Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Bild: IT Security Journal

Cybersecurity, Schutz der Privatsphäre und Cyberforensik: ein Widerspruch?

Referat Connecta 2019 (22.10.2019)

Prof. Dr. Eric Dubuis
Berner Fachhochschule

- Research Institute for Security in the Information Society

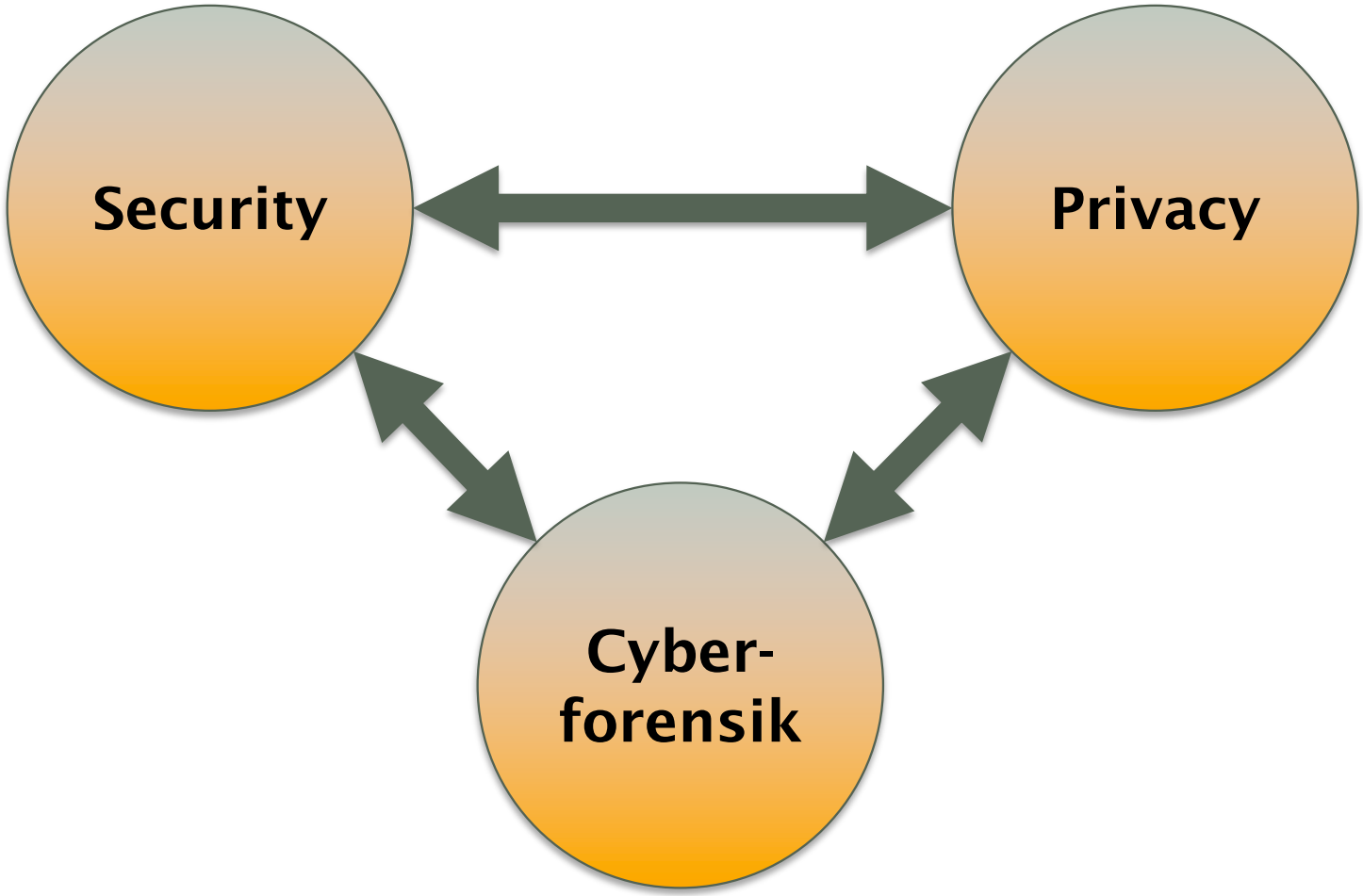
Zu mir…

- Leiter des BFH-Forschungsinstitut RISIS
  - Malware, Security Engineering
  - Privacy-Themen, z.B. Schutz von Patienteninformationen, E-Voting…
  - IT-Forensik

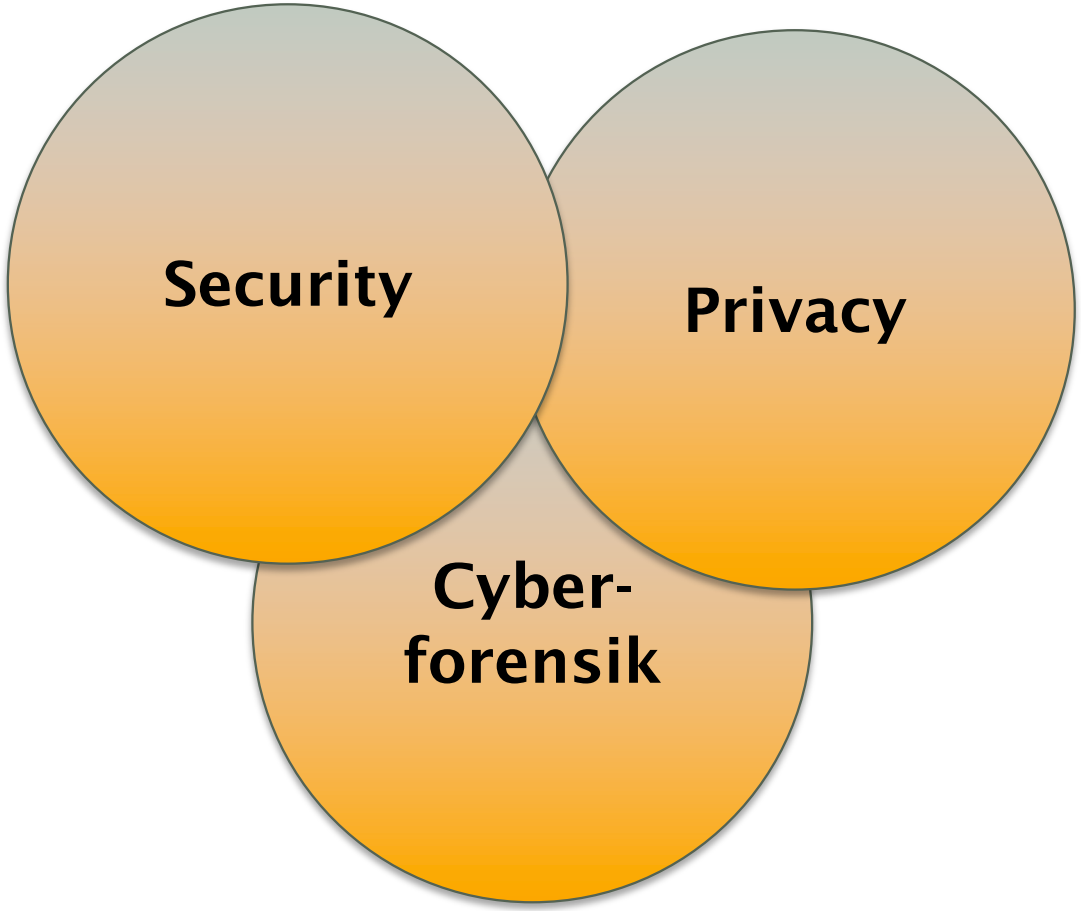
- Verantwortlich für den Studiengang BSc Informatik der BFH
  - Neuer Studienplan, u.a. mit Kotlin

Das Thema heute

Ist es eher so…



… oder so?



