



Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences



Bild: [IT Security Journal](#)

IT-Security in der Informationsgesellschaft: Neue Herausforderungen

Prof. Dr. Eric Dubuis

► Research Institute for Security in the Information Society

Referent

▶ Eric Dubuis

Abteilungsleiter Informatik
Professor für Informatik

Leiter des Instituts
Research Institute for Security in the
Information Society (RISIS)



Was wir tun...

- ▶ *Malware-Forschung und Threat Intelligence*
- ▶ IT-Forensik und *Law Enforcement*
- ▶ Anonymisierung von (Gesundheits-) Daten
- ▶ Dark Net
- ▶ Elektronische Identitäten (im Schwesterinstitut ICTM)
- ▶ Schutz der Privatsphäre
- ▶ E-Voting

Fragestellungen

No Security?

- ▶ Welche Bedrohungen sind akut für Privatpersonen und Organisationen?
- ▶ Welche Gefahren werden unterschätzt oder nicht angemessen wahrgenommen?

Cybersecurity für Unternehmen?

- ▶ Wie schützen sich Unternehmen vor den aktuellen Gefahren?
- ▶ Welche Organisationen sind besonders gefährdet?
- ▶ Cybersecurity Capability Maturity – Wie kann man das Management von Security anpacken?
- ▶ Welchen Reifegrad haben wir?

Security Engineering?

- ▶ Neue Technologien bedeutet neue Risiken – Neue Risiken erfordern neue Technologien. Welche?
- ▶ Mobile Devices, Internet of Things, Artificial Intelligence – Welche Risiken sind im Anzug, welche Massnahmen bieten sich an?

Fragestellungen

No Security?

- ▶ Welche Bedrohungen sind akut für Privatpersonen und Organisationen?
- ▶ Welche Gefahren werden unterschätzt oder nicht angemessen wahrgenommen?

Cybersecurity für Unternehmen?

- ▶ Wie schützen sich Unternehmen vor den aktuellen Gefahren?
- ▶ Welche Organisationen sind besonders gefährdet?
- ▶ Cybersecurity Capability Maturity – Wie kann man das Management von Security anpacken?
- ▶ Welchen Reifegrad haben wir?

Security Engineering?

- ▶ **Neue Technologien** bedeutet neue Risiken – Neue Risiken erfordern neue Technologien. Welche?
- ▶ **Mobile Devices, Internet of Things, Artificial Intelligence** – Welche Risiken sind im Anzug, welche Massnahmen bieten sich an?


Gliederung

- ▶ Situation heute
- ▶ Wege in eine bessere Zukunft
 - ▶ Resilient (Software) Design
 - ▶ Privacy by Design
 - ▶ E-Voting
- ▶ Take away

Situation heute

[Security](#) > [7-Tage-News](#) > [07/2018](#) > SmartThings Hub: Samsung patcht gegen unbefugten Remote-Zugriff

SmartThings Hub: Samsung patcht gegen unbefugten Remote-Zugriff

 **Alert!** 27.07.2018 14:51 Uhr – Olivia von Westernhagen



«Das Threat-Intelligence-Team Cisco Talos hat **über 30 Lücken entdeckt**, deren Schweregrad variiert. Einzelne sind mitunter schwer ausnutzbar – allerdings gäbe es mehrere denkbare Kombinationsmöglichkeiten zu so genannten ‘Exploit-Chains’.»



de fr it

Zürich 26° 

Schweiz

Ausland

Wirtschaft

Sport

People

Entertainment

Digital

Wissen

Zürich

Bern

Basel

Zentralschweiz

Ostschweiz

Energy Challenge

Ihre Story, Ihre Informationen, Ihr Hinweis? feedback@20minuten.ch 

Gestohlene Mietvelos

13. August 2018 13:23; Akt: 13.08.2018 16:05 

Etliche Publibikes in Bern mit Handys geknackt

In Bern hat sich eine Methode herumgesprochen, wie Publibikes geknackt werden können. Der Vermieter sucht nach einer Lösung.



Die Spione in der Steckdose

SonntagsZeitung Swisscom-Smart-Meter erlaubten Hackern, in private WLAN-Netze einzudringen. [Mehr...](#)

ABO+ Barnaby Skinner. 13.08.2018

«Via den MyStrom-Smart-Meter könnten Cyberkriminelle sogar auf TVs, Handys oder Notebooks zugreifen [...].»

«Die MyStrom-Entwickler hatten allerdings geschlampt. [...] entdeckte im Quellcode der Software **Logins** und **Passwörter** zweier Entwickler.»

'Insight' into Home Automation Reveals Vulnerability in Simple IoT Product

By [Douglas McKee](#) on Aug 20, 2018

Eoin Carroll, Charles McFarland, Kevin McGrath, and Mark Bereza contributed to this report.

«Discoveries such as CVE-2018-6692 underline the **importance of secure coding practices on *all* devices**. IoT devices are frequently overlooked from a security perspective; this may be because many are used for seemingly innocuous purposes such as simple home automation. However, these devices run operating systems and require just as much protection as desktop computers.»



