Technischer Datenschutz

Technischer Datenschutz – juristische Aspekte

Katrin Kirchert

Technischer Datenschutz – technische Aspekte

Jörn Erbguth

Technischer Datenschutz in der Praxis

Alvar C. H. Freude

Moderation: Rigo Wenning

Technischer Datenschutz
Technische Aspekte

Jörn Erbguth, Berater zu Blockchain und Datenschutz, Datenschutzbeauftragter (udis zert.)

EDV Gerichtstag, Saarbrücken 20. September 2019

joern@erbguth.ch +41 787256027

Agenda

- Informationssicherheit ist Bestandteil des Datenschutzes
- Technische Zweckbindung
  - Verschlüsselung
  - Hash-Funktionen
- Technisch verhandelter Datenschutz
  - Do Not Track (DNT)

Informationssicherheit ist Bestandteil des Datenschutzes

Art. 32 DSGVO

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

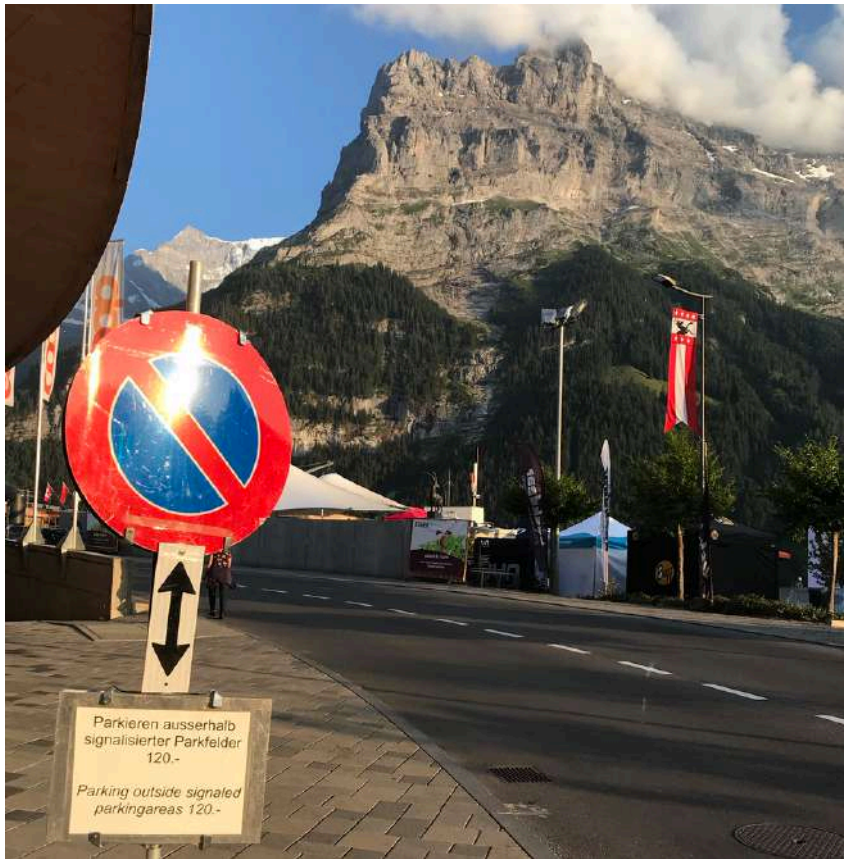
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Technische Zweckbindung

Juristische Zweckbindung:



