secunet

Architektur einer selbstverwalteten, substantiellen Bürgeridentität für Behörden und Wirtschaft

22.06.2022 | Thomas Maier

E-Government

Studie Kompetenzzentrum öffentliche IT:

Bürger wird durchschnittlich 1,5 Verwaltungskontakte im Jahr haben

» **zu wenig, damit sich ein System etabliert**

Quelle: Kompetenzzentrum öffentliche IT: BÜROKRATIEABBAU DURCH DIGITALISIERUNG: KOSTEN UND NUTZEN VON E-GOVERNMENT FÜR BÜRGER UND VERWALTUNG

Agenda

01 **Motivation und Sichten**

- **Behörden / Staat**
- **Industrie**
- **Bürger**

02 **Erfahrungen aus der Vergangenheit**

03 **Denkanstoß**

04 **Ausblick und Diskussion**

Workshop

Unterbrechungen erwünscht!
Für Diskussionen, Ideen, Anregungen und Fragen bitte jederzeit unterbrechen.

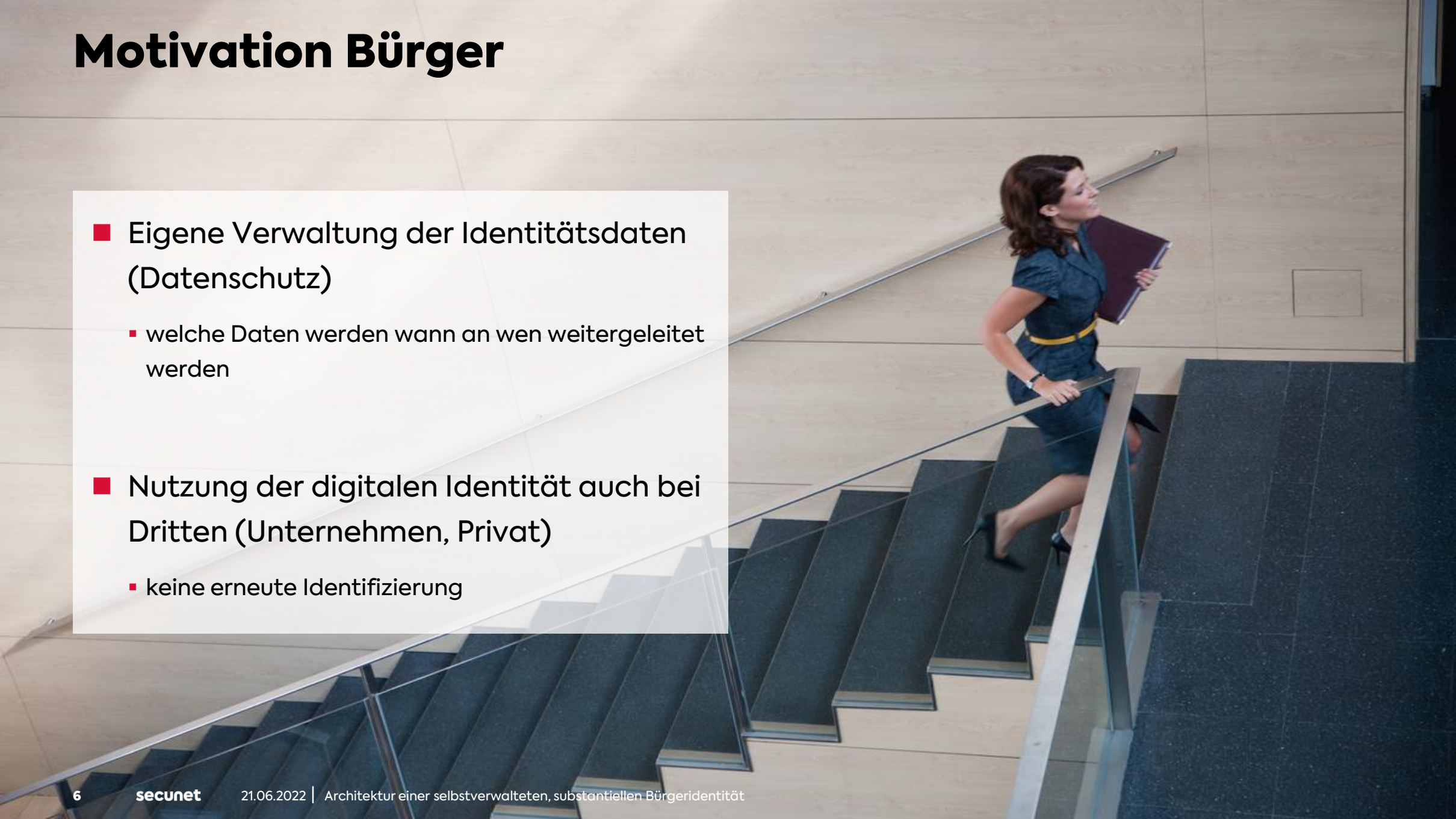
Motivation Behörde

- Höchstmögliche Sicherheit
  - Person ist die, die sie vorgibt zu sein
  - Schutz gegen Missbrauch
  - Vertrauensverlust bei Verletzungen der Vertraulichkeit
- Datenqualität

Motivation Industrie und Wirtschaft

- Verlässliche Daten zur Abwicklung der Geschäfte
  - Verlässlichkeit bedeutet, dass der rechtliche Rahmen eingehalten wird und das Geschäft zuverlässig abgewickelt werden kann
- Ggfls. Kosteneinsparungen
- Aktualität der Daten: Einfache Aktualisierung der Identitätsdaten
- Identifizierung hoch, für Authentisierung reicht meistens substantiell
- Mögliche Szenarien
  - Kundenkonto
  - Freischaltung einer SIM-Karte
  - Lotto
  - Versicherung abschließen
  - Altersverifikation

Motivation Bürger



- Eigene Verwaltung der Identitätsdaten (Datenschutz)
  - welche Daten werden wann an wen weitergeleitet werden
- Nutzung der digitalen Identität auch bei Dritten (Unternehmen, Privat)
  - keine erneute Identifizierung

Erfahrungen im E-Government

Bürger

- Geringe Usability
  - PIN vergessen
  - Lesegerät oder kompatibles Smartphone benötigt
  - Personalausweis nicht greifbar
  - Geringe Anzahl an Akzeptanzstellen
- Nicht jeder besitzt einen Personalausweis (Preis: 37€)
- Verlust und Defekt Prozesse (Dauer: 2 – 4 Wochen)

Industrie

- Aufwendig zu integrieren
- Hohe Wartungsaufwände
- Hohe formale Hürden
- Hoher Aufwand um Berechtigungszertifikate zu erhalten
- Hohe Kosten
- Aktualität der Daten

Aktuell nur wenig im Einsatz

Mögliche Datenquelle: Melderegister

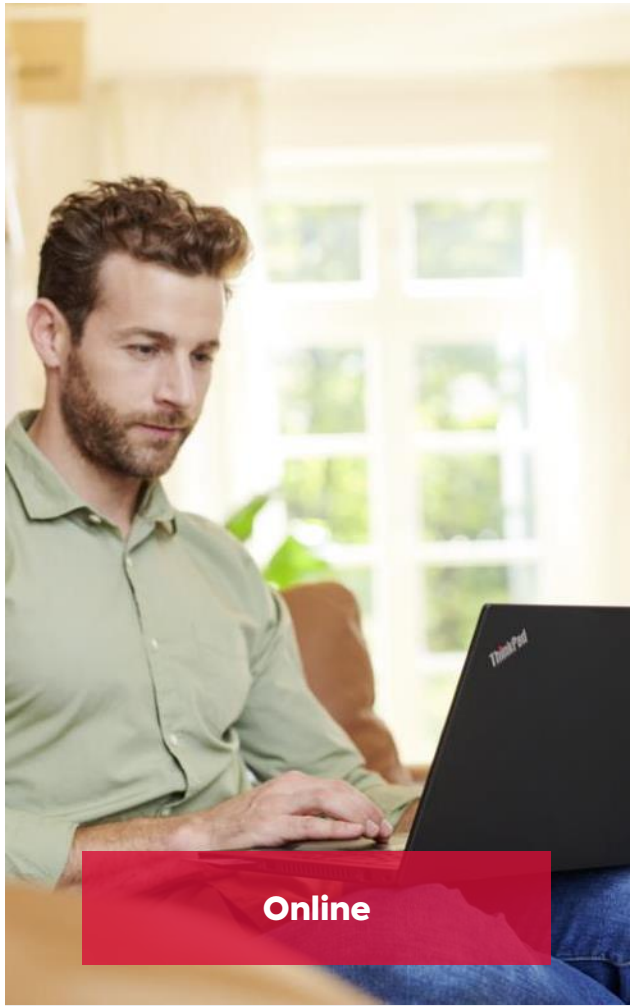
Denkanstoß


Üblicher Behördengang
(1 – 5 pro Jahr)
Vorlage
Identitätsnachweise
Erstellung eines
Authentisierungsmediums
auf Niveau substantiell
Nutzung als BürgerID

Schritt 1: Üblicher Behördengang

- Anmeldung an neuem Wohnort
- Beantragung Personalausweis
- Beantragung Reisepass
- Beglaubigung Dokumente
- Ferienpass
- Saisonkarte lokales Freibad
- Beantragung Subventionen