TOPTHEMEN: URHEBERRECHT DSGVO WINDOWS 10 ANDROID 9 KRYPTOWÄHRUNG

heise online > News > 07/2018 > **Datenleck: 47.000 sensible Dokumente von Autobauern im Internet...**

21.07.2018 12:29 Uhr

Datenleck: 47.000 sensible Dokumente von Autobauern im Internet öffentlich

Was geht ab bei VW & Co.? Sensible Informationen vieler Autobauer fanden sich öffentlich im Netz – dank eines Datenlecks bei einem Dienstleister.

von **Oliver Bünte**



[News >](#)[Schweiz >](#)**Datenkrake Auto**

Wie uns Autobauer ausspähen

In modernen Autos sind bis zu 200 Sensoren eingebaut. Die Technik sammelt haufenweise Daten: Vom Standort über die abgespielte Musik bis zu den Handy-Kontaktdaten. Was die wenigsten Autofahrer wissen: Diese Daten werden direkt an den Hersteller geschickt.

Magnus Renggli

Dienstag, 21.02.2017, 21:09 Uhr

Aktualisiert um 22:00 Uhr

Was können wir tun?

- ▶ Resilient (Software) Design
- ▶ Privacy by Design
- ▶ E-Voting

Modellierung der Angreifer

Wir haben es mit sehr starken Angreifern («adversaries») zu tun:

- ▶ beliebige Rolle
- ▶ viele Identitäten
- ▶ grosse Rechenkapazität
- ▶ grosse Macht bis hin zu Staatsmacht

Die Angreifer können nicht:

- ▶ Kryptographie «brechen»
- ▶ Kommunikation *per se* unterbinden

Endsysteme kompromittieren?

Resilient (Software) Design

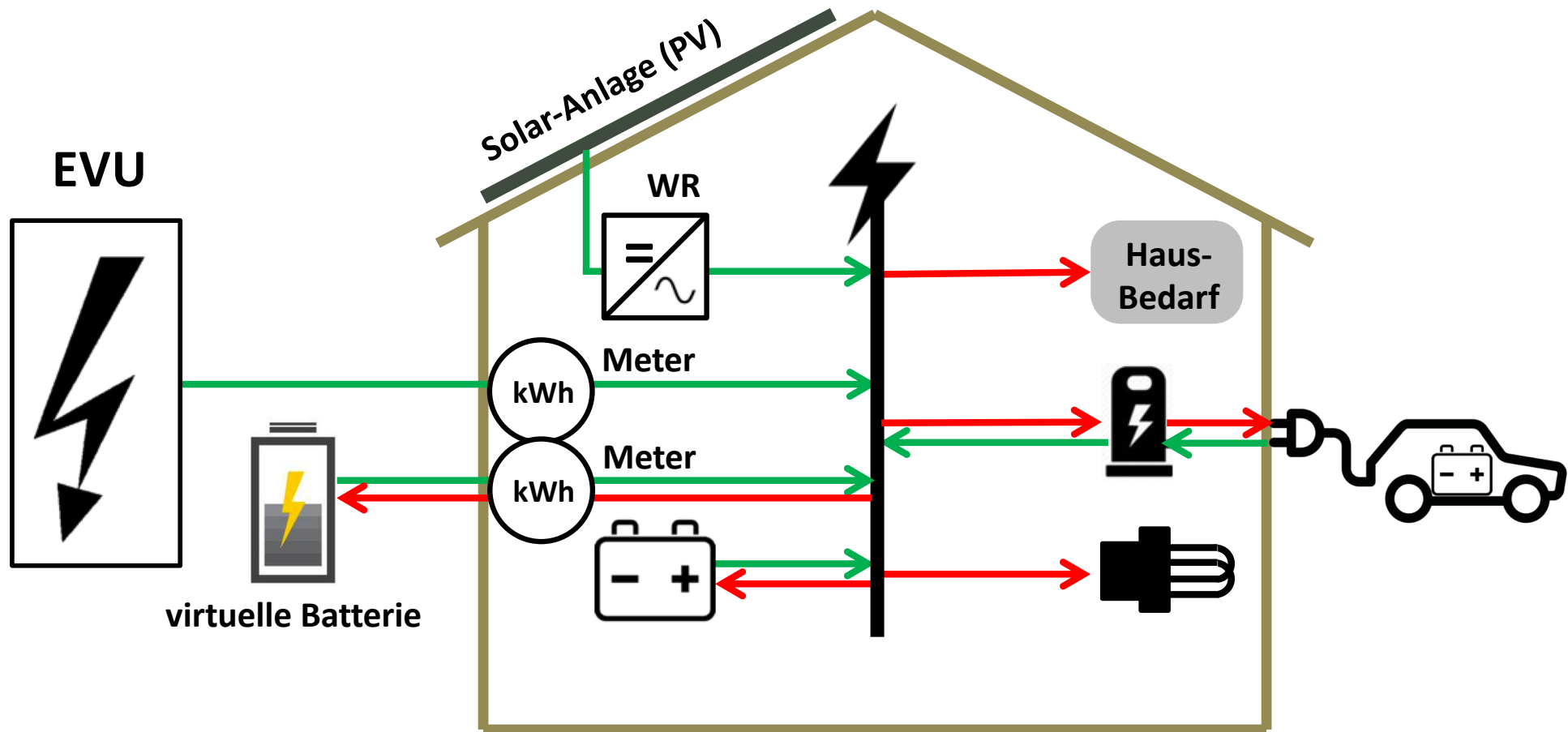
... eine Definition

«*Resilient Software Design* beschreibt die Gestaltung und Umsetzung einer Software-basierten Lösung auf eine Weise, dass im Falle einer unerwarteten Fehlersituation

