STRUKTURRISIKOANALYSE

BWS-SR-2026-09-13 · EIGENSTÄNDIGES DOKUMENT

Strukturrisiko Digitale Zwangsidentität

Pflichtbürgerkonto (DeutschlandID) und Pegasus-Klasse Spyware — Konvergenz zweier Entwicklungslinien

Dokument-ID	BWS-SR-2026-09-13
Datum	13. September 2026
Autor	Christer Häberli, philosophenstudio.de
Status	Öffentlich
Bezug	BWS I-V, EA-2026-09-13

1. Vorbemerkung

Dieses Dokument analysiert eine strukturelle Risikokonstellation, die durch die Konvergenz zweier unabhängig voneinander verlaufender Entwicklungslinien entsteht:

- Die geplante gesetzliche Einführung eines Pflichtbürgerkontos (DeutschlandID) durch die Bundesregierung
- Die nachgewiesene Existenz und der nachgewiesene Einsatz von Pegasus-Klasse Spyware gegen Personen in EU-Mitgliedstaaten

Weder die Technologie des Pflichtbürgerkontos noch Pegasus-Klasse Software wird hier als inhärent problematisch bewertet. Die Analyse beschränkt sich auf die strukturelle Risikoerhöhung durch Zentralisierung digitaler Identität im Kontext nachgewiesener staatlicher Überwachungswerkzeuge.

> GRUNDSATZ
>
> Technologie ist neutral. Maßgeblich ist ausschließlich der Anwendungskontext. Dieses Dokument bewertet keine Absichten, sondern Strukturen.

2. Das Pflichtbürgerkonto — Technische Struktur

2.1 Rechtliche Grundlage und Planungsstand

Der Koalitionsvertrag von CDU, CSU und SPD (2025) enthält folgende Formulierung:

> „Jeder Bürger und jede Bürgerin erhält verpflichtend ein Bürgerkonto und eine digitale Identität."
> — Koalitionsvertrag CDU/CSU/SPD, 2025

Zum Stand September 2026 ist diese Pflicht noch nicht gesetzlich umgesetzt (§ 3 OZG sieht Freiwilligkeit vor). Die Umsetzung ist angekündigt. Die technische Infrastruktur (BundID → DeutschlandID) existiert bereits und wird aktiv ausgebaut.

2.2 Architektur des Systems

Komponente	Funktion	Status
BundID	Zentrales Nutzerkonto für Verwaltungsleistungen (Bund + Länder)	aktiv

DeutschlandID	Weiterentwicklung der BundID, einheitliche digitale Identität	in Entwicklung
EUDI-Wallet	EU-weite digitale Brieftasche, Anbindung an BundID geplant	Sandbox ab 01/2026
Digitale Signatur	Rechtsgültige Signaturen über die Wallet	geplant
Pseudonyme Logins	Login-Funktion ohne Klarnamenangabe	geplant
Zahlungsfreigabe	Finanztransaktionen über die Wallet	geplant

2.3 Zentralisierungsgrad

Das System konsolidiert an einem einzigen digitalen Punkt:

- Verwaltungskommunikation (Anträge, Bescheide, Behördenkontakt)
- Identitätsnachweis (Ausweis-Funktion)
- Dokumentenspeicherung (Führerschein, Ausweise, Zertifikate)
- Digitale Signaturen (Rechtsgültigkeit)
- Zahlungsvorgänge (nach vollständiger Implementierung)

> STRUKTURELLE FESTSTELLUNG
>
> Ein zentralisierter Identitätspunkt für alle Lebensbereiche (Verwaltung, Identität, Finanzen, Kommunikation) maximiert die Angriffsfläche strukturell — unabhängig davon, wer das System betreibt oder kontrolliert.
>
> Das gilt für externe Angreifer ebenso wie für staatliche Akteure anderer Länder und für interne Missbrauchsszenarien.

3. Pegasus — Technische Charakteristik und dokumentierte Einsätze

3.1 Was ist Pegasus?

Pegasus ist eine kommerzielle Überwachungssoftware (Spyware) der israelischen Firma NSO Group Technologies Ltd. Sie ist für den Verkauf an staatliche Akteure bestimmt und gilt als eine der technisch fortschrittlichsten Überwachungslösungen ihres Typs.

