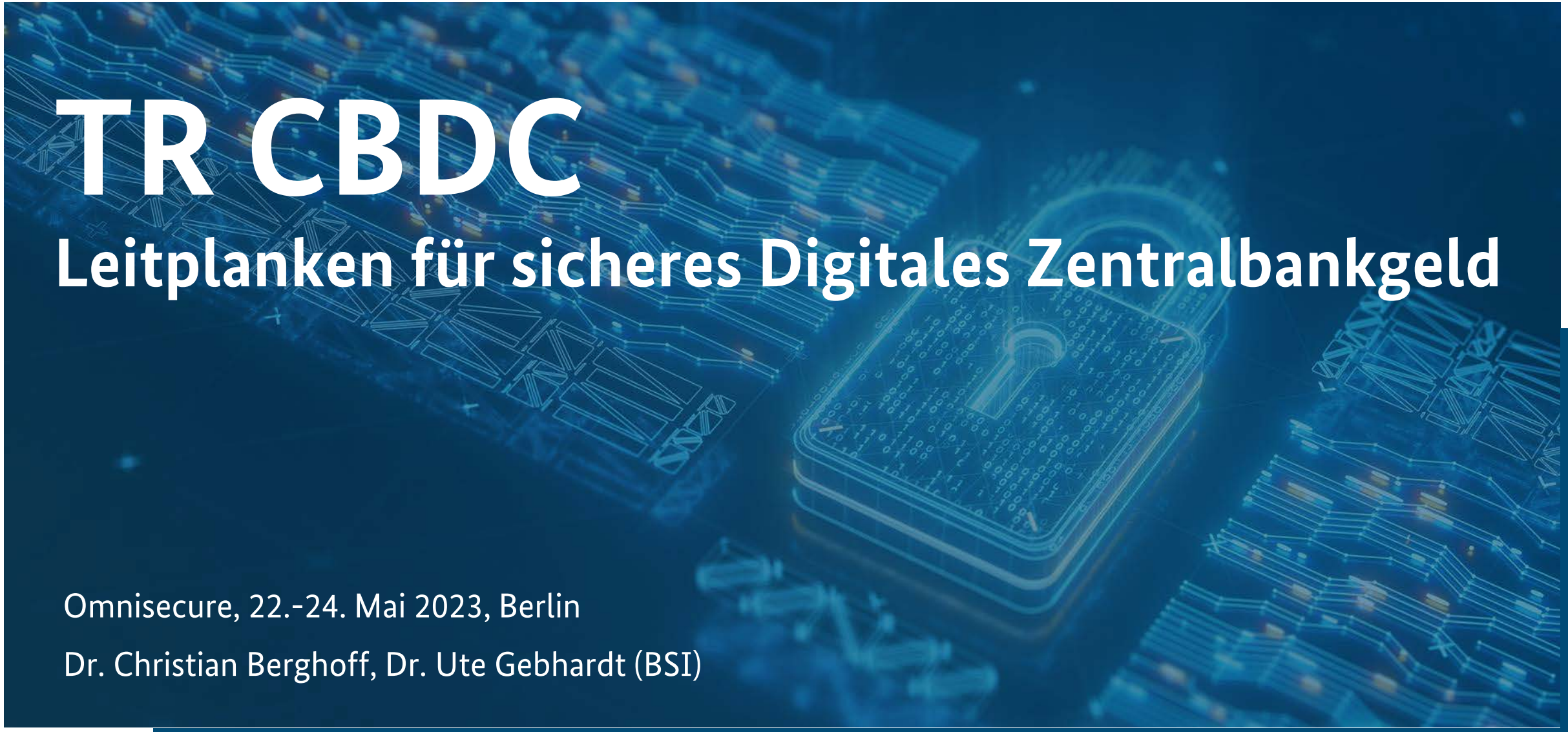
Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•



TR CBDC

Leitplanken für sicheres Digitales Zentralbankgeld

Omnisecure, 22.-24. Mai 2023, Berlin

Dr. Christian Berghoff, Dr. Ute Gebhardt (BSI)

CBDC – Rolle des BSI

- Verschiedene Projekte zu CBDCs (Central Bank Digital Currency) weltweit
- EZB prüft CBDC, positive Entscheidung über Einführung 2023 erwartet
- Viele Diskussionen, aber nicht konkret zur **IT-Sicherheit**
- Digitaler Euro als kritische Infrastruktur → „**Security by design**“ erforderlich
- Neuartige Herausforderungen → kaum Rückgriff auf bestehende Dokumente
- **Aufgabe des BSI**, Anforderungen an IT-Sicherheit zu gestalten

→ **Entwicklung der TR-03179 („TR CBDC“)**

Designziele

Designziele von CBDC

- Digitale Ergänzung zum Bargeld
- Direkte Forderung gegenüber Zentralbank, Kontrolle über Geldmenge
- Weitere je nach politischen Rahmenbedingungen
  - Offline-Zahlungen
  - Anonyme Zahlungen