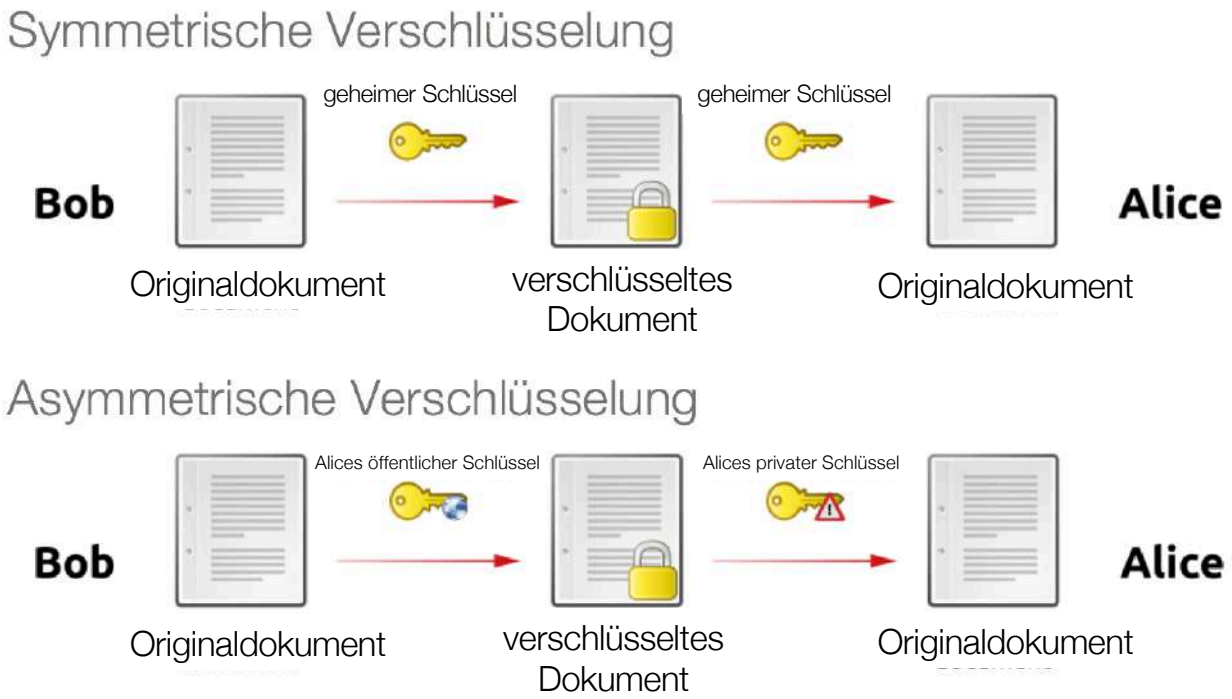
Verbot

Technische Zweckbindung:

Technische Barriere

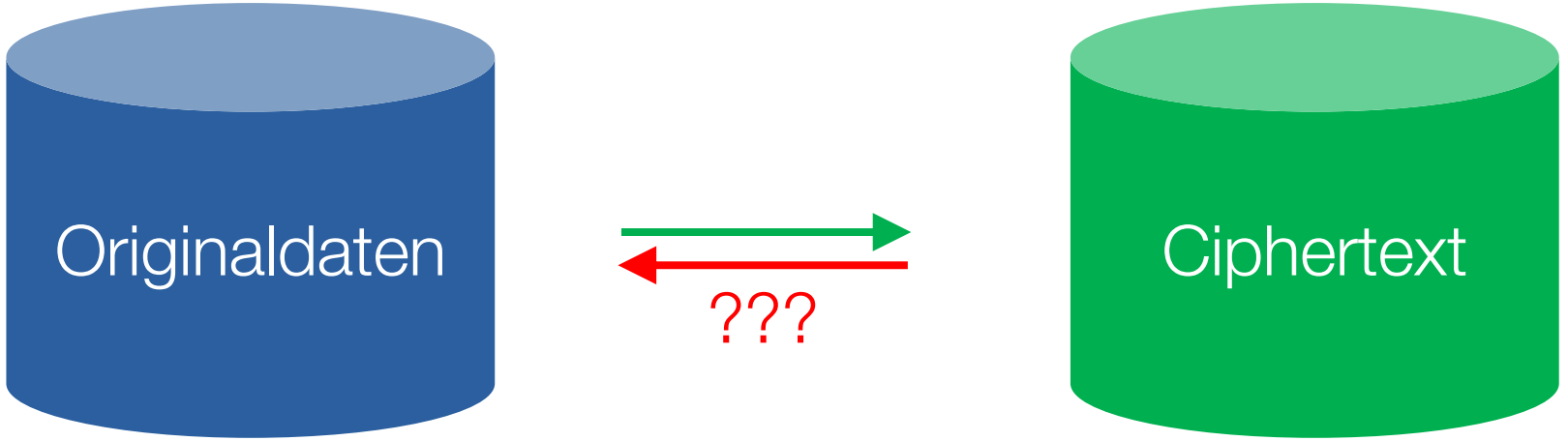
Walter j. Pilsak, Waldsassen (https://commons.wikimedia.org/wiki/File:Poller_2.jpg)

