GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

[code blau] security concepts

[1] Code Blau GmbH

Freie Universität Berlin

[2] Freie Universität Berlin

Gefördert von der EU im Rahmen des NGI Pointer Programmes, Projekt: *AP*³

Projekt: *Concrete Contracts*
concretecontracts.codeblau.de

Alt genug, um das zu kaufen?

Altersrestriktion mit Datenschutz im E-Commerce

Özgür Kesim[1,2] oec@codeblau.de @oec@mathstodon.xyz

Matthias Wählisch[2] m.waehlisch@fu-berlin.de

Problemstellung

Wie können wir das Mindestalter in E-Commerce-Anwendungen verifizieren und dabei Datenschutz und die Privatsphäre eines Kunden bewahren?

Wir wollen ein Schema zur Altersrestriktion spezifizieren und implementieren, welches

1. an die **Zahlungsfähigkeit** gekoppelt ist,
2. die **Unverknüpfbarkeit von Käufen** garantiert,
3. das **Prinzip der Subsidiarität** anwendet und
4. **praktisch und effizient** ist.

Ansatz: Spezifikation eines Schemas und Implementierung eines Proof-of-Concepts in GNU Taler, einem datenschutzfreundlichen, elektronischen Bezahlsystem.

Relevanz der Lösung

Bisherige Verfahren zur Altersverifikation sind nicht datenschutzfreundlich, verletzen die Privatsphäre von Personen oder basieren auf Identitätsmanagement-Systemen (IDM), die einer externen Autorität bedürfen, oder beides.

Unser Verfahren im Vergleich:

	bisher	unser Ansatz
schützt die Privatsphäre	(✓)	✓
kommt ohne IDM aus	(✓)	✓
basiert auf Subsidiarität	✗	✓
effizient und praktikabel	✗	✓

Bisherige Ergebnisse

- Schema zur Altersrestriktion in GNU Taler ab Version 0.9.0 verfügbar [1]
- Verwendet Signaturverfahren Edx25519 [2]
- Wirksamkeit, Sicherheit und Effizienz analysiert [2]