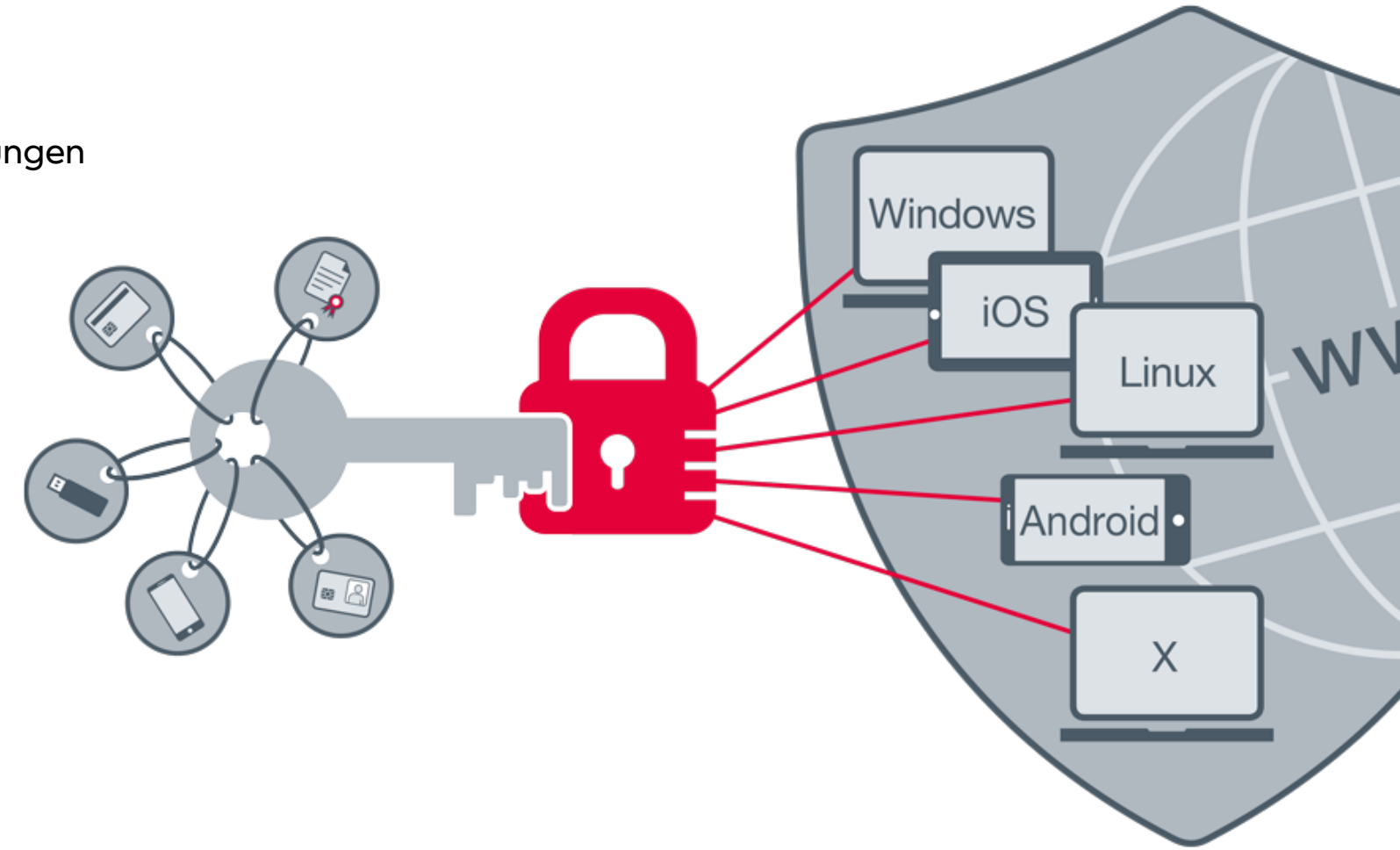
Schritt 2: Identifizierung hoch



Schritt 3: Ausstellung Authentisierungsmedium

Schritt 4: Nutzung der Büger ID

- Selbstauskunft der Meldedaten
- Behördengänge
- Städtische und kommunale Einrichtungen
  - Saisonkarte Freibad
  - Bibliotheksausleihe
  - ÖPNV (z.B. Förderung Schülerticket)
- Anwendungsfälle neben OZG
  - Darlehensabschluss
  - Abschluss Mobilfunktarif
  - Wechsel der Krankenkasse
  - Altersnachweis
  - Abschluss Versicherung



Beispiel: Altersverifikation für Onlineglückspiel

Schritt 1: Ausfüllen der Registrierungsdaten

Casinowelt: Deutschlands Nr. 1 kostenloses Online-Casino

FSK ab 18

Registrierung

Benutzername

Casino-Genie

Weiter mit BürgerID

Schritt 1: Ausfüllen der Registrierungsdaten

Casinowelt: Deutschlands Nr. 1 kostenloses Online-Casino

FSK ab 18

Registrierung

Benutzername

Casino-Genie

Altersverifikation mit deiner Bürger ID:

Es wird nur bestätigt, dass du über 18 Jahre alt bist, es werden für das kostenlose Spielerlebnis keine weiteren Daten übertragen

Schritt 2: Authentisieren gegenüber der Meldebehörde

Casinowelt: Deutschlands Nr. Online-Casino

FSK ab 18

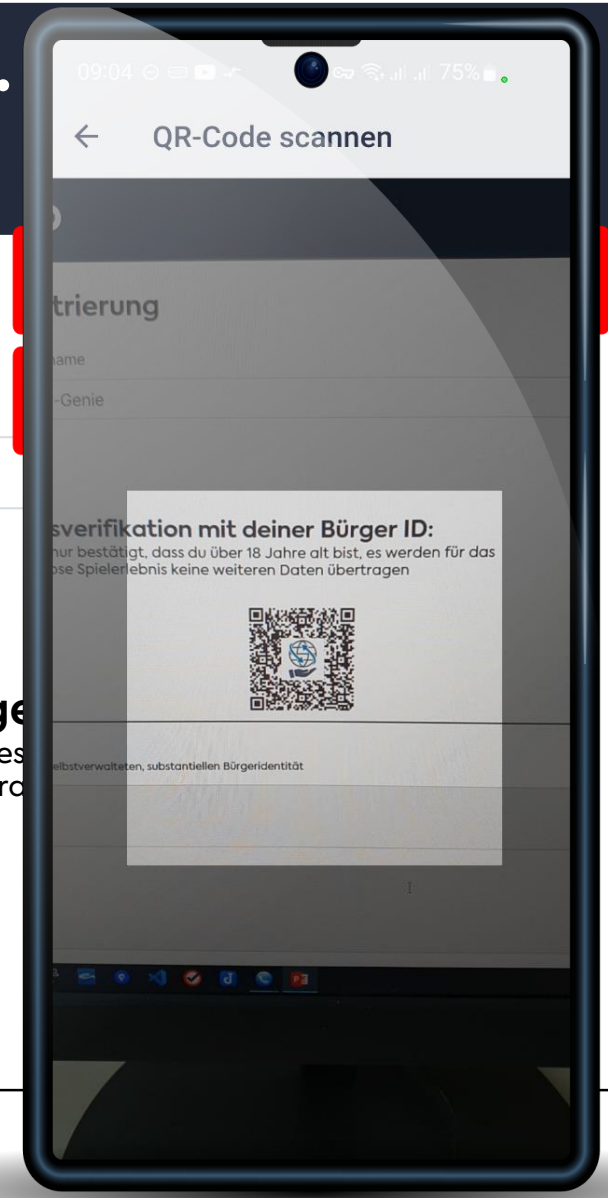
Registrierung

Benutzername

Casino-Genie

Altersverifikation mit deiner Bürge

Es wird nur bestätigt, dass du über 18 Jahre alt bist, es
kostenlose Spielerlebnis keine weiteren Daten übertra



Schritt 2: Authentisieren gegenüber der Meldebehörde

Casinowelt: Deutschlands Nr. Online-Casino

FSK ab 18

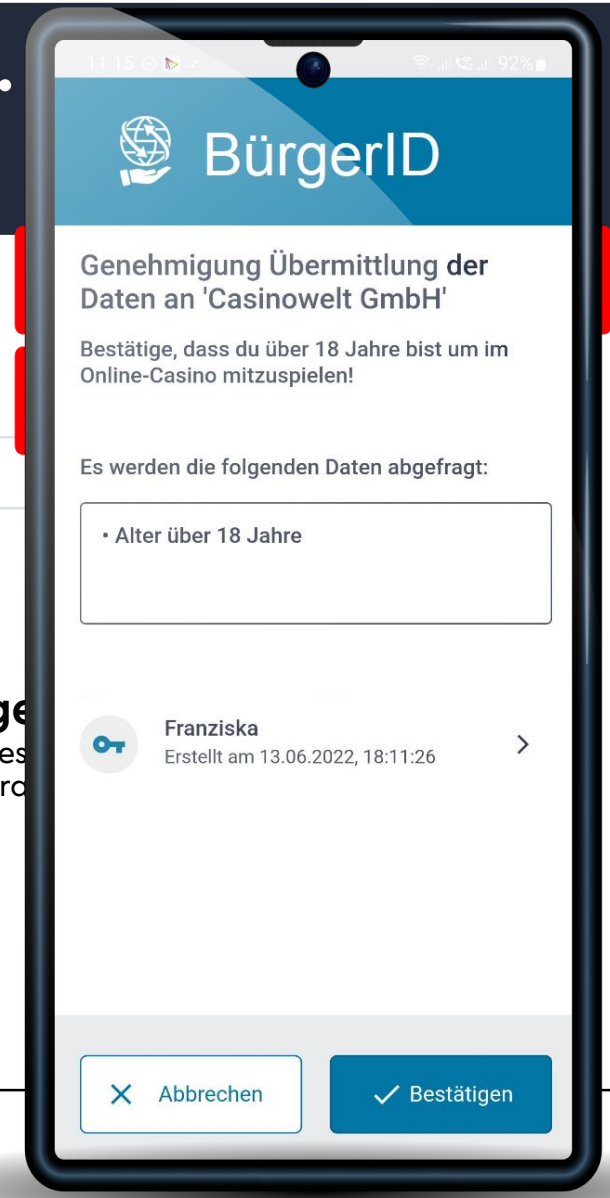
Registrierung

Benutzername

Casino-Genie

Altersverifikation mit deiner Bürge

Es wird nur bestätigt, dass du über 18 Jahre alt bist, es
kostenlose Spielerlebnis keine weiteren Daten übertra



