Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

TR-03179 „CBDC“

Leitplanken für sicheres Digitales Zentralbankgeld

Omnisecure, 22.01.2025, Berlin

Sabine Mull, Roland Kirsch – BSI, Referat D24 Gesundheits- und Finanzwesen

Aufgabenbereiche D24 - Finanzwesen

Projektarbeit

- Loyalitycards
- Banking as a Service
- ePayment (Behördenwegweiser)
- LaSiFi (Lagebild zur Cybersicherheit im Finanzwesen)

Arbeitsgruppen

- DIN
  - NaFin
  - Normungsroadmap KI 2
  - Div. DIN Spec.
- Bitkom
- (EU-)Regulierung

Anlassbezogene Tätigkeiten

- TR CBDC (Central Bank Digital Currency)
- TR Anforderungen an Anwendungen im Finanzwesen
- TAN-Verfahren / App-Sicherheit

Veröffentlichungen:
https://www.bsi.bund.de/payment

Wovon sprechen wir?

- CBDC = Central Bank Digital Currency
- Digitales Pendant zu Bargeld
- Von einer Zentralbank herausgegeben
- Verschiedene Projekte zu CBDCs weltweit
- Bewusst keine Beschränkung auf den Euroraum (Digitaler €)

„Out of Scope“

Nicht in der TR CBDC enthalten sind

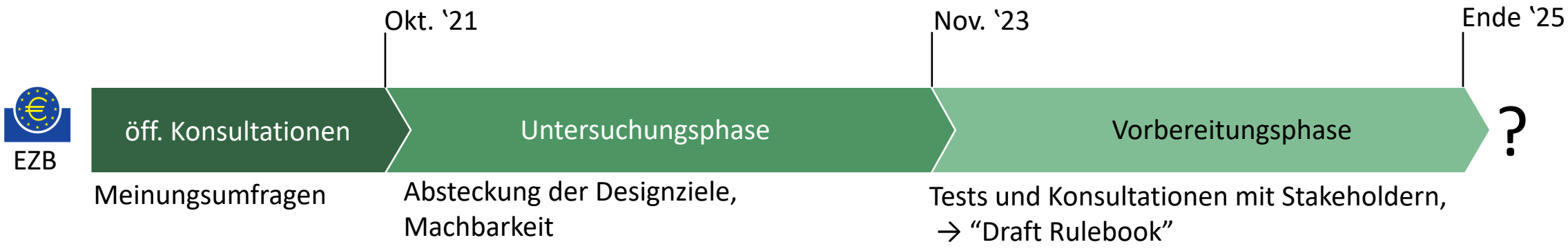
- Kryptowährungen
  - *Grundsätzlich anderes Konzept*
- Smart Contracts, Programmierbarkeit etc. → nicht im Kontext Retail CBDC
  - *Zusätzliche Layers aber denkbar*
- Verbindliche Vorgaben zu KYC, AML, DSGVO
  - *Grundkonzepte enthalten*
  - *Details im Einzelfall zu prüfen – in Absprache mit den zuständigen Stellen*
- Vorgaben der technischen Grundlage wie z.B. Distributed-Ledger-Technologie (DLT) /Blockchain

CBDC – Rolle des BSI

- Verschiedene Projekte zu CBDCs (Central Bank Digital Currency) weltweit
- EZB prüft Einführung des D€, positive Entscheidung über potenziellen Launch im Oktober 2025 erwartet
- Viele Diskussionen, jedoch vordergründig zur Fachlichkeit und zu Usecases
- Zum Startzeitpunkt der Erstellung der TR jedoch 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“)**

Digitaler Euro



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 Walletbetreibern

- Wo möglich, Orientierung an bestehenden Vorgaben
- In vielen Fällen neuartige Anforderungen erforderlich

