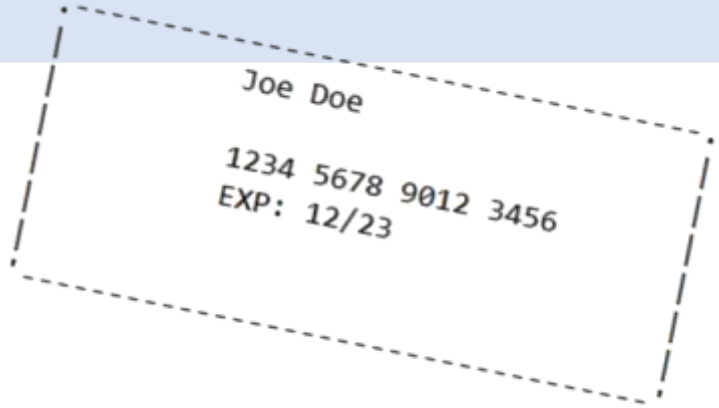


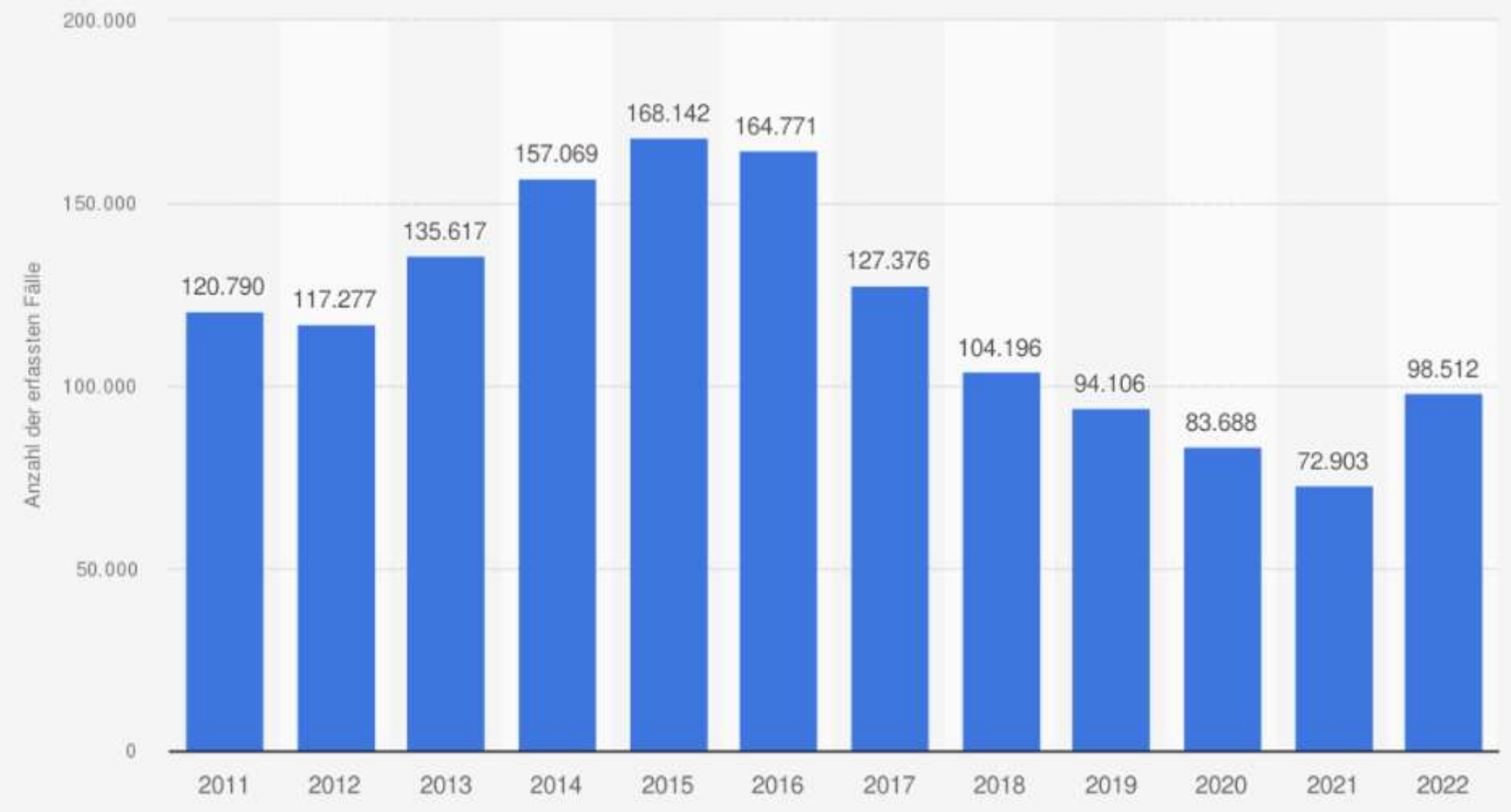
Oh no: KUNO
Gesperrte Girocards entsperren

Tim Philipp Schäfers (TPS)

37. Chaos Communication Congress (37c3)

30. Dezember 2023, Hamburg

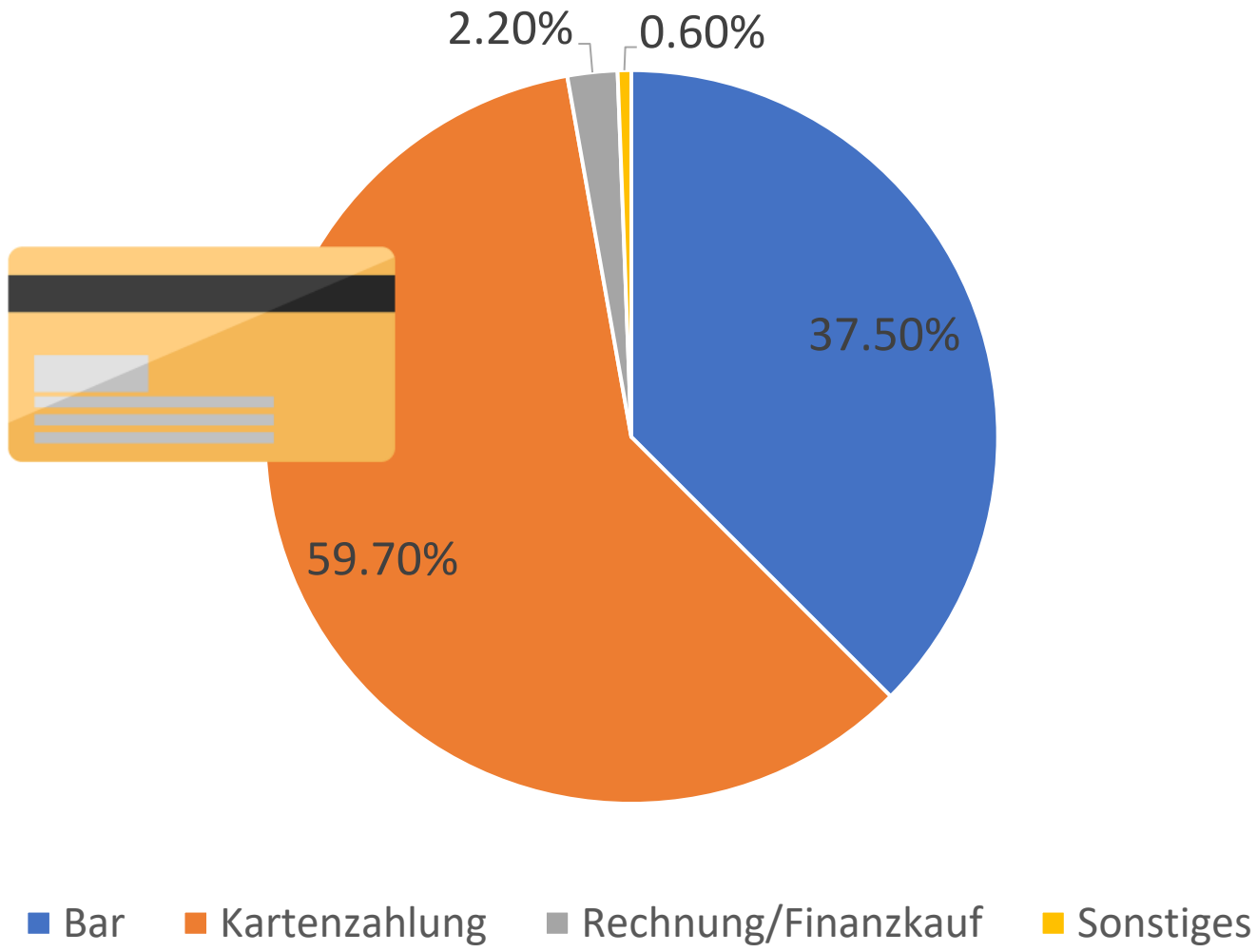
Statistik zu Taschendiebstahl in Deutschland



Quelle: BKA - Polizeiliche Kriminalstatistik (PKS)

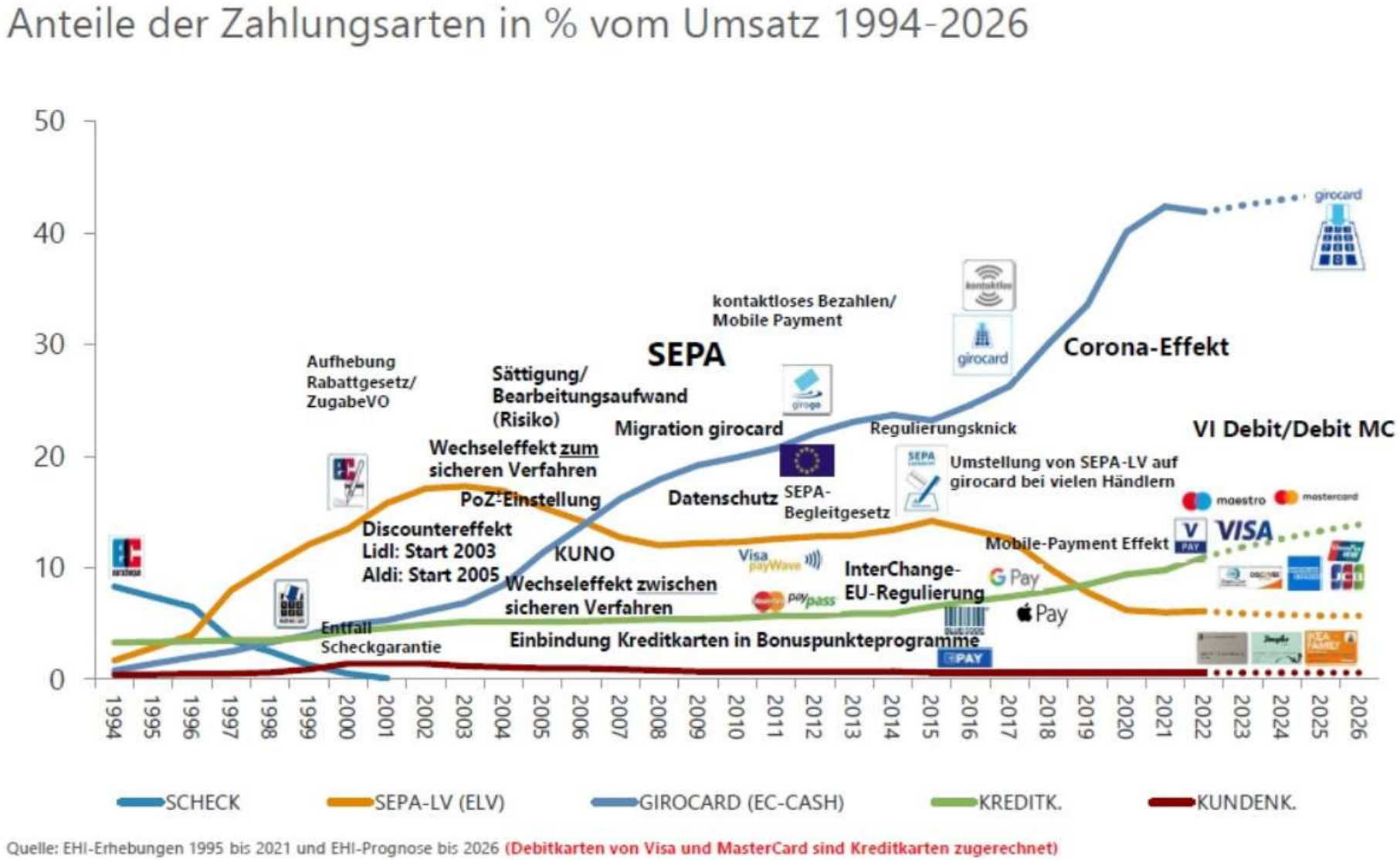
(Bargeldlose) Zahlungsmittel

Verteilung Zahlungsmittel 2022



Quelle: EHI-Studie „Zahlungssysteme im Einzelhandel 2023“ (im stationären Handel)