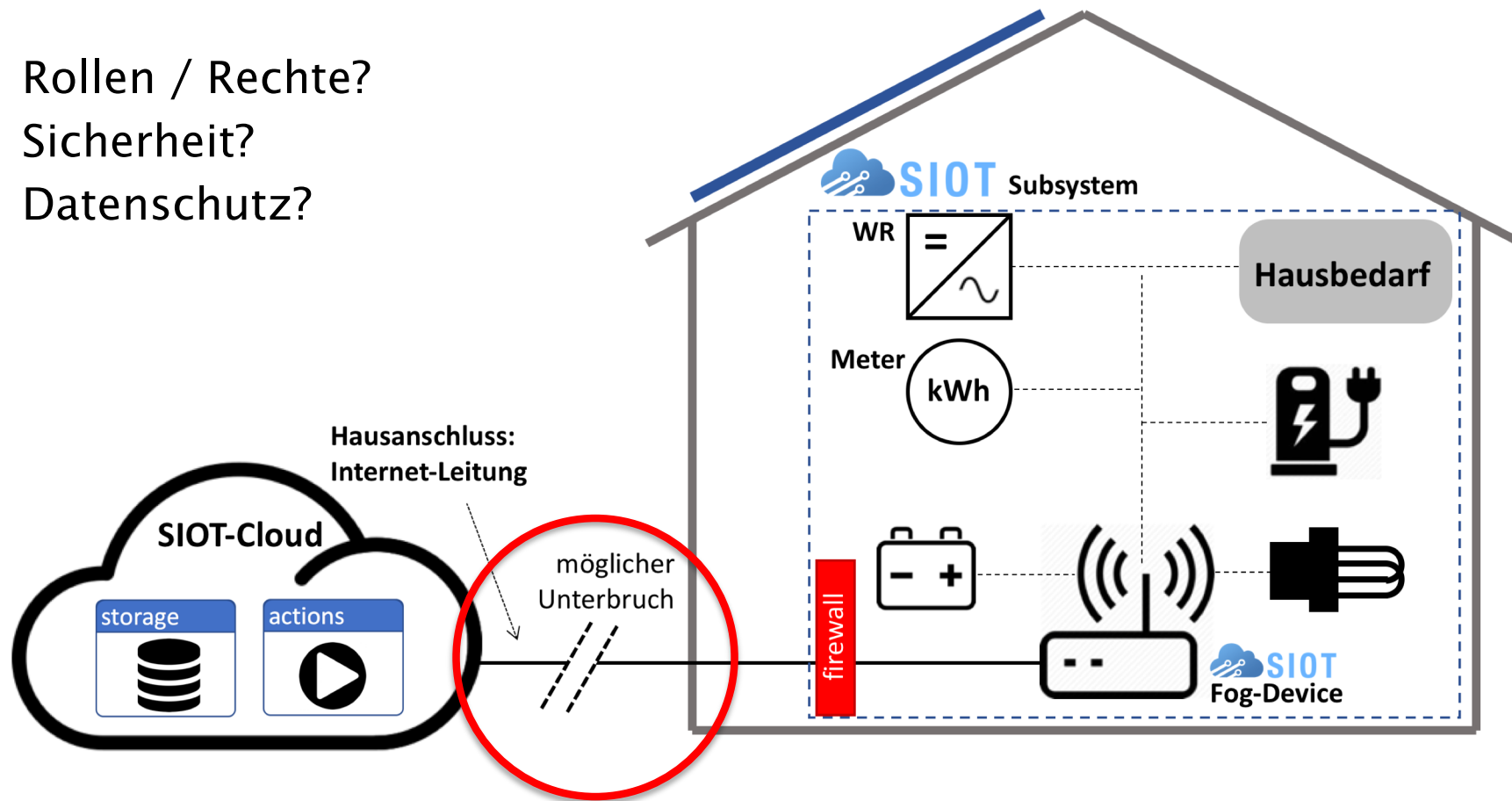
- ▶ der Nutzer im besten Fall überhaupt nichts davon bemerkt,
- ▶ die Lösung anderenfalls in einem definierten, reduzierten Service-Level weiterarbeitet.»

Quelle: [Informatik Aktuell vom 31.5.2016 \(21.08.2018\)](#)

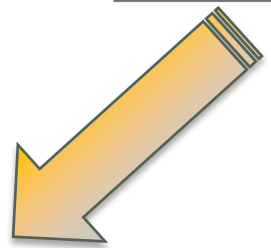
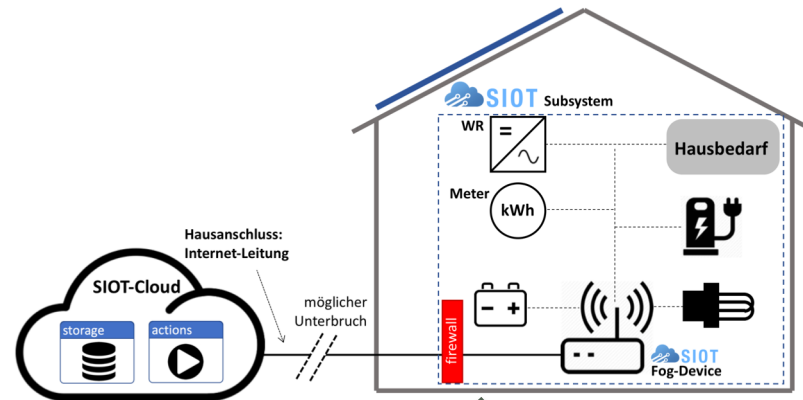
... am Beispiel «Energieversorgung»



- ▶ Rollen / Rechte?
- ▶ Sicherheit?
- ▶ Datenschutz?