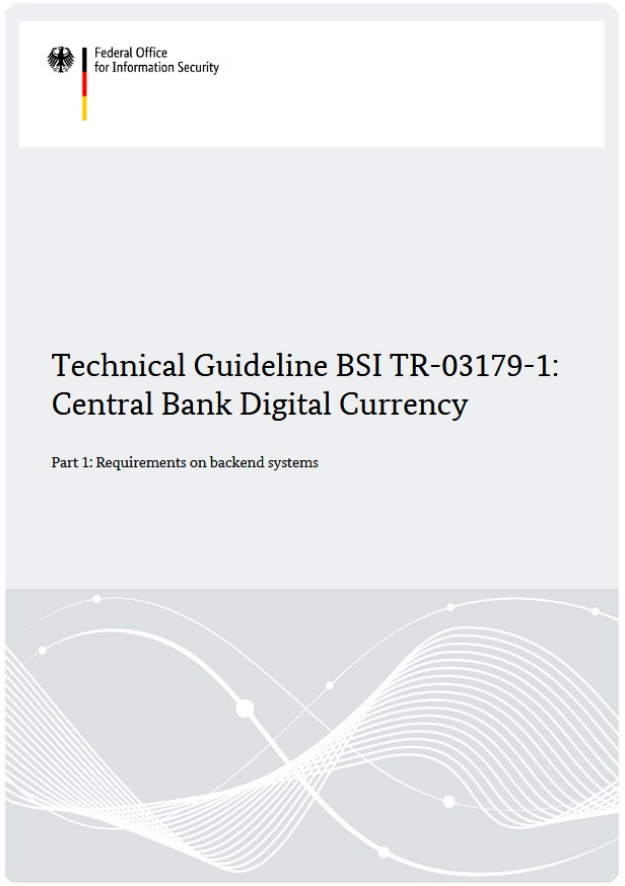
TR CBDC – relevanter Lebenszyklus

Inhalt

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

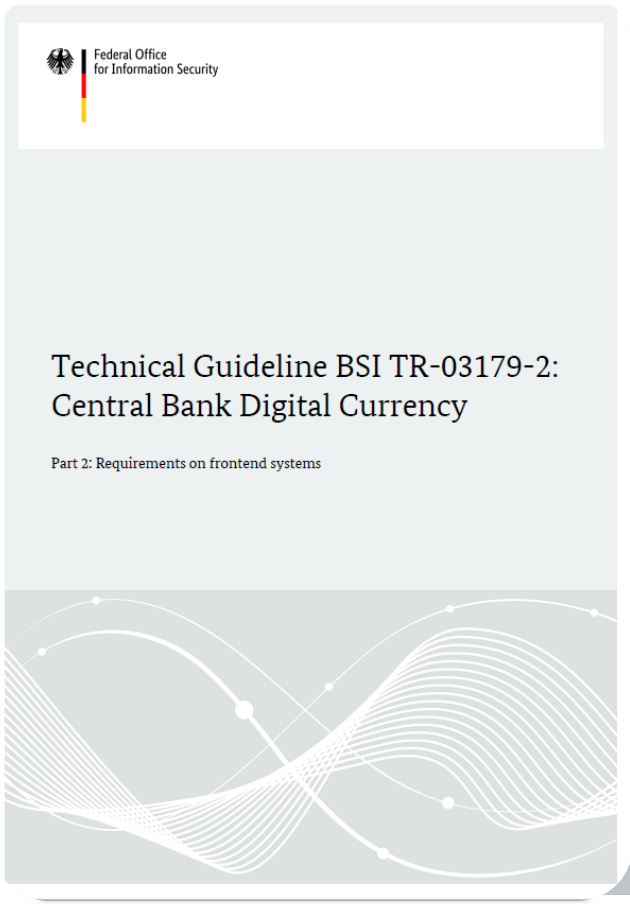
Abbildungsquelle: BSI

TR-03179 – Ein erster Überblick

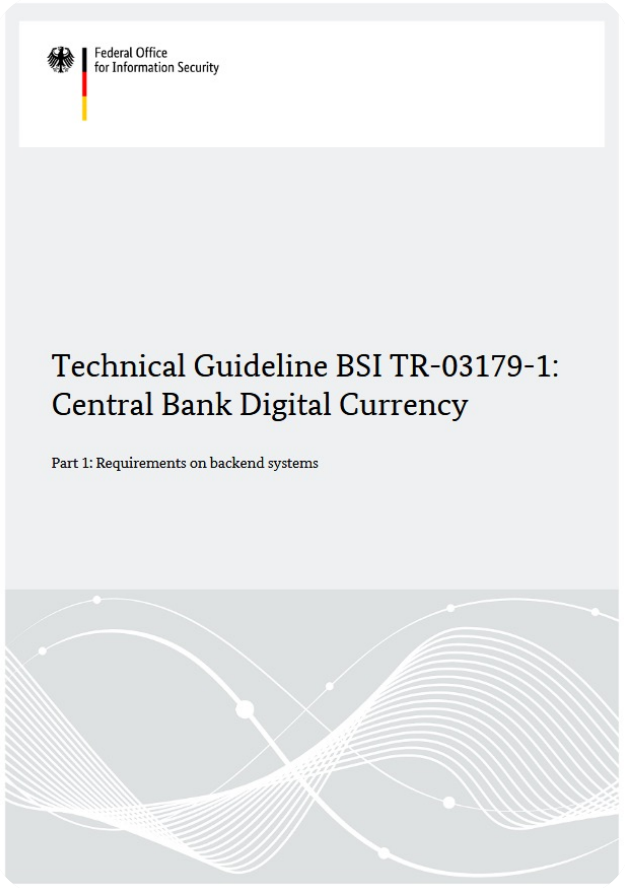


- Schlagen Rollen vor
- Definieren „Schutzziele“
- Adressieren Bedrohungen
- Leiten Anforderungen ab

- Unterschiedliche Schwerpunkte
- Unterschiedliche Zielgruppen



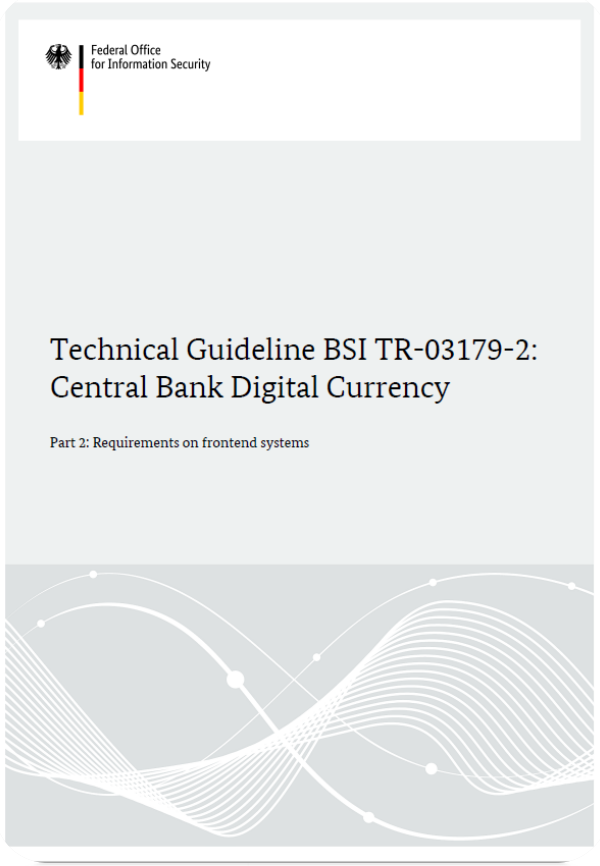
TR-03179-1 „Backend-Systeme“



Anforderungen an

- CBDC notes
- Ausgabe- und Verteilprozesse
- Gültigkeitsprüfung
- Offline und Online-Transaktionen
- Vermeidung von Double Spending
- Privacy
- Monitoring von sicherheitsrelevanten Vorfällen
- Update-Prozesse
- Allgemeines Sicherheitsmanagement des Backends

TR-03179-2 „Frontends“



Anforderungen an

- Generelle Funktionen
- Hardware und Schnittstellen
- Authentifizierung und Autorisierung
- Personalisierung
- Sperrprozesse
- Synchronisation mit dem Backend
- Updates von Wallets und Notes
- „Buchhaltung“
- Betreiber
- Transaktionen

