UNIVERSITÄT PASSAU

Kryptographie – die neue Generation sicherer Cloud-Services?

Henrich C. Pöhls

@henrichpoehls

Universität Passau

prisma cloud

UNIVERSITÄT PASSAU

Existierende kryptographische Methoden werden bisher

nicht (konsequent genug)

zum Schutz der Cloud-Anwender genutzt

Herausforderungen

- EU Datenschutz-Grundverordnung (GDPR)
- Quantum Computing
- Gesteigertes Verlangen nach Vertraulichkeit
- Daten-Authentizität in Multi-Cloud-Anwendungen

Forschungs-Projekt www.PRISMACLOUD.eu

UNIVERSITÄT PASSAU

Entwurf und Entwicklung von praxis-tauglicher Kryptographie zur Sicherung von Cloud-Services

Atos

etra I+D

IBM

interoute
from the ground to the cloud

MIKROPLAN

XITRUST
SECURE TECHNOLOGIES

LOMBARDIA INFORMATICA

FCSR
Fondazione
CENTRO SAN RAFFAELE

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

cea leti

TECHNISCHE UNIVERSITÄT DARMSTADT

UNIVERSITÄT PASSAU

Newcastle University

IAIK TU Graz

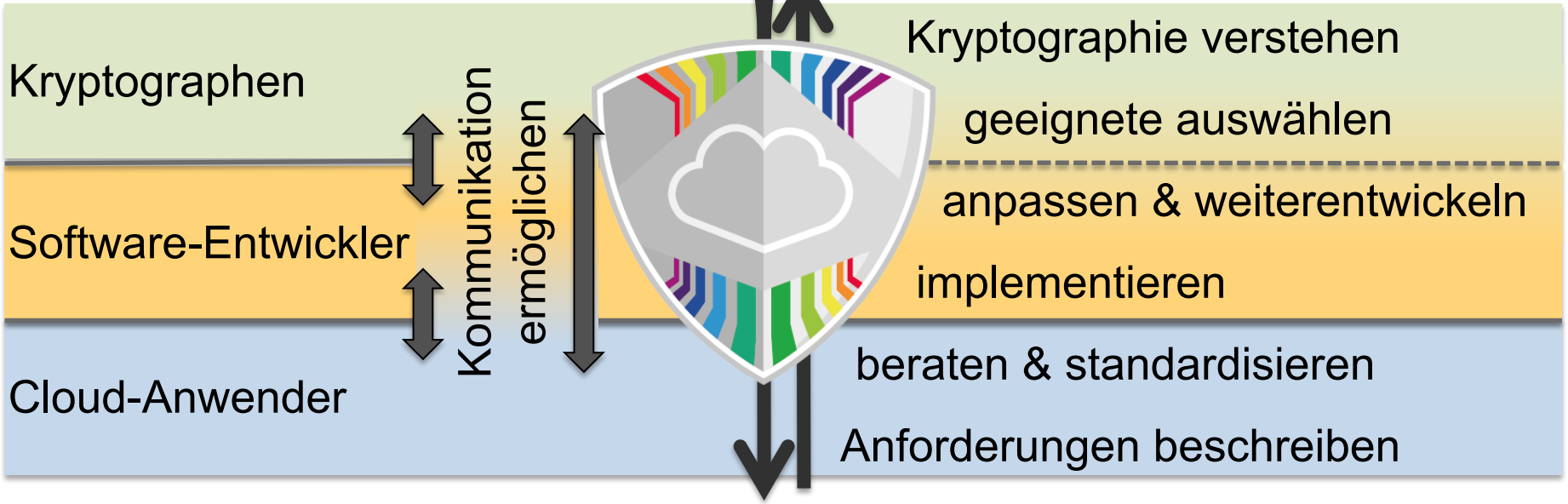
KARLSTADS UNIVERSITET

Unil
UNIL | Université de Lausanne

prisma cloud

UNIVERSITÄT PASSAU

cryptographic mechanisms



cryptographically enhanced cloud services

2 Probleme

1. **Datensparsamkeit durch Schwärzen von authentischen Medizindaten**

2. **Gemeinsamer Zugriff auf vertrauliche Daten in der Cloud**

2 Beispiele

1. **Redactable Signature Schemes (RSS)**

– 2001/2002: Steinfeld et al. [SBZ], Johnson et al. [JMDW].