Bei Unterbruch (lies: DoS-Attacke)
arbeitet das siot-Subsystem autark



Privacy by Design

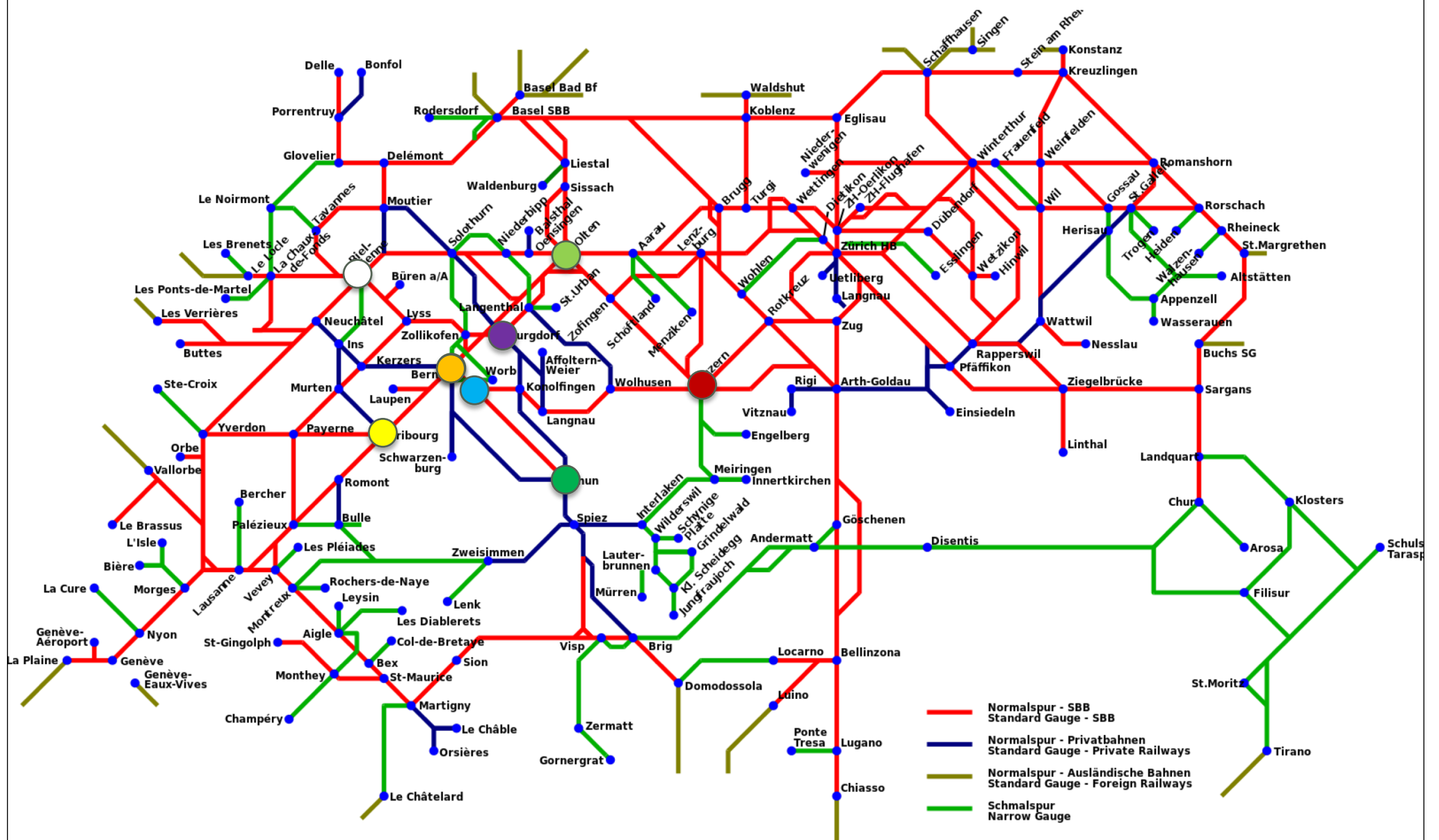
... eine Umschreibung

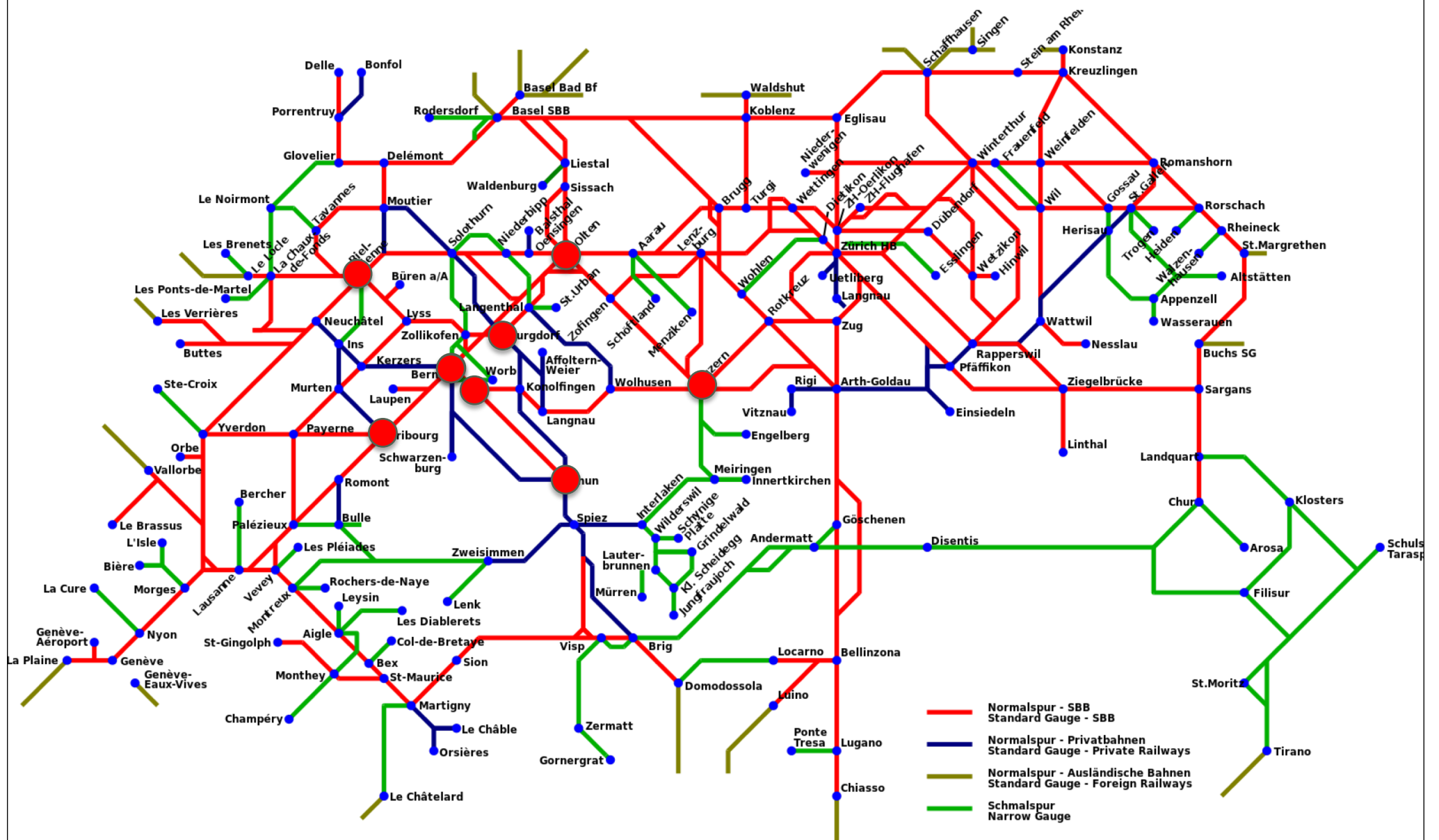
«*Privacy by Design* bedeutet, dass der Datenschutz bereits bei der Konzipierung und Entwicklung von Software und Hardware zur Datenverarbeitung berücksichtigt wird. [...]»

Quelle: [Jörg Schliske, TÜV Nord Group \(21.08.2018\)](#)