Fähigkeit	Beschreibung	Nachweis
Zero-Click-Infektion	Gerätekompromittierung ohne jede Nutzerinteraktion	Citizen Lab, 2021
Mikrofon-Zugriff	Echtzeit-Abhören von Gesprächen (auch offline)	Amnesty International Tech, 2021
Kamera-Zugriff	Bildaufnahme ohne Kamera-LED-Aktivierung	Citizen Lab, 2021
Nachrichtenextraktion	Vollzugriff auf SMS, WhatsApp, Signal, iMessage	Pegasus Project, 2021
Standortüberwachung	Echtzeit-GPS-Tracking	Forensic Methodology Report, 2021
Passwort-Extraktion	Zugriff auf gespeicherte Credentials und Schlüsselbunde	Citizen Lab, 2021
Spurenlosigkeit	Selbstlöschung bei Entdeckungsrisiko	Amnesty Tech Forensics, 2021

3.2 Dokumentierte Einsätze in EU-Mitgliedstaaten

Der EU-Untersuchungsausschuss PEGA (Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware) dokumentierte in seinem Abschlussbericht (Mai 2023) folgende bestätigte Einsätze innerhalb der Europäischen Union:

Land	Betroffene Personen	Nachweis-Status
Spanien	Katalanische Politiker, Anwälte, Journalisten (Catalangate)	**forensisch bestätigt**
Ungarn	Journalisten, Oppositionspolitiker, Anwälte	**forensisch bestätigt**
Polen	Oppositionspolitiker, Staatsanwälte	**forensisch bestätigt**
Griechenland	Journalist Nikos Androulakis (PASOK-Vorsitzender)	**forensisch bestätigt**

> Quelle: European Parliament, PEGA Committee – Final Report, Mai 2023.
> „The use of Pegasus and equivalent surveillance spyware in the European Union has been confirmed in several Member States, targeting journalists, lawyers, politicians, and civil society activists."

3.3 Technische Angriffsvektoren auf digitale Identitätssysteme

Pegasus und Spyware derselben Klasse greifen Zielgeräte an — also Smartphones und Computer, auf denen digitale Identitätssysteme betrieben werden. Daraus ergeben sich folgende Zugriffspfade auf ein Pflichtbürgerkonto-Ökosystem:

```
Gerät kompromittiert
      │
      ├── Zugriff auf EUDI-Wallet / DeutschlandID-App
      │       → Identitätsdaten, Dokumente, Signaturen
      │
      ├── Zugriff auf Authentifizierungs-Tokens
      │       → Impersoation: Behördenanträge, Bescheide
      │
      ├── Zugriff auf Zahlungsfreigabe-Funktion
      │       → Finanztransaktionen im Namen des Opfers
      │
      ├── Extraktion biometrischer Daten (wenn hinterlegt)
      │       → Dauerhafte Identitätskompromittierung
      │
      └── Echtzeit-Monitoring aller Behördenkommunikation
              → Vollständiges Staatsbürger-Profil des Opfers
```

4. Risikoanalyse — Konvergenz der Entwicklungslinien

4.1 Das Zentralisierungsparadox

Dezentrale Systeme verteilen Risiken. Ein kompromittierter Datenpunkt liefert begrenzte Information. Zentralisierte Systeme bündeln Risiken: Ein kompromittierter Datenpunkt liefert alle Information.

DEZENTRALES SYSTEM	ZENTRALISIERTES PFLICHTBÜRGERKONTO
Kompromittierung eines Punktes = partieller Datenverlust	**Kompromittierung eines Punktes = Vollprofil der Person**

Das Pflichtbürgerkonto konsolidiert sämtliche staatsbürgerlich relevanten Daten und Funktionen an einer einzigen Stelle, die auf einem einzigen Endgerät operiert. Pegasus-Klasse Software kompromittiert genau dieses Endgerät — vollständig, spurenlos, ohne Nutzerinteraktion.

