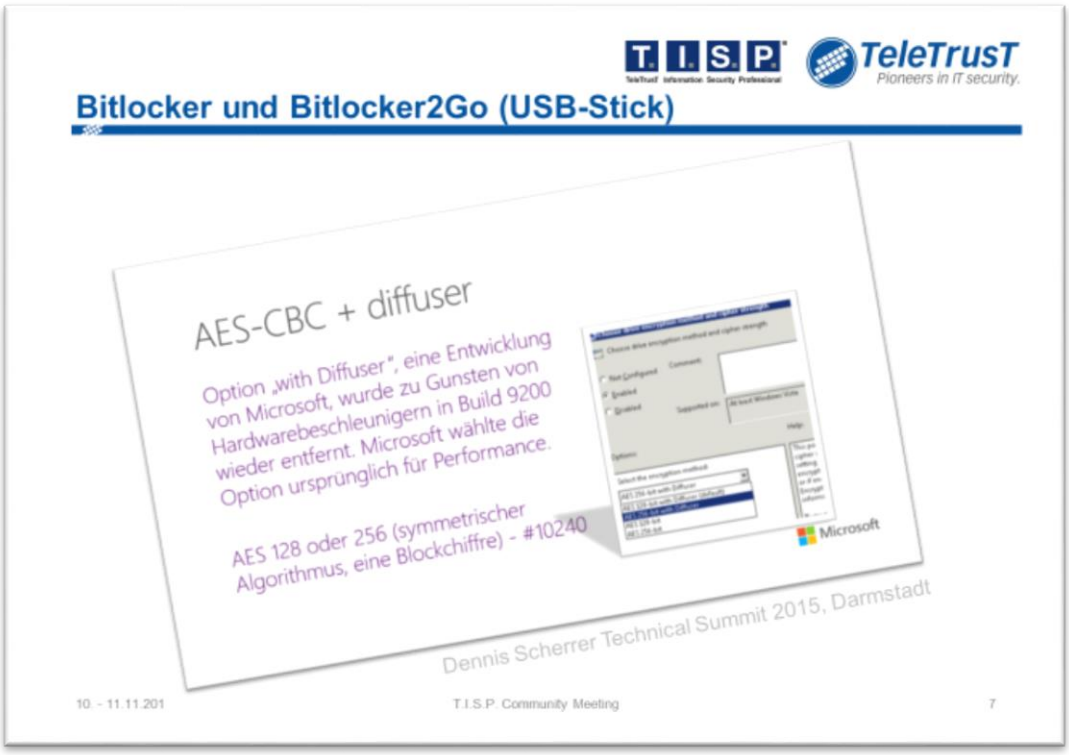
Android Mobile http://www.idc.com/prodserv/smartphone-os-market-share.jsp 85%+, https://de.wikipedia.org/wiki/Samsung_Galaxy_S5

Firefox https://www.mozilla.org/de/firefox/sync/

Chrome https://www.google.com/intl/de/chrome/browser/features.html#signin (http://gs.statcounter.com/#browser-eu-monthly-201510-201610)

KitKat (Android 4.4)
https://source.android.com/security/encryption/full-disk.html