CBDC - Erwartungsmanagement

Sicher

Die Sicherheit darf den heutigen digitalen Bezahlmöglichkeiten in nichts nachstehen

Verfügbar

Anytime – Anywhere

Selbst unter den schlechtesten Rahmenbedingungen

Belastbar

Transaktionen müssen nachvollziehbar sein

Instantan

Sofortige Transaktionsbestätigung

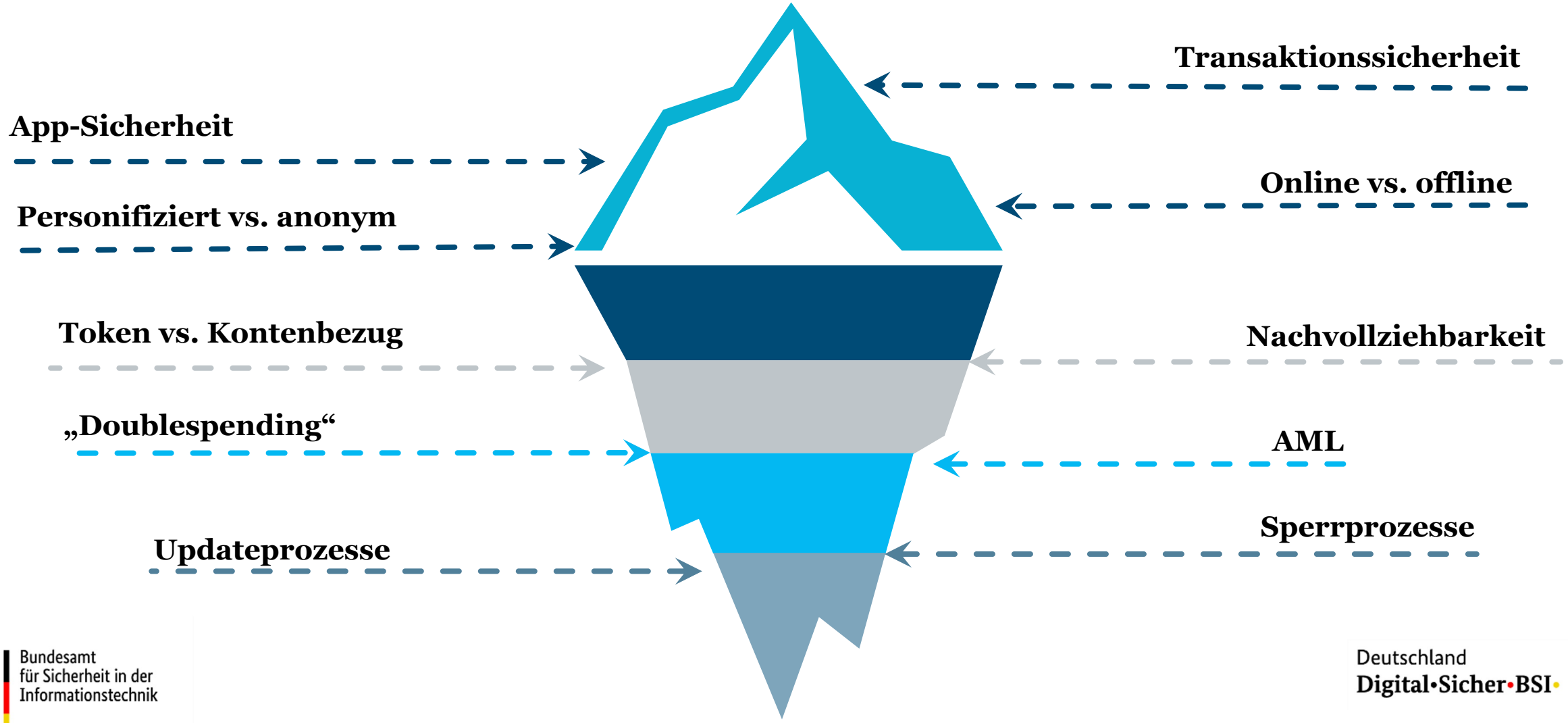
„Anonym“ wie Bargeld

Eine Zahlung ohne persönliche Informationen muss möglich sein

Barrierefrei

Zugang für alle

Offensichtliche Anforderungen trifft auf verdeckte Komplexität



TR-03179-2 „Frontends“

Wesentliche Cyber-Sicherheitserkenntnisse

Konformität von Wallets (zur TR) ist zu bestätigen

Eine einheitliche Sicherheitsbasis, unabhängig vom Formfaktor, ist zu etablieren und einzuhalten.