Entwicklung von unbaren Zahlungsarten



Quelle: Hanno Bender & Horst Rüter (EHI), https://www.bargeldlosblog.de/die-lange-geschichte-der-lastschrift/

Zahlungsarten bei Kartenzahlung 2022

Zahlungsart	Beginn / Ende	Marktanteil*
Elektronisches Lastschriftverfahren (ELV) / SEPA-Lastschrift	Seit 1984	6,1 % 28,365,000,000 €
Girocard (Maestro)	1990er (EC & ECD) ab 2007 (Umbenennung der EC-Karte) 2007-2027 (geplantes Ende der Maestro-Karte)	41,9 % 194,835,000,000 €
Kreditkarte	-	8,2 % (38,130,000,000 €)
Debit International	-	2,9 % (13,485,000,000 €)
Handelskarte	-	0,6 % (2,790,000,000 €)

* Quelle: EHI-Studie „Zahlungssysteme im Einzelhandel 2023“

* Marktanteil im Stationären Handel 2022 nach (exkl. Kfz, Mineralöl, Apotheken, E-Commerce/Versandhandel, inkl. Tankstellen-Shopumsätze)

Zahlungsarten bei Kartenzahlung 2022

Zahlungsart	Beginn / Ende	Marktanteil*
Elektronisches Lastschriftverfahren (ELV) / SEPA-Lastschrift	**Seit 1984**	6,1 % 28,365,000,000 €
Girocard (Maestro)	1990er (EC & ECD) ab 2007 (Umbenennung der EC-Karte) 2007-2027 (geplantes Ende der Maestro-Karte)	41,9 % 194,835,000,000 €
Kreditkarte	-	8,2 % (38,130,000,000 €)
Debit International	-	2,9 % (13,485,000,000 €)
Handelskarte	-	0,6 % (2,790,000,000 €)

* Quelle: EHI-Studie „Zahlungssysteme im Einzelhandel 2023“

* Marktanteil im Stationären Handel 2022 nach (exkl. Kfz, Mineralöl, Apotheken, E-Commerce/Versandhandel, inkl. Tankstellen-Shopumsätze)

Tagesschau vom 28.12.1984 (erster Congress)

Quelle: Auszug Tagesschau vom 28.12.1984 (ARD)

„[…] Möglichkeiten und Mängel des Computers selbst beurteilen können.“

➔Sperrsysteme für Bankkarten …*

(͡° ͜ʖ ͡°)

* Fokus auf Girocards
Entsprechende Sicherheitslücken wurden im Rahmen von Responsible Disclosure Meldungen den Betreibern gemeldet.

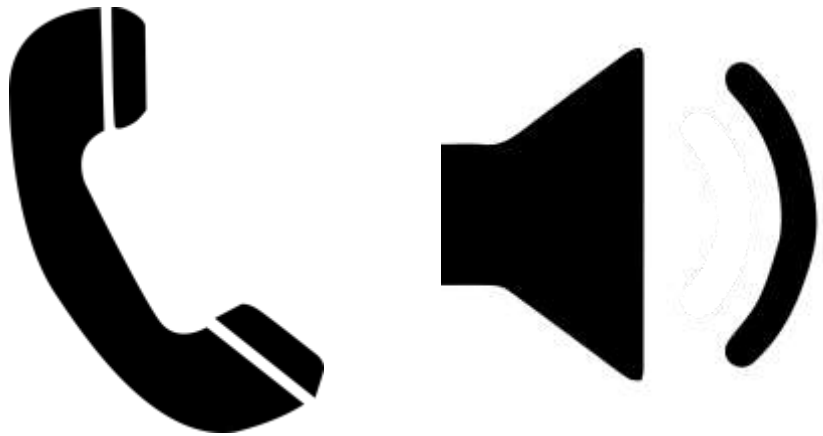
Sperr-Notruf

- Sperr-Notruf 116 116 e.V.
- 2002 gegründeter Verein
- 1,5 Millionen Sperrungen und Sperrvermittlungen im Jahr
- > 1.200 angeschlossene Banken + weitere Organisationen
- Sperrung weiterer Karten möglich: Personalausweis, Mitarbeiterausweise, etc.
- technische Realisierung: SERVODATA GmbH

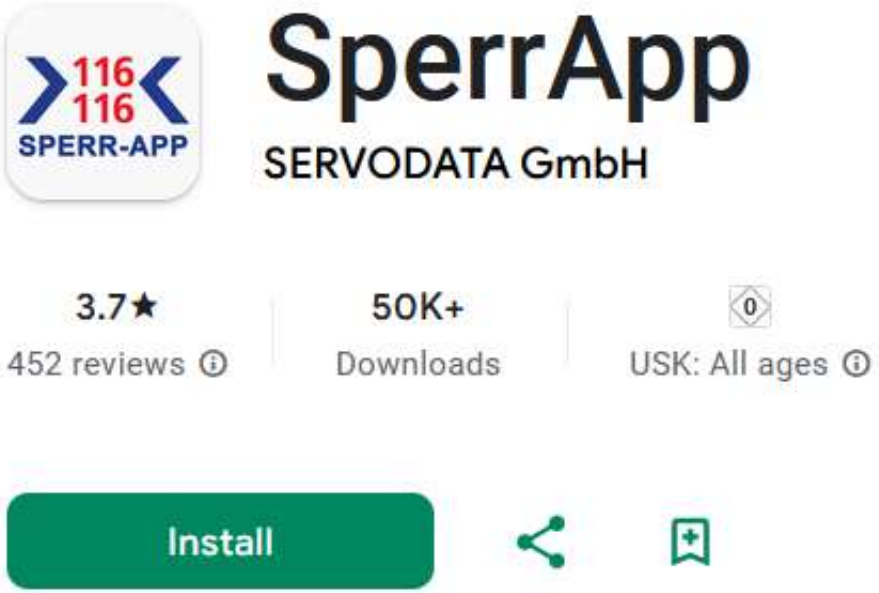
Sperr-Notruf

SPERR-NOTRUF
116 116

- Automatisierter Ablauf für Sperrungen
- Verbindung von einem „Sprachcomputer“ zum anderen
- Anschließende Weiterleitung der Sperre an zuständige Bank