(IT-) Sicherheit ja aber…

Bild: Dubuis

Welche Aspekte umfasst die IT-Sicherheit?

Es sind dies:

- Haftung (accountability)
- Nachvollziehbarkeit (auditability)
- Authentizität (authenticity)
- Verfügbarkeit (availability)
- Vertraulichkeit (confidentiality)
- Integrität (integrity)
- Nichtabstreitbarkeit (non-repudiation)
- ***Privatsphäre (privacy)***

Also…

Forensik?

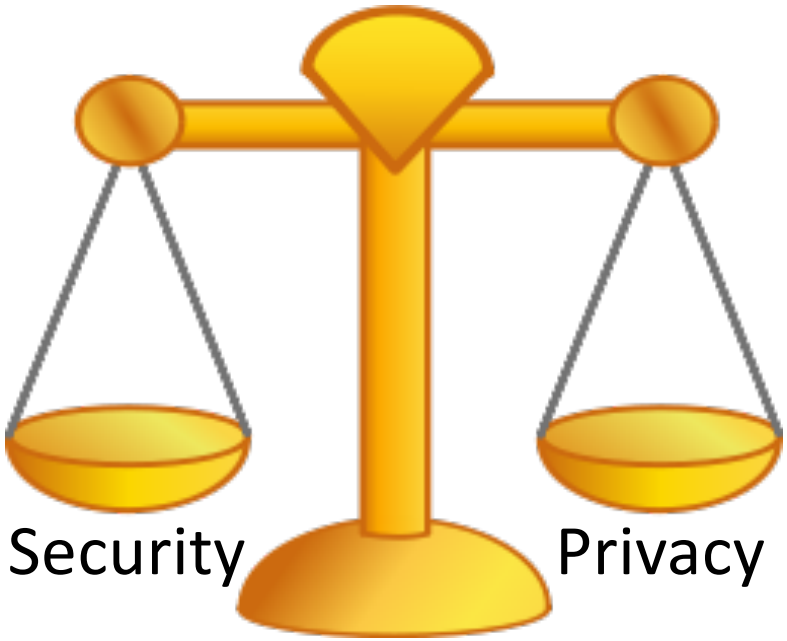


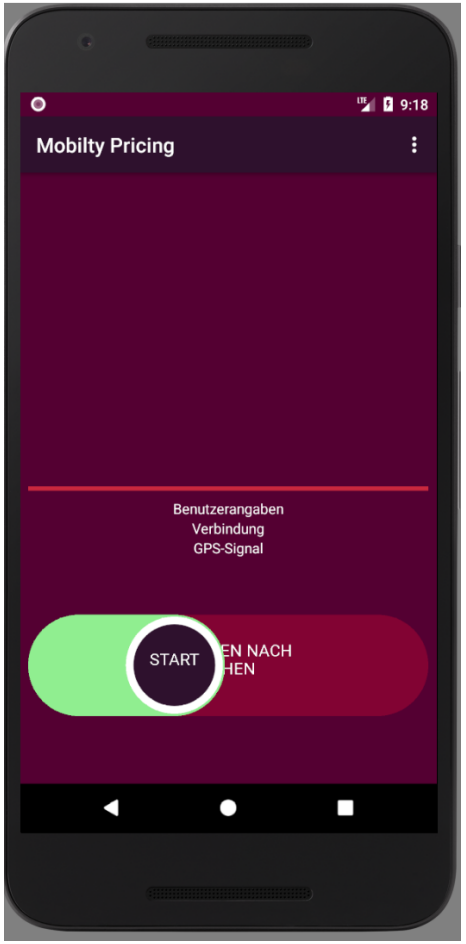
Bild: Wikipedia

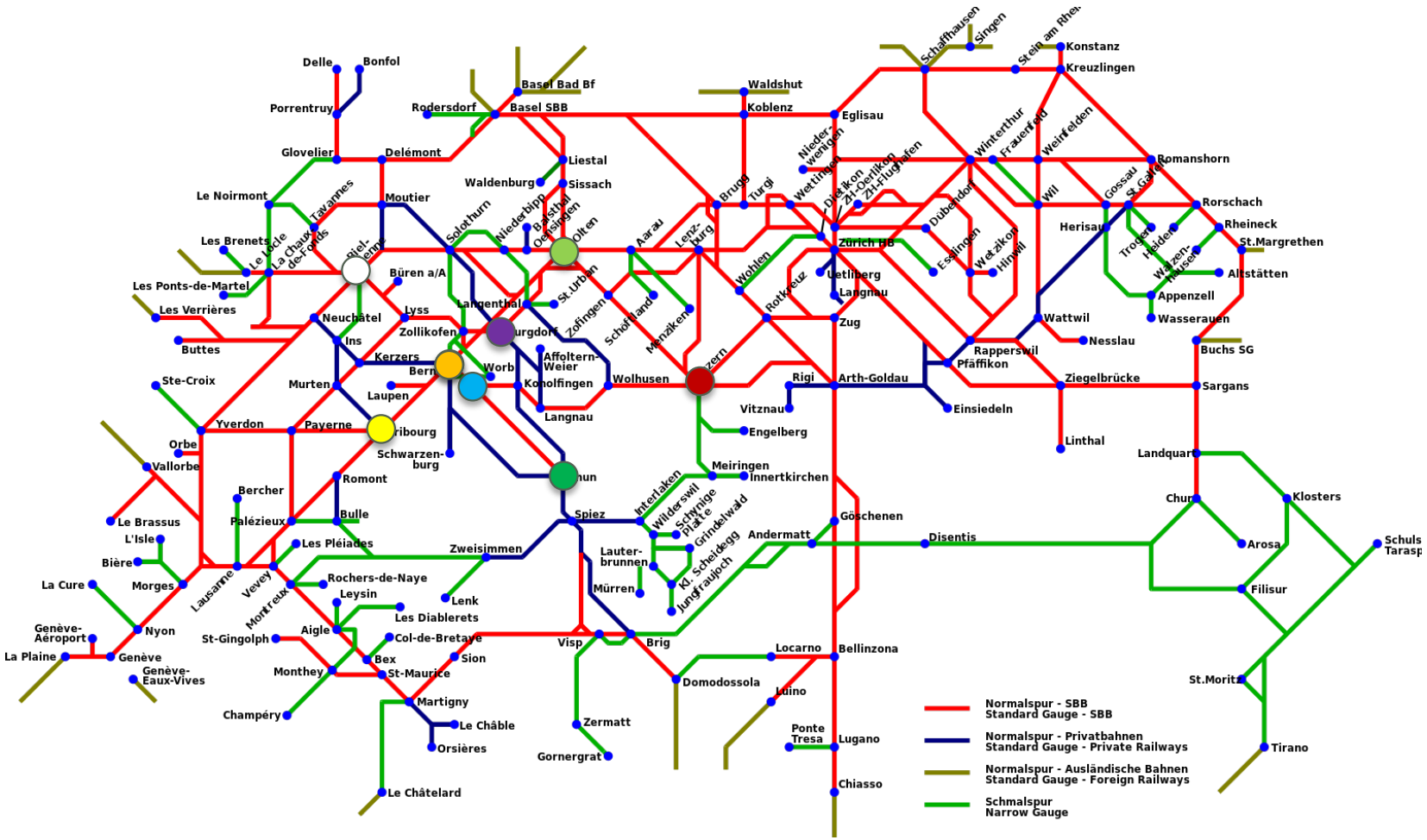
Wo könnte die Privacy gefährdet sein?