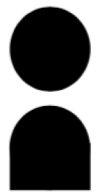
... am Beispiel von «Mobility Apps» wie





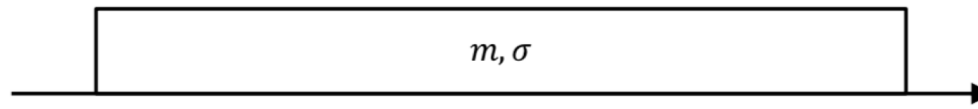


Digitale Signatur kurz erklärt



Alice
 $pk(A)$
 $sk(A)$

Nachricht m
Signatur σ
 $\sigma = Sig_A(m)$



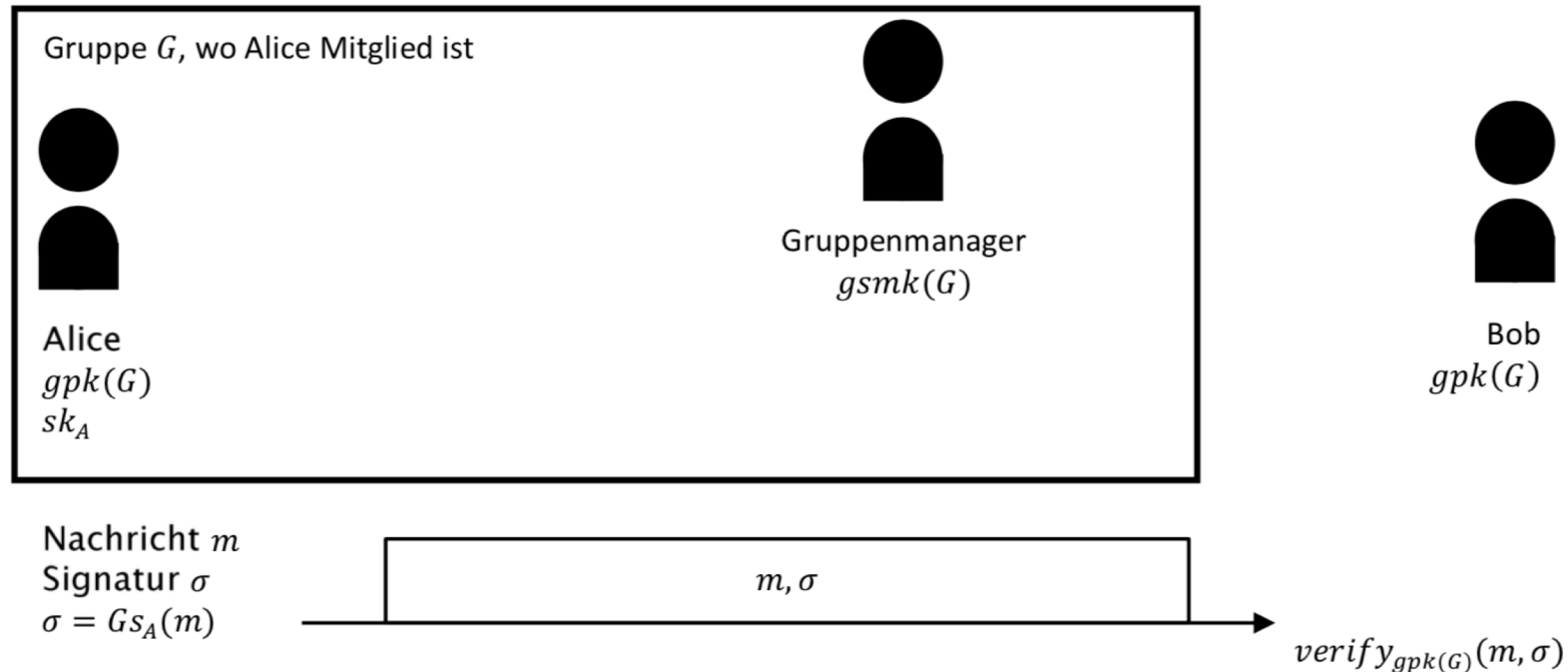
Bob
 $pk(A)$

$verify_{pk(A)}(m, \sigma)$

Dank der Signatur kann Bob:

- ▶ die Integrität der Nachricht sicherstellen
- ▶ beweisen, dass Alice m signiert hat

Gruppensignatur kurz erklärt



Dank der Signatur kann Bob:

- die Integrität der Nachricht sicherstellen
- beweisen, dass die Nachricht von einem Mitglied der Gruppe G stammt

Nur der **Gruppenmanager** kann bei Bedarf mit $gsmk(G)$ die Signatur öffnen und beweisen, dass Alice m signiert hat

Erkenntnisse

Der Lösungsansatz

- ▶ ... ist vielversprechend

Aber

- ▶ er ist inkompatibel mit der bestehenden zentralen Infrastruktur (NOVA) der ÖV-Unternehmungen

Das heisst also:

- ▶ **Um die positiven Seiten der Digitalisierung ausnützen zu können, braucht es oft neue Lösungsansätze**

E-Voting

E-Voting-Gruppe der BFH