Schritt 2: Authentisieren gegenüber der Meldebehörde

Casinowelt: Deutschlands Nr. Online-Casino

FSK ab 18

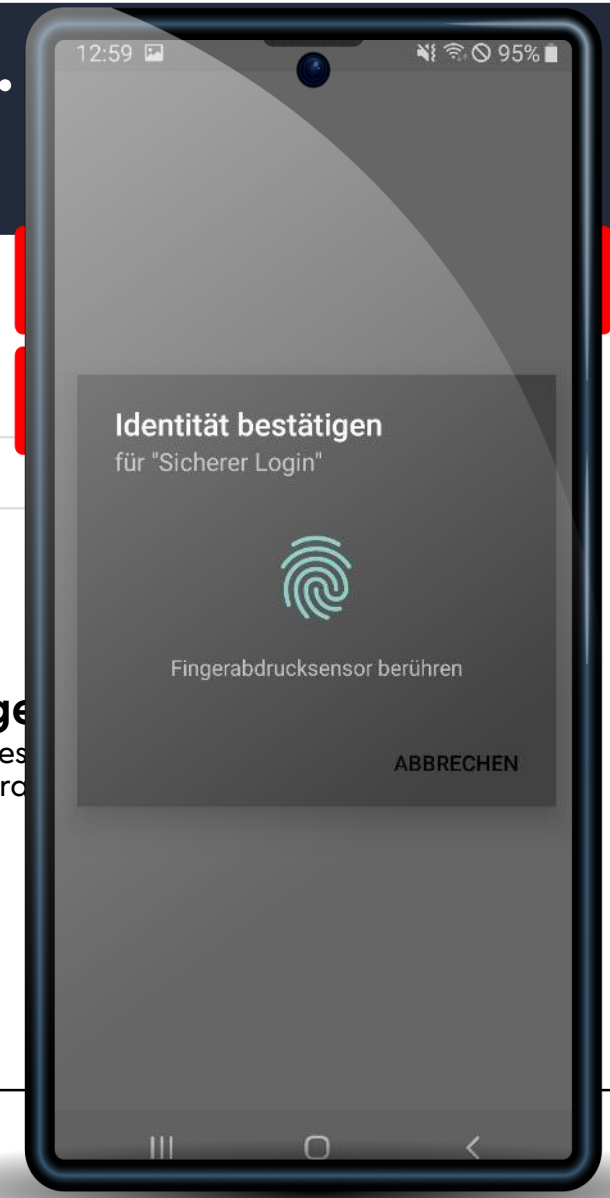
Registrierung

Benutzername

Casino-Genie

Altersverifikation mit deiner Bürge

Es wird nur bestätigt, dass du über 18 Jahre alt bist, es
kostenlose Spielerlebnis keine weiteren Daten übertra



Schritt 3: Übermittlung der Daten an den Dienst

Casinowelt: Deutschlands Nr. Online-Casino

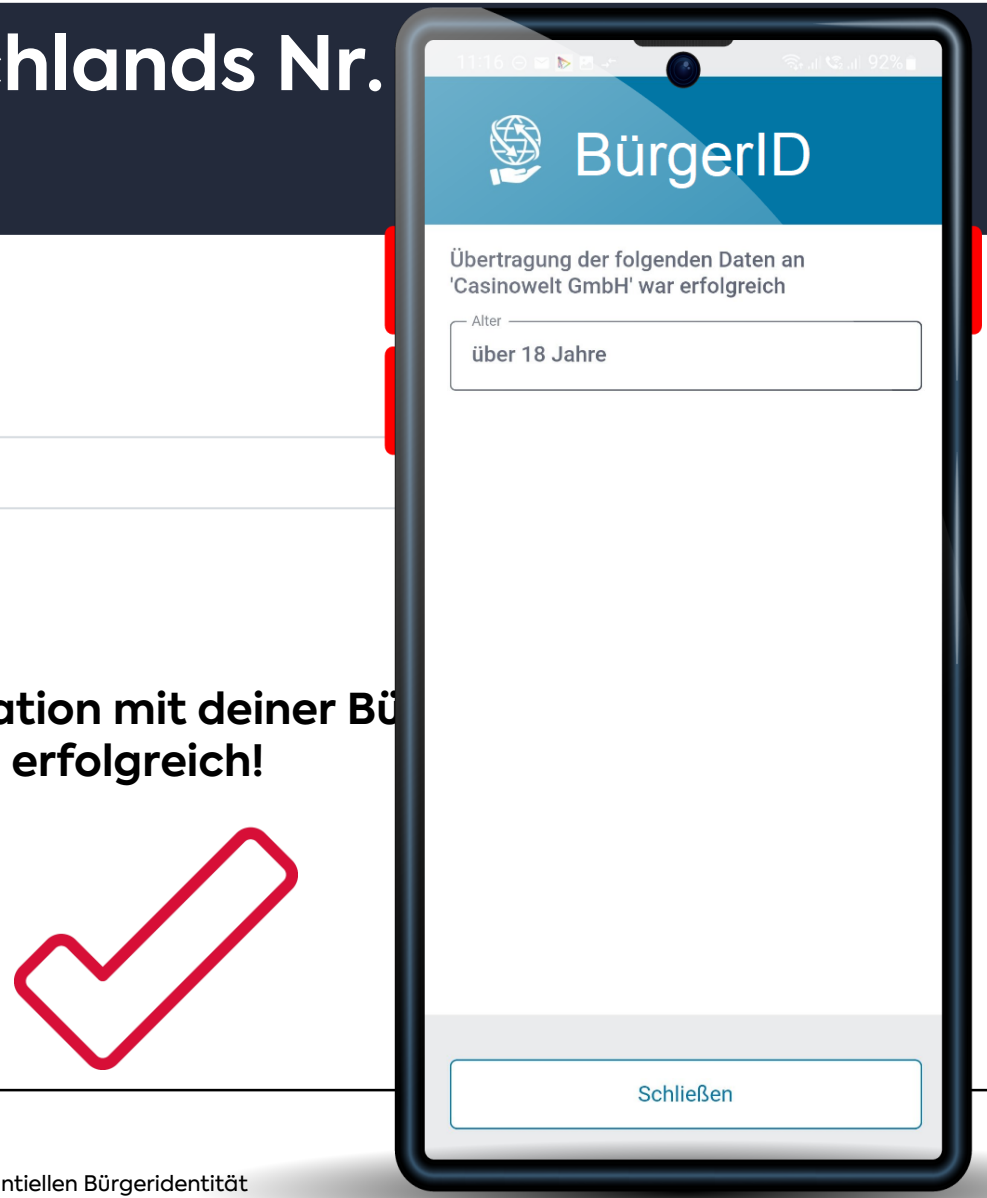
FSK ab 18

Registrierung

Benutzername

Casino-Genie

Altersverifikation mit deiner Bü
erfolgreich!