... beim Aufzeichnen der Trackingdaten

lezzgo

FAIRTIQ





Quelle : Wikipedia (20.08.2018)

Was können wir tun?

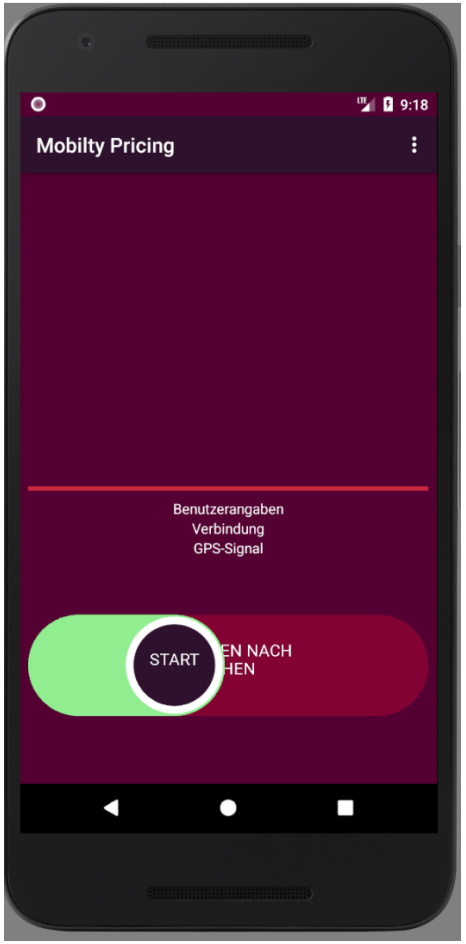
«*Privacy by Design* bedeutet, dass der Datenschutz bereits bei der Konzipierung und Entwicklung von Software und Hardware zur Datenverarbeitung berücksichtigt wird. [...]»

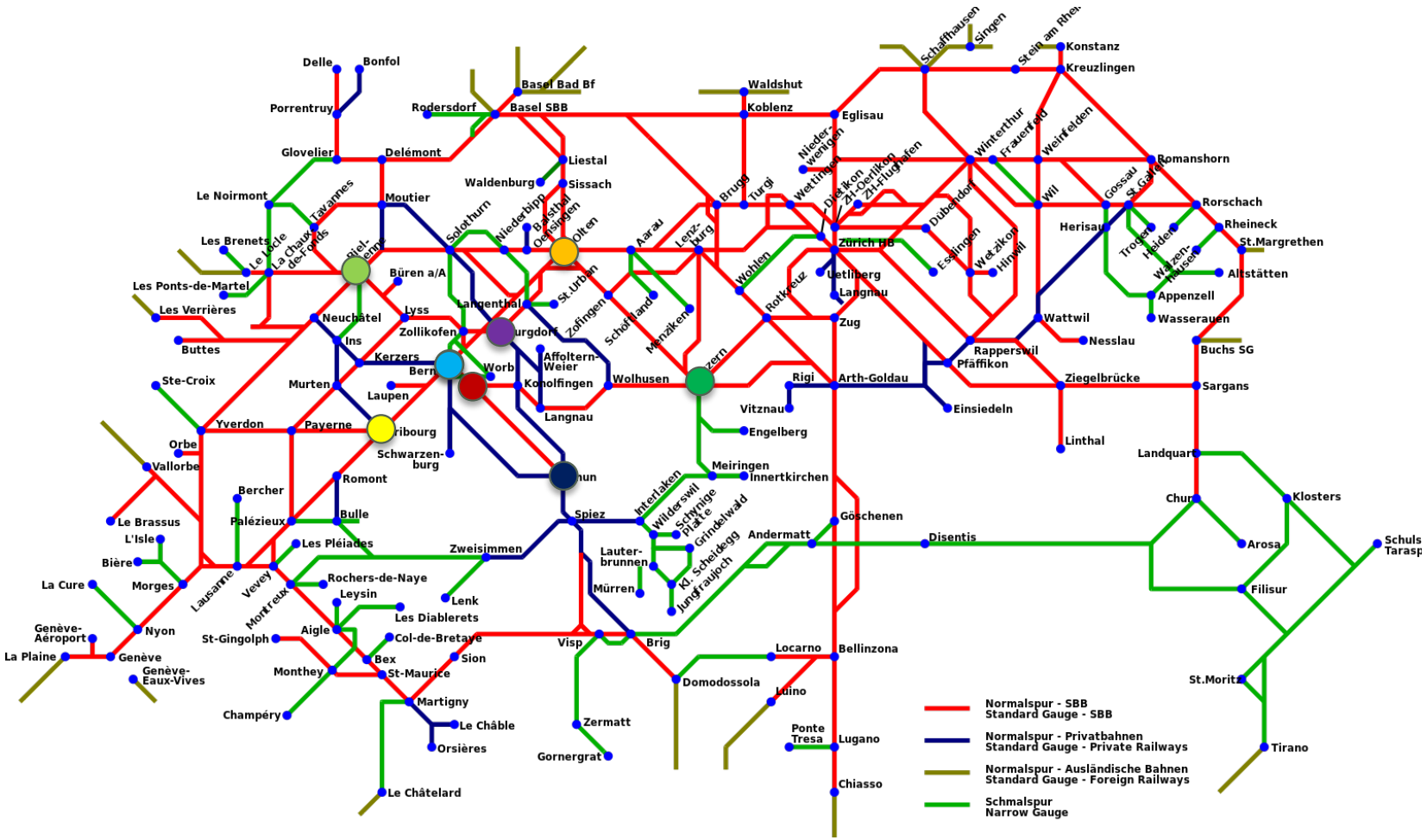
Quelle: Jörg Schlisske, TÜV Nord Group (21.08.2018)