- ▶ Gründung Ende 2007 durch Kollege Rolf Haenni und mich
- ▶ Über 20 Forschungsartikel (*peer-reviewed*)
- ▶ Mitglieder der Programmkomitees von E-VOTE, VoteID, E-Vote-ID, CeDEM
- ▶ Organisator der VoteID'15 in Bern
- ▶ Swiss E-Voting Workshop 2009, 2010, 2012, 2014
- ▶ Betreuung von mehreren Doktoranden rund ums Thema E-Voting

Link: <https://e-voting.bfh.ch>

Projekte / Aktivitäten

- ▶ FIDIS: Future of Identity in Information Society (2006–2009)
- ▶ SwissVote: Secure E-Voting in Switzerland (2009–2012)
- ▶ VIVO: Verifiable Internet Voting (2012–2015)
- ▶ UniVote: Secure E-Voting in Switzerland (2013–2017)
- ▶ UniBoard: Spezifikation und Development eines *Public Bulletin Board* für Online-Wahlen(2014–2017)
- ▶ CHVote: Cryptographic System Specification of the Geneva E-Voting System (seit 2016)
- ▶ Verifikations-Software für E-Voting-Lösung der Schweizerischen Post (seit 2017)

Verordnung «Elektronische Stimmabgabe»

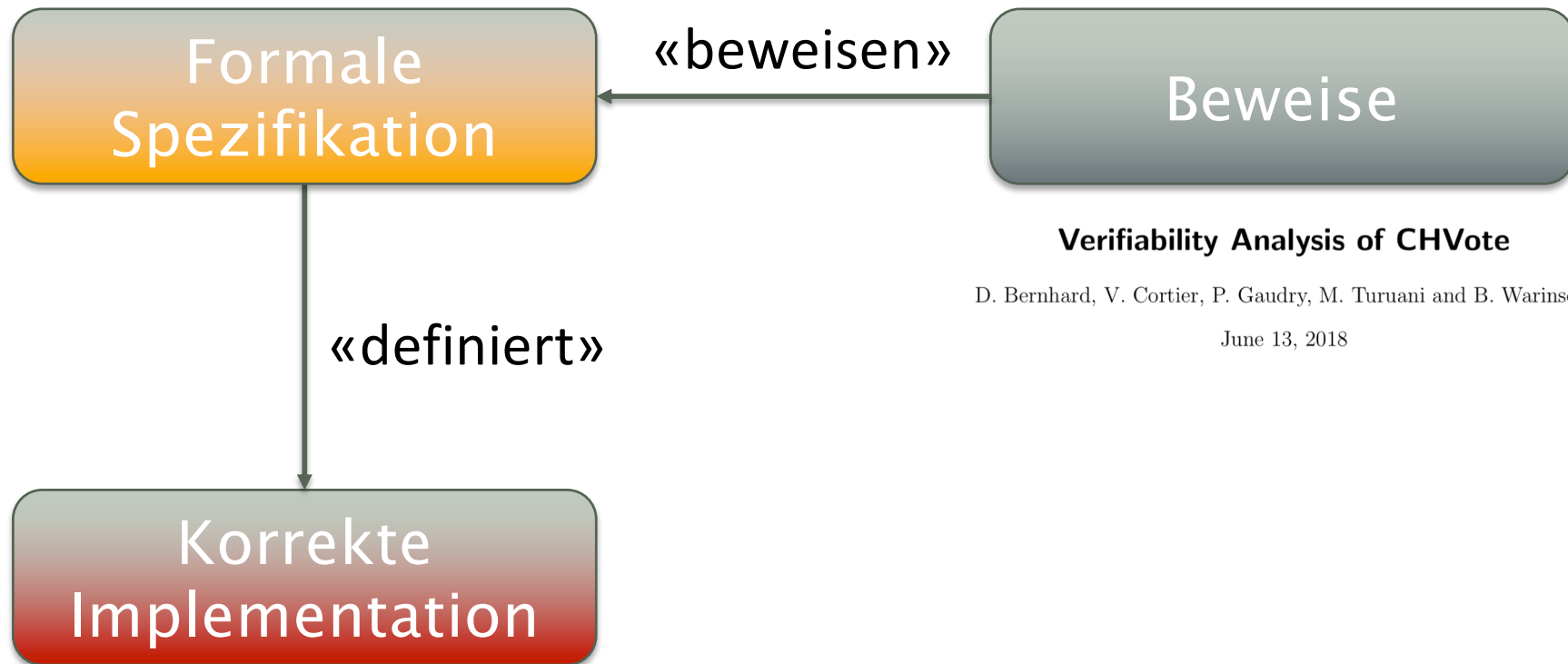
Verordnung der BK über die elektronische Stimmabgabe (VEleS) vom 13. Dezember 2013 (Stand am 1. Juli 2018)