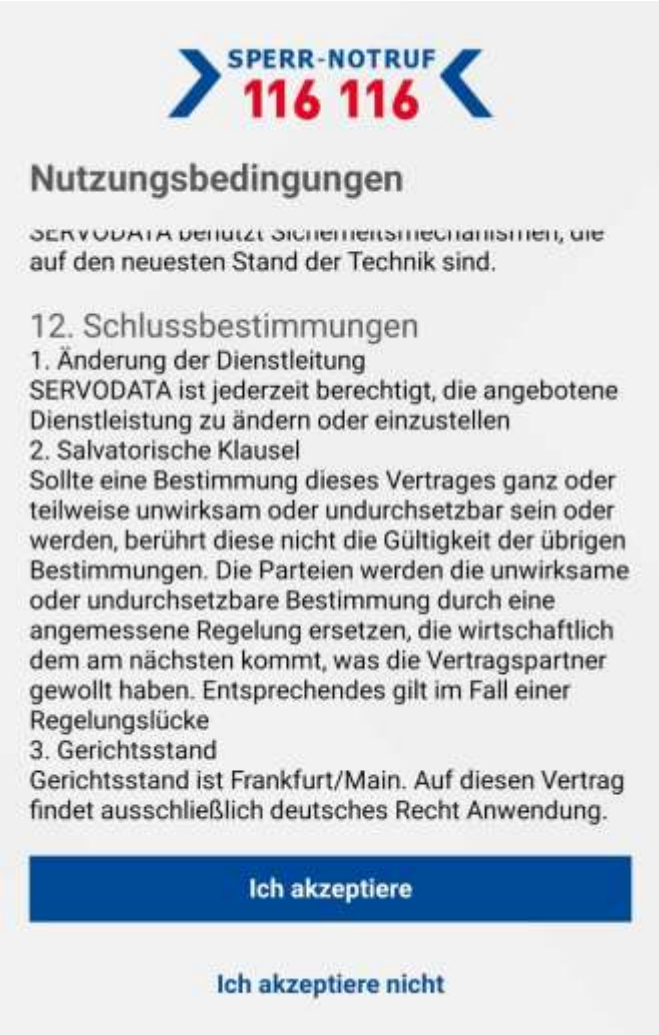
SperrApp

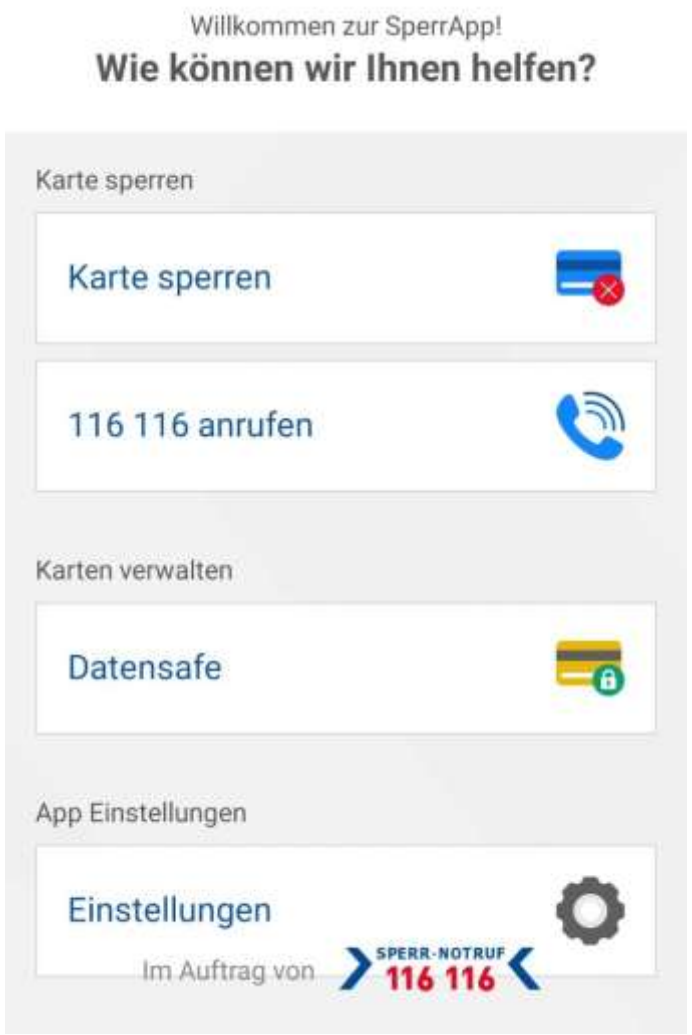


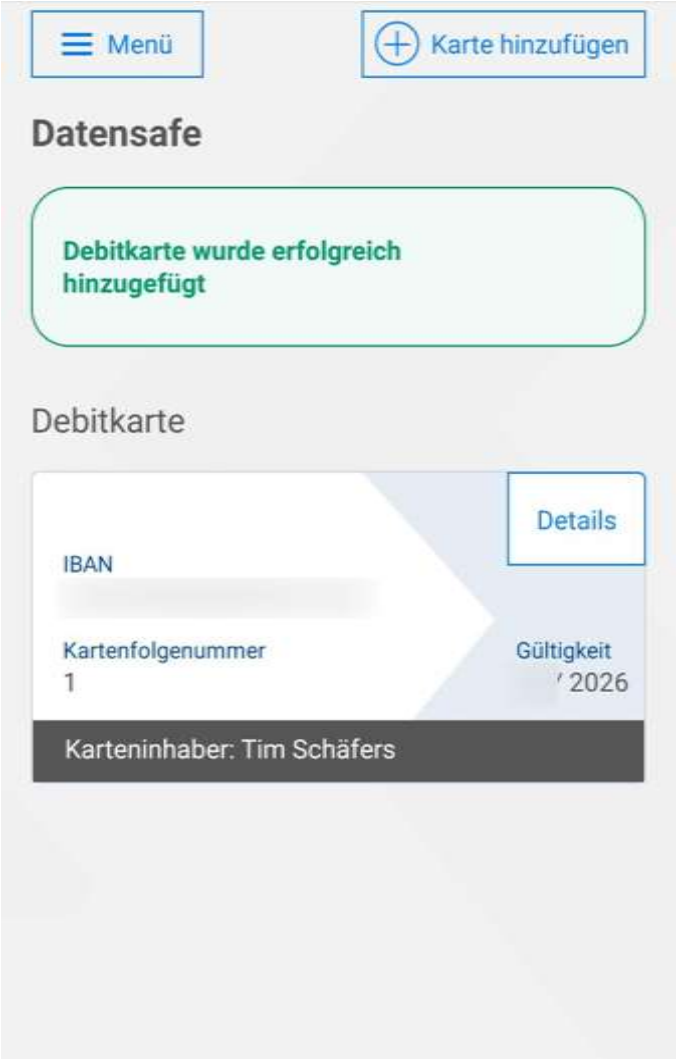
https://play.google.com/store/apps/details?id=de.servodata.sperrapp