… am Beispiel Mobility Apps

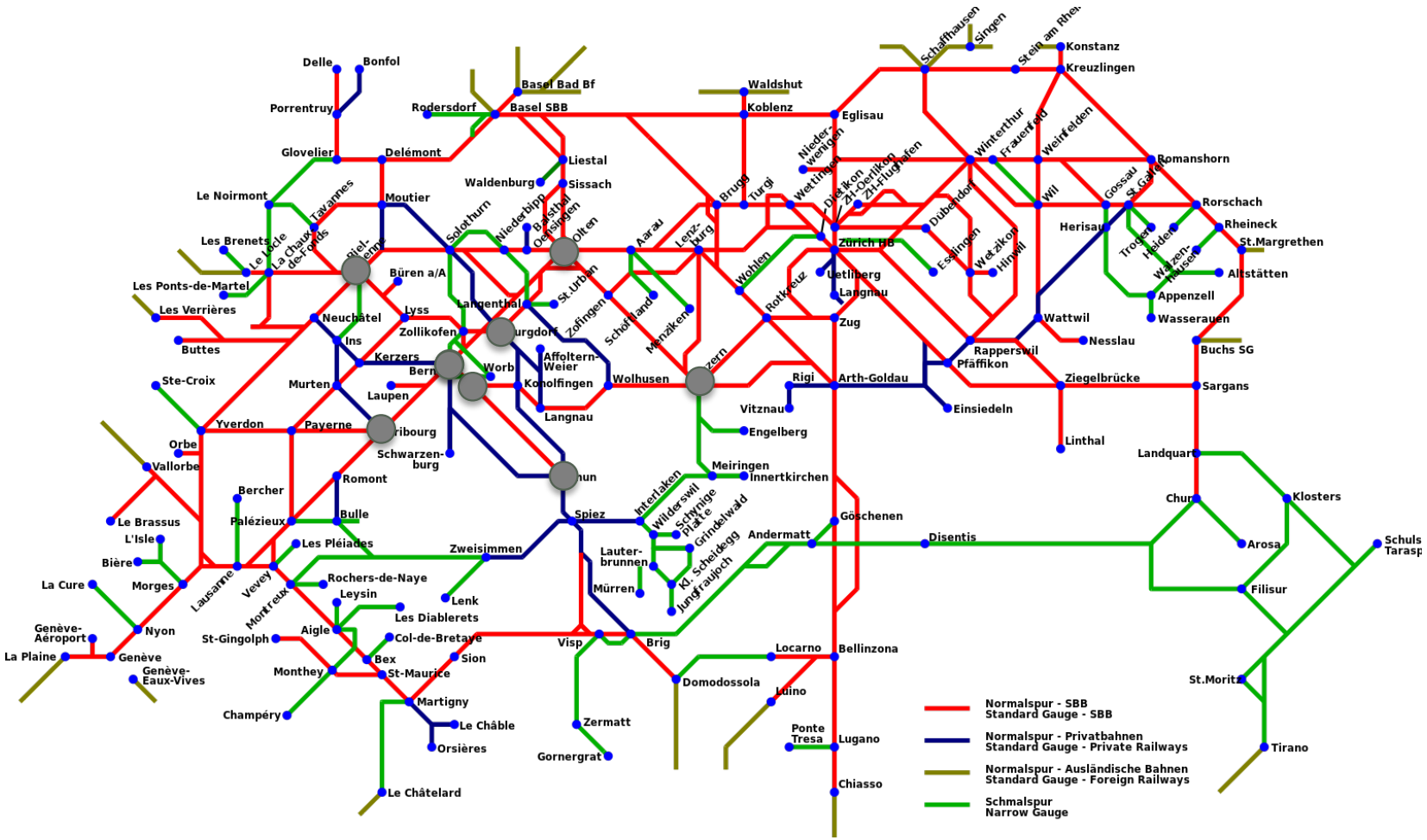
lezzgo

FAIRTIQ





Quelle : Wikipedia (20.08.2018)

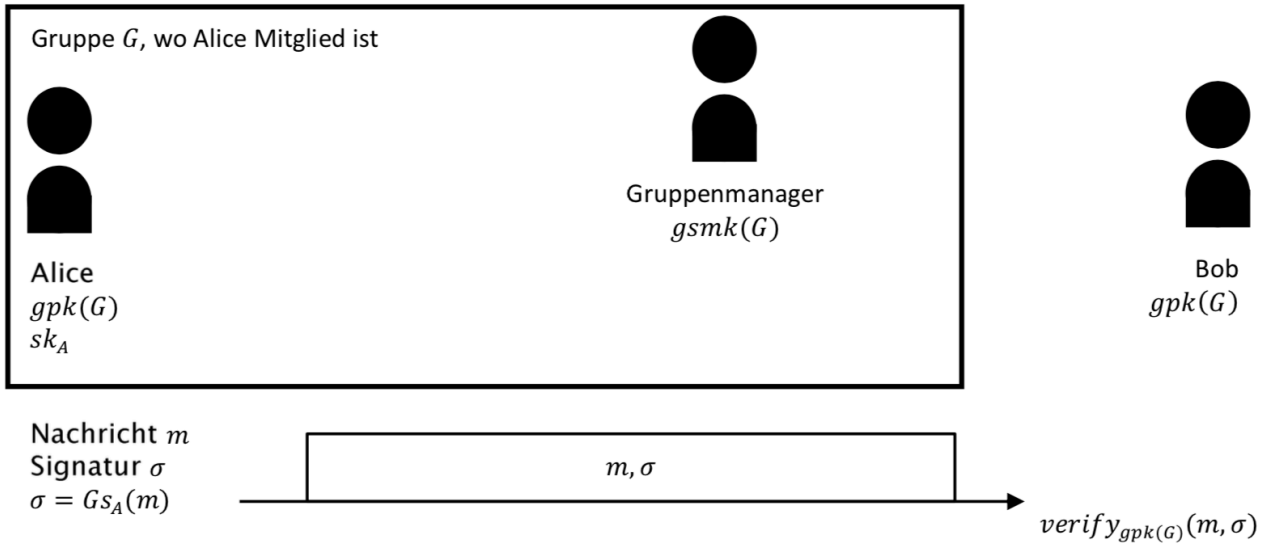


Quelle : Wikipedia (20.08.2018)

Anonyme Mobilität kurz erklärt…

Etwas Kryptographie

Gruppensignatur kurz erklärt



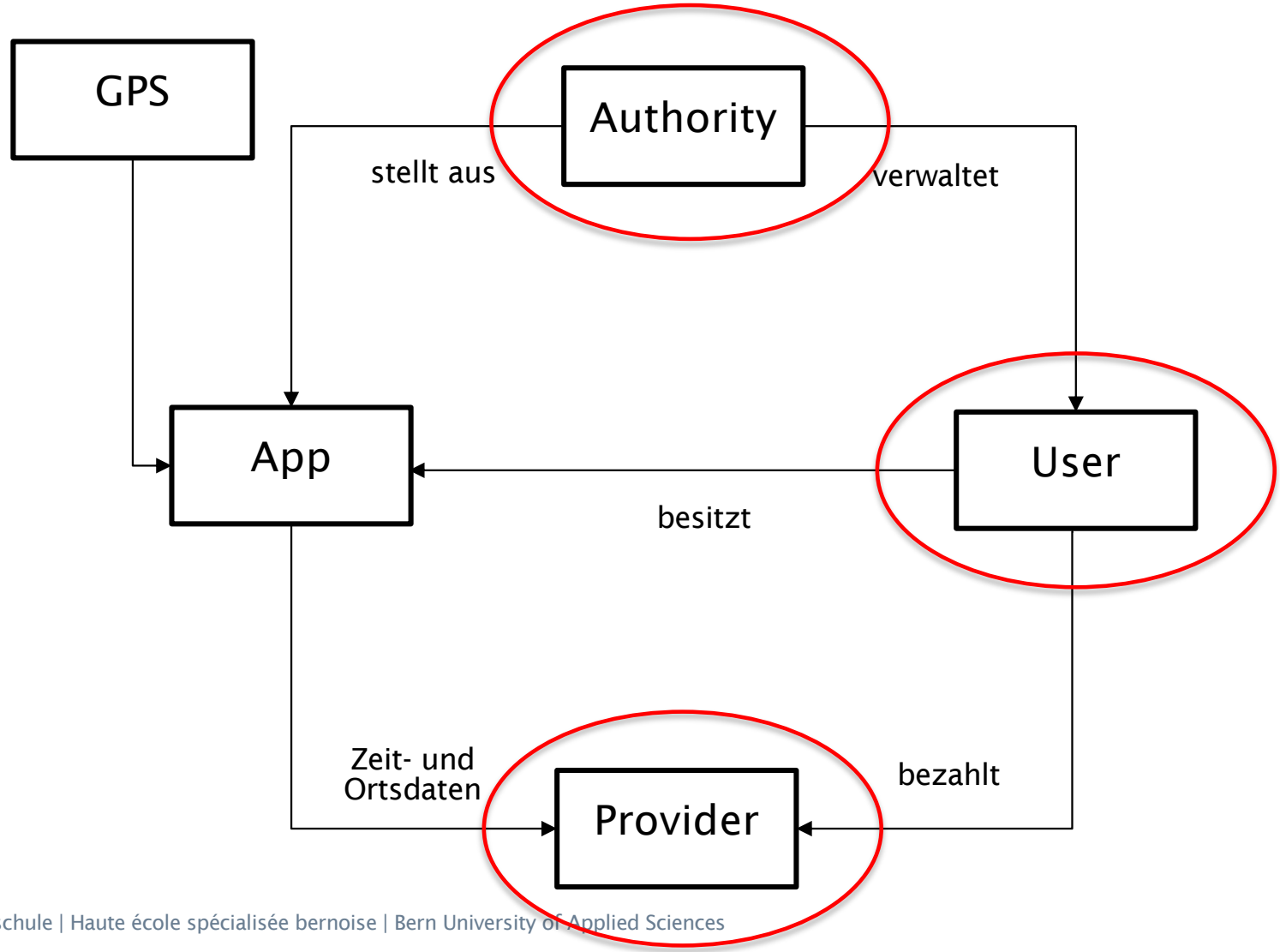
Nur der **Gruppenmanager** kann bei Bedarf mit $gsmk(G)$ die Signatur öffnen und beweisen, dass Alice m signiert hat.