iOS Security Guide
https://www.apple.com/business/docs/iOS_Security_Guide.pdf

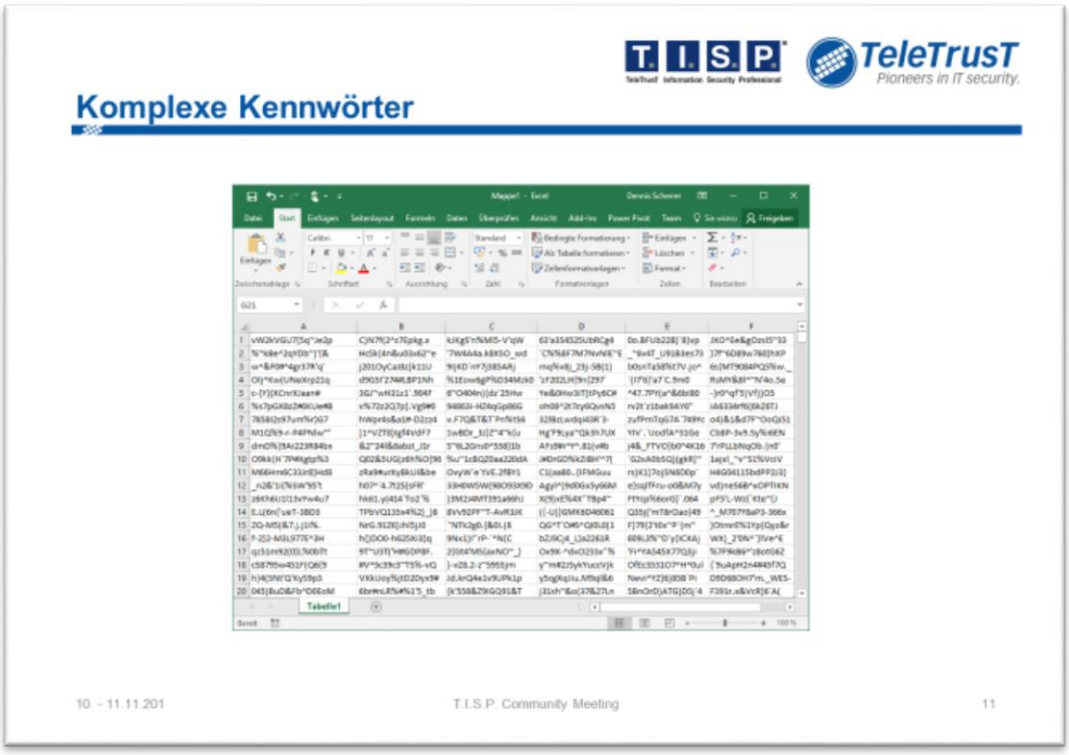


Dennis Scherrer Technical Summit 2015, Darmstadt
http://www.microsoft.com/germany/technical-summit/speaker-2015.aspx

WinZip http://www.winzip.de/wzfeatures-protect.htm

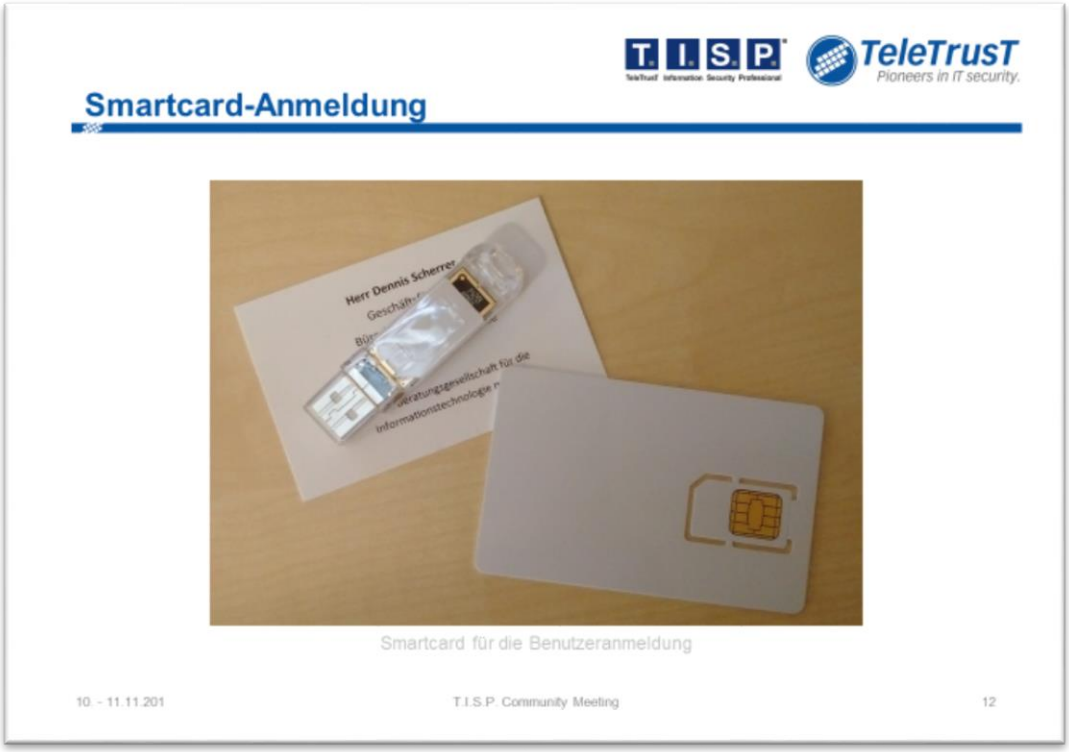
Dropbox https://www.dropbox.com/security#protection