– Ermöglicht Authentizitätsprüfung von signierten Dokumenten, aufgeteilt in bestimmte Teile, obgleich einzelne Teile nachträglich geschwärzt wurden

→ Verifizierbare **Integrität (**  **) &** gleichzeitig **Datensparsamkeit (**  **)**

2. **Secret Sharing Schemes (SSS)**

– 1979: Shamir's Secret Sharing [Shamir]

– Dokument wird umgewandelt in "Shares", einzelner Share enthält keine Information, erst aus einer festgelegten Menge von Shares, z.B. 2/3, rekonstruiert sich das Dokument

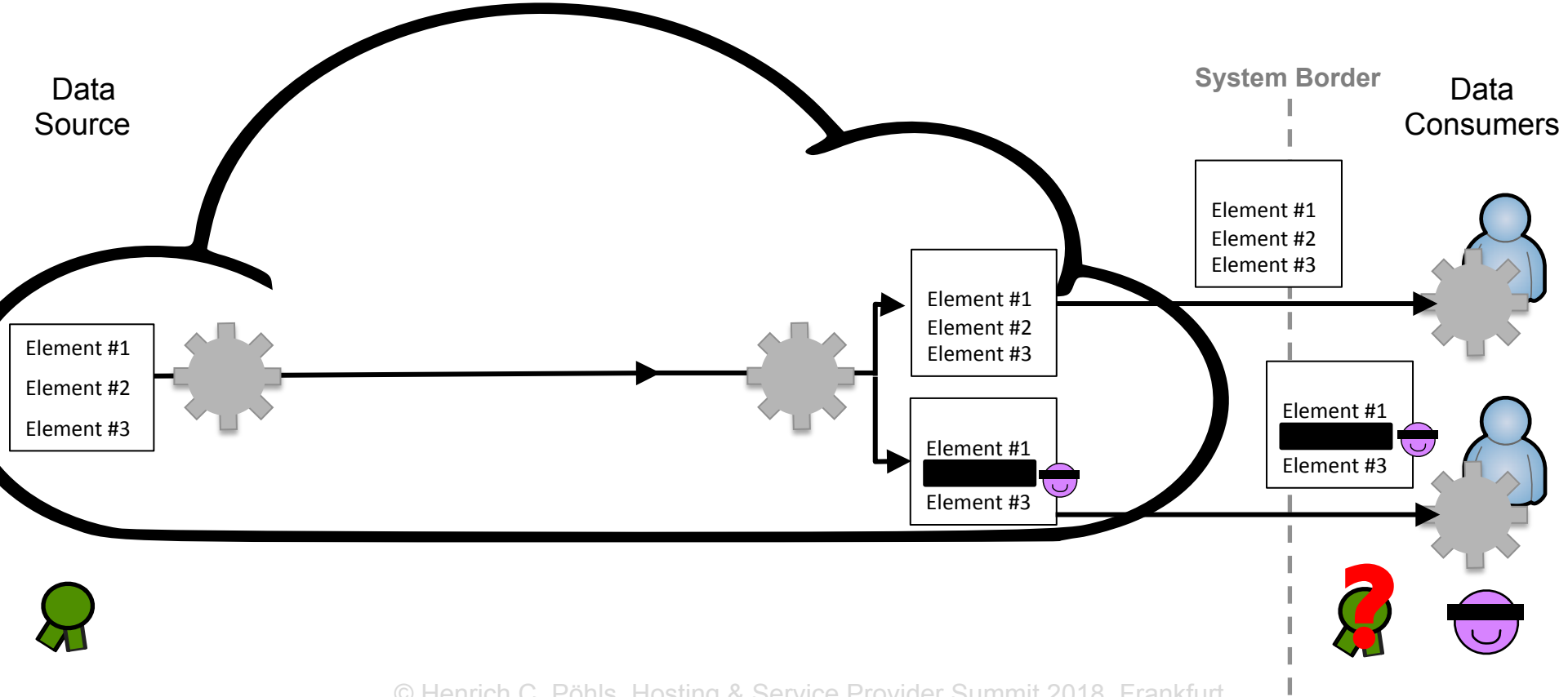
→ Schutz der **Vertraulichkeit (**  **) &** erhöhte **Verfügbarkeit (** **)**

[SBZ] R. Steinfeld, L. Bull, and Y. Zheng. Content extraction signatures. In Proc. of International Conference on Information Security and Cryptology (ICISC 2001). Springer, 2002.