Homomorphe Verschlüsselung

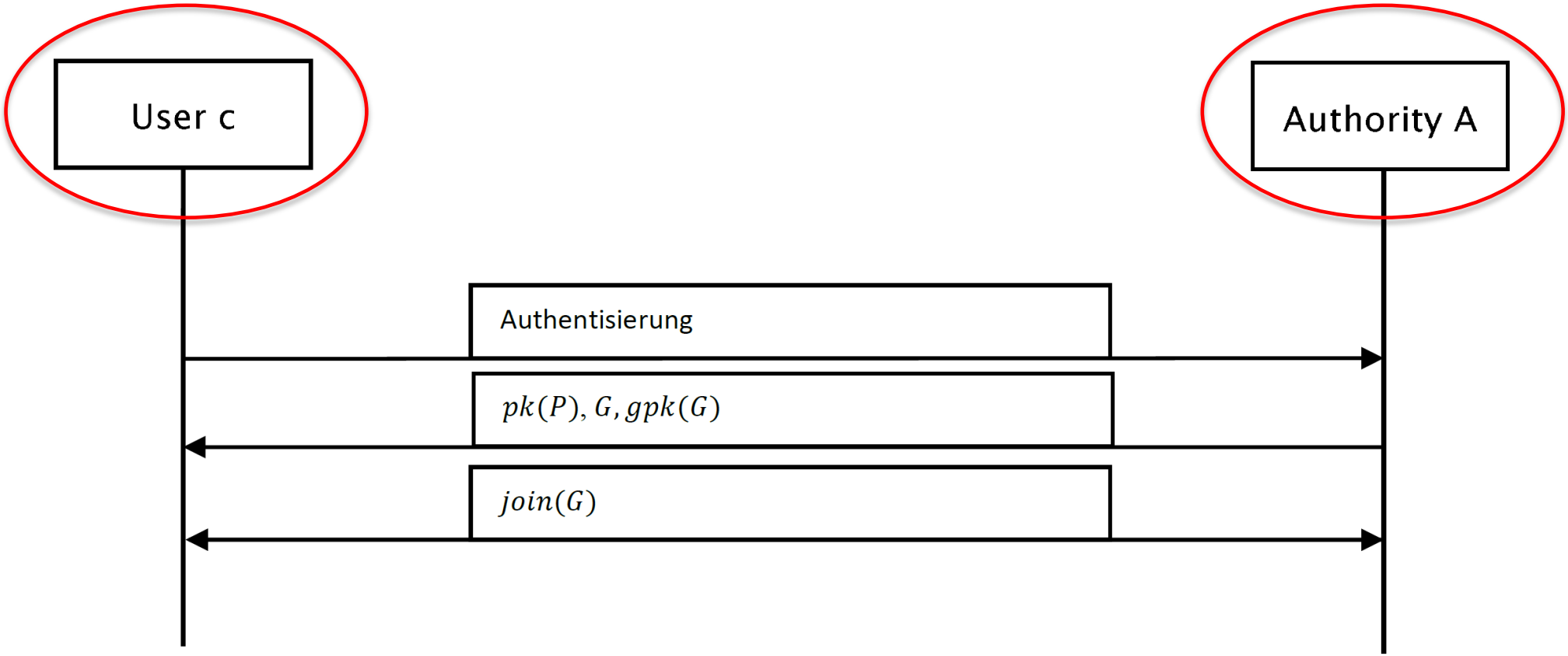
$$\mathcal{E}_X(m_1) \cdot \mathcal{E}_X(m_2) = \mathcal{E}_X(m_1 + m_2)$$

Das Produkt zweier verschlüsselten Nachrichten ist gleich der Verschlüsselung der Summe beider Nachrichten.

Anonymes E-Ticketing kurz erklärt

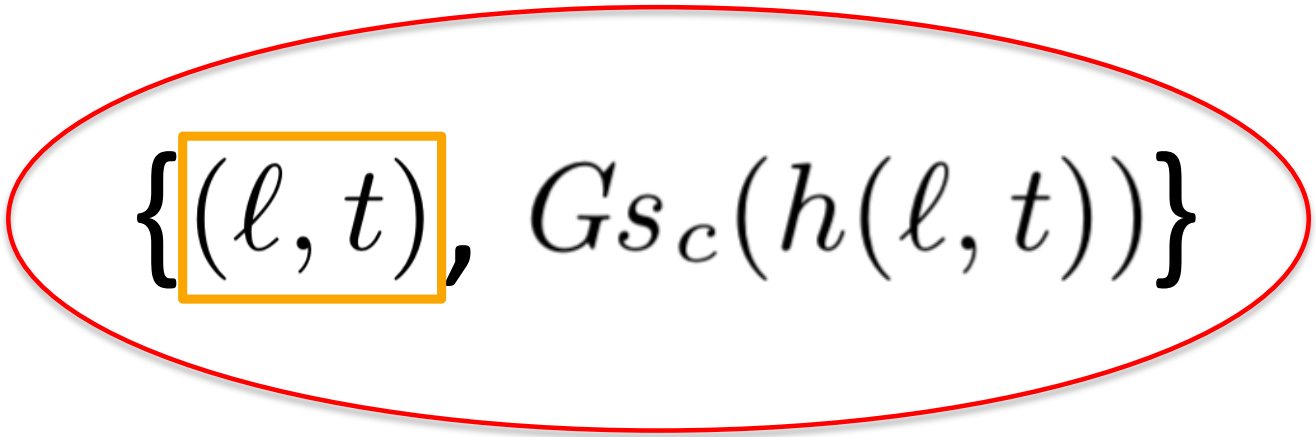

GPS
Authority
stellt aus
verwaltet
App
User
besitzt
Zeit- und
Ortsdaten
Provider
bezahlt