Microsoft Office Dateischutz
https://support.office.com/de-de/article/Festlegen-eines-Kennworts-zum-Öffnen-oder-Ändern-eines-Dokuments-einer-Arbeitsmappe-oder-einer-Präsentation-EF163677-3195-40BA-885A-D50FA2BB6B68



Jörg Riether „Fast aussichtslos“ iX vom Juli 2016, Heise Verlag

Software „Password List Generator 2“ von Arunas Skirius
http://www.arunass.net



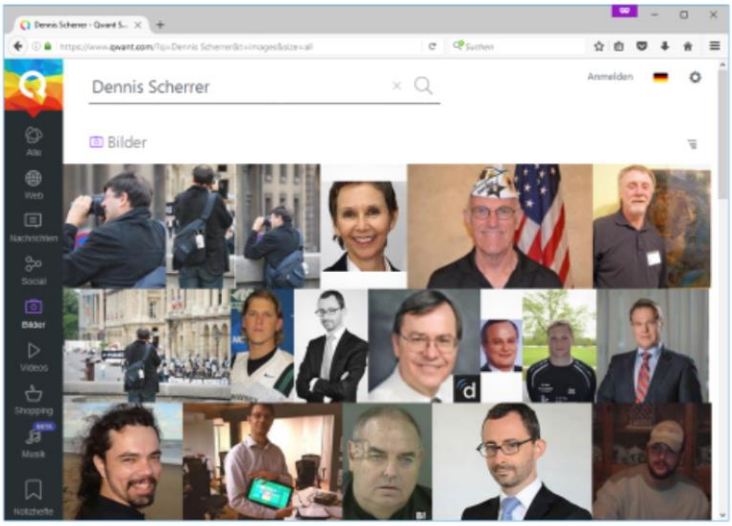
Smartcards mit verschiedenen COS
http://www.cryptoshop.com

http://winfwiki.wi-fom.de/index.php?title=Der_neue_Reisepass_im_Lichte_des_Datenschutzes

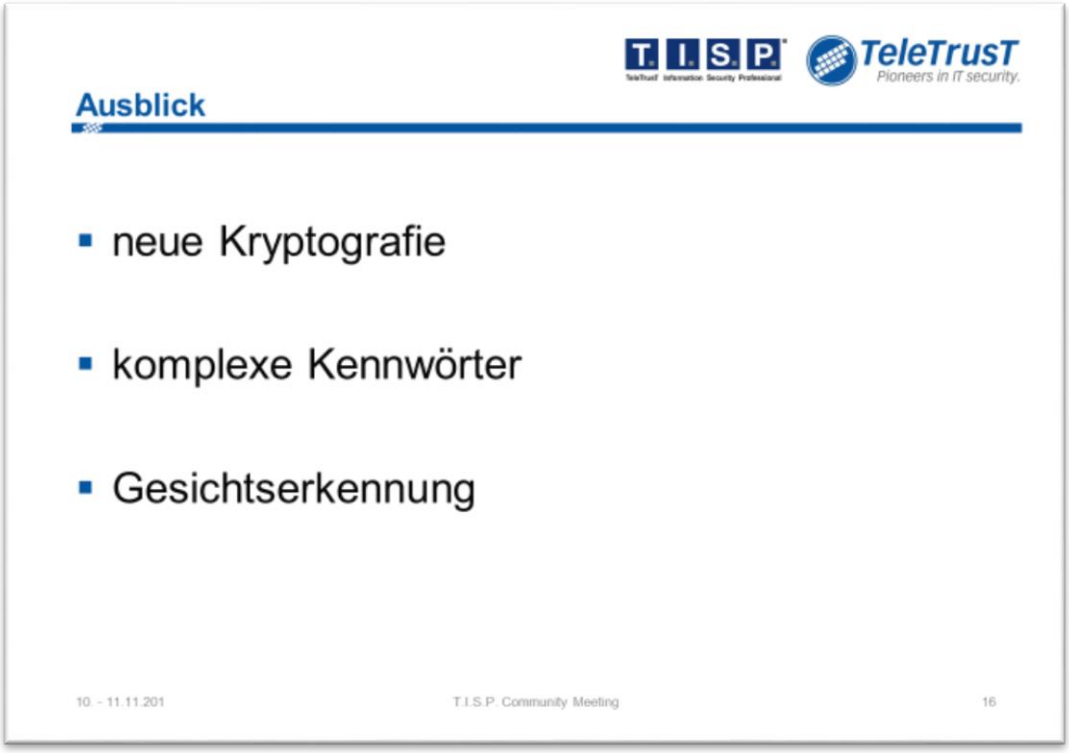
Signaturwaffe mit Fingerabdruckerkennung
https://de.wikipedia.org/wiki/Signaturwaffe