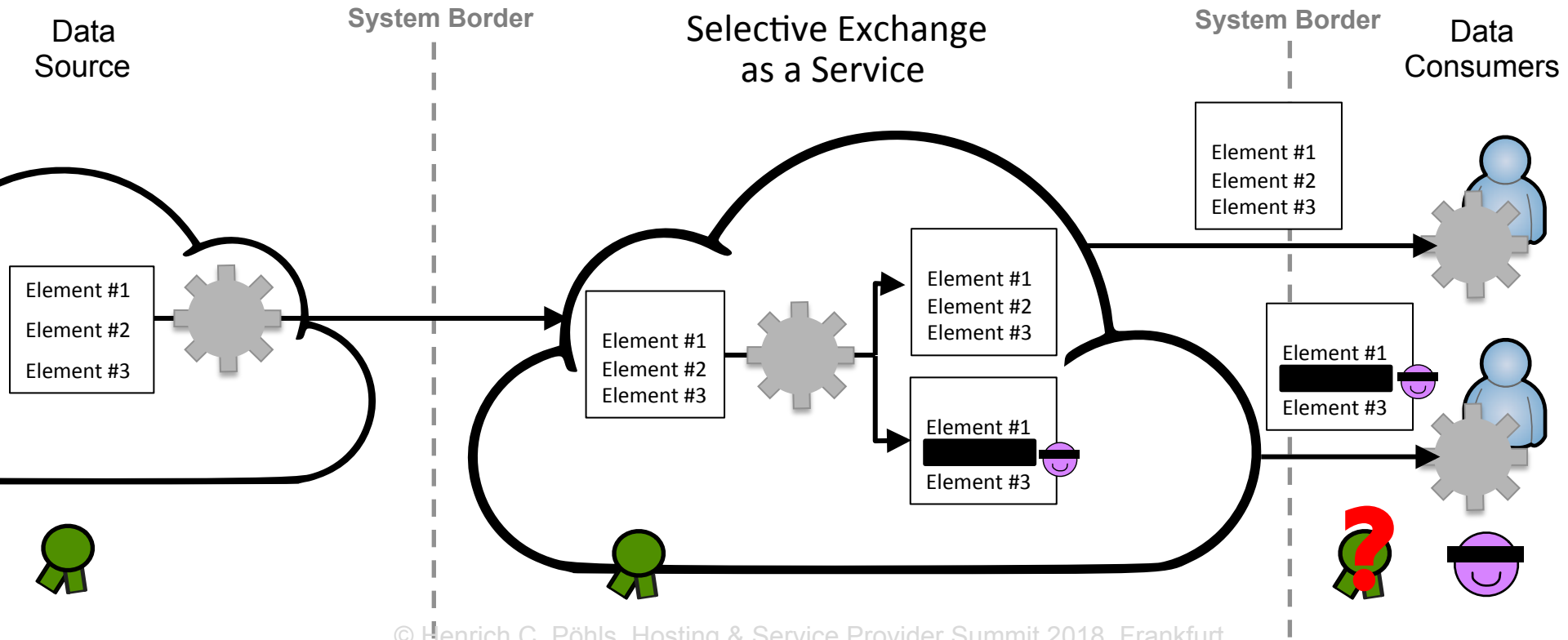
[JMDW] R. Johnson, D. Molnar, D. Song, and D. Wagner. Homomorphic signature schemes. In Proc. RSA Security Conference - Cryptographers Track. Springer, 2002.

[Shamir] A. Shamir: How to share a secret. In: Communications of the ACM, vol. 22. ACM, 1979.