Umfassende Sicherheitsanforderungen

- ▶ End-zu-End-Verschlüsselung
- ▶ Verifizierbarkeit
 - ▶ **individuelle** Verifizierbarkeit
«Wurde meine Stimme unverändert vom System erfasst?»
 - ▶ **universelle** oder vollständige (in VEleS) Verifizierbarkeit
«Wurden alle korrekt erfassten, gültigen Stimmen (und nur solche) richtig gezählt?»
- ▶ Aufteilung von «Vertrauen» auf mehrere unabhängige Systemteile (*distribution of trust*)
 - ▶ verifizierbares Mix-Net
 - ▶ Splitten des Entschlüsselungsschlüssels

Was braucht es? («Security Engineering»)

<https://eprint.iacr.org/2017/325>



Verifiability Analysis of CHVote

D. Bernhard, V. Cortier, P. Gaudry, M. Turuani and B. Warinski

June 13, 2018

Beispiel: Von der «Spezifikation» ...

Algorithm: GenBallot(X, \mathbf{s}, pk)

Input: Voting code $X \in A_X^{\ell_X}$

Selection $\mathbf{s} = (s_1, \dots, s_k), 1 \leq s_1 < \dots < s_k$

Encryption key $pk \in \mathbb{G}_q \setminus \{1\}$

$x \leftarrow \text{ToInteger}(X)$ // see Alg. 4.7

$\hat{x} \leftarrow \hat{g}^x \bmod \hat{p}$

$\mathbf{q} \leftarrow \text{GetSelectedPrimes}(\mathbf{s})$ // $\mathbf{q} = (q_1, \dots, q_k)$, see Alg. 7.19

$m \leftarrow \prod_{i=1}^k q_i$

if $m \geq p$ **then**

return \perp // (k, n) is incompatible with p

$(\mathbf{a}, \mathbf{r}) \leftarrow \text{GenQuery}(\mathbf{q}, pk)$ // $\mathbf{a} = (a_1, \dots, a_k), \mathbf{r} = (r_1, \dots, r_k)$, see Alg. 7.20

$a \leftarrow \prod_{i=1}^k a_i \bmod p$

$r \leftarrow \sum_{i=1}^k r_i \bmod q$

$b \leftarrow g^r \bmod p$

$\pi \leftarrow \text{GenBallotProof}(x, m, r, \hat{x}, a, b, pk)$ // $\pi = (t, s)$, see Alg. 7.21

$\alpha \leftarrow (\hat{x}, \mathbf{a}, b, \pi)$

return (α, \mathbf{r}) // $\alpha \in \mathbb{Z}_{\hat{q}} \times \mathbb{G}_q^k \times \mathbb{G}_q \times ((\mathbb{G}_{\hat{q}} \times \mathbb{G}_q^2) \times (\mathbb{Z}_{\hat{q}} \times \mathbb{G}_q \times \mathbb{Z}_q)), \mathbf{r} \in \mathbb{Z}_q^k$