https://apps.apple.com/de/app/sperrapp/id765585858

SperrApp

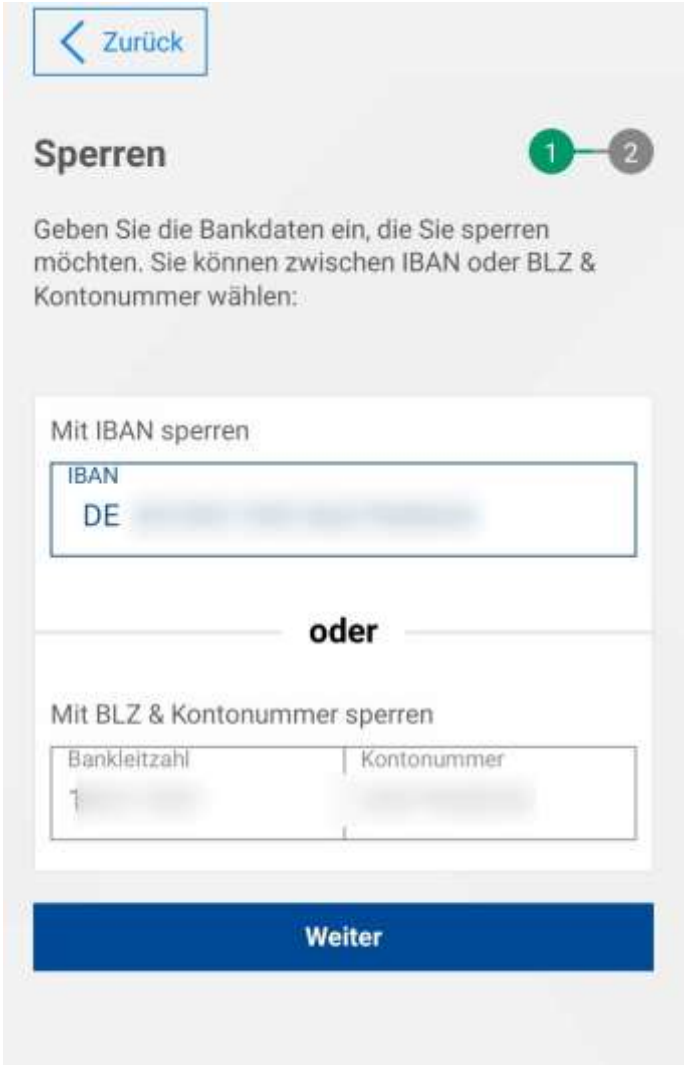






Eigene Screenshots

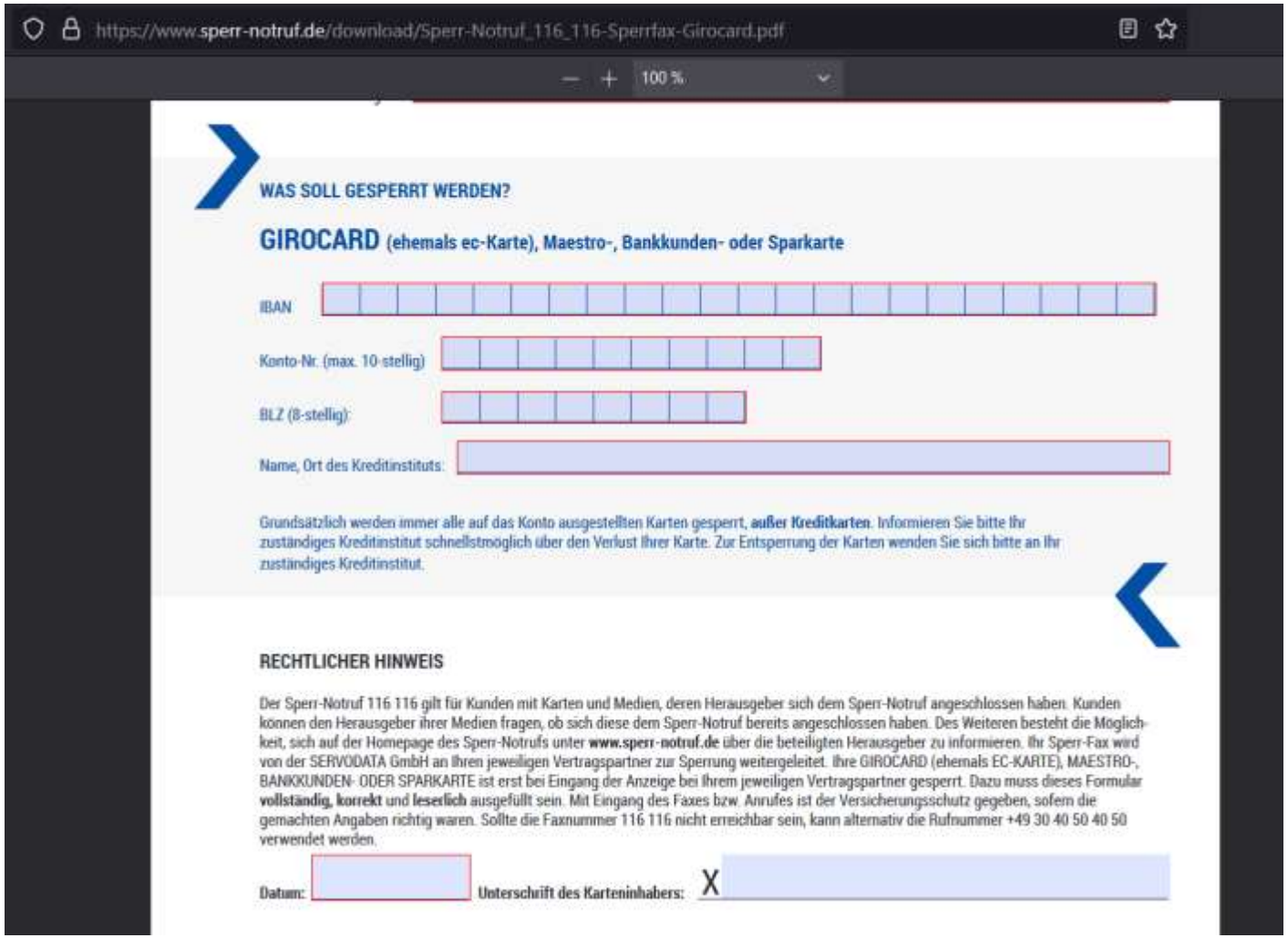
SperrApp



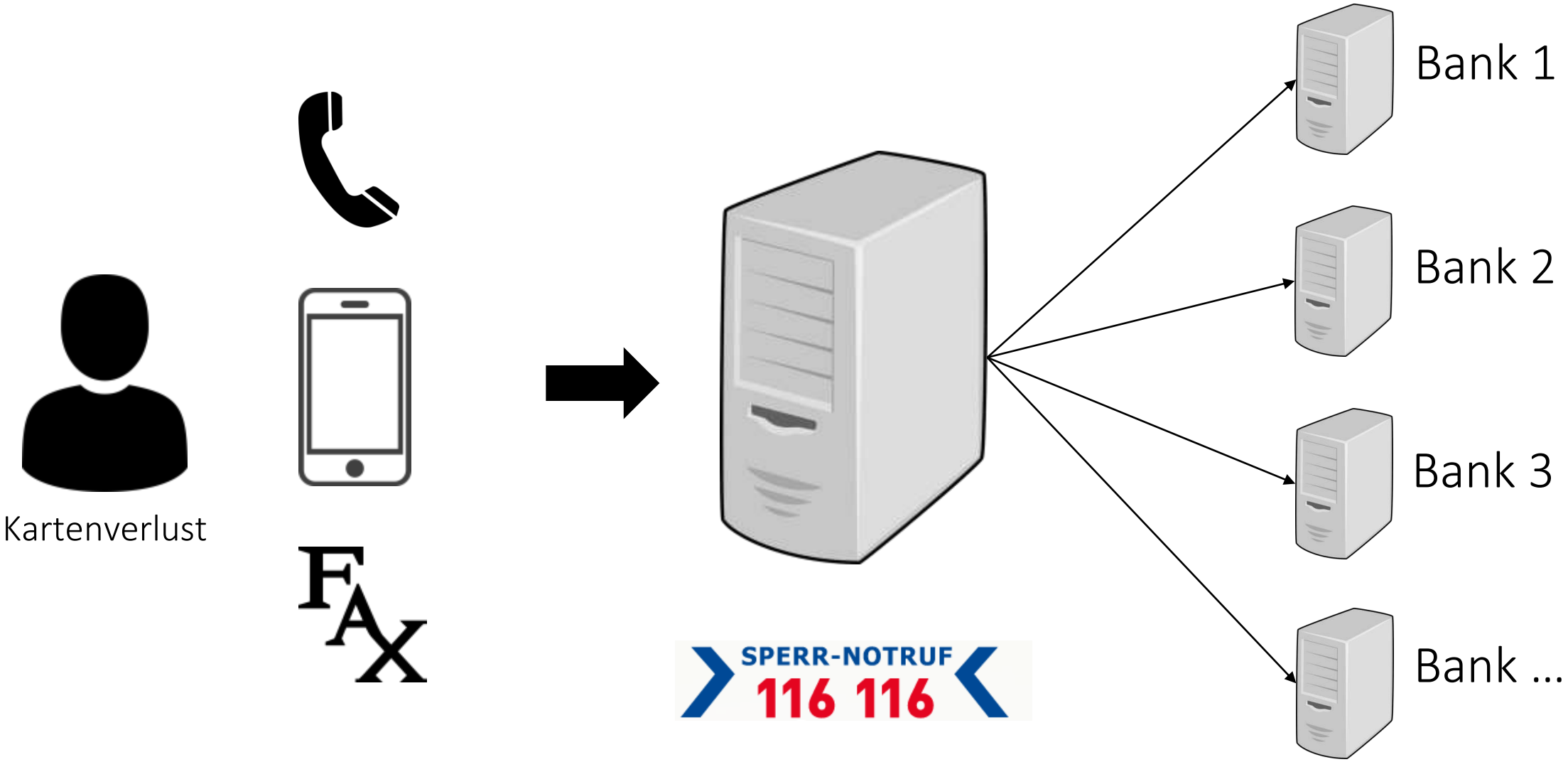
Eigene Screenshots

Sperren 2023 – aber wie?

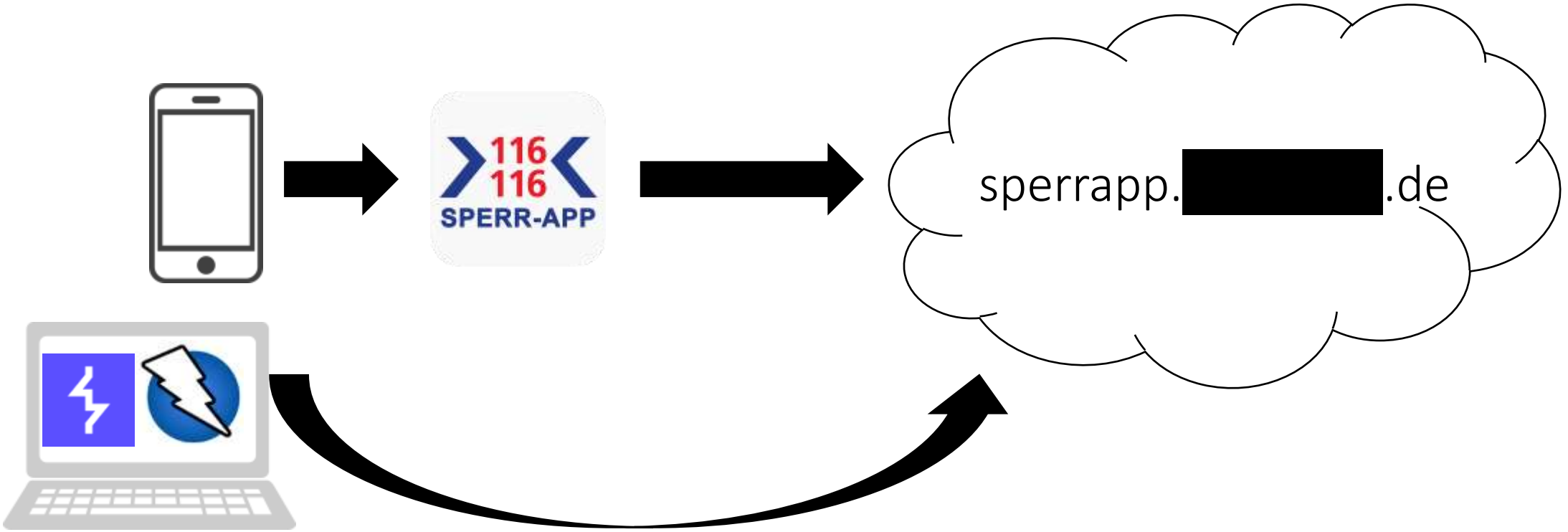
Quelle: https://www.sperr-notruf.de/sperr-fax-sperr-app.html