Initialisierung



Beim Reisen…

Die Mobilapplikation sendet Positions-Tupel an den Provider



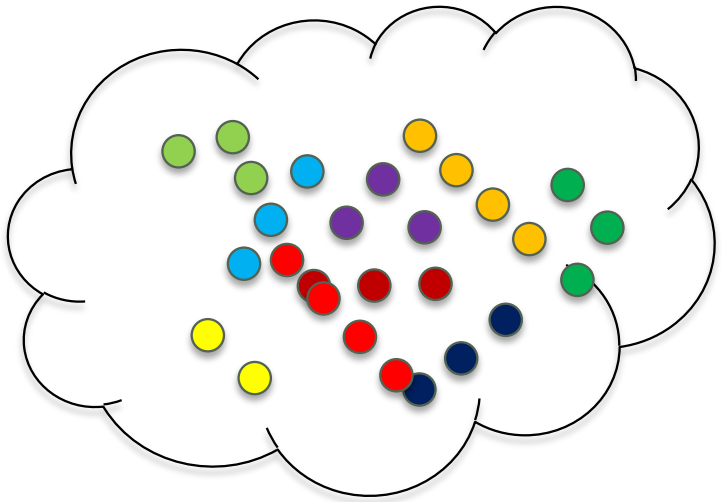
User c

(ℓ, t)

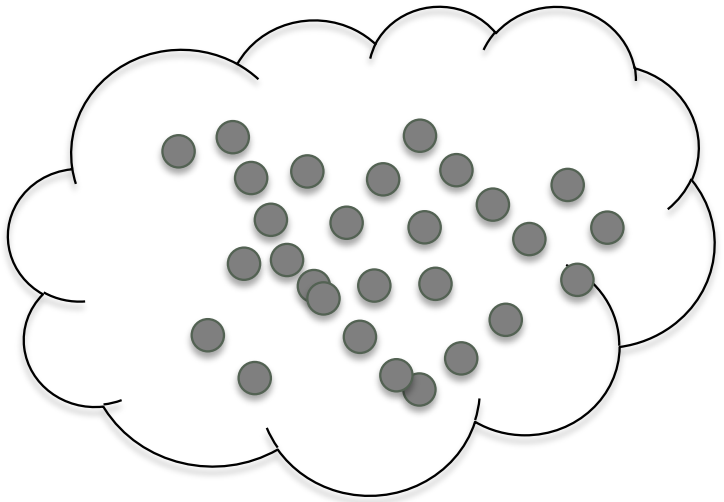
(ℓ, t)

(ℓ, t)

(ℓ, t)