Schritt 3: Übermittlung der Daten an den Dienst

Casinowelt: Deutschlands Nr. 1 kostenloses Online-Casino

FSK ab 18

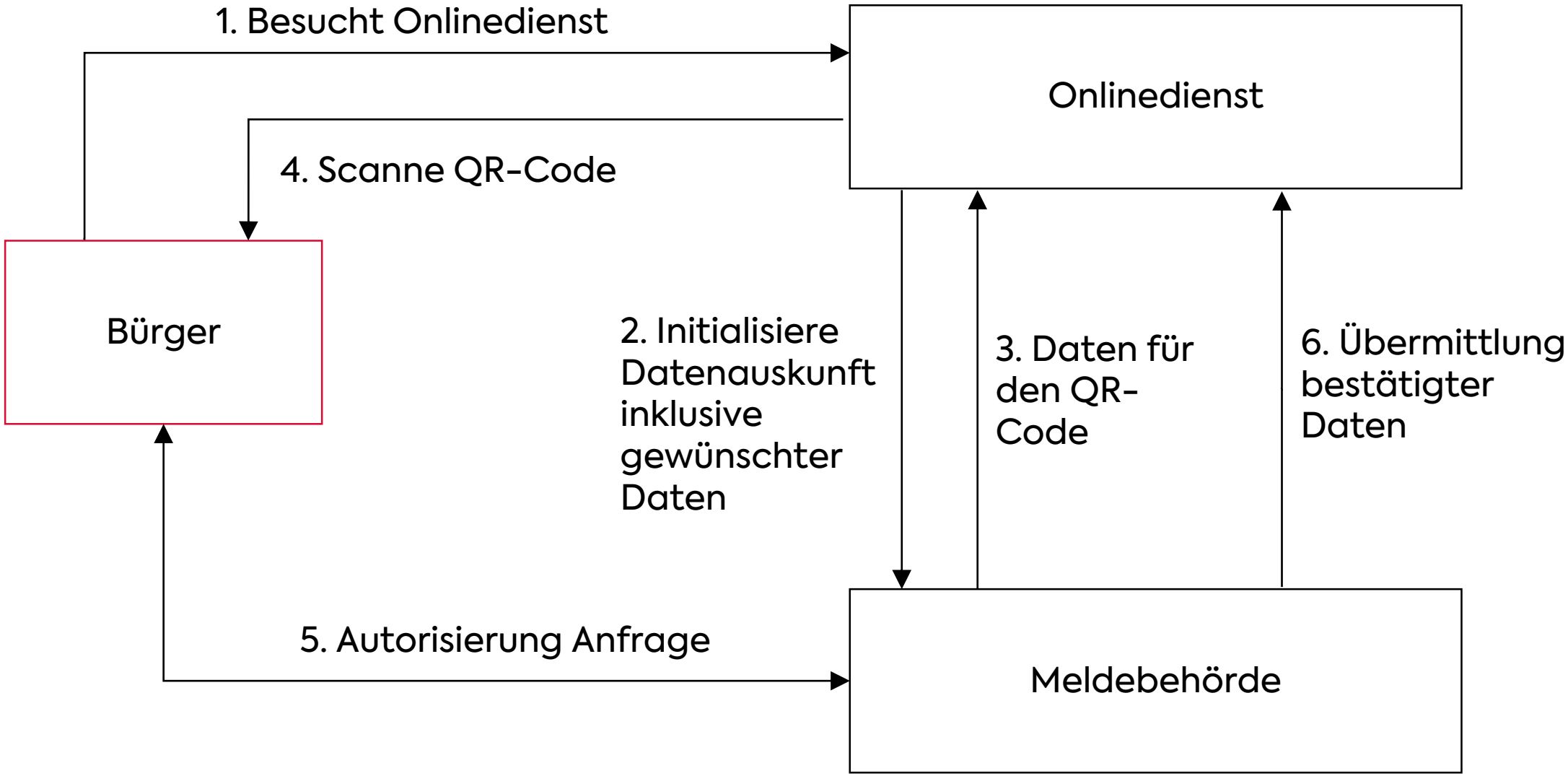
Registrierung

Benutzername

Casino-Genie

Altersverifikation mit deiner Bürger ID erfolgreich!

Ablauf der Datenübermittlung



Beispiel : DroneSafe – Drohnen-versicherung

Schritt 1: Ausfüllen der Versicherungsseite

DroneSafe

Dein Drohnen-Versicherungs-Angebot

Produkt

Drohnen Alles-drin Haftpflichtversicherung

Beschriftung Datum

01.07.2022

Deckungssumme

50 Millionen €

Postleitzahl

12345

Weiter

Schritt 2: Authentisieren gegenüber der Meldebehörde

DroneSafe

Dein Drohnen-Versicherungs-Angebot

Produkt

Drohnen Alles-drin Haftpflichtversicherung

Beschriftung Datum

01.07.2022

Deckungssumme

50 Millionen €

Postleitzahl

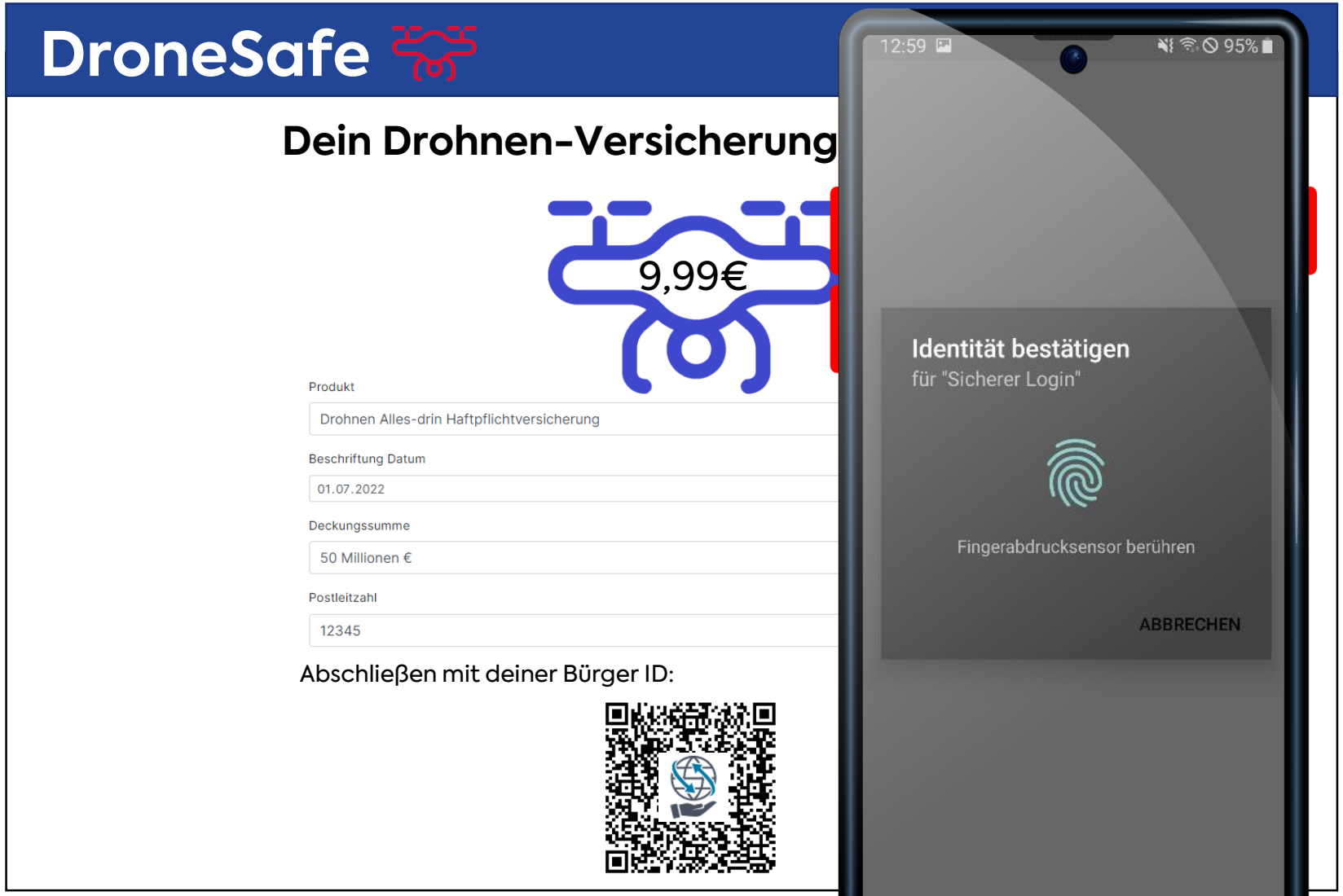
12345

Abschließen mit deiner Bürger ID:

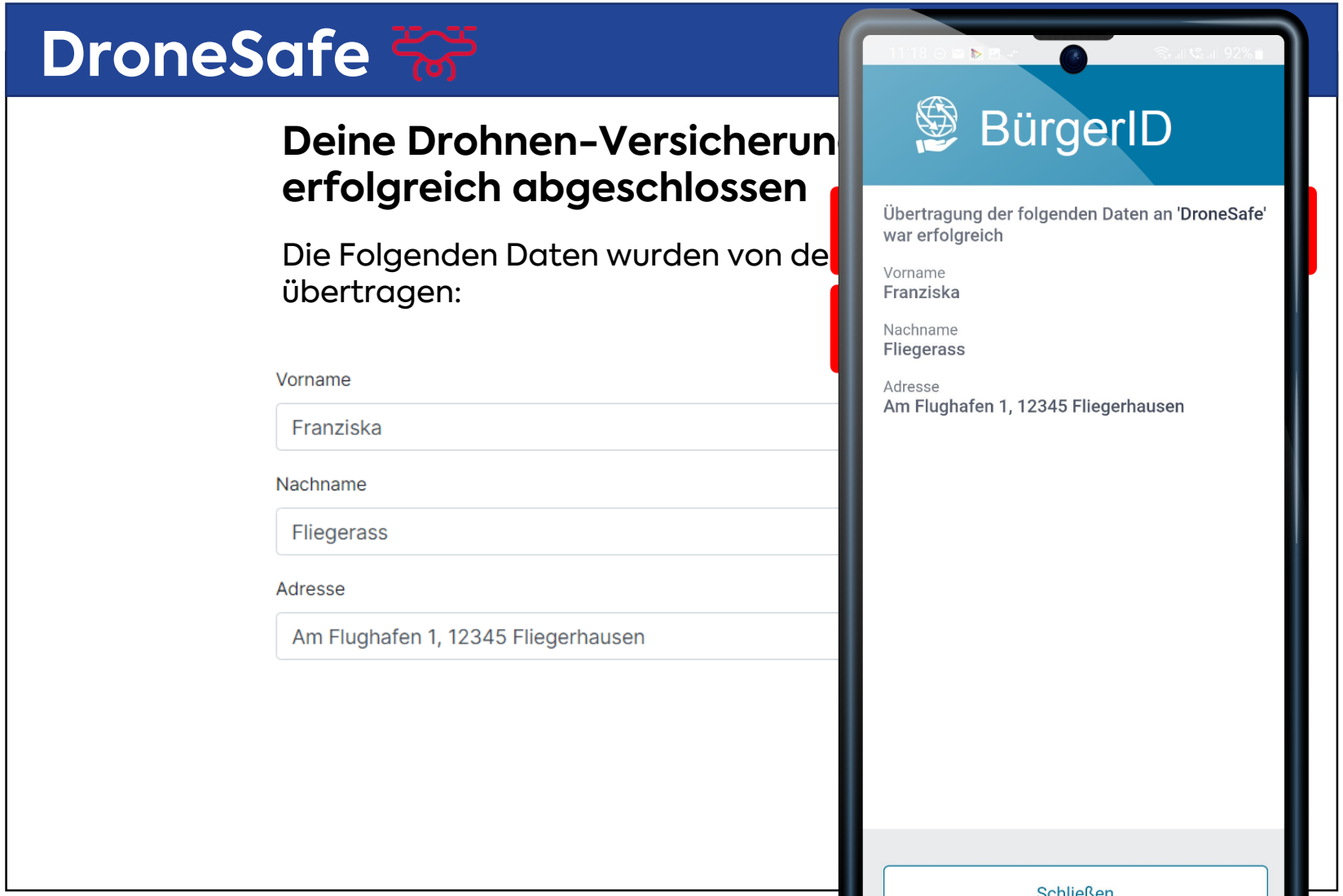
Schritt 2: Authentisieren gegenüber der Meldebehörde