Mögliche Varianten

- token-basiert vs. kontenbasiert
- Wiederherstellung verlorener Notes möglich?
- …

→ **technologieneutral formulierte Sicherheitsanforderungen**

„Out of Scope“

Nicht in der TR CBDC enthalten sind

- Kryptowährungen
  - *grundsätzlich anderes Konzept*
- Smart Contracts, Programmierbarkeit etc.
  - *zusätzliche Layers aber denkbar*
- Verbindliche Vorgaben zu KYC, AML, DSGVO
  - *Grundkonzepte enthalten*
  - *Details im Einzelfall zu prüfen – in Absprache mit den zuständigen Stellen*

Struktur TR CBDC

TR in zwei Teile gegliedert:

TR 03179-1 „Backend“
Prozesse bei Zentralbank, ggf. Geschäftsbanken

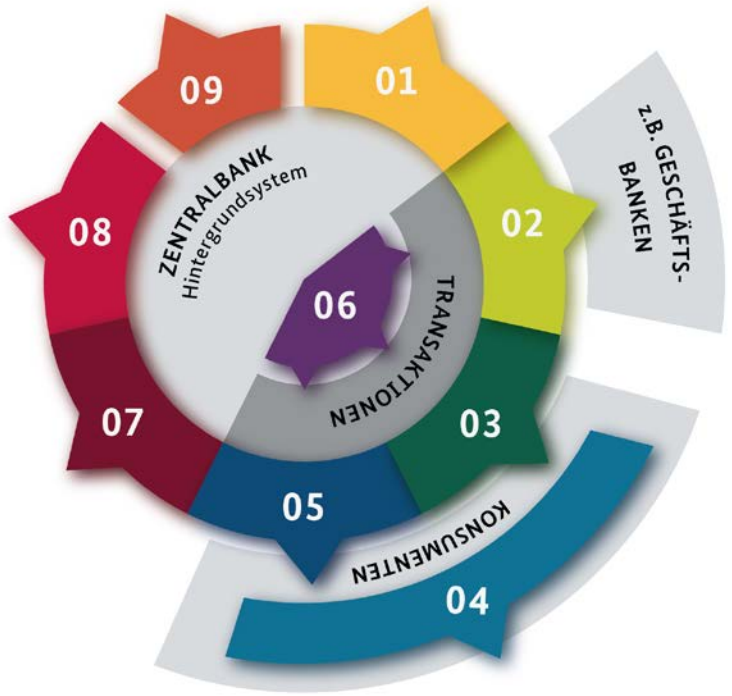
TR 03179-2 „Frontend“
Prozesse beim Nutzer und den Wallets

- Wo möglich, Orientierung an bestehenden Vorgaben
- In vielen Fällen neuartige Anforderungen erforderlich (speziell Backend)

TR CBDC – Backend

Inhalt

- Anforderungen an Prozesse entlang des CBDC-Lebenszyklus
- Übergreifende Sicherheitsanforderungen für verschiedene Transaktionstypen
- Allgemeine Sicherheitsanforderungen (z. B. ISMS, Kryptografie, Personal, IT-Systeme, physische Sicherheit)

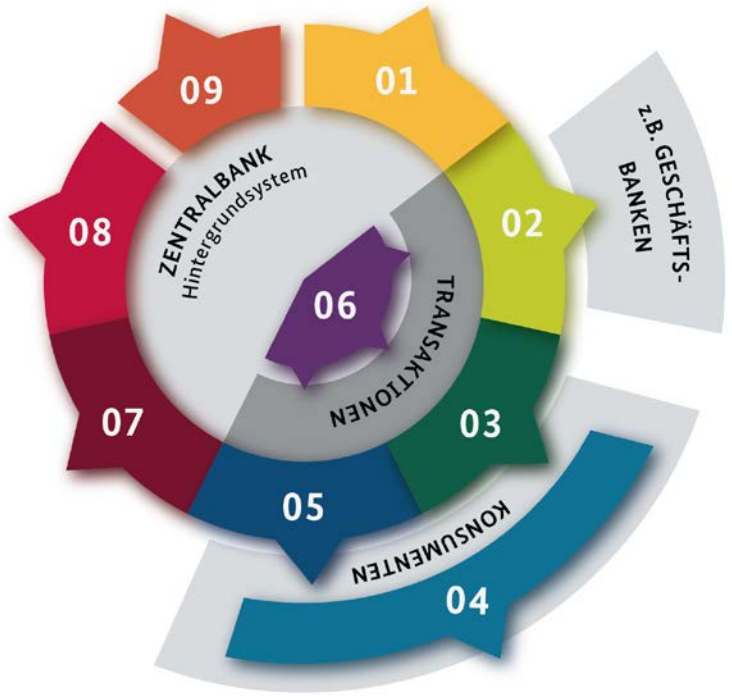


01 ERZEUGUNG
02 VERTEILUNG
03 GELDWECHSEL
04 SPEICHERUNG
05 ZAHLUNG
06 GÜLTIGKEITSPRÜFUNG
07 AKTUALISIERUNG
08 RÜCKRUF
09 WIEDERHERSTELLUNG (OPTIONAL)