Microsoft Halo
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/manage-identity-verification-using-microsoft-passport

Gesichtserkennung

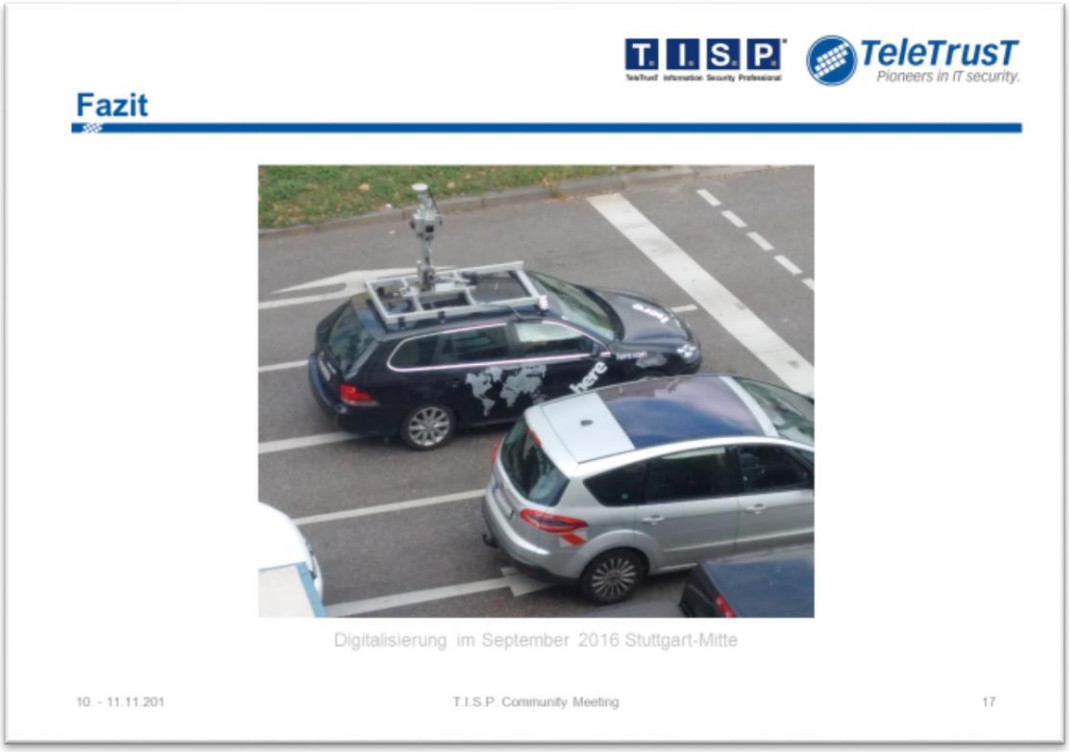


https://www.wired.com/2016/10/cops-database-117m-faces-youre-probably/



NSA Quantum Computer FAQ
https://www.iad.gov/iad/customcf/openAttachment.cfm?FilePath=/iad/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/assets/public/upload/CNSA-Suite-and-Quantum-Computing-FAQ.pdf

Kreditkarte mit eingebautem Fingerabdruckleser
http://zwipe.com/products



Information technology - Security techniques, http://www.iso.org

- Security requirements for cryptographic modules (ISO/IEC 19790:2012)
- Test requirements for cryptographic modules (ISO/IEC 24759:2014)
- Verification of cryptographic protocols (ISO/IEC 29128:2011)