Schritt 2: Authentisieren gegenüber der Meldebehörde

Schritt 2: Authentisieren gegenüber der Meldebehörde

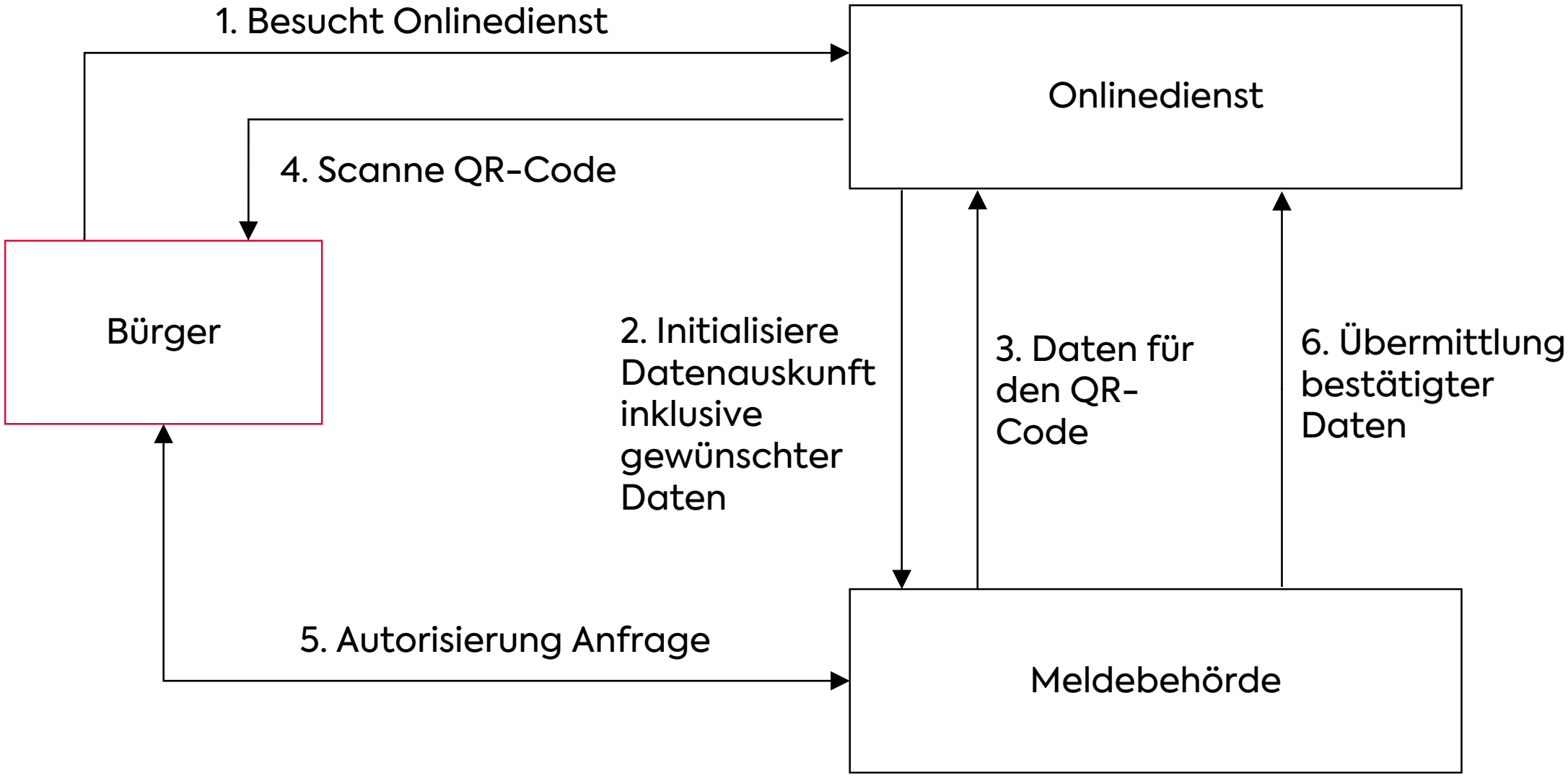


Schritt 2: Authentisieren gegenüber der Meldebehörde



Schritt 2: Authentisieren gegenüber der Meldebehörde

Ablauf der Datenübermittlung



Vorteile der Lösung

- Daten sind immer auf dem aktuellsten Stand (Meldedaten)
- Bestehende (hohe) Identifizierungsverfahren können für die Initialisierung genutzt werden
- Nutzung der BürgerID als substantielles Identifizierungsverfahren
- Die Verantwortung der Daten bleibt bei der bisherigen Stelle
- Bürger hat die Datenkontrolle
- Es können mehrere Token für eine Person ausgestellt werden bzw. vom Nutzer selbst ausgestellt und verwaltet werden, was auch Ersatzprozesse ermöglicht bei Verlust oder Defektes eines Geräts.
- Gleichzeitig ein Anmelde- und Identifizierungsverfahren für Bürgerservices
- Zutritt zu Kurleistungen, Bibliothek, Bäder, Museen, jegliche kommunal subventionierten Leistungen, ...

Ausblick und Diskussion

- Möglich jede Weitergabe der Daten an Dritte in Zukunft zu autorisieren
- Auch möglich für Unternehmen – Gewerberegister
  - Rollenmodelle


secunet

secunet.com

secunet Security Networks AG

Web & Application Security, München
Thomas.Maier@secunet.com
+49 170 5094550

secunet

We are hiring!

12 Standorte
in Deutschland

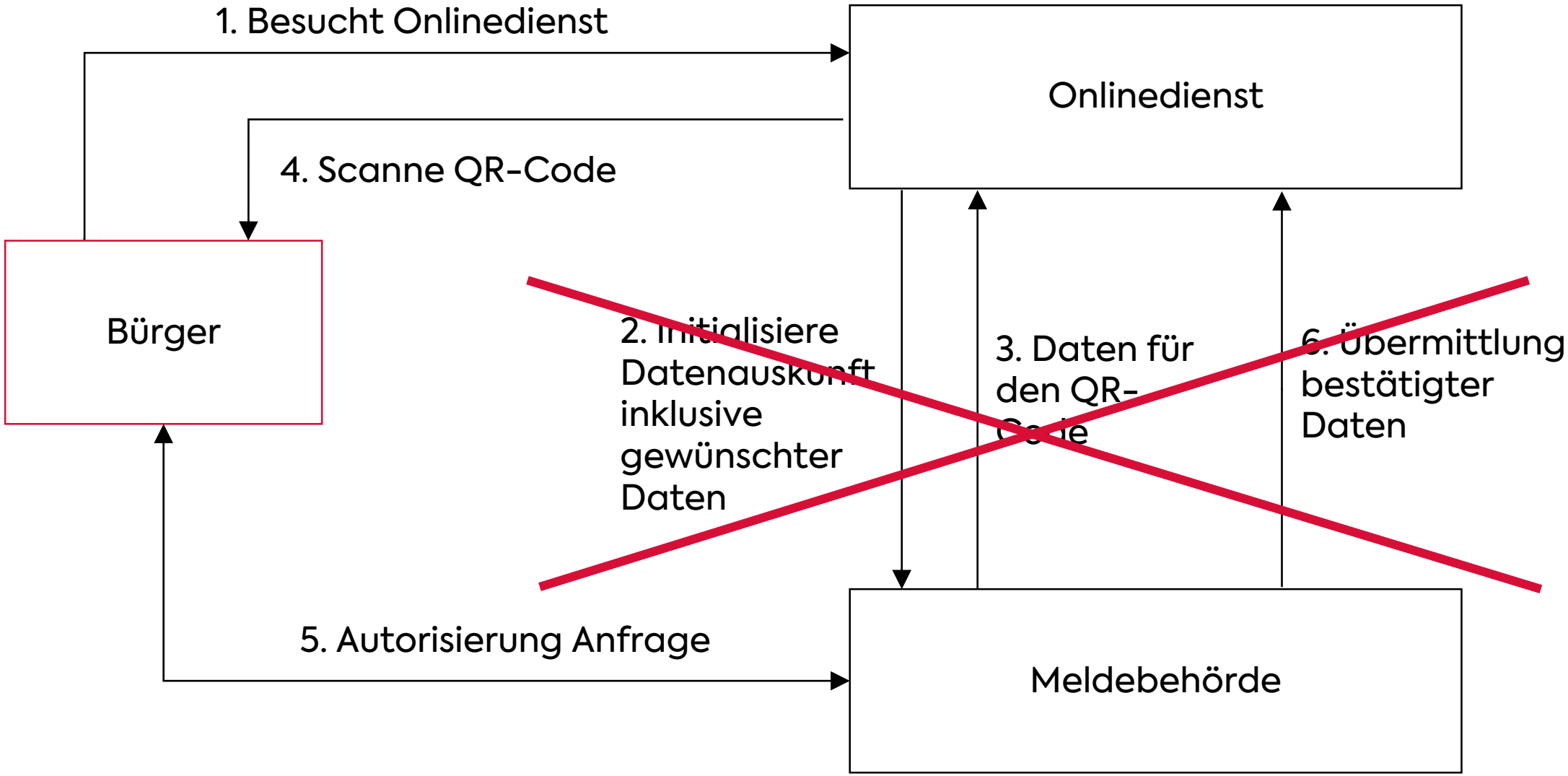
über 700
MitarbeiterInnen

secunet.com/jobs

Backup

Casino Royal: Ohne Auftragsdaten-verarbeitungsvertrag

Ablauf der Datenübermittlung



Schritt 1: Ausfüllen der Registrierungsdaten

Casinowelt: Deutschlands Nr. 1 kostenloses Online-Casino

FSK ab 18

Registrierung

Benutzername

Casino-Genie

Weiter zur Altersverifikation mit deiner BürgerID:

Es wird nur bestätigt, dass du über 18 Jahre alt bist, es werden für das kostenlose Spielerlebnis keine weiteren Daten übertragen

Weiter

Schritt 2: Authentisieren gegenüber der Meldebehörde

BürgerID

Freigabe der BürgerID Daten für das Unternehmen „Casinowelt GmbH“

Bestätige, dass du über 18 Jahre bist um online spielen zu können!