Verschlüsselung



Sind verschlüsselte Daten personenbezogene Daten?

Sind verschlüsselte Daten personenbezogene Daten?



- Entschlüsselungskey kann mit Ciphertext zusammengebracht werden
- Verschlüsselungsverfahren ist unsicher

Wann ist ein Verfahren sicher?

- Verfahren ist mathematisch bewiesen sicher
- Kein Mensch kann es knacken
- Nur ein Mensch in Deutschland könnte es knacken
- Weniger als 0,001% aller Menschen könnten es knacken

Heutige Kryptographie bald unsicher

Impact of Quantum Computing on Common Cryptographic Algorithms

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

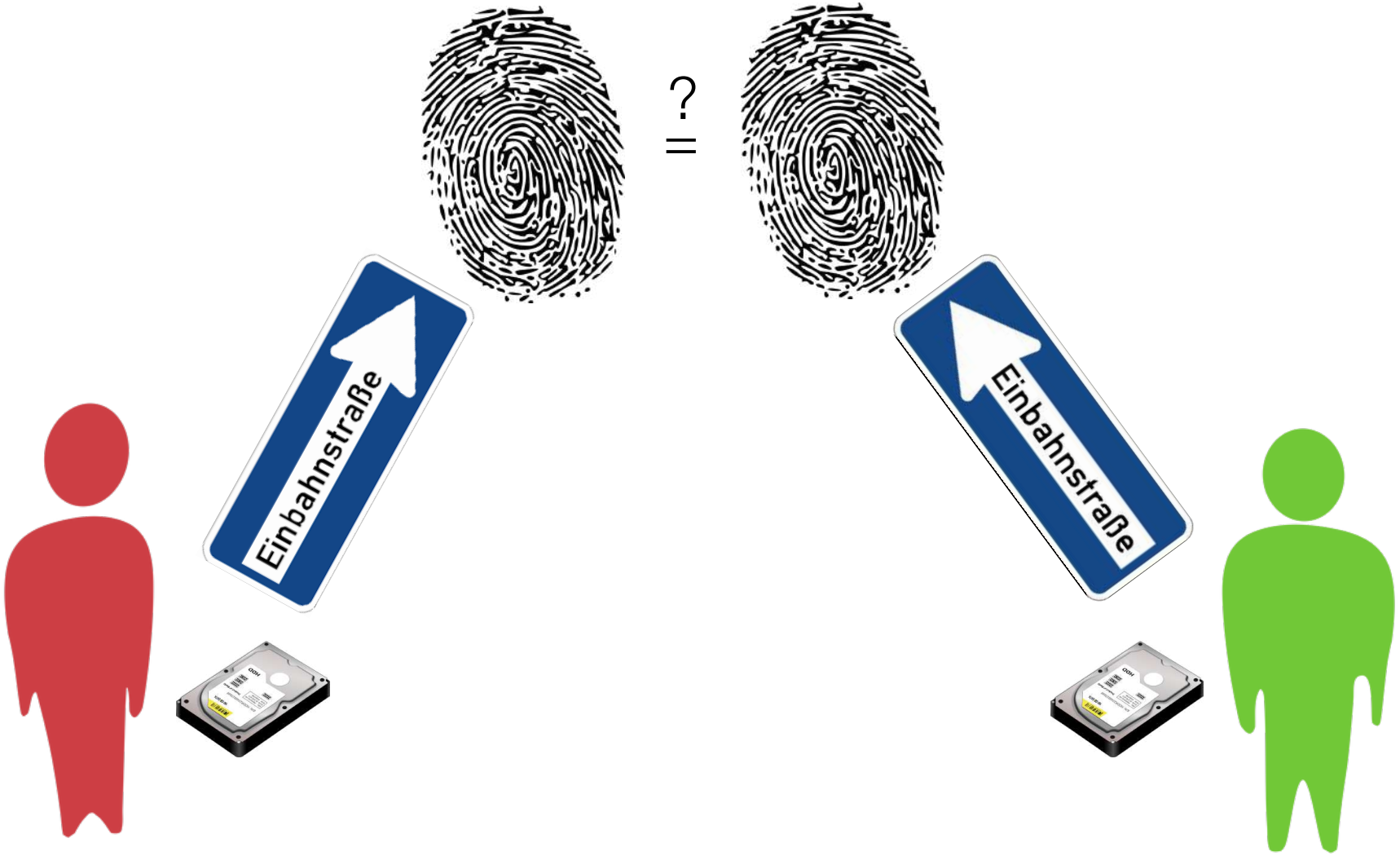
Quelle: NISTIR 8105, Report on Post-Quantum Cryptography, Chen/Jordan/Liu/Moody/Peralta/Perlner/Smith-Tone