116 116 Sperr-Notruf - Funktionalität

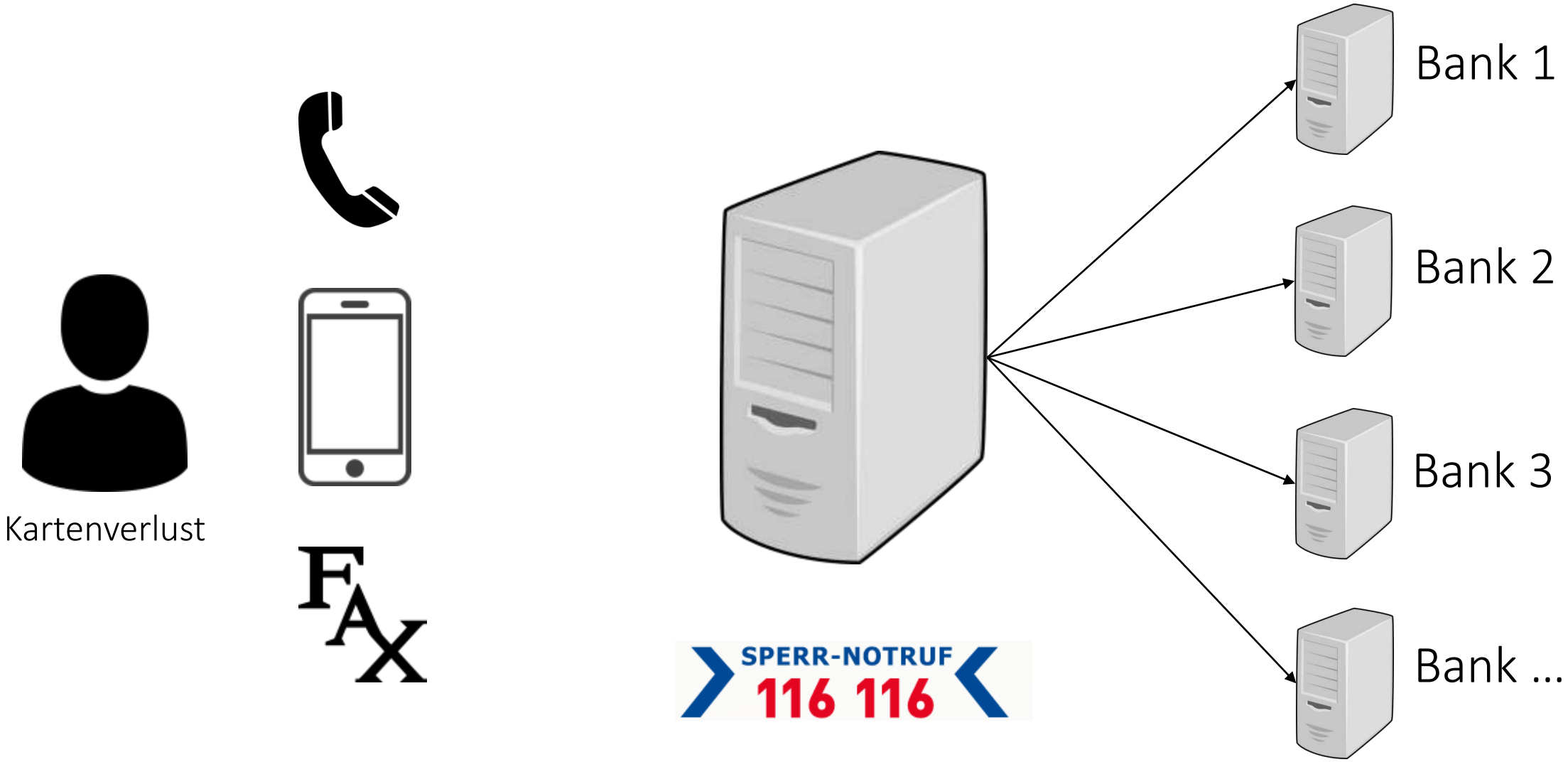


Sperr-App

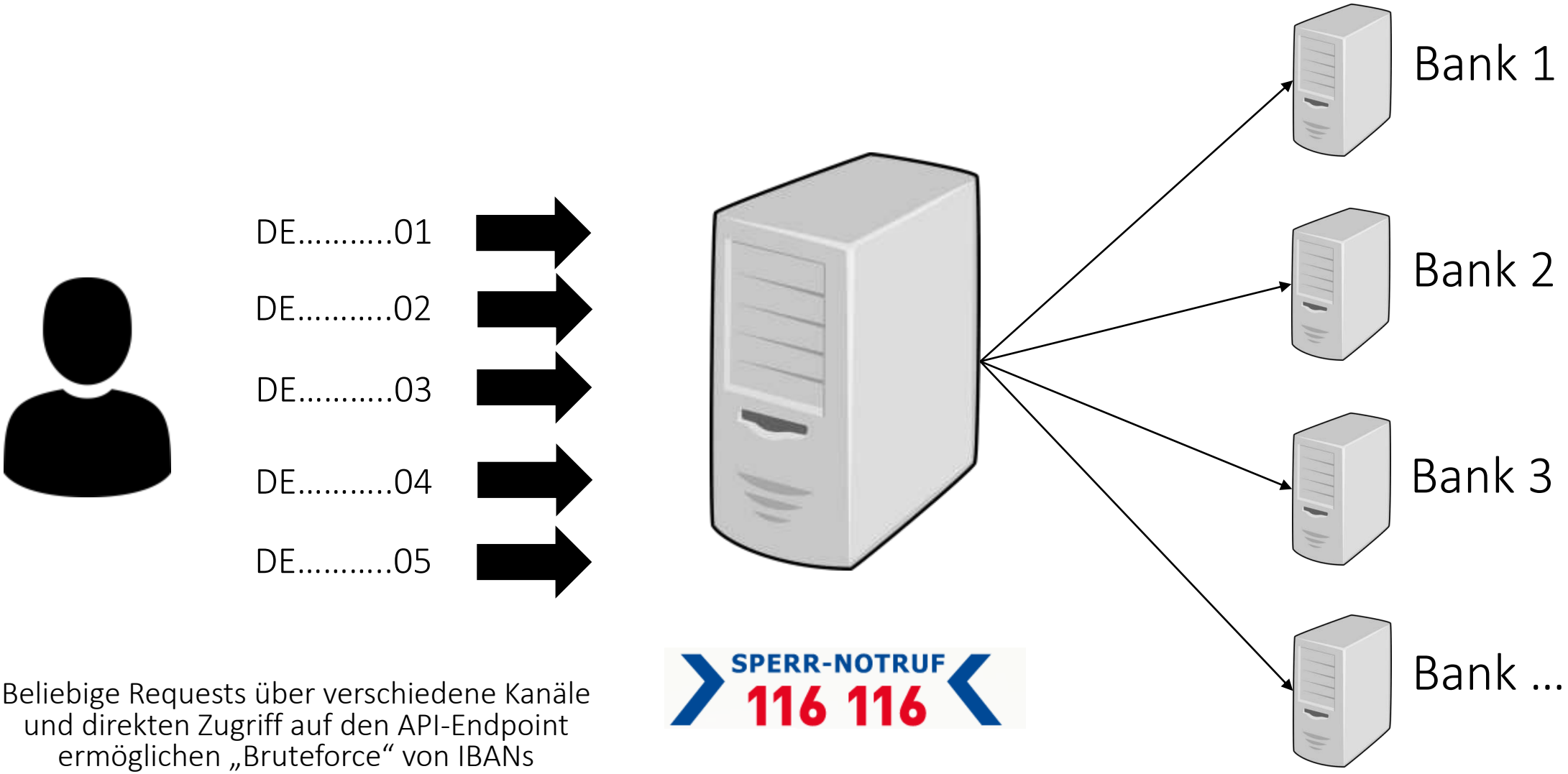


Ratelimiting Bypass via
Intercepting Proxy auf lokalem Rechner

Sperr-Notruf - Funktionalität



Sperr-Notruf - Massensperrung

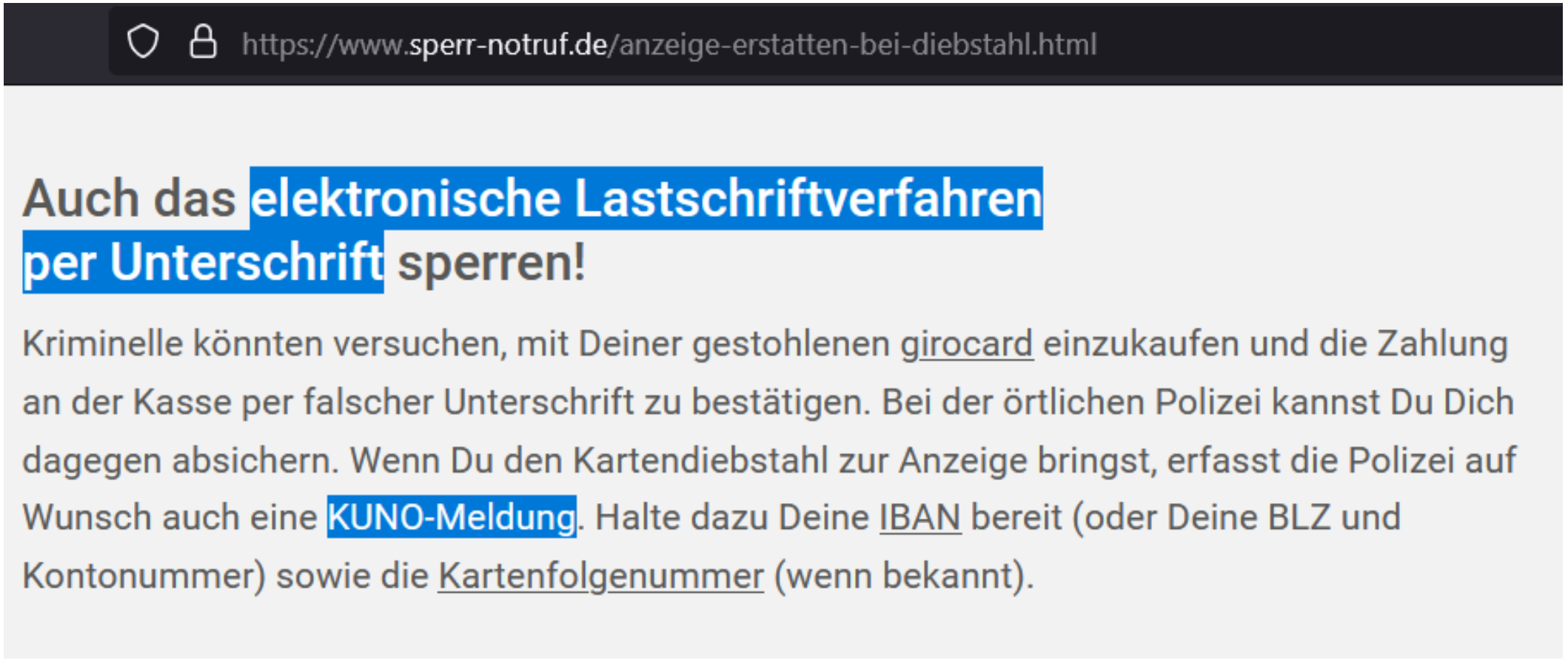


Beliebige Requests über verschiedene Kanäle und direkten Zugriff auf den API-Endpoint ermöglichen „Bruteforce“ von IBANs

Karte gesperrt, alles gut? 😊
Leider nicht ganz …

Nicht alles wurde gesperrt 😮?

Quelle: https://www.sperr-notruf.de/anzeige-erstatten-bei-diebstahl.html



KUNO? 😉

Quelle: privat | Kuni

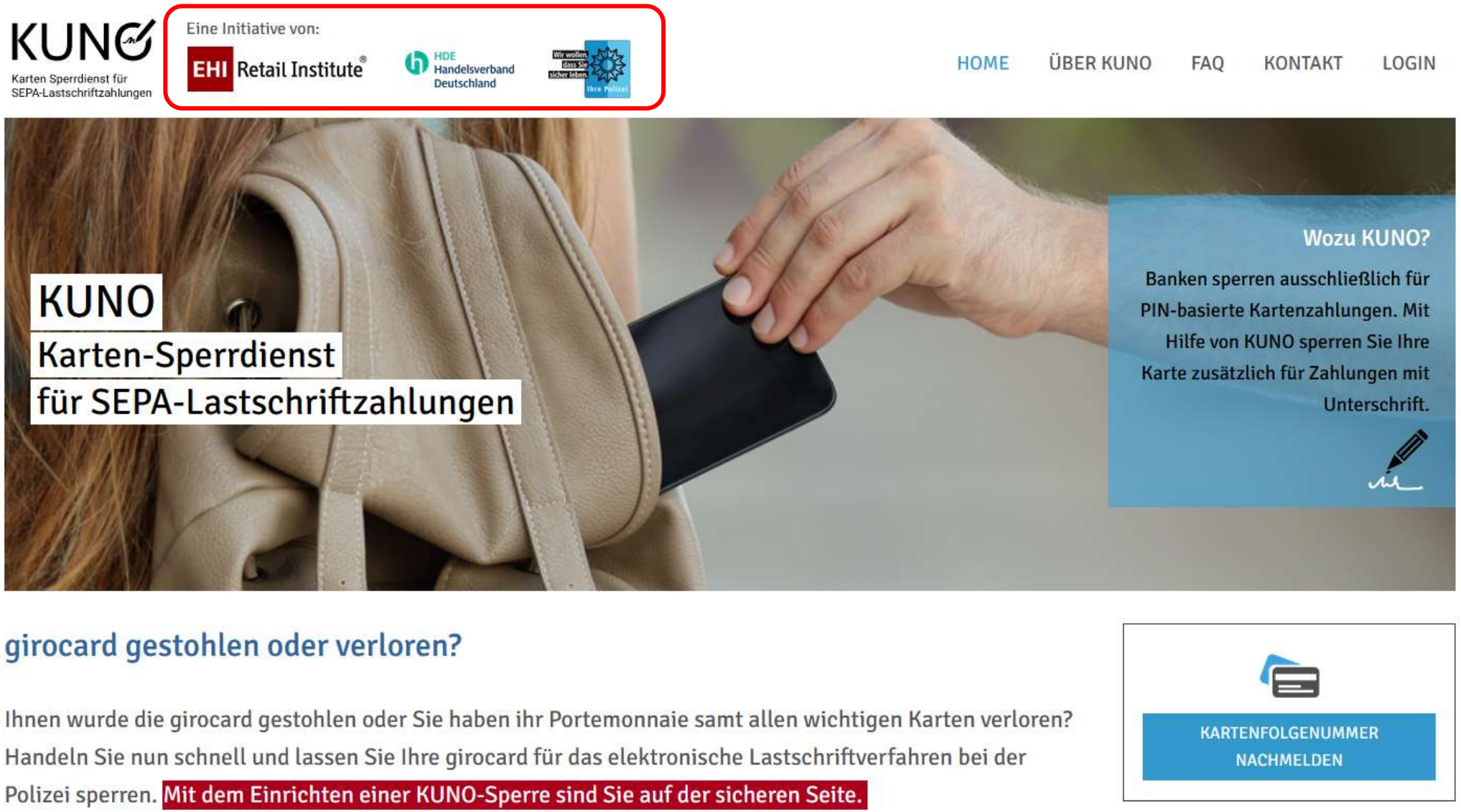
KUNO? 😉

Quelle: Pixabay | maminounou

KUNO-Sperrsystem

Quelle: Auszug ZDF WISO vom 09.05.2016 (ZDF)

KUNO-Sperrsystem



Wofür steht KUNO? 

K

U

N

O

Wofür steht KUNO? 🧐

K riminalitätsbekämpfung im
U nbaren Zahlungsverkehr durch
N utzung nichtpolizeilicher
O rganisationen

KUNO-Sperrsystem

KUNO
Karten Sperrdienst für
SEPA-Lastschriftzahlungen

Betreiber:

- EHI Retail Institute GmbH
- Handelsverband Deutschland
- Deutsche Polizei - ProPK (Polizeiliche Kriminalprävention der Länder und des Bundes)

- Sperrung der SEPA-Lastschrift (ELV) pro IBAN durch Eintrag in Sperrdatei
- Testsystem 2001, Ausweitung ab 2005 nach Beschluss der Innenministerkonferenz
- > 120.000 Sperrungen im Jahr
- technische Realisierung: EHI Retail Institute GmbH (mit Dienstleistern)