Durch die Bestätigung mit „Sicherer Login“ übermitteln Sie die folgenden Daten:

- Alter über 18 Jahre

Schritt 2: Authentisieren gegenüber der Meldebehörde

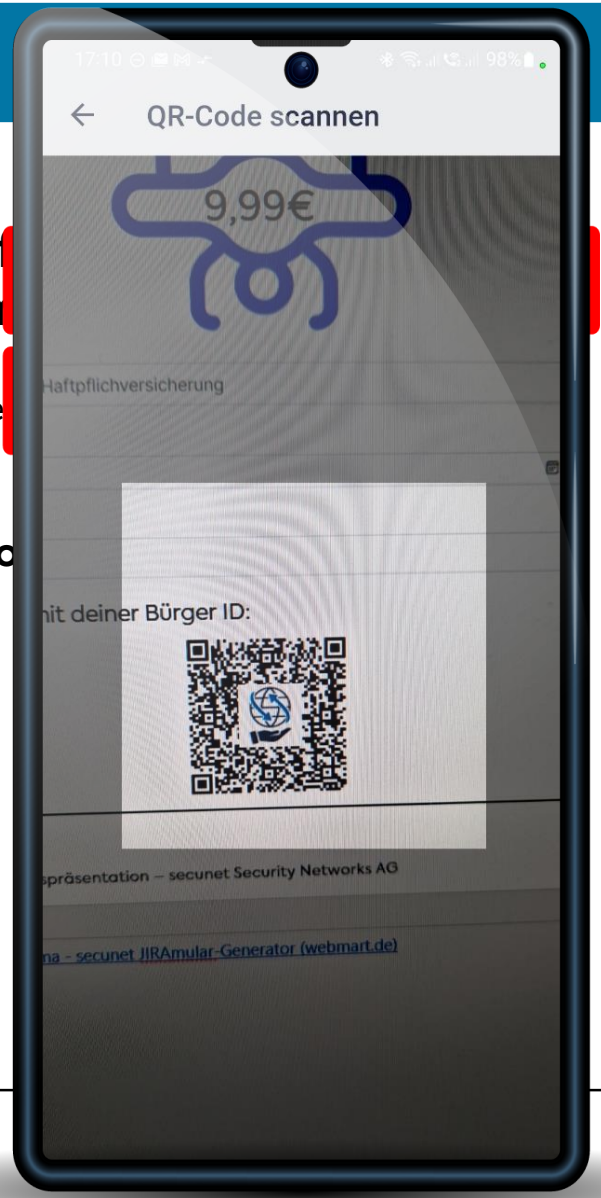
BürgerID

Freigabe der BürgerID Daten f
Unternehmen „Casinowelt Gm

Bestätige, dass du über 18 Jahre bist um online
können!

Durch die Bestätigung mit „Sicherer Lo
Sie die folgenden Daten:

- Alter über 18 Jahre



Schritt 2: Authentisieren gegenüber der Meldebehörde

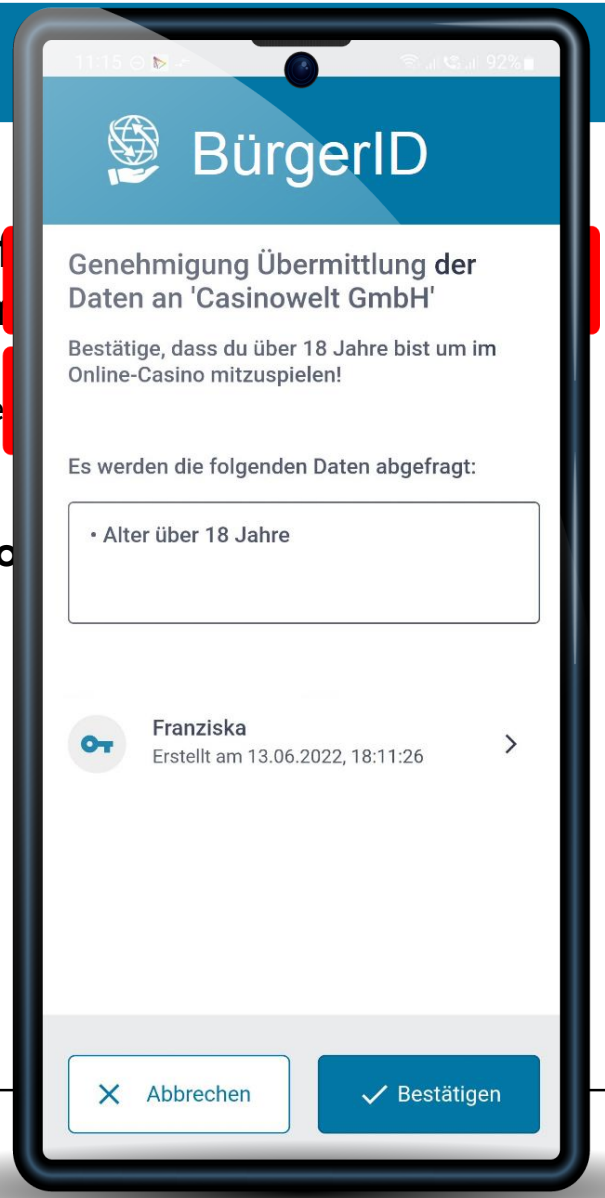
BürgerID

Freigabe der BürgerID Daten f
Unternehmen „Casinowelt Gm

Bestätige, dass du über 18 Jahre bist um online
können!

Durch die Bestätigung mit „Sicherer Lo
Sie die folgenden Daten:

- Alter über 18 Jahre



Schritt 2: Authentisieren gegenüber der Meldebehörde

BürgerID

Freigabe der BürgerID Daten f
Unternehmen „Casinowelt Gm

Bestätige, dass du über 18 Jahre bist um online
können!

Durch die Bestätigung mit „Sicherer Lo
Sie die folgenden Daten:

- Alter über 18 Jahre

Schritt 2: Authentisieren gegenüber der Meldebehörde

BürgerID

Freigabe der BürgerID Daten f
Unternehmen „Casinowelt Gm

Bestätige, dass du über 18 Jahre bist um online
können!

Durch die Bestätigung mit „Sicherer Lo
Sie die folgenden Daten:

- Alter über 18 Jahre

Weiterleitung auf „Elbe

Schritt 2: Authentisieren gegenüber der Meldebehörde

BürgerID

Freigabe der BürgerID Daten für das Unternehmen „Casinowelt GmbH“

Bestätige, dass du über 18 Jahre bist um online spielen zu können!

Durch die Bestätigung mit „Sicherer Login“ übermitteln Sie die folgenden Daten:

- Alter über 18 Jahre

Weiterleitung auf „Elbenschlacht“

Schritt 3: Übermittlung der Daten an den Dienst

Casinowelt: Deutschlands Nr. 1 kostenloses Online-Casino

FSK ab 18

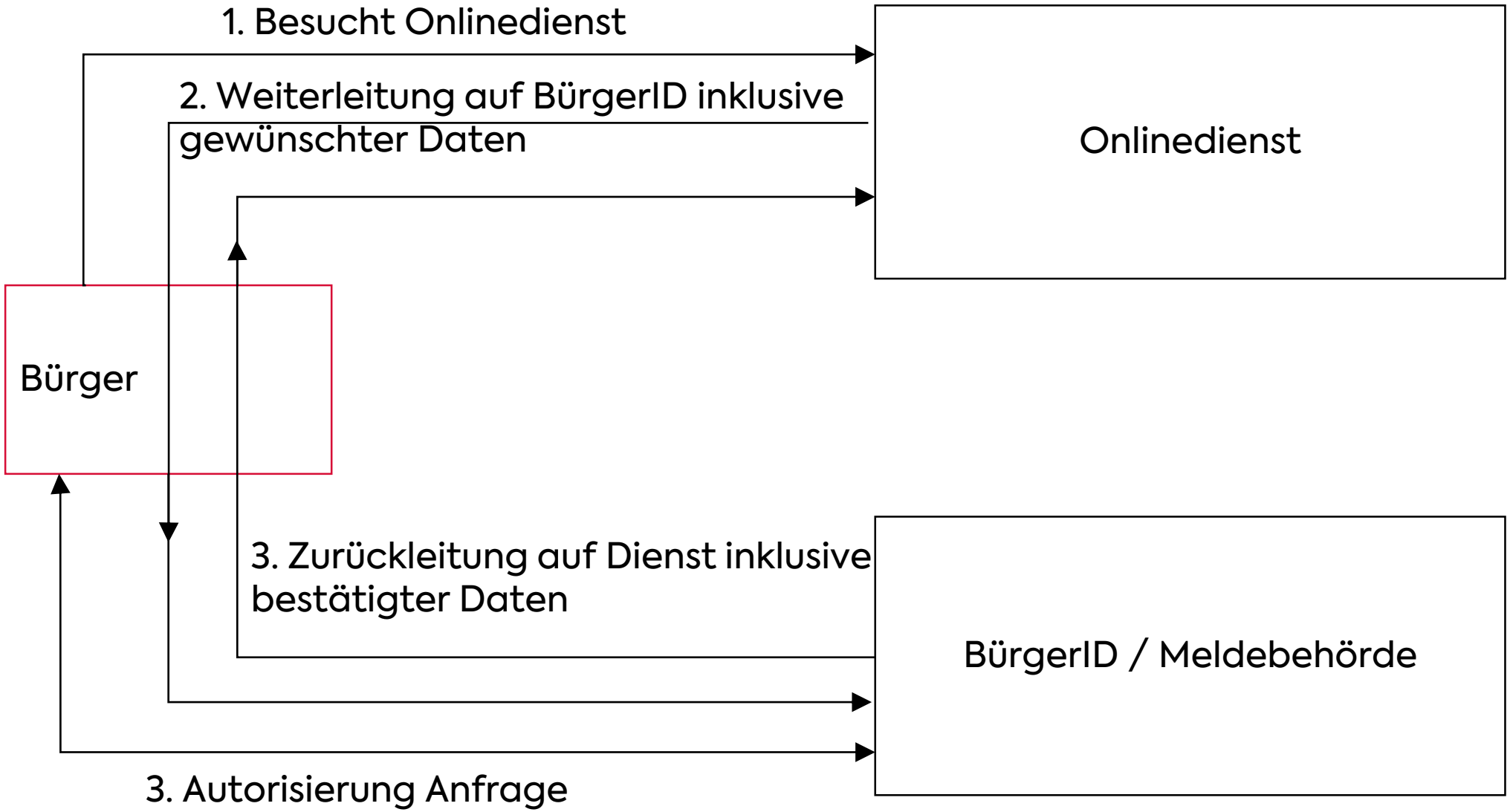
Registrierung

Benutzername

Casino-Genie

Altersverifikation mit deiner Bürger ID erfolgreich!

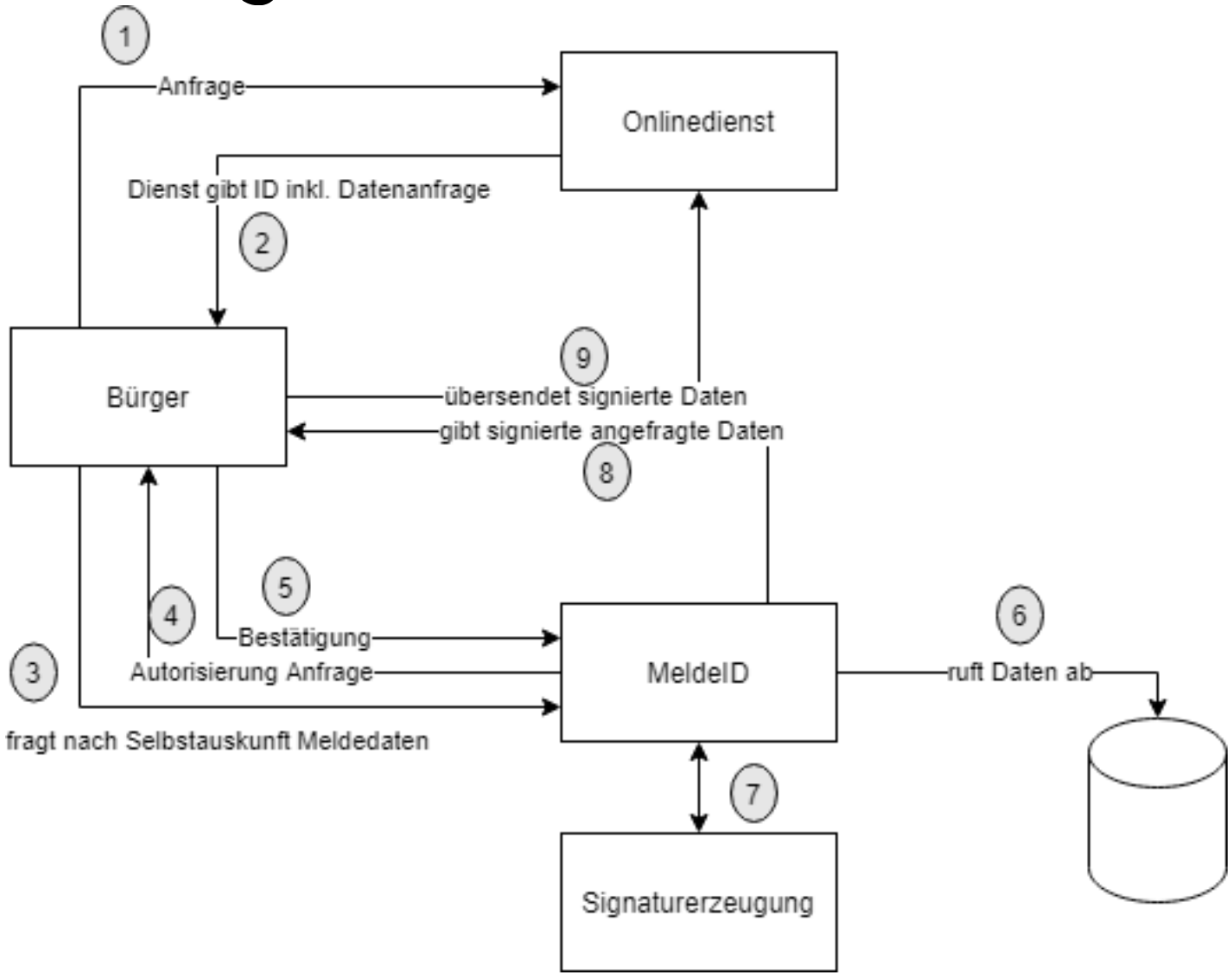
Ablauf der Datenübermittlung




Beispiel:
Altersverifikation
für
Onlineglückspiel


Beispiel :
DroneSafe –
Drohnen-
versicherung

Ablauf für Nutzung



Abgrenzung der aktuellen eID-Systeme

System	Idee Melde-ID	nPA	Smart eID (auf nPA)	eID-Wallet / SSI	Bayern-ID	Elster-ID	Verimi	netID.de / Google / Facebook	Amazon
Datenaktualität	++ Originaldaten des Meldedatensatzes	+ gesetzl. Auflage	o keine Pflicht zur Aktualisierung	noch nicht definiert	- keine gesetzliche Auflage	+ keine Originaldaten, Dritt-DBs wie nPA	- keine Pflicht zur Aktualisierung	+ (Funktion unbekannt)	+ anlassbezogen z.B. wg. Paketzustellung oder Bezahlung
Datenverlässlichkeit	++	++	++	+	++	++	+	-	O
Datenspeicherung	Dezentral / in Kommune	Dezentral / Secure Element	Dezentral / App / secure Element	Dezentral / noch nicht spezifiziert.	Zentral / Land BY/AKDB	Zentral / D / KONSENS	Zentral / D	Dezentral / in D bei Google/FB in USA	Zentral / USA
Usability	+	o	o	gibt es noch nicht				+	++
Dig. Marktdurchdringung (Nutzer) 2021	gibt es noch nicht 80 Mio. (analog) 0 Mio. (digital)	-- 6..8% der Besitzer	-- Start nach 2022 verschoben, handyabhängig	- Start verschoben, unbestimmt	-- kaum Nutzer	ca. 8 Mio. Bürger, alle Firmen in DE	Potentiell 20 Mio., real k.A.	unbekannt	Unbekannt
Potenzielle OZG-/private Dienste Durchdringung	++ Potenziell alle Kommunalleistungen und Privatwirtschaft	o			+ Kommunalportale	+ (Steuer)	+ 40 Use Cases von 30 Anbietern	- nur für private Dienste	- nur für private Dienste
eIDAS Level (höchster erreichbarer)	substantiell	hoch	substantiell	substantiell	hoch (mit nPA)	substantiell	substantiell	normal	normal
Authentifizierung	Smartphone mit PIN; Zertifikat mit PWD; SmartCards mit PIN; USB-Token und weitere Token	User : Ausweis + PIN 6stellig Dienst: Zertifikat	User : Ausweis + Smartphone evtl. Biometrie Dienst: Zertifikat	User: PIN und Smartphone Dienst: nein	verschiedene Level möglich	Zertifikat, Name+Passwort, MFA mit secunet P4U ab Q2/2022	Smartphone mit Biometrie (?)	User: Email + Passwort; MFA optional	User: Name + Passwort, MFA optional
Auflagen / Identifizierung	Persönlich, Papierdokumente, Postzustellung, nPA	Persönlich, Papierdokumente, Postzustellung	Ausweis	Je ID unterschiedlich	nPA, Adresse + Brief	Steuer-ID, Brief	Basic: Email, Voll: nPA/RP	Account beim Anbieter / Email-, Handy-Verifikation	Handynummer / Email, Kreditkarte,
Betriebsaufwand	mittel/gering	hoch (eID-Server)	hoch (eID Server)		gering	mittel	mittel	gering	Gering
Integrationsaufwand	O	-	-	-		o	o	++	++
Mindestalter Nutzer	0 zzgl. Einwilligung	16	siehe nPA	siehe nPA	siehe nPA	18	unbekannt (18?)	unbekannt	unbekannt