Übergabepunkte zwischen Frontend und Backend

Technologieabhängig ist zu definieren welche Funktionen von welchem Teil der Infrastruktur zu übernehmen sind. Hierbei sind vor allem Use-Cases, Anwendungsszenarien und Formfaktoren zu berücksichtigen.

Offlinezahlungen nur mit sicherem Hardwareanker

Technische Prüfroutinen sind bei einer „Online-Nutzung“ über das Backend abbildbar. Für das Offline-Anwendungsszenario sind dezentrale Maßnahmen zu treffen.

TR-03179-2 „Frontends“

Wesentliche Cyber-Sicherheitserkenntnisse

Sicherheitsanforderungen müssen skalierbar sein

Ein hohes Risiko erfordert starke Schutzmaßnahmen; Vor dem Hintergrund der Nutzbarkeit sollte „ohne Risiko“ Niederschwelligkeit ermöglicht werden

Limitierungen haben auch einen Nutzen

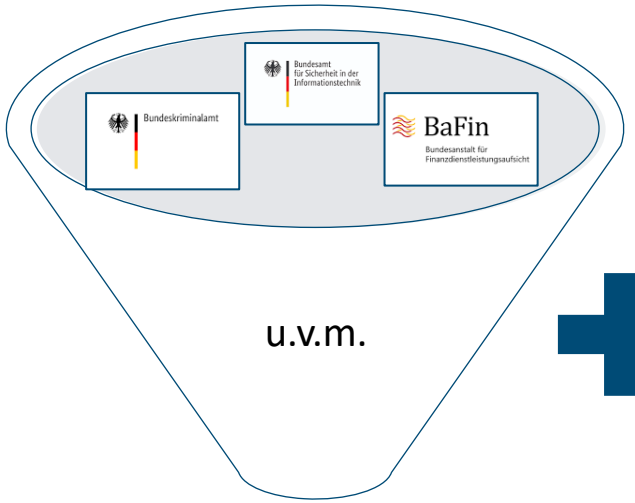
Neben der Einhaltung gültiger finanzwirtschaftlicher Anforderungen und Vorschriften, können Limitierungen auch Nutzungsszenarien ermöglichen und damit die Anwendbarkeit fördern

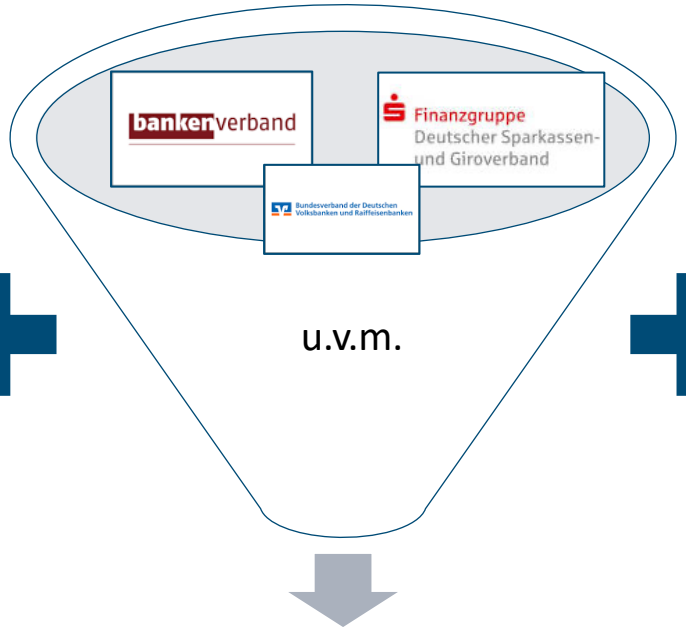
Zentral- und Dezentral ausgelöste Sperrungen sind zu berücksichtigen

Technische Prüfroutinen sind bei einer „Online-Nutzung“ über das Backend abbildbar. Für das Offline-Anwendungsszenario sind dezentrale Maßnahmen zu treffen.