KUNO-Sperrsystem - Versprechen

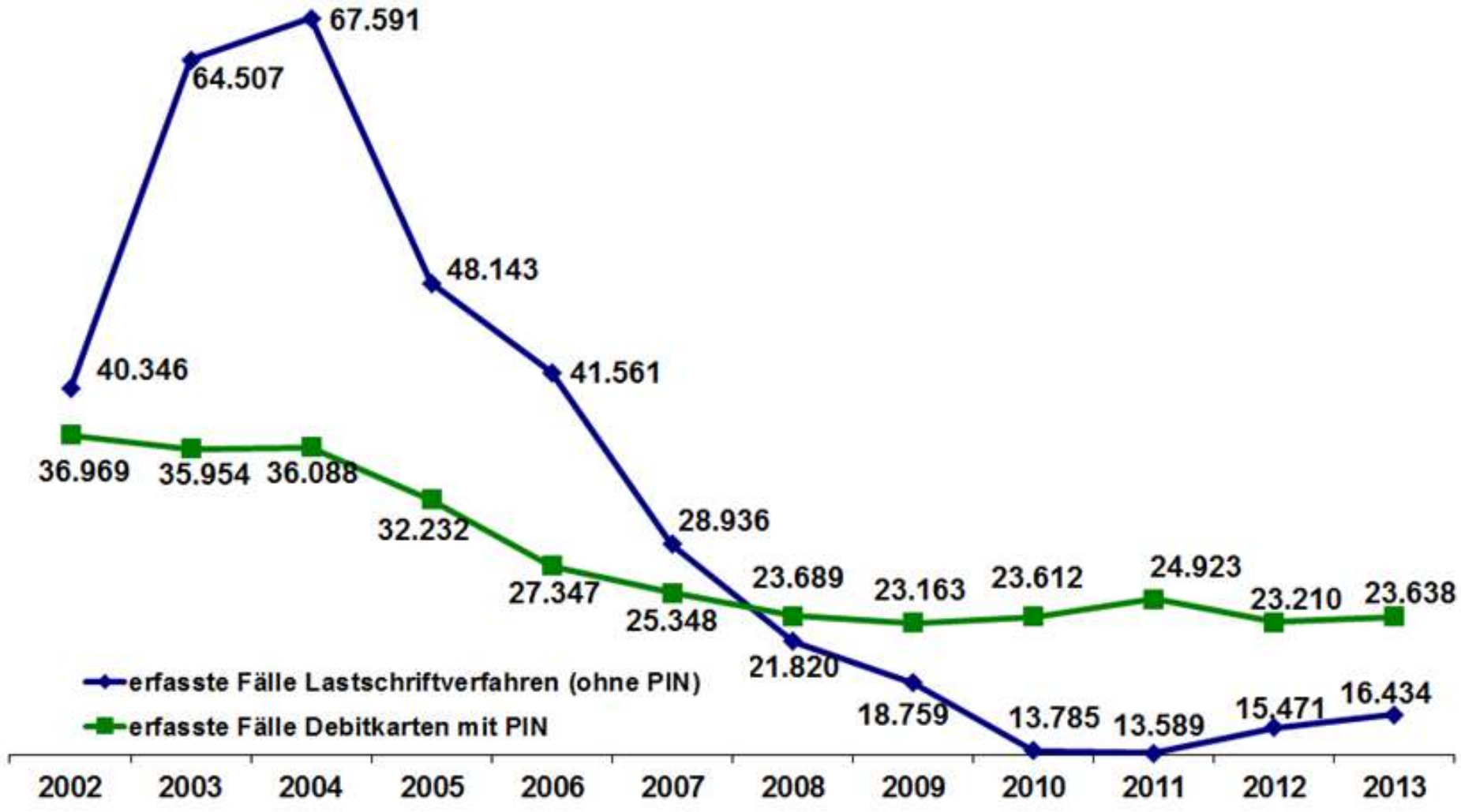
„Mit dem Einrichten einer KUNO-Sperre sind Sie auf der sicheren Seite.“
KUNO – Startseite

„[…] Es ist ein Beitrag zu mehr Sicherheit in unserem Land. Die erweiterte Kartensperre schützt Bürger und Handel vor Scheckkarten-Betrügern […]“
Innenminister Jörg Schönbohm
(Ministerium des Innern Brandenburg, 2003)

„So können Sie geklaute EC-Karten effektiv sperren lassen.“
Handwerksblatt 2016

„KUNO stellt ein simples, aber wirkungsvolles Sperrsystem dar […]“
KUNO – Über uns

KUNO-Sperrsystem zeigt Wirkung



Quelle: https://einzelhandel.de/themeninhalte/zahlungssysteme/281-nachrichten/6502-polizeiliche-kriminalstatistik-betrug-im-elv-verfahren-weiter-auf-niedrigem-niveau / Polizeiliche Kriminalstatistik 2002-2013

KUNO-Sperrsystem - Funktionalität

Meldung an KUNO

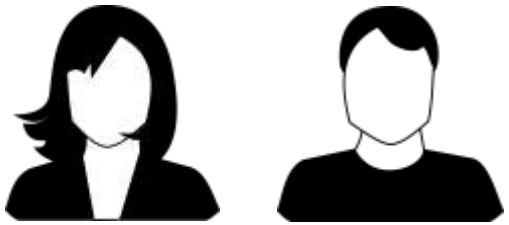
KUNO

Karten Sperrdienst für SEPA-Lastschriftzahlungen

Self-Service*

3.) Betroffene Personen

Freischaltung oder Meldung der Kartenfolgenummer



1.) Polizei

Aufnahme von zu sperrendem Konto bei Anzeige von Diebstahl

Bezug der Sperrdatei

2.) Handel & Payment Dienstleister

Abgleich mit Sperrdateien/ Zurückweisung von gestohlenen Debitkarten

* 3 Bundesländer (Mecklenburg-Vorpommern, Rheinland-Pfalz, Sachsen) erlauben kein Self-Service.

Karte gesperrt, alles gut? 😊
Leider nicht ganz …

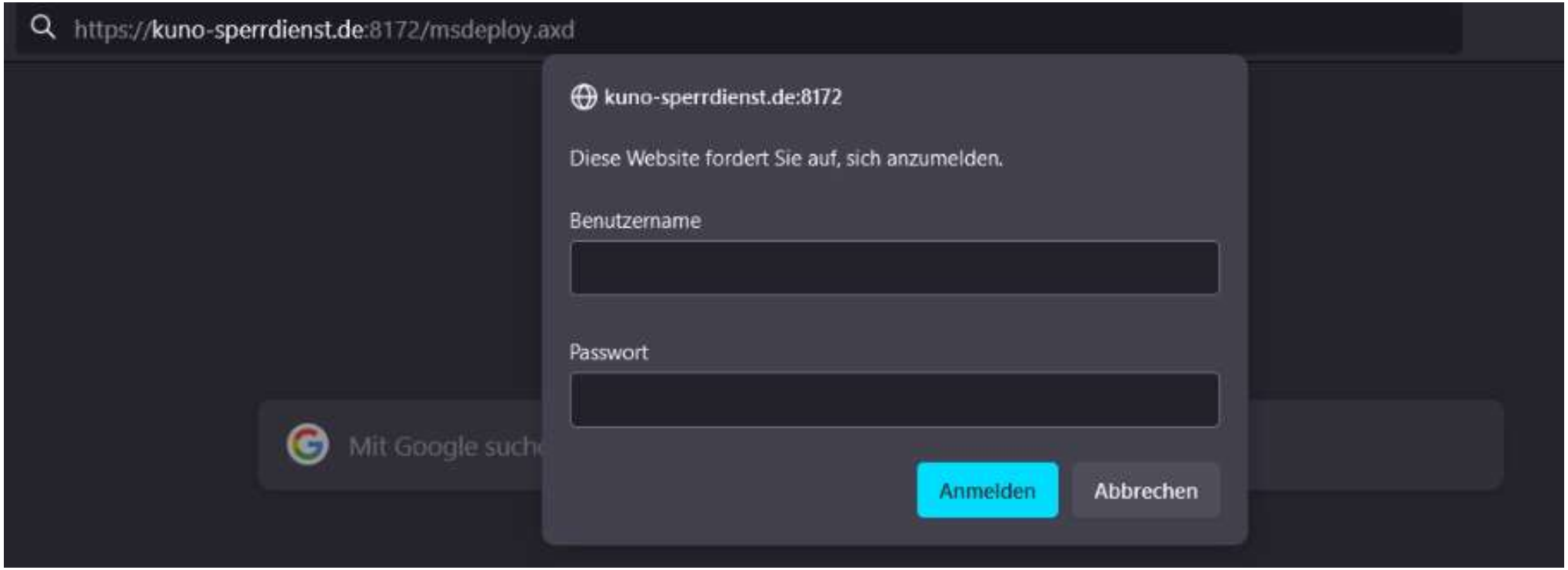
Auszug: **Sicherheits- & Datenschutzprobleme** aus der Responsible Disclosure Meldung

32-seitiger Report

Port Scan …

nmap -p 1-65535 -T4 -A -v kuno-sperrdienst.de
PORT STATE SERVICE VERSION
80/tcp open http
[…]
443/tcp open ssl/https Microsoft-IIS/10.0
[…]
| http-methods:
| Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Willkommen bei KUNO Sperrdienst - Eine Initiative von EHI, HDE...
[…]
1221/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
[…]
3544/tcp closed teredo
4022/tcp open dnox?
4024/tcp open tnp1-port?
8172/tcp open ssl/http Microsoft IIS httpd 10.0

IIS Management Port im Internet



Port 8172 - Standard-Port des IIS Management Services

Webserver auf Microsoft Azure …
Bereitstellung von Webpaketen mittels MSDeploy (Username/Passwort)

IIS Management Port im Internet

Azure App Service - How to block MsDeploy.axd on port 8172

Ask Question

Asked 3 years, 7 months ago Modified 3 years, 7 months ago Viewed 968 times

Part of Microsoft Azure Collective

4

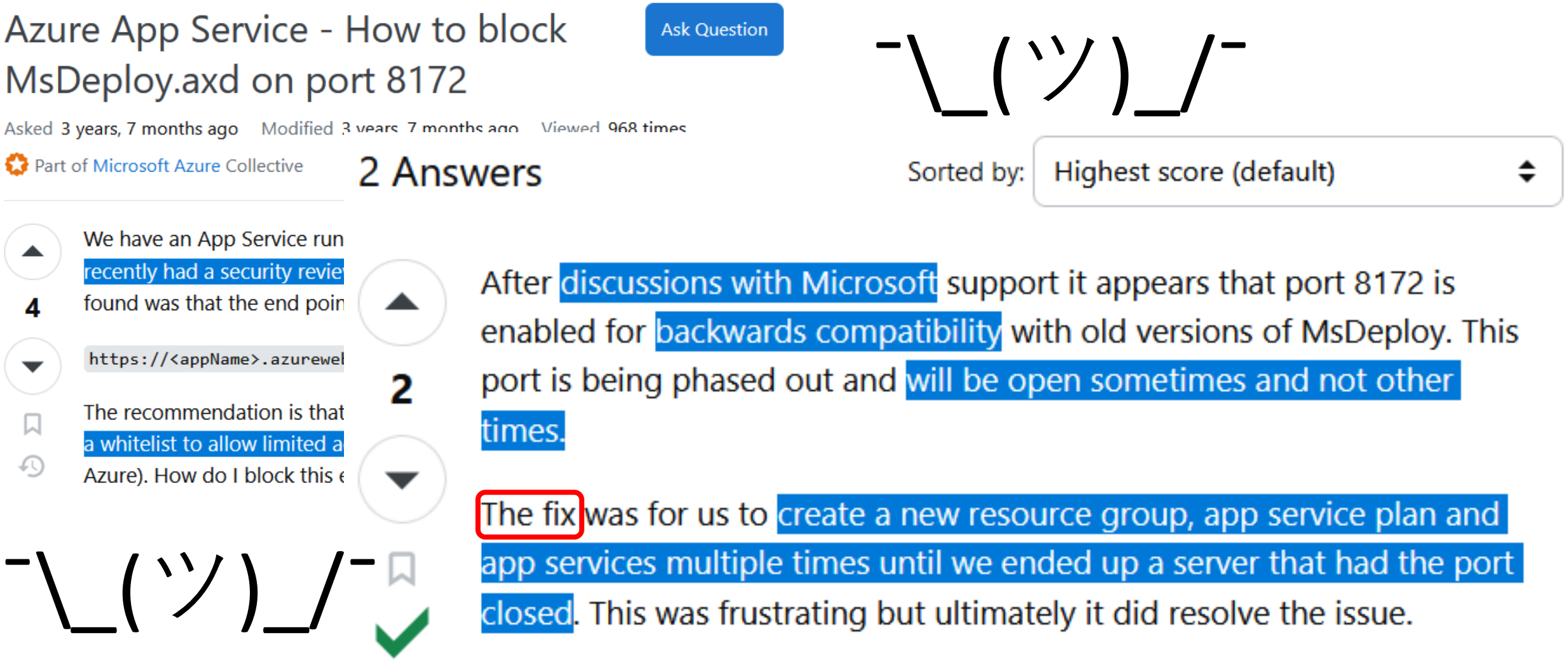
We have an App Service running in Azure that hosts a website. We've recently had a security review on the web site and one of the items found was that the end point below was exposed.

```
https://<appName>.azurewebsites.net:8172/msdeploy.axd
```

The recommendation is that this end point should be blocked and using a whitelist to allow limited access (e.g. the build machine that deploys to Azure). How do I block this end point?