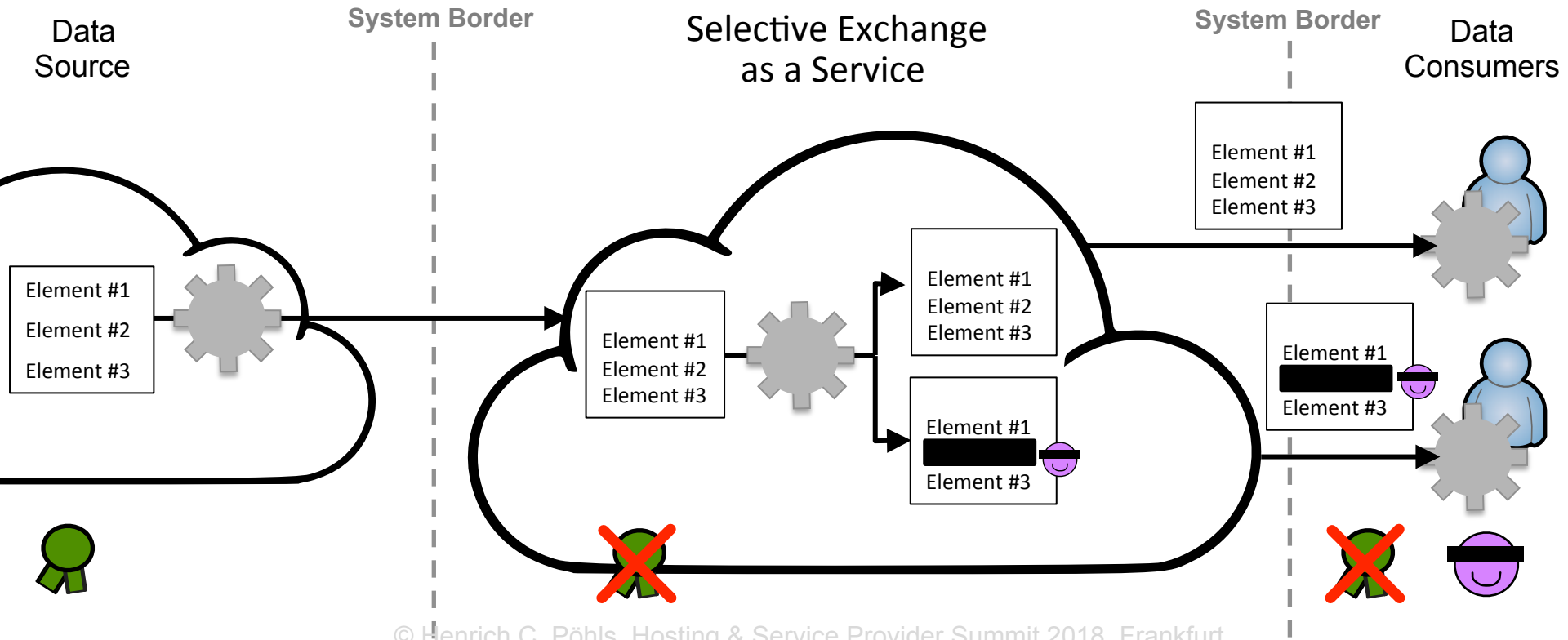
Redactable Signature



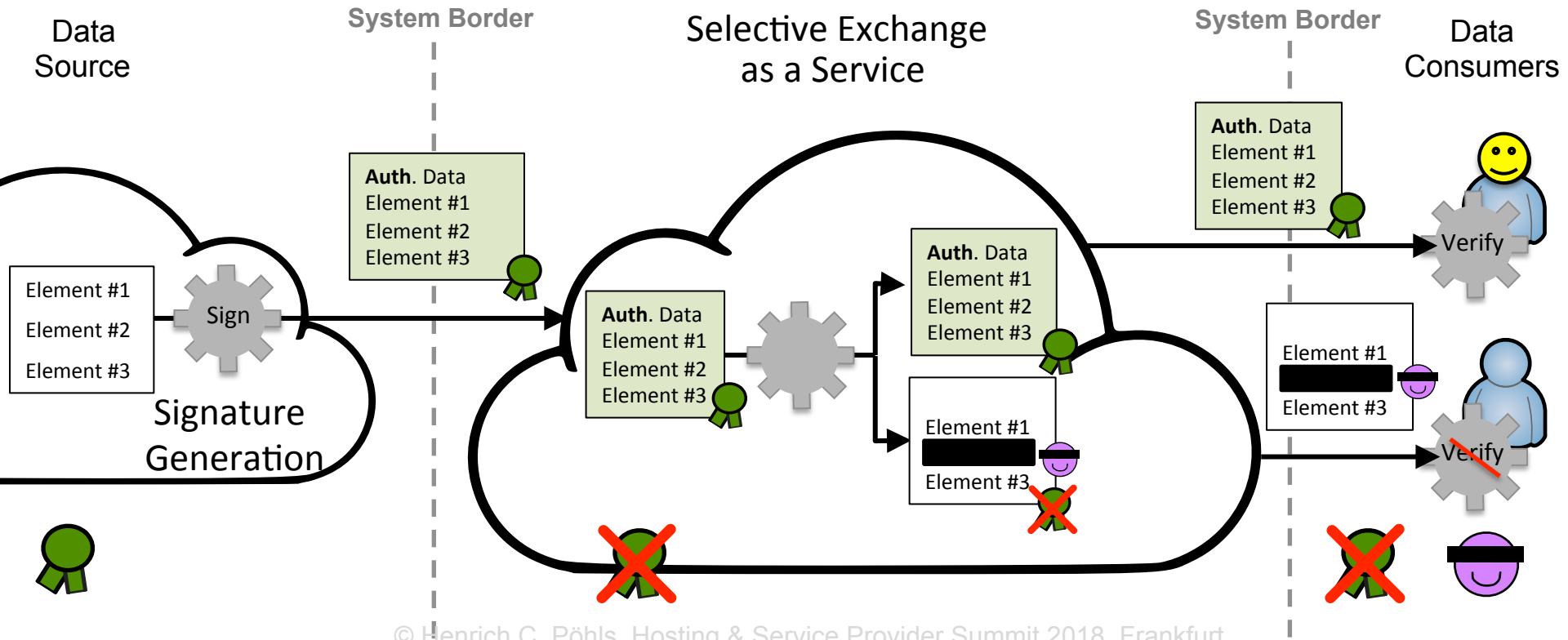
Redactable Signature



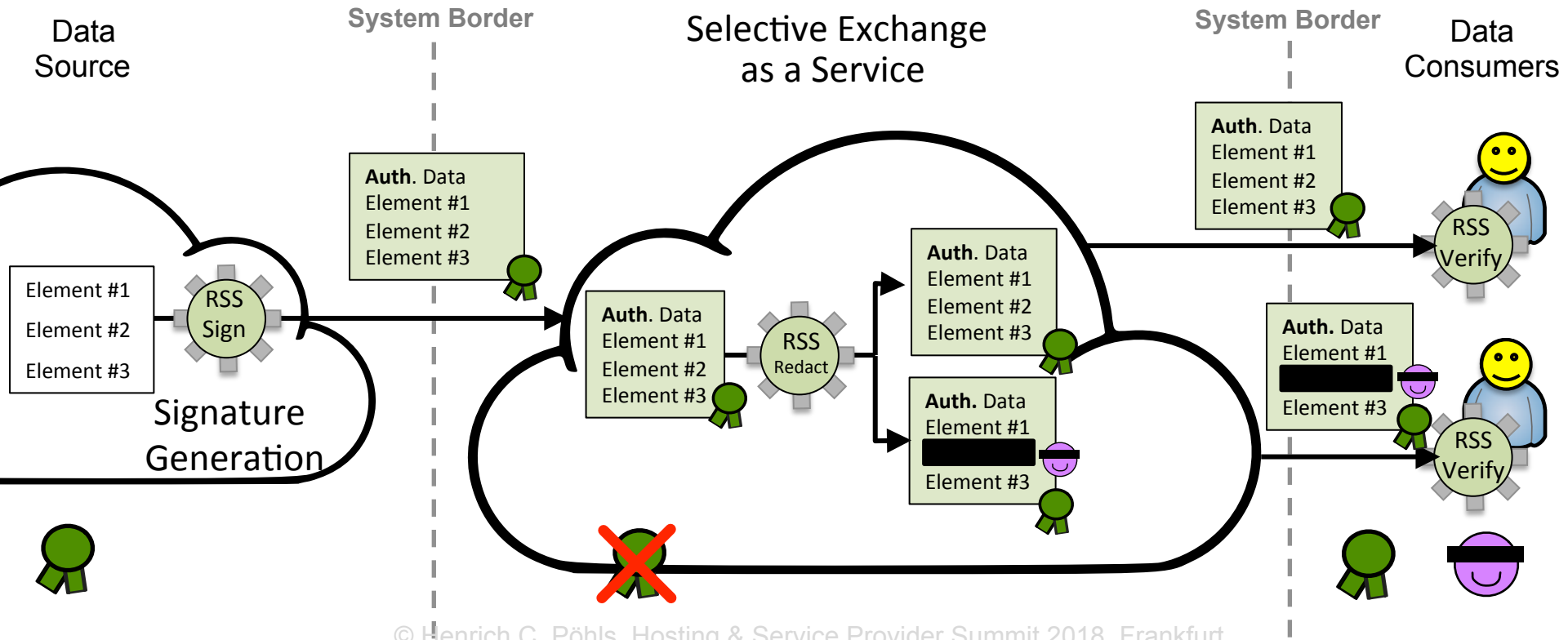
Redactable Signature



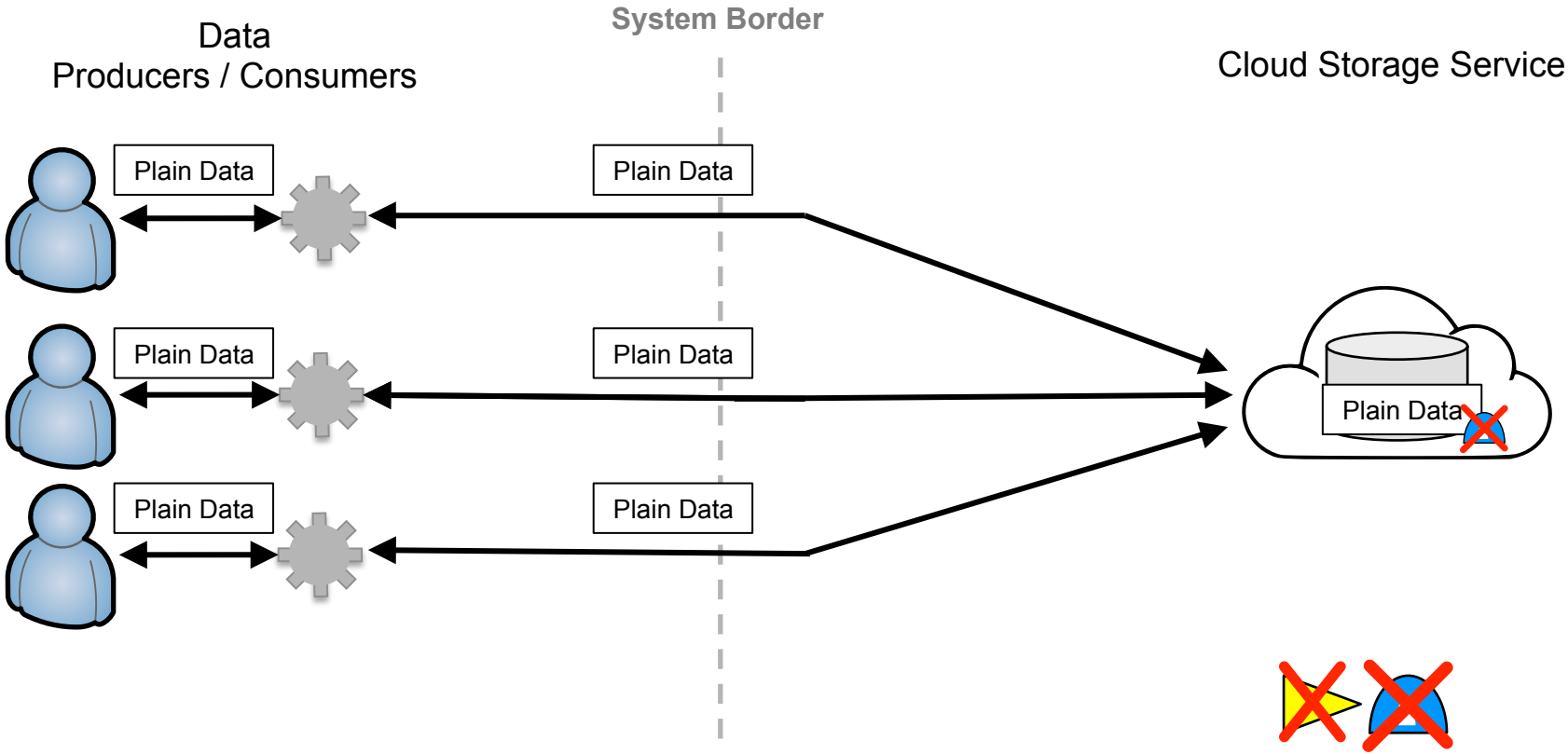
Redactable Signature