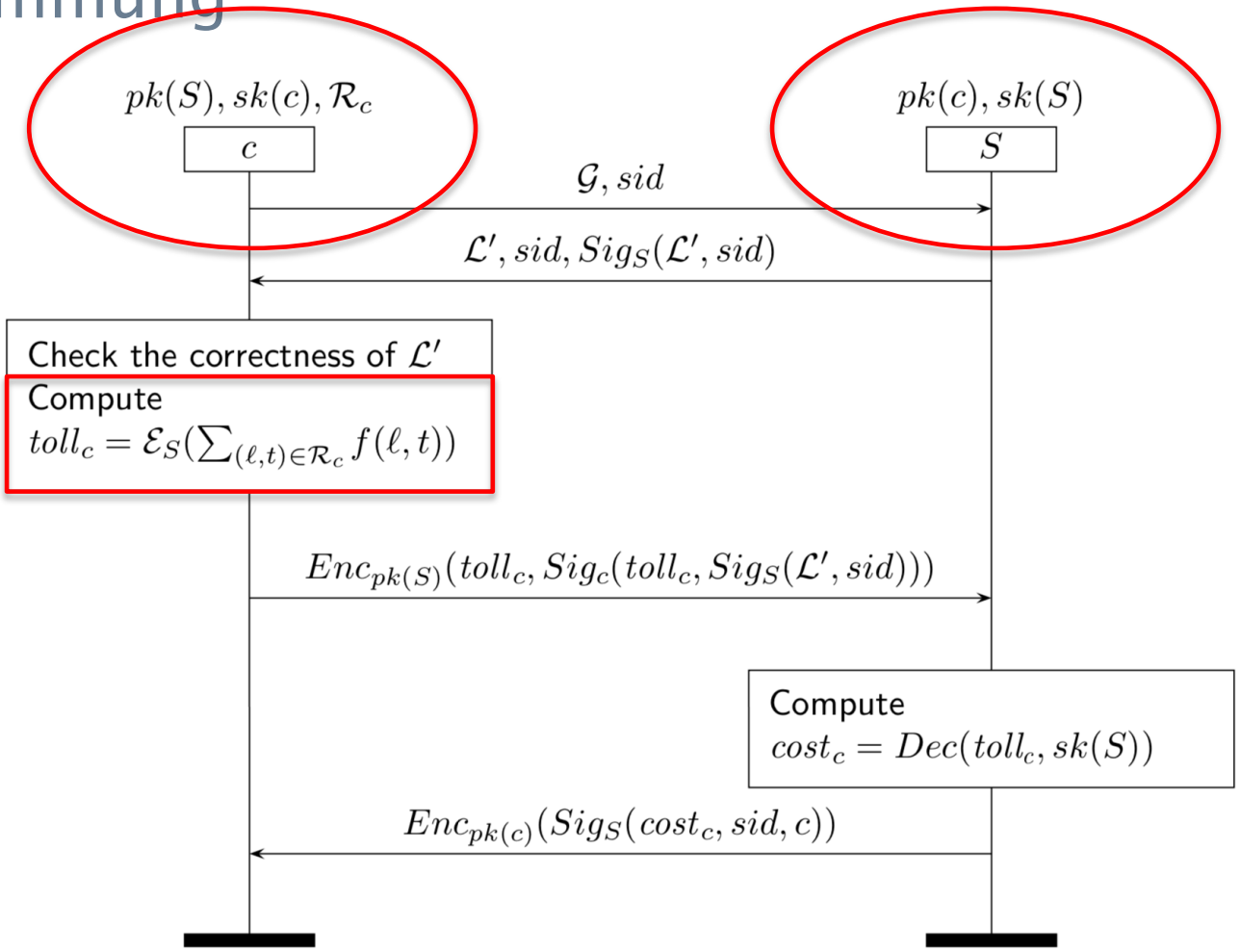


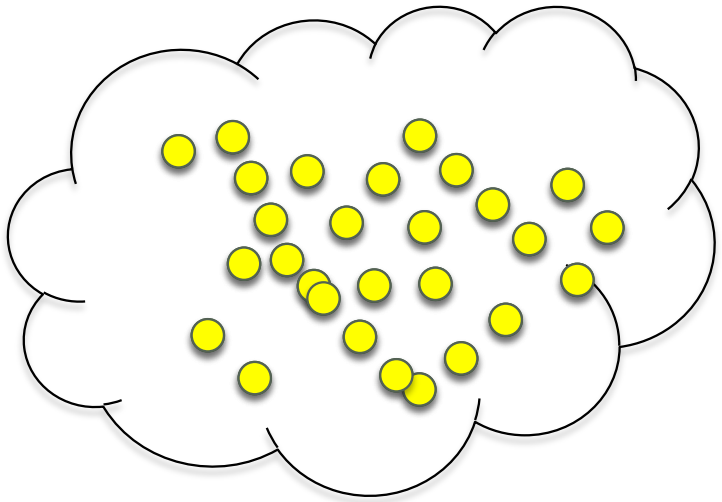
Provider



Provider

Preisbestimmung





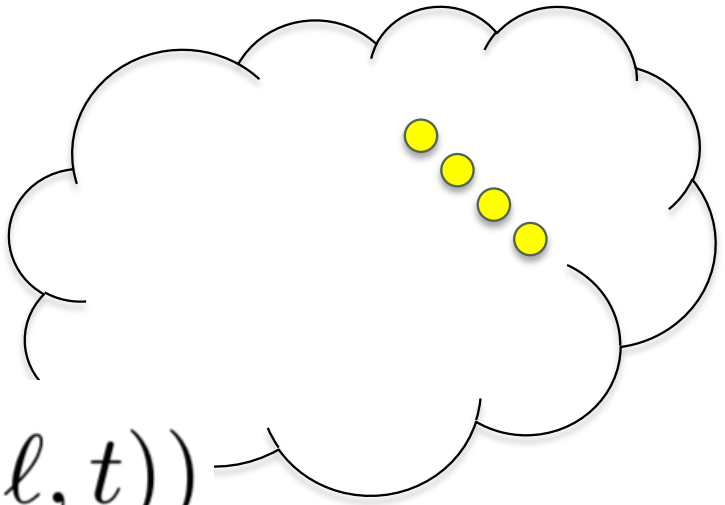
$$\{(h(\ell,t),\mathcal{E}_S(f(\ell,t)))\}$$

Provider

Preis

Alle User berechnen ihre Fahrkosten

User *c*



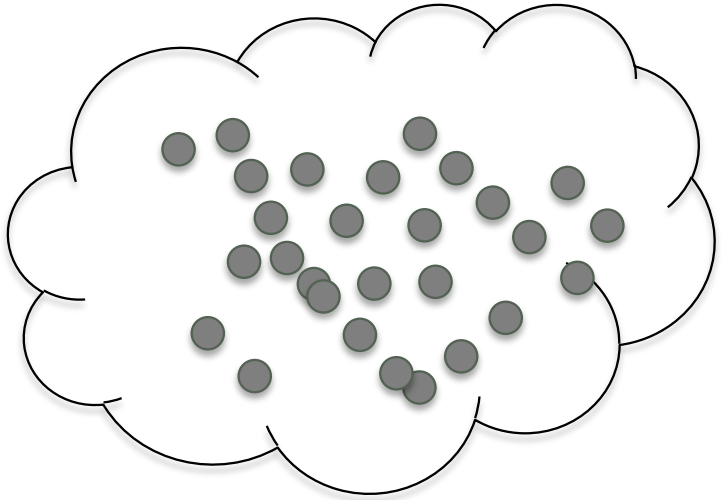
$$toll_c = \prod_{(\ell,t)\in\mathcal{R}_c} \mathcal{E}_S(f(\ell,t))$$

$$toll_c = \mathcal{E}_S(\sum_{(\ell,t)\in\mathcal{R}_c} f(\ell,t))$$

Provider

Preis

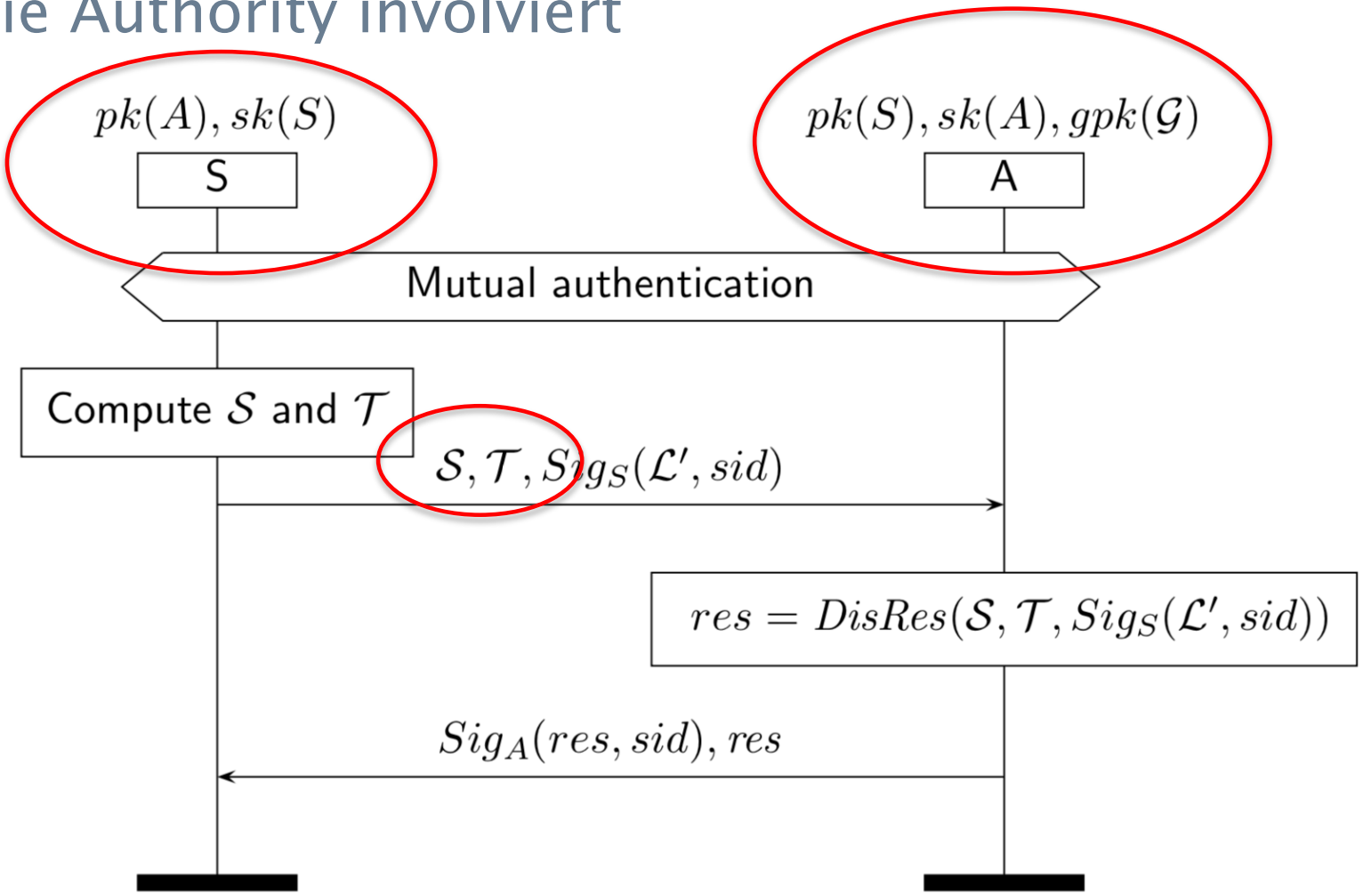
Und beim Streitfall …



Provider

$$\sum_{c \in \mathcal{G}} cost_c \neq \sum_{(\ell,t) \in \mathcal{L}} f(\ell, t)$$

… wird die Authority involviert



$$\mathcal{S} = \{\langle h(\ell, t), \mathcal{E}_S(fee(\ell, t)), G_{\mathcal{S}_c}(h(\ell, t))\rangle \mid \forall (\ell, t) \in \mathcal{L}, \forall c \in \mathcal{G}\}$$

$$\mathcal{T} = \{\langle c, toll_c, Sig_c(toll_c, Sig_S(\mathcal{L}', sid))\rangle \mid \forall c \in \mathcal{G}\}$$

Die Authority berechnet die effektiven *verschlüsselten* Preise

$res := \emptyset;$
$\overline{toll_c} := 0;$
for all $(hashLoc, feeLoc, gsign) \in \mathcal{S}$ **do**
  if VERIFY$(gsign, hashLoc) = false$ **then**
    return 'Faked location signatures' ;
  else
    $c =$OPEN$(gsign)$;
    $\overline{toll_c} :=$ (**if** $\overline{toll_c} = 0$ **then** $feeLoc$ **else** $\overline{toll_c} \cdot feeLoc$);
end for
for all $\overline{toll_c} \neq toll_c$ **do**
  $res := res \cup \{(c, \overline{toll_c})\}$;
end for

- Preis, verschlüsselt

Erreichte Schutzziele

- Der Provider weiss nicht, welche Wege die User *c* gefahren sind
- Die Autorität erfährt auch im Konfliktfall nicht, welche Wege die User *c* gefahren sind
- Der betrügerische User c wird entdeckt

Wozu die Cyberforensik?