Quelle: https://stackoverflow.com/questions/61905095/azure-app-service-how-to-block-msdeploy-axd-on-port-8172

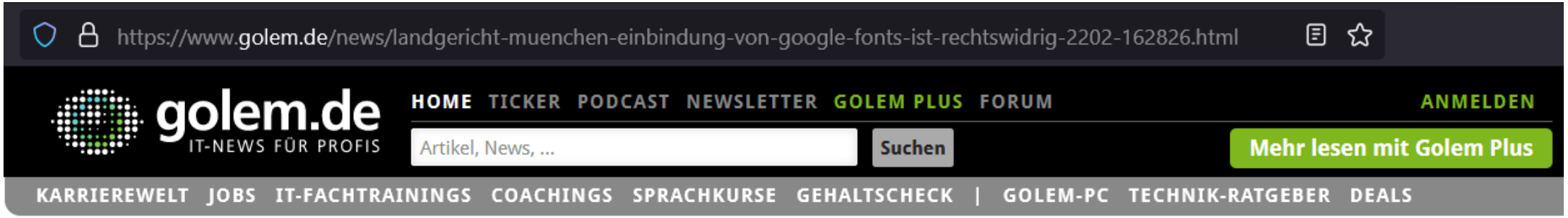
IIS Management Port im Internet



Quelle: https://stackoverflow.com/questions/61905095/azure-app-service-how-to-block-msdeploy-axd-on-port-8172

Datenschutz: Google Fonts 😑💥

Quelle: https://www.golem.de/news/landgericht-muenchen-einbindung-von-google-fonts-ist-rechtswidrig-2202-162826.html



LANDGERICHT MÜNCHEN

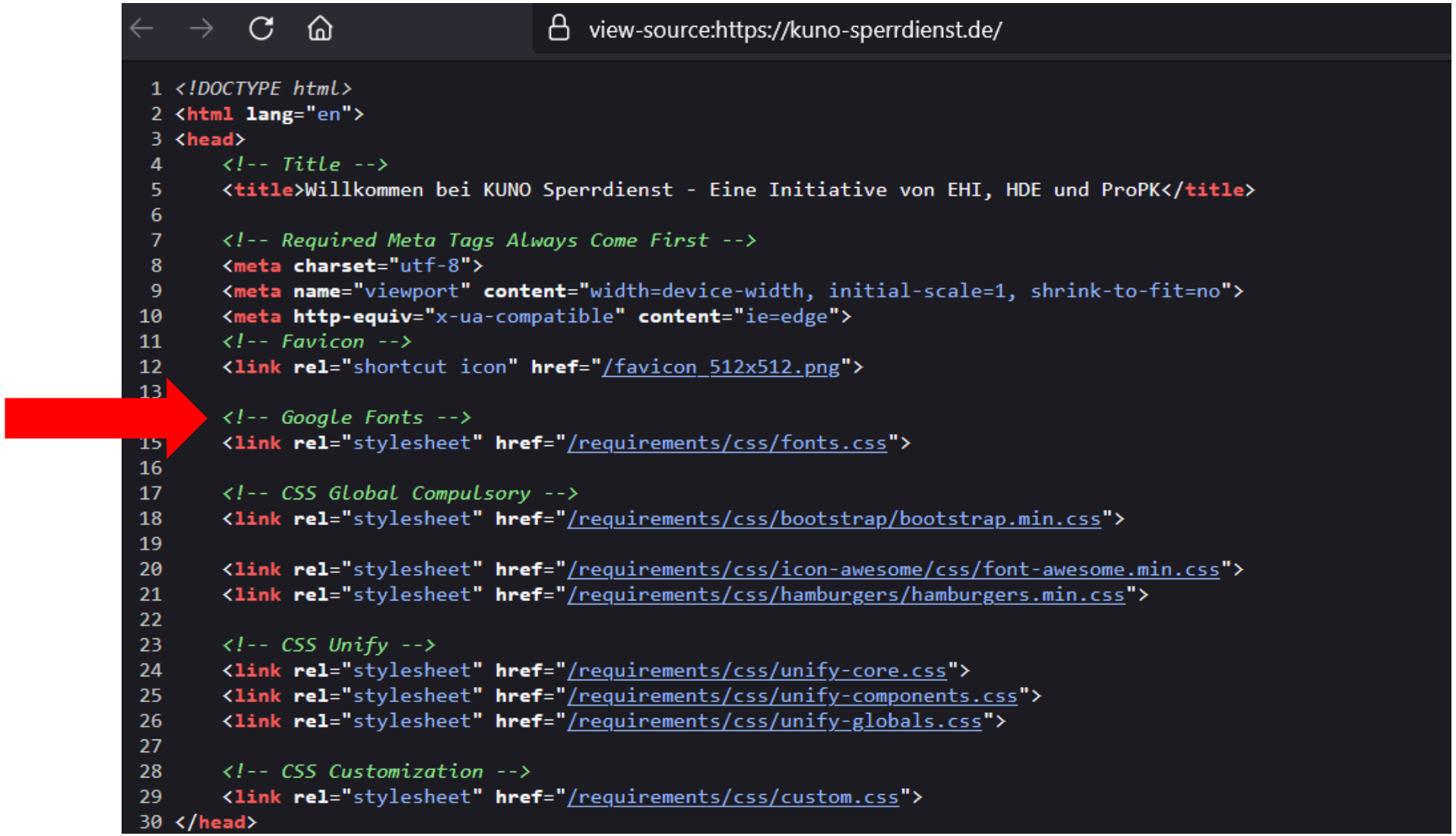
Einbindung von Google Fonts ist rechtswidrig

Wer Schriftarten von Google-Servern ohne Zustimmung einbindet, verstößt gegen die DSGVO. Die Gerichtsentscheidung betrifft aber auch andere CDNs.

in Pocket speichern | merken

1. Februar 2022, 11:26 Uhr, Moritz Tremmel

Fix: Entwickler tun genau was sie sollen 😉😊



Datenschutz: Fragwürdiges Cookie Banner

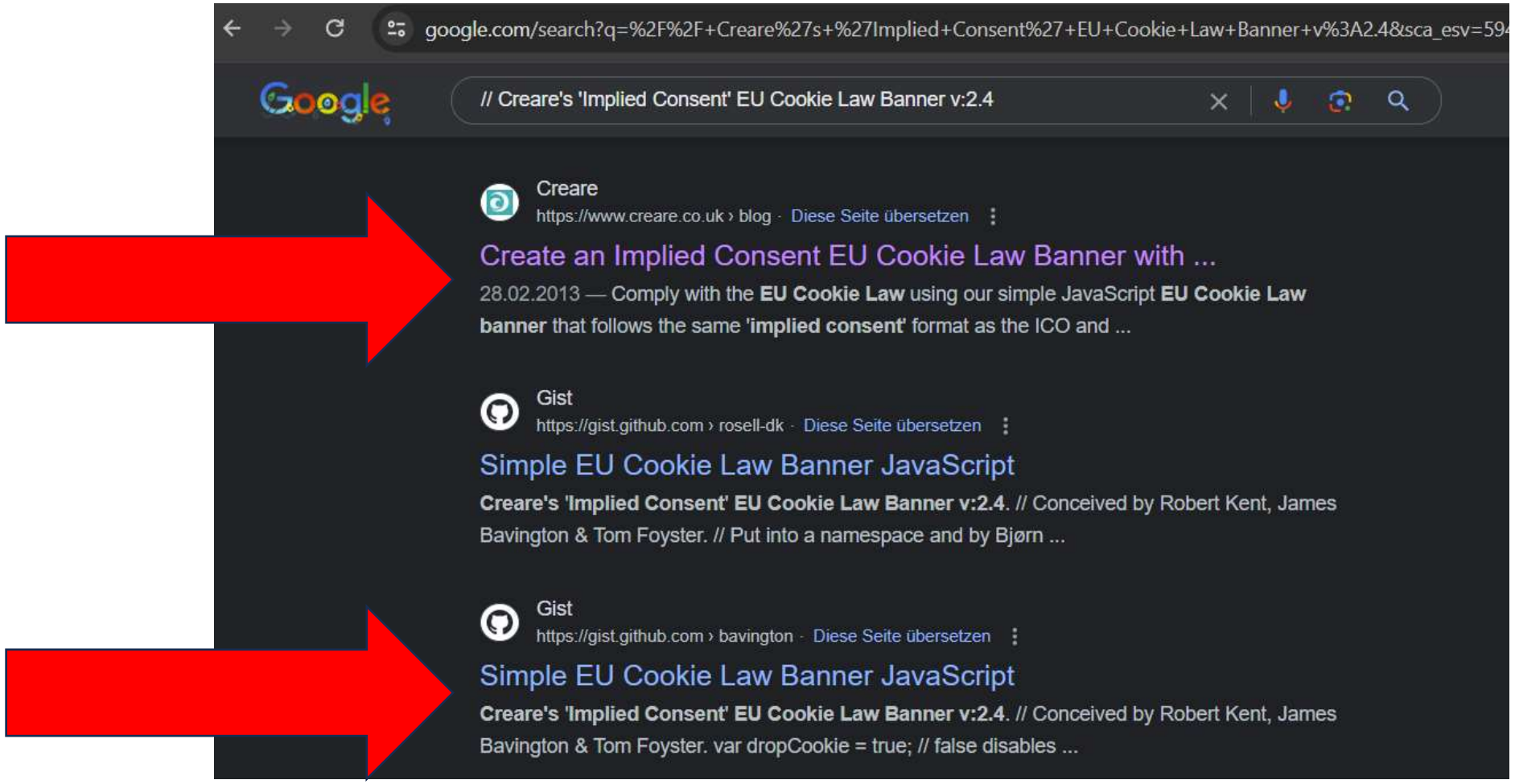
Datenschutz: Fragwürdiges Cookie Banner

😉 https://www.kuno-sperrdienst.de/requirements/js/eu-cookie-banner.js

```
// Creare's 'Implied Consent' EU Cookie Law Banner v:2.4
// Conceived by Robert Kent, James Bavington & Tom Foyster
// Put into a namespace and by BjÃ.rn Rosell
//   Also changed behaviour so you have to click accept to make the banner stay away.
//   To make it behave like the original, set "createCookieWhenBannerIsShown" to true.

var CookieBanner = (function () {
    return {
        'createCookieWhenBannerIsShown': false,
        'createCookieWhenAcceptIsClicked': true,
        'cookieDuration': 14,                   // Number of days before the cookie expires, and the banner reappears
        'cookieName': 'cookieConsent',          // Name of our cookie
        'cookieValue': 'accepted',              // Value of cookie

        '_createDiv': function (html) {
            var bodytag = document.getElementsByTagName('body')[0];
            var div = document.createElement('div');
            div.setAttribute('id', 'cookie-law');
            div.innerHTML = html;

            // bodytag.appendChild(div); // Adds the Cookie Law Banner just before the closing </body> tag
            // or
            bodytag.insertBefore(div, bodytag.firstChild); // Adds the Cookie Law Banner just after the opening <body> tag

            document.getElementsByTagName('body')[0].className += ' cookiebanner'; //Adds a class tothe <body> tag when the banner is visible

            if (CookieBanner.createCookieWhenBannerIsShown) {
                CookieBanner.createAcceptCookie();
            }
        },
```