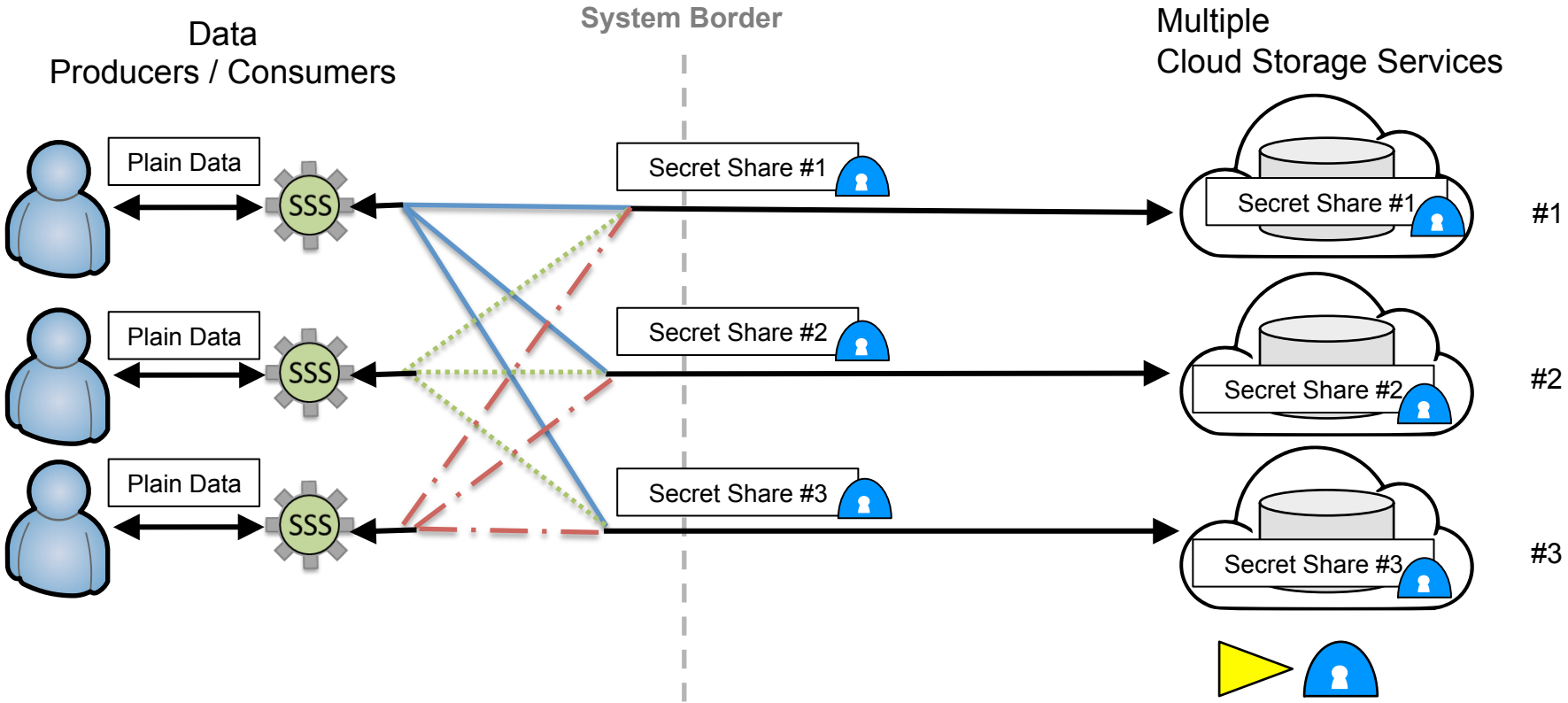
Redactable Signature



Secret Sharing



Secret Sharing



Kryptographie “hilft”

- Passende Kryptographie existiert oft und ist praxis-tauglich implementierbar
  - Redactable Signature Schemes
  - Secret Sharing Schemes
- Entwicklung einsetzbarer Kryptographie braucht Kommunikation zwischen verschiedenen Stakeholdern
  - Kryptographen ↔ Software-Entwickler ↔ Cloud-Anwender
- Kryptographie unterstützt bei der Einhaltung der EU Datenschutz-Grundverordnung (GDPR) → Sichert bestehende Absatzmärkte
- kryptographische Sicherheitszusagen statt “nur” rechtliche Zusicherung → neue technische Anreize für den Weg in die Cloud → Neue Märkte

Danke! Henrich C. Pöhls @henrichpoehls

@prismacloud

https://prismacloud.eu

@henrichpoehls

http://henrich.poehls.com

hp@sec.uni-passau.de