LaSiFi - Lagebild zur aktuellen Cyber-Sicherheit im Finanzwesen

stark vereinfacht





Vorfälle, Risiken und Gefährdungslage

Digitalisierungsaktivitäten und -trends, Risiken

Risikoanalyse und Handlungsempfehlungen

TR-Familie: Anforderungen an Anwendungen im Finanzwesen

- Erweiterung der bestehenden TR-03174 auf TR-Familie bestehend aus Anforderungen für:
  - mobile Anwendungen (TR-03174-1)
  - Web-Anwendungen (TR-03174-2)
  - Hintergrundsysteme (TR-03174-3)
- TR-Familie wurde am 03.06.2022 für das Gesundheitswesen (GW) etabliert.
- Zugelassene Prüfer für die TR im GW
- Veröffentlichung erfolgt unmittelbar

Vielen Dank für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI•

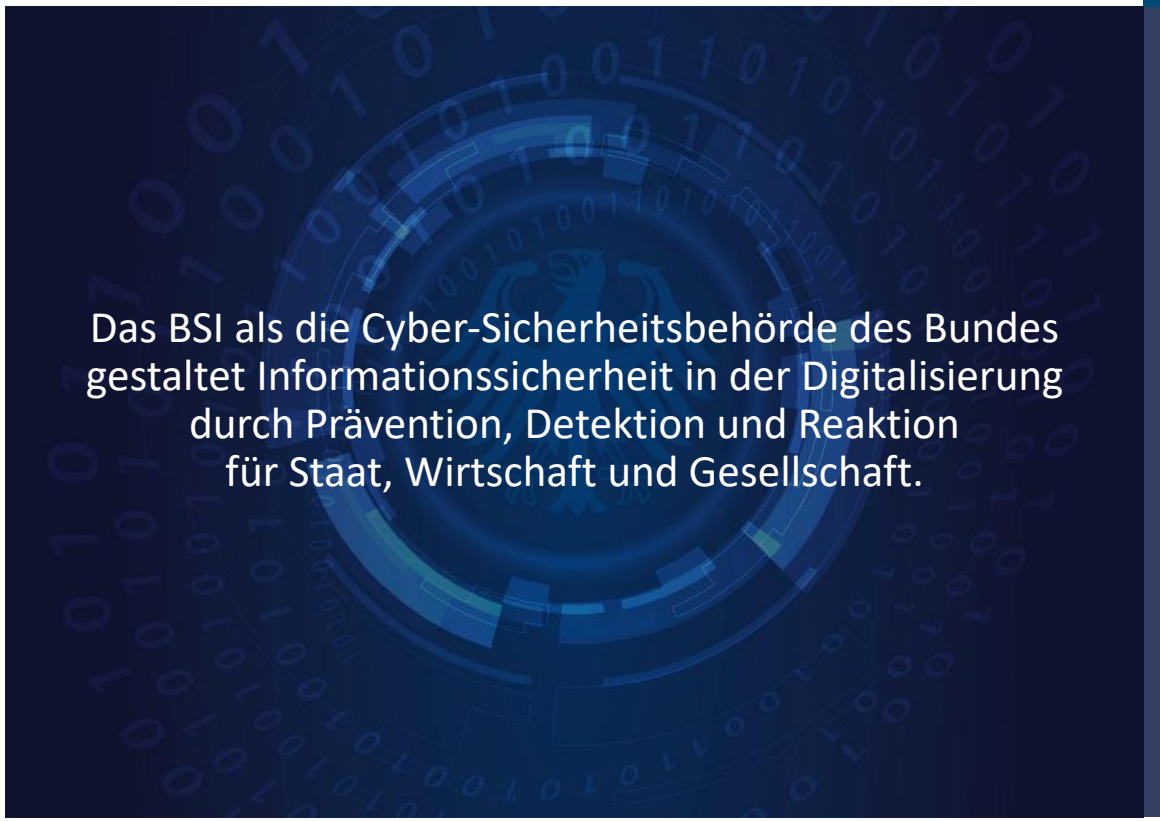
Kontakt

Roland Kirsch

- Cybersicherheit im Gesundheits- und Finanzwesen -

Referat-d24@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn
www.bsi.bund.de