Bedarf / Zielsetzung

Neue Varianten des nPA/Smart-eID geplant

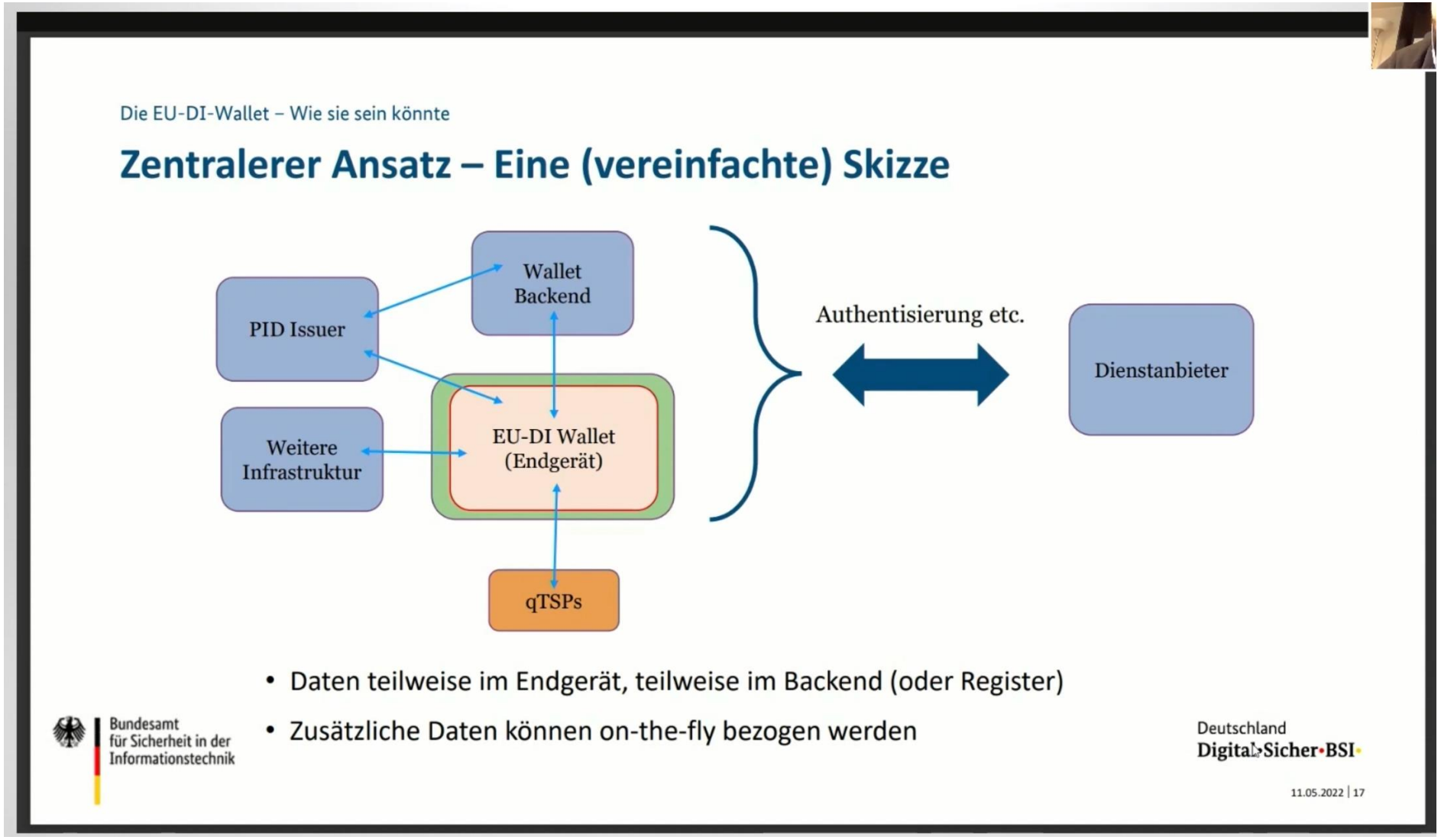
- **Variante 1: Smart eID mit vollem Leistungsumfang (BMI)**
  - kann den Personalausweis vollständig ersetzen
  - Mobiltelefone müssen vom BSI zugelassen werden; aktuell nur Samsung mit S20-Serie aktiv
  - BSI will Daten auf Handy eventuell auch verschlüsselt ablegen, was die Modellabhängigkeit beendet.
- **Variante 2: Smart eID mit reduziertem Leistungsumfang (BMI)**
  - niedrigeres Sicherheitsniveau
- **Variante 3: Basis-ID-Wallet (Bundeskanzleramt)**
  - noch weniger Leistungsumfang als Variante 2; keine Anwendungen mit hohen Sicherheitsanforderungen wie z.B. BAFÖG
  - nicht kompatibel mit den BMI-Varianten; eigene Infrastruktur
  - geeignet z.B. für Hotel-Check-In oder Anmietung von Fahrzeugen/Carsharing
  - Pilotprojekt ‚digitaler Führerschein' zunächst gescheitert

Quelle 10/2021: https://www.heise.de/news/E-Perso-Der-Personalausweis-kommt-in-drei-Varianten-aufs-Smartphone-6194859.html

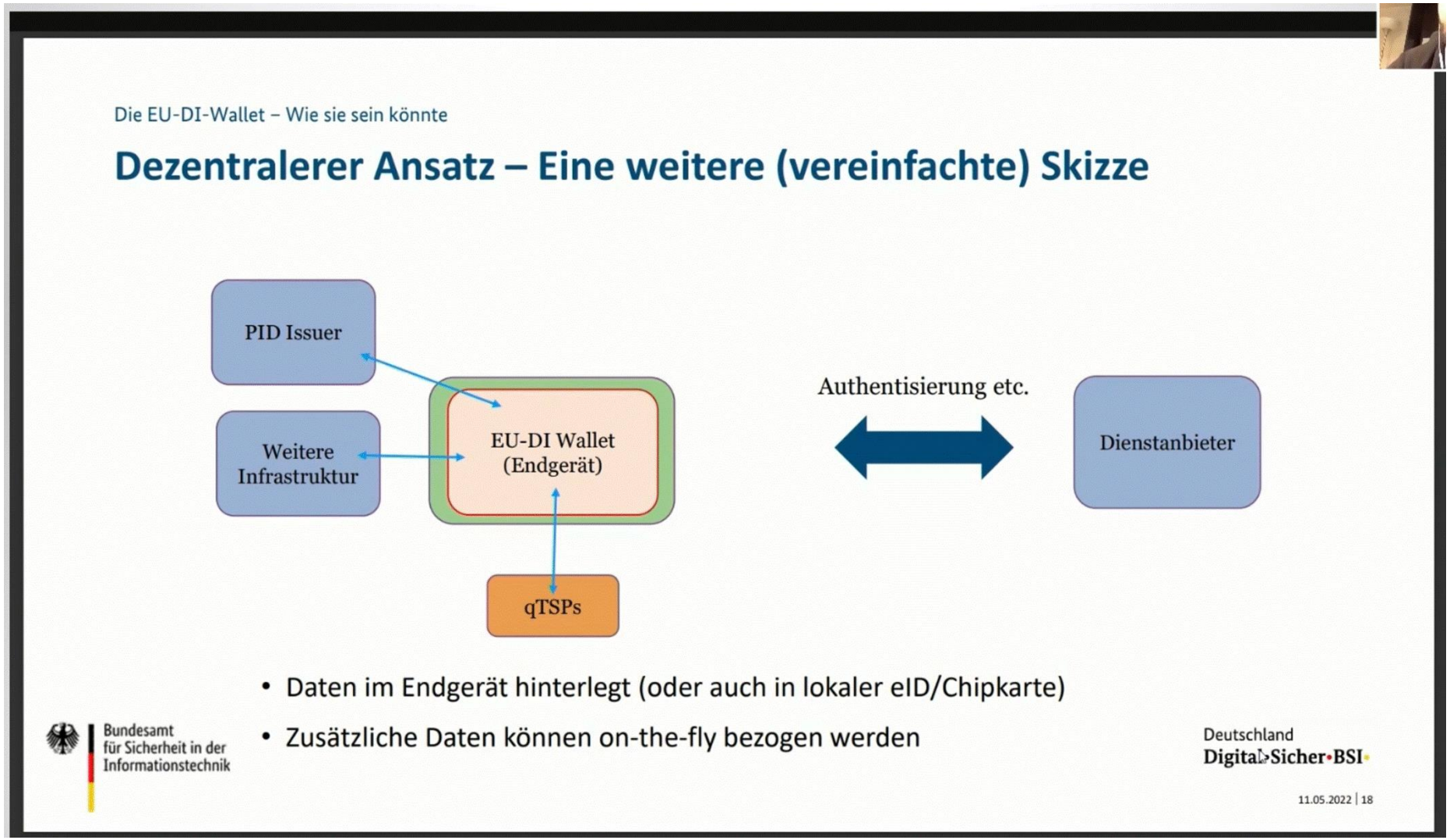
Allgemeine Punkte

- SSI
  - Wer bezahlt die Infrastruktur?
  - Wer ist verantwortlich?
  - Wer führt die Prozesse durch?

eID Summit: Felix Bleckmann



eID Summit: Felix Bleckmann



Statistiken

▼ Ist bei Ihrem Personalausweis die Online-Ausweisfunktion einsatzbereit? Haben Sie die Online-Ausweisfunktion Ihres Personalausweises schon einmal genutzt? Über welche Schnittstelle?

97 % Befragte mit gültigem Personalausweis

Genutzt | Einsatzbereit, aber nicht genutzt | Nicht einsatzbereit | Weiß nicht / k.A.

BASIS: Alle Befragten mit gültigem Personalausweis – DE (n = 7.364); Hinweis: andere Darstellung als im eGovernment MONITOR 2020, Zahlen aufgrund unterschiedlicher Basis nicht vergleichbar.

BASIS: Alle Befragten mit gültigem Personalausweis, die schon einmal die Online-Ausweisfunktion genutzt haben – DE (n = 659)