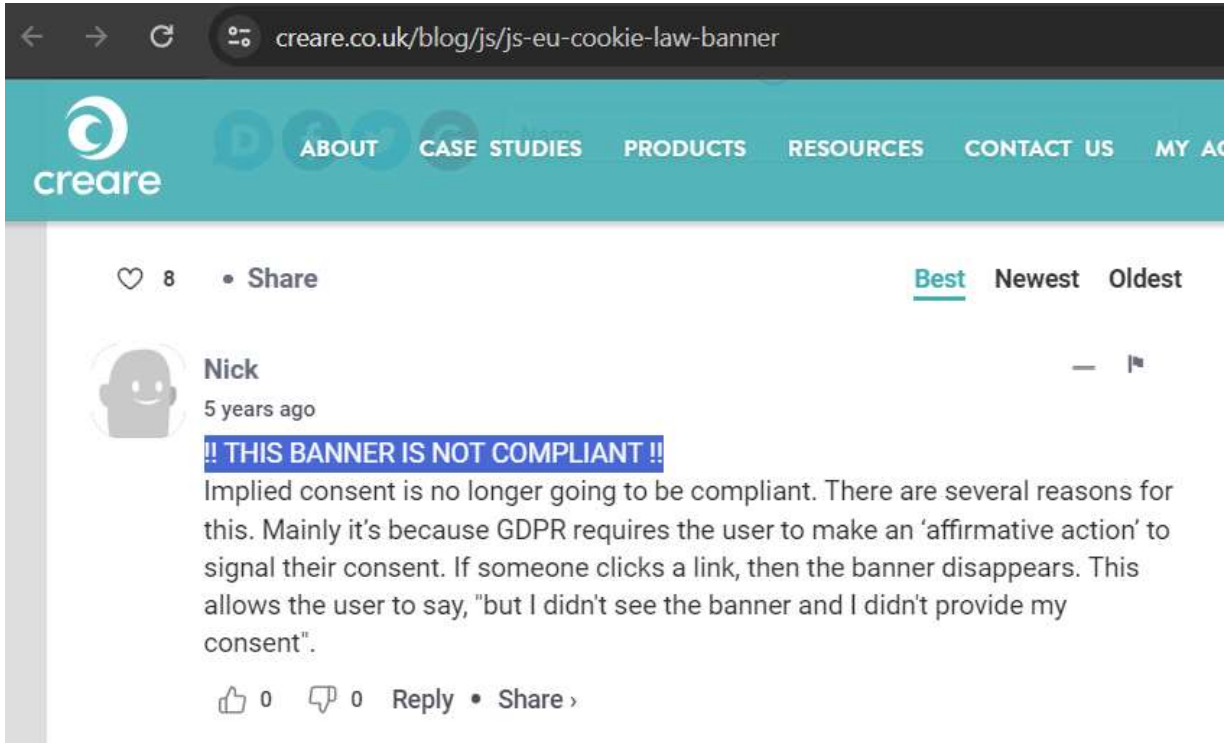
Datenschutz: Fragwürdiges Cookie Banner

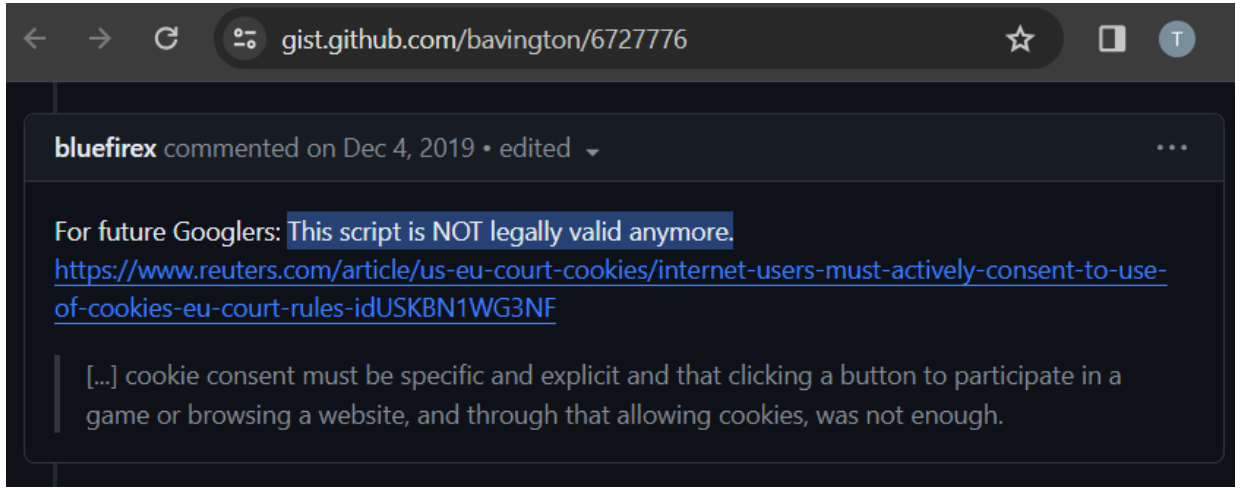
🧐 Suche nach der JavaScript-Datei – **zahlreiche Hinweise auf „Non-Compliance“**



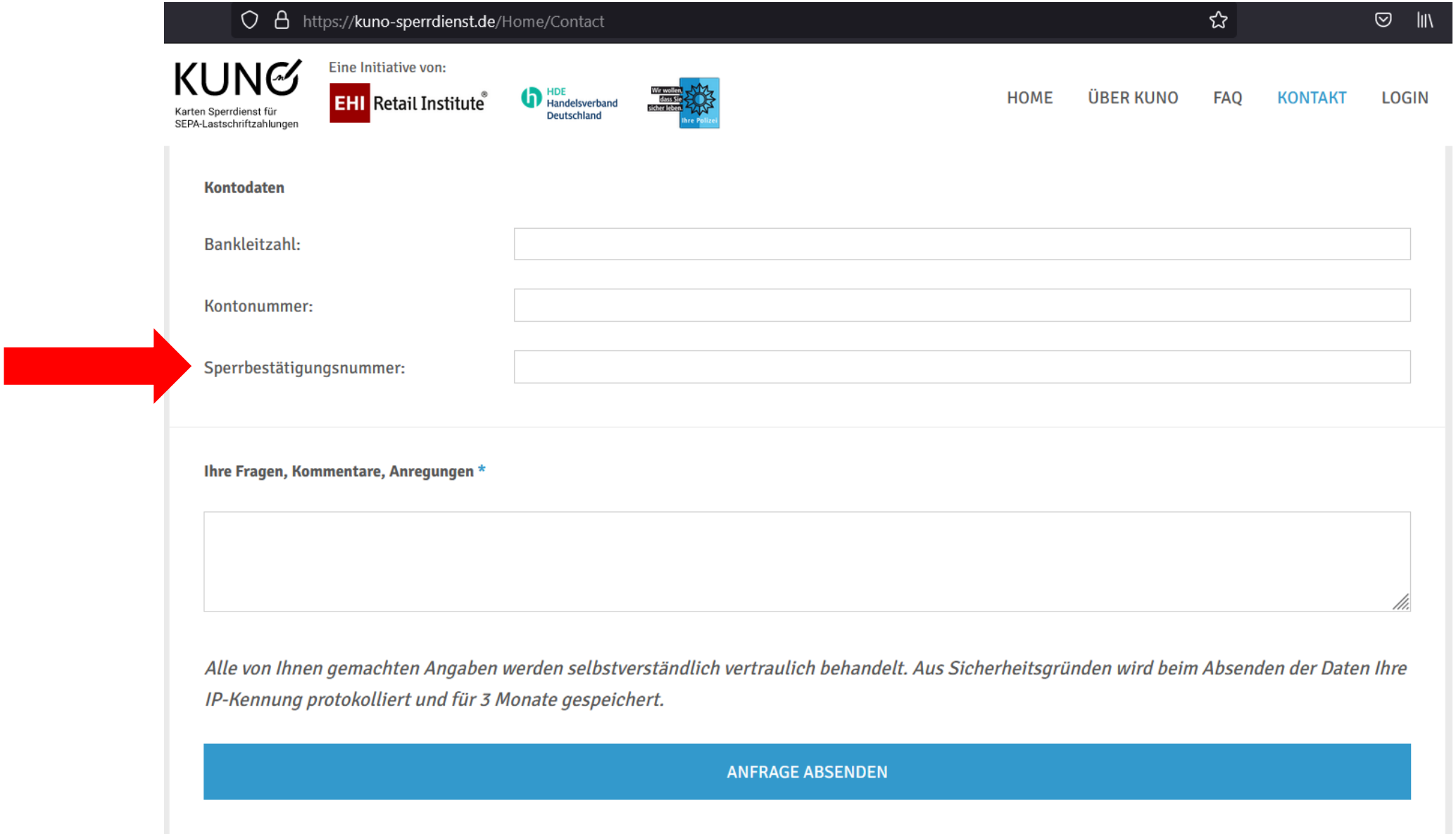
Datenschutz: Fragwürdiges Cookie Banner

😉 Suche nach der JavaScript-Datei – **zahlreiche Hinweise auf „Non-Compliance“**





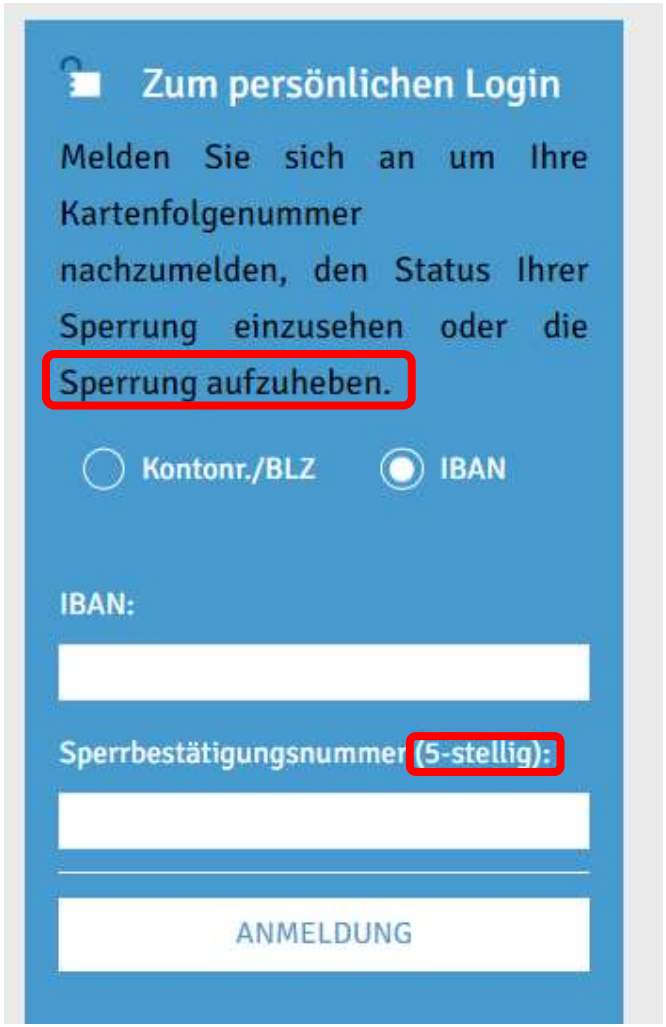
Security: Kontaktformular fragt nach „Sperrnummer“



Sperrbestätigungsnummer? 🤔

Quelle: https://www.hna.de/lokales/witzenhausen/ec-karte-weg-neues-sperrsystem-polizei-hessen-hilft-9554676