Ausblick

- Nicht-subsidiärer Fall spezifiziert [3]
- Implementierung in GNU Taler folgt

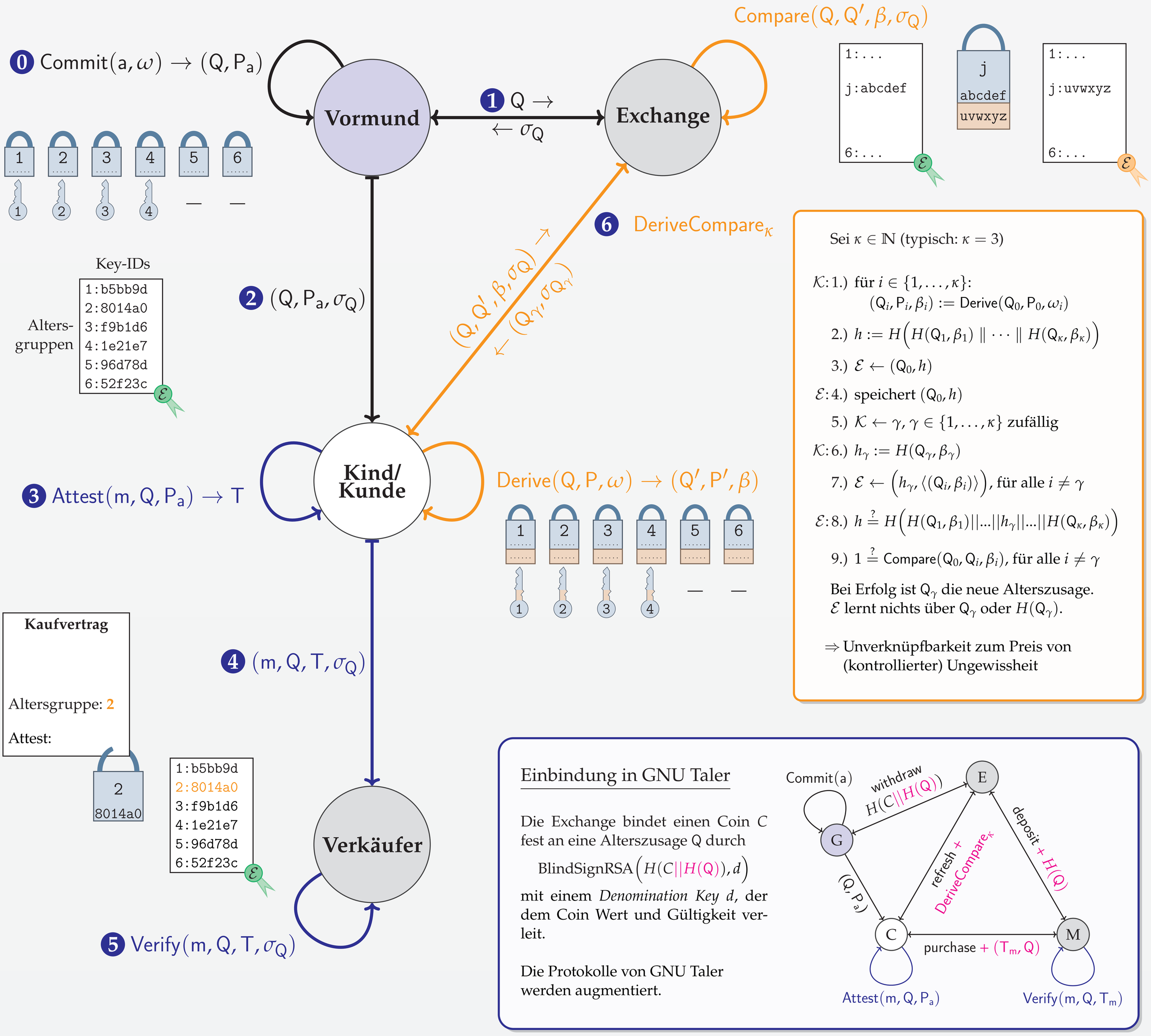
Referenzen

[1] *GNU Taler – Softwarequellen*. URL: https://git.taler.net/.

[2] Özgür Kesim u. a. "Zero-Knowledge Age Restriction for GNU Taler". In: *Computer Security – ESORICS 2022*. Springer International Publishing, 2022, S. 110–129. URL: https://taler.net/papers/esorics2022-age-restriction.pdf.

[3] *Design Document 24: Anonymous Restriction Extension for GNU Taler*. URL: https://docs.taler.net/design-documents/024-age-restriction.html#withdraw.

Schema für die Altersrestriktion im subsidiären Fall



Sei $\kappa \in \mathbb{N}$ (typisch: $\kappa = 3$)

$\mathcal{K}$: 1.) für $i \in \{1, \ldots, \kappa\}$:
$(Q_i, P_i, \beta_i) := \mathsf{Derive}(Q_0, P_0, \omega_i)$

2.) $h := H\Big(H(Q_1, \beta_1) \parallel \cdots \parallel H(Q_\kappa, \beta_\kappa)\Big)$

3.) $\mathcal{E} \leftarrow (Q_0, h)$

$\mathcal{E}$: 4.) speichert (Q_0, h)

5.) $\mathcal{K} \leftarrow \gamma, \gamma \in \{1, \ldots, \kappa\}$ zufällig

$\mathcal{K}$: 6.) $h_\gamma := H(Q_\gamma, \beta_\gamma)$

7.) $\mathcal{E} \leftarrow \Big(h_\gamma, \langle (Q_i, \beta_i) \rangle\Big)$, für alle $i \neq \gamma$

$\mathcal{E}$: 8.) $h \stackrel{?}{=} H\Big(H(Q_1, \beta_1) || \ldots || h_\gamma || \ldots || H(Q_\kappa, \beta_\kappa)\Big)$

9.) $1 \stackrel{?}{=} \mathsf{Compare}(Q_0, Q_i, \beta_i)$, für alle $i \neq \gamma$

Bei Erfolg ist Q_γ die neue Alterszusage.
$\mathcal{E}$ lernt nichts über Q_γ oder $H(Q_\gamma)$.

⇒ Unverknüpfbarkeit zum Preis von (kontrollierter) Ungewissheit

Einbindung in GNU Taler

Die Exchange bindet einen Coin C fest an eine Alterszusage Q durch

$$\mathrm{BlindSignRSA}\Big(H(C||H(Q)), d\Big)$$

mit einem *Denomination Key* d, der dem Coin Wert und Gültigkeit verleit.

Die Protokolle von GNU Taler werden augmentiert.