4.2 Asymmetrie der Verteidigungsposition

Ein strukturelles Merkmal dieser Konstellation ist die fundamentale Asymmetrie zwischen Angreifer und Verteidiger:

Dimension	Angreifer (Pegasus-Klasse)	Betroffene Person
Technisches Wissen	vollständig, professionell	nicht vorauszusetzen
Erkennbarkeit des Angriffs	keine (Zero-Click, keine Symptome)	Angriff nicht erkennbar
Schutzmaßnahmen	Spyware umgeht alle bekannten Schutzmaßnahmen	keine wirksame Option
Zugriff auf kompromittierte Daten	vollständig, in Echtzeit	Person weiß nichts davon
Rechtsschutz	Angriff erfolgt spurenlos	Nachweis hochgradig erschwert

4.3 Skalierungseffekt durch Pflicht

Ein freiwilliges System erreicht einen Bruchteil der Bevölkerung. Ein Pflichtsystem erreicht alle. Der Skalierungseffekt für potenzielle Angreifer — staatliche wie nicht-staatliche — ist proportional zur Größe der Pflichtnutzerbasis.

> QUANTIFIZIERUNG
>
> Bevölkerung Deutschland (2026): ca. 84 Millionen
> Pflichtnutzerbasis bei vollständiger Umsetzung: ca. 84 Millionen
> Einheitlicher technischer Standard: ein System, eine Architektur, eine Angriffsfläche
> Einheitliches Endgerät-Ökosystem (iOS/Android): zwei dominante Betriebssysteme

4.4 Staatliche Angreifer in EU-Mitgliedstaaten

Der PEGA-Ausschuss stellte fest, dass Pegasus in den dokumentierten EU-Fällen von staatlichen Stellen der jeweiligen Mitgliedstaaten eingesetzt wurde — gegen eigene Staatsbürger. Das bedeutet:

- Staatliche Stellen verfügen über Zugang zu Pegasus-Klasse Software
- Diese Software wurde nachweislich gegen Journalisten, Anwälte und Oppositionspolitiker eingesetzt

- Die Zielpersonen operierten innerhalb derselben rechtlichen Schutzrahmen, die für alle EU-Bürger gelten
- Die Infektion war für die Betroffenen nicht erkennbar

> PEGA Final Report (2023): „In several Member States, Pegasus was used by state authorities against their own citizens in ways that appear incompatible with EU fundamental rights law."

5. Strukturelle Schlussfolgerung

Die Konvergenz der beiden Entwicklungslinien erzeugt eine strukturelle Risikokonstellation, die unabhängig von Absichten und Intentionen einzelner Akteure besteht:

Entwicklungslinie	Richtung	Struktureffekt
Pflichtbürgerkonto	Maximale Zentralisierung digitaler Identität	Angriffsfläche ↑
Pegasus-Klasse Spyware	Zugriff auf Endgeräte ohne Nutzerinteraktion	Angriffstiefe ↑
Pflichtnatur des Kontos	Alle 84 Millionen Bürger als Pflichtnutzer	Skalierung ↑
Dokumentierte EU-Einsätze	Einsatz gegen eigene Staatsbürger nachgewiesen	Realitätsbezug ↑

STRUKTURELLE FESTSTELLUNG

Ein Pflichtbürgerkonto, das alle verwaltungsrelevanten Daten, Identitätsfunktionen und Zahlungsvorgänge zentralisiert, und Pegasus-Klasse Software, die Endgeräte vollständig und spurenlos kompromittiert, ergeben zusammen eine Struktur, in der die Kompromittierung einer Person durch einen entsprechend ausgestatteten Akteur technisch vollständig und für die betroffene Person nicht erkennbar möglich ist.

Diese Feststellung ist kein Urteil über Absichten. Sie ist eine Beschreibung von Strukturen, die aus zwei unabhängig dokumentierten Entwicklungslinien folgen.

6. Quellenverzeichnis

#	Quelle	Dokumenttyp	Jahr
01	Koalitionsvertrag CDU/CSU/SPD — Kapitel Digitalisierung	Politisches Dokument	2025
02	Bundesministerium des Inneren — BundID / DeutschlandID	Behördliche Publikation	2025–2026
03	OZG (Onlinezugangsgesetz) § 3	Gesetzestext	aktuell
04	Citizen Lab — Pegasus Technical Analysis (University of Toronto)	Forensischer Bericht	2021
05	Amnesty International Tech — Forensic Methodology Report	Forensischer Bericht	2021
06	Forbidden Stories / Pegasus Project — Investigativkonsortium (17 Redaktionen)	Investigativrecherche	2021
07	European Parliament — PEGA Committee Final Report	Parlamentarischer Bericht	2023
08	Citizen Lab — Catalangate (65 katalanische Zielpersonen)	Forensischer Bericht	2022