TR CBDC – Backend

Herausforderungen

- Double Spending, Gültigkeitsprüfung
- Offline-Zahlungen
- Nachvollziehbarkeit von Zahlungen vs. Privacy
- Updates
- Technologieneutralität der TR



TR CBDC – Frontend

Wallets

- Formfaktoren
- Hardware-Sicherheitsanforderungen
- funktionale Anforderungen
- Accounts und Berechtigungen
- Management von Updates
- …

Transaktionen

- anonym vs. personalisiert
- Nachvollziehbarkeit eigener Transaktionen
- …

Use Cases

- P2P, P2B, M2M,
- …

Aktueller Stand und Ausblick

TR 03179-1 „Backend“

✓ erste Kommentierungsrunden abgeschlossen

> Sommer 2023:
Veröffentlichung eines Community Drafts auf der BSI-Website geplant
→ *Gelegenheit zur Kommentierung*

TR 03179-2 „Frontend“

> Sommer 2023:
erste Kommentierungsrunden geplant

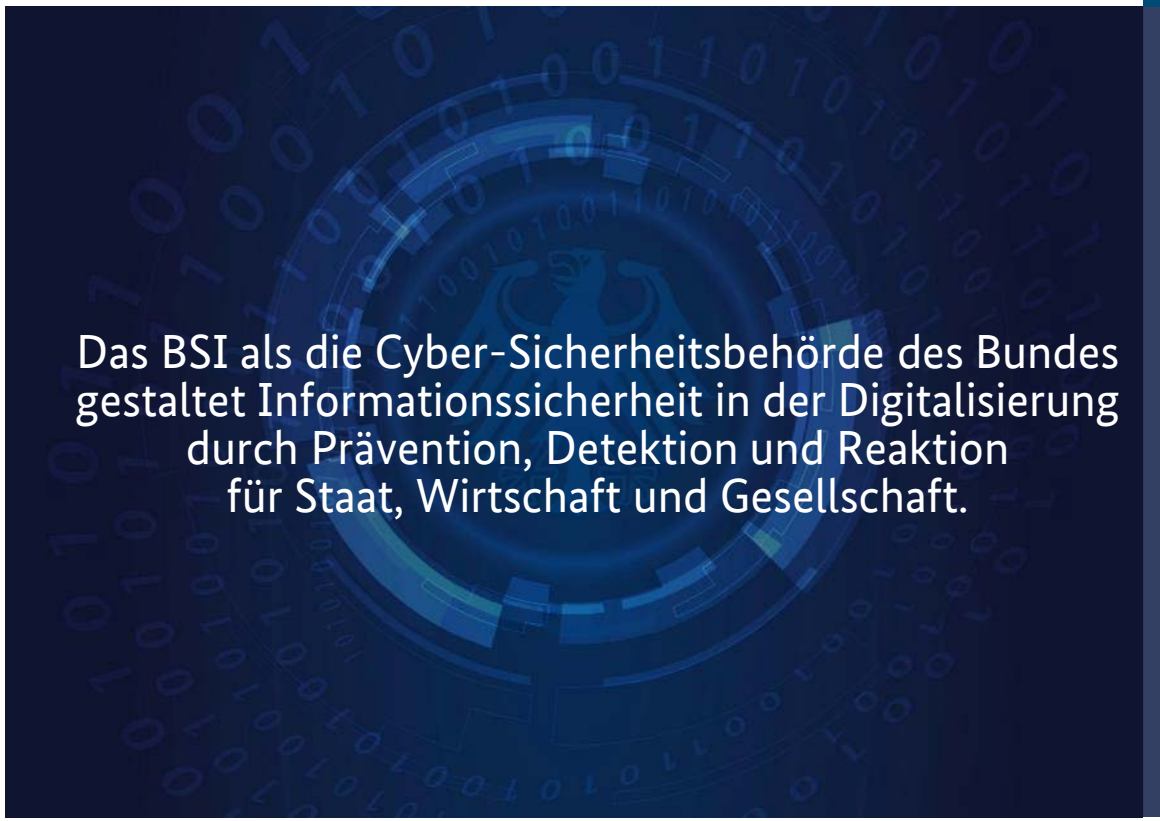
Vielen Dank
für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI•

Kontakt
Dr. Ute Gebhardt
Referentin

ute.gebhardt@bsi.bund.de
referat-di11@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185–189
53175 Bonn
www.bsi.bund.de



Bundesamt
für Sicherheit in der
Informationstechnik