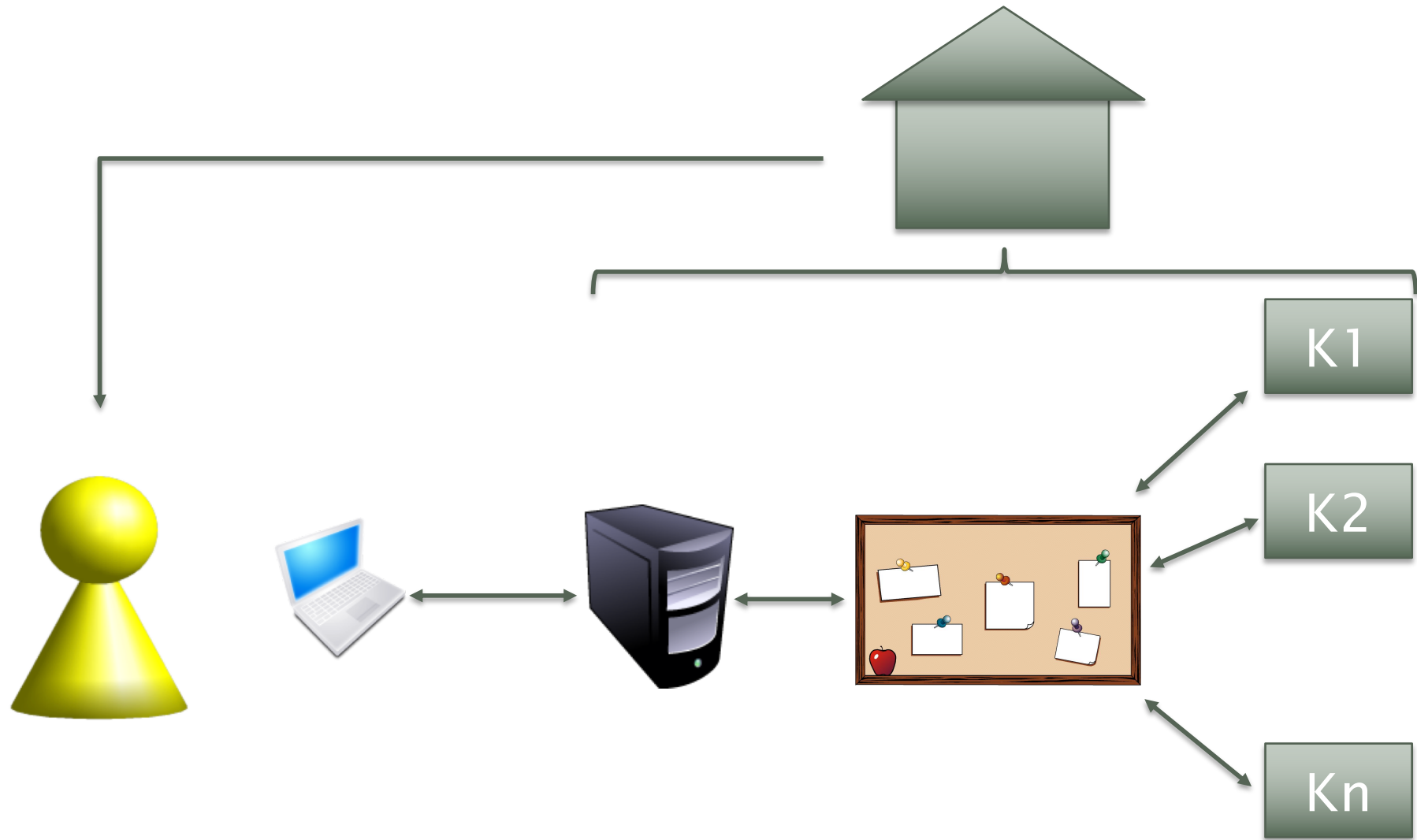
Algorithm 7.18: Generates a ballot based on the selection \mathbf{s} and the voting code X .

... zur Implementation

```
1 /**
2  * Algorithm 7.18: GenBallot
3  *
4  * @param upper_x the voting code
5  * @param bold_s voters selection (indices)
6  * @param pk      the public encryption key
7  * @return the combined ballot, OT query and random elements used
8  */
9 public BallotQueryAndRand genBallot(String upper_x, List<Integer> bold_s, EncryptionPublicKey pk) {
10     BigInteger x = conversion.toInteger(upper_x, publicParameters.getUpper_a_x());
11     BigInteger x_circ = modExp(g_circ, x, p_circ);
12     List<BigInteger> bold_q = computeBoldQ(bold_s);
13     BigInteger m = computeM(bold_q, p);
14     ObliviousTransferQuery query = genQuery(bold_q, pk);
15     BigInteger a = computeA(query, p);
16     BigInteger r = computeR(query, q);
17     BigInteger b = modExp(g, r, p);
18     NonInteractiveZKP pi = genBallotProof(x, m, r, x_circ, a, b, pk);
19     BallotAndQuery alpha = new BallotAndQuery(x_circ, query.getBold_a(), b, pi);
20
21     return new BallotQueryAndRand(alpha, query.getBold_r());
22 }
```

Auszug (mit Kürzung) aus: [CHVote Prof-of-Concept](#)

Grobstruktur CHVote



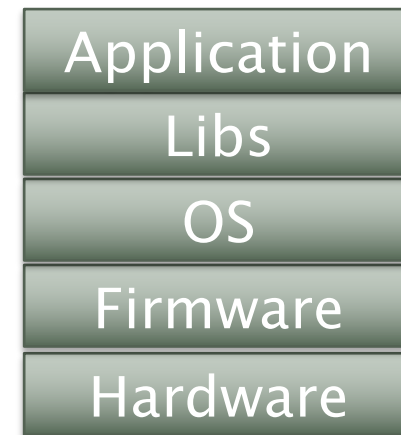
Vertrauensannahmen

Korrektheit des **Ergebnisses**, **Stimmgeheimnis**
(sonst wird es gemerkt):

- ▶ Druckerei
- ▶ Maximal eine Kontrollkomponente

Privacy

- ▶ Kein «*side channel*» beim Gerät des Stimmenden



Take away

Anregungen zum Mitnehmen

- ▶ Die Digitalisierung bedeutet neue Chance in vielen Bereichen der modernen Informationsgesellschaft
- ▶ Sie ruft aber (neue) Problem hervor, die gezielt angegangen werden müssen
- ▶ Wird Bestehendes digitalisiert, so müssen die Themen
 - ▶ Vertraulichkeit
 - ▶ Integrität
 - ▶ Authentizität
 - ▶ Schutz der Privatsphärevon Anfang an angegangen werden
- ▶ In der Lehre müssen entsprechende Lehrgefäße bereitgestellt werden

Eric Dubuis
eric.dubuis@bfh.ch

RISIS
risis.bfh.ch