Aus Wikipedia…

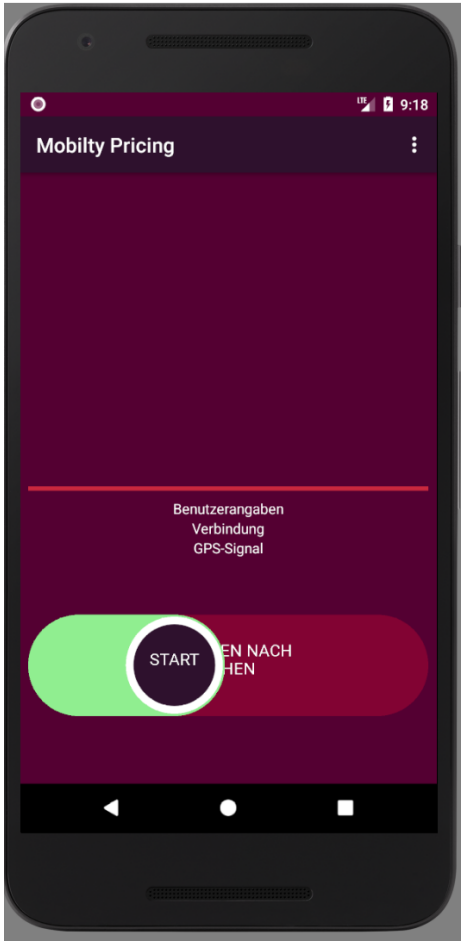
[…] IT-Forensik [bezeichnet] die *wissenschaftliche Expertise*, die eine Beurteilung und Würdigung von Informationstechnik durch die Öffentlichkeit oder innerhalb eines Gerichtsverfahrens ermöglicht.

Bild: security-insider.de

Untergebiete der Cyberforensik [Quelle: Wikipedia]

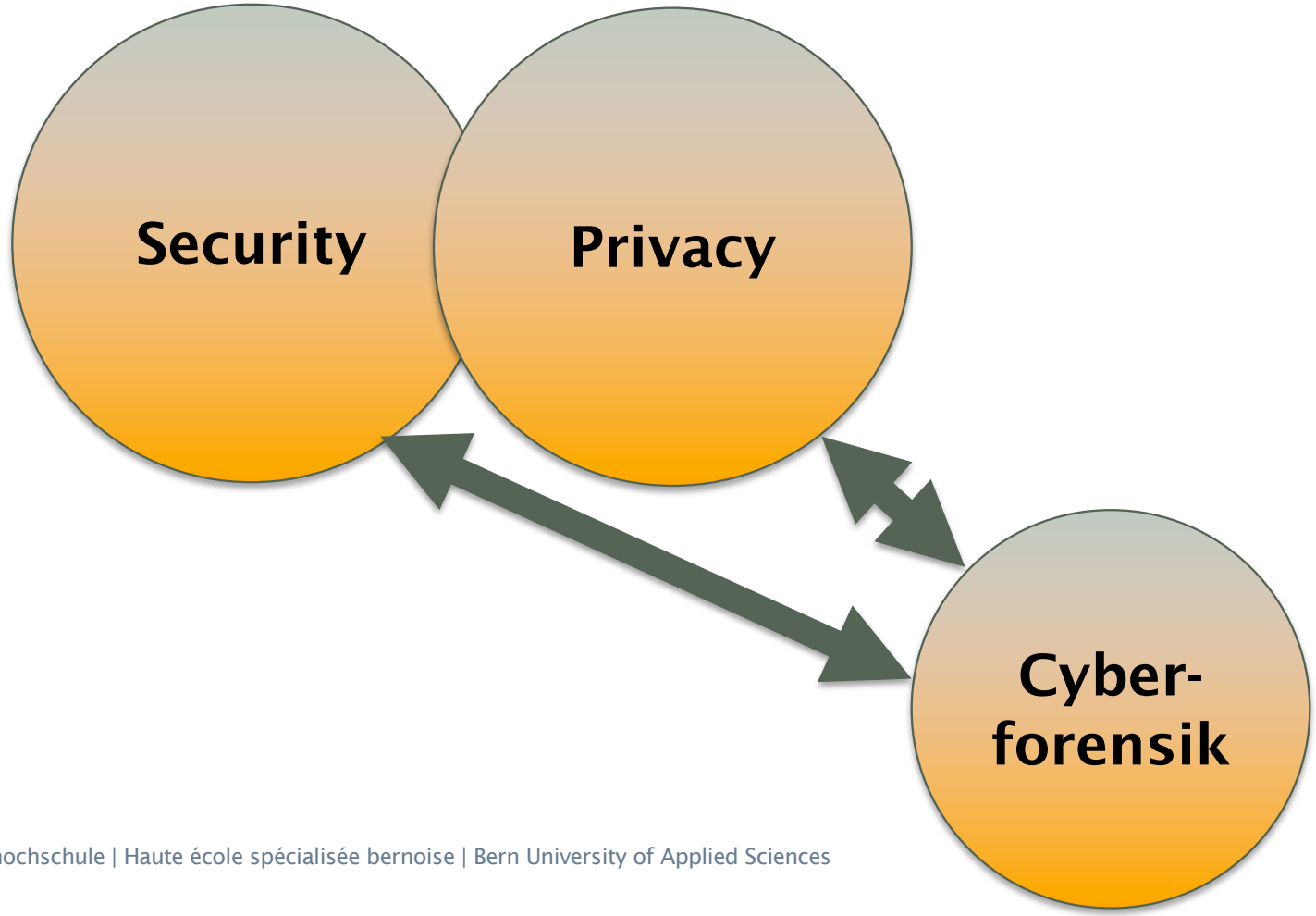
- Betriebssystem-Forensik
- Cloud-Forensik
- Digitale Multimediaforensik
- Malware-Forensik
- Netzwerk-Forensik

- *Smartphone-Forensik*



Take away

Wie stehen Security, Privacy und Forensik zueinander?



Take away

- (Hypothese) Privacy wird mehr und mehr ein Thema
- (Mehr) Privacy ist machbar
- Security und Privacy zu kombinieren, ist schwierig, aber (oft) machbar

Das heisst auch:

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

Zur Forensik:

- Es braucht sie, aber:
- (Hypothese) Es wird immer schwieriger…

Eric Dubuis
eric.dubuis@bfh.ch

RISIS
risis.bfh.ch