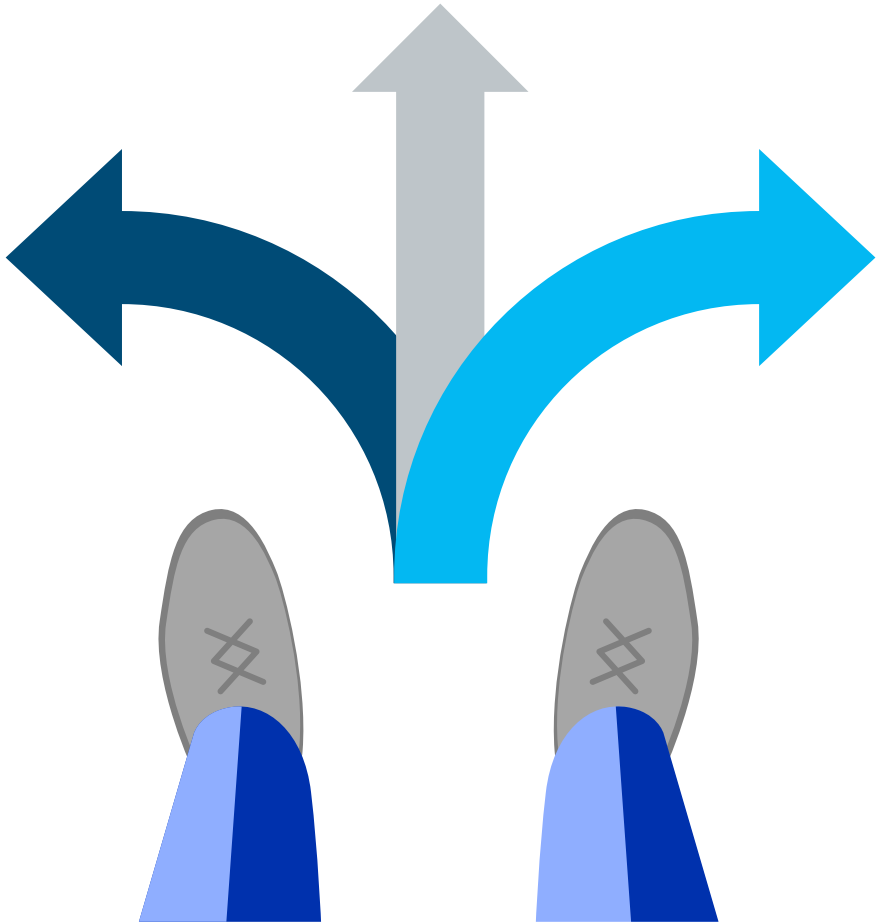


Bundesamt
für Sicherheit in der
Informationstechnik

Wallettypen – basierend auf dem Grad der Anonymität

Hybrid

Darstellung technisch hoch komplex



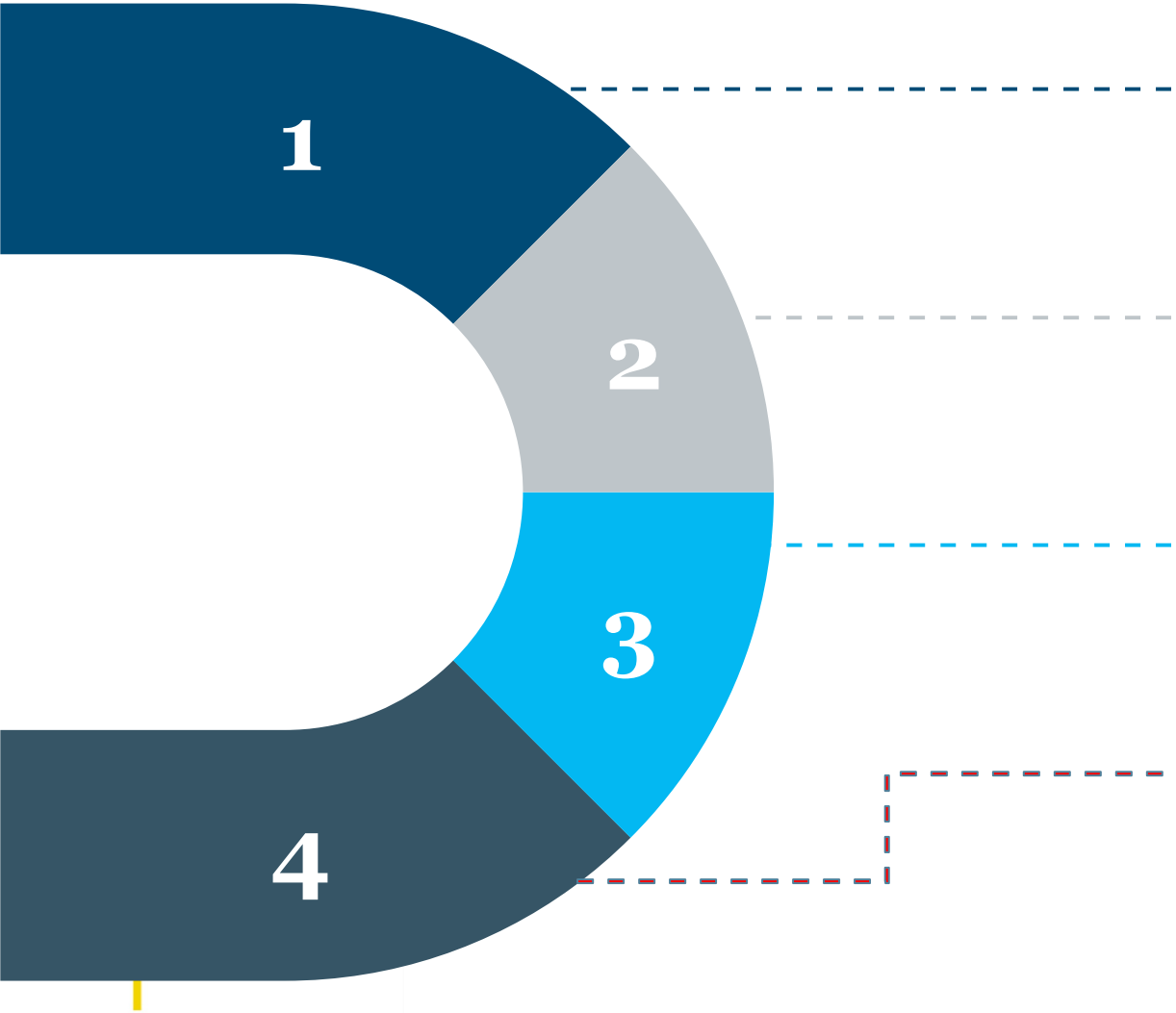
Personifiziert

Maximale Transparenz, maximale Sicherheit, maximale Nachvollziehbarkeit, größter Anwendungsraum

Anonym

Eingeschränkte Nutzungsmöglichkeiten, starke Limitierung, einfacher Zugang

Token oder Kontenbezug



Bezug einer Wallet

Unter der Annahme, dass eine vorhandene Kunde – Bank Beziehung existiert, geringere Hürden bis zur initialen Nutzung einer Wallet bei Kontobezug

„Aufladen“ oder vielleicht doch „Durchreichen“

Etablierte Prozesse bei Kontenbezug können voraussichtlich genutzt werden

Verlust der Wallet

Ein Bezug zum Konto kann erneut hergestellt werden, ein Token ist potenziell „verloren“

Anonymität

Hybride Wallets? Höhere Hürden zur Gewährleistung einer potenziellen Anonymität bei Kontenbezug?

Deutschland Digital•Sicher•BSI•