Kryptographische Hashfunktionen

- Digitaler „Fingerabdruck“
- Praktisch eindeutig
- Gleiche Länge
- Für Objekte beliebiger Größe
- Kann (praktisch) nicht zurückgerechnet werden

Demo 2

Abgleich von Daten mit Hashfunktionen

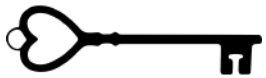


Passwortprüfung über Hashwerte

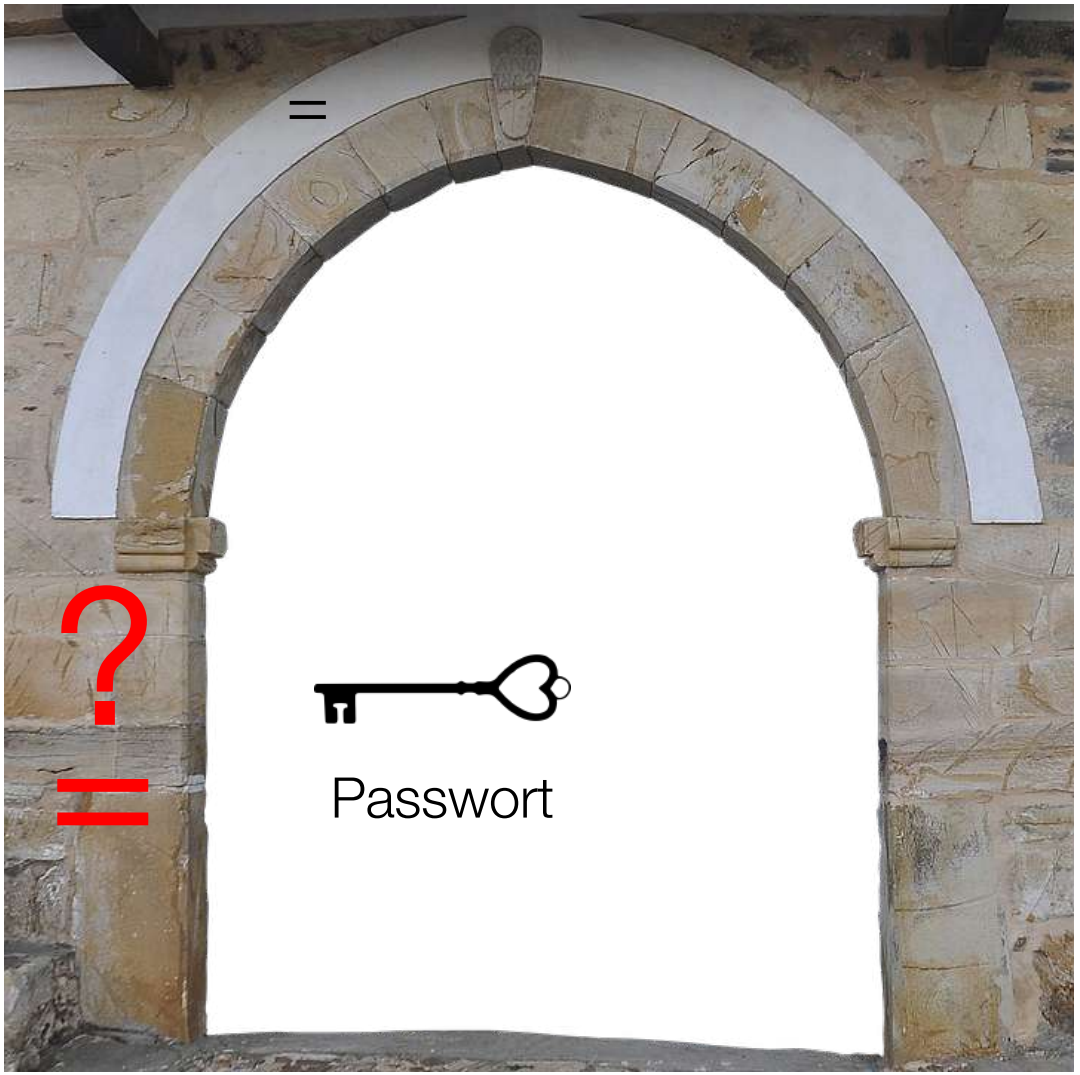
Problem:

Kann man Passwörter prüfen,
ohne sie abspeichern zu müssen?

Passwortprüfung über Hashwerte

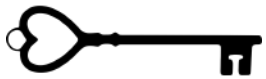


Passwort



Passwort

Passwortprüfung über Hashwerte



Passwort

Hashwerte personenbezogene Daten?

- Zu wenig Entropie ⇒ Ausprobieren möglich

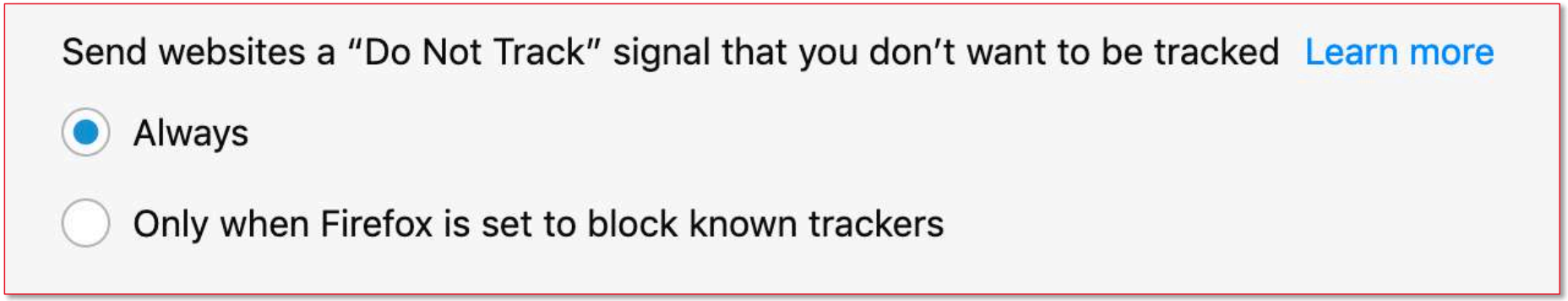
- Hashfunktion in eine Richtung offen
  - Abgleich
  - Gehashtes Objekt wird zum „Schlüssel“ zur Zuordnung weiterer Information
- Hashwert wird als ID verwendet
- Unsichere Hashfunktion beeinträchtigt nur Beweisfunktion

Hashwert von personenbezogenem Datum häufig selbst personenbezogenes Datum

Technisch verhandelter Datenschutz

- Regelbasierte Einwilligung
- Regelbasierter Widerspruch
- Einwilligungsmanagement
- Einwilligungshistorie

Do Not Track



Vielen Dank für Ihre Aufmerksamkeit!

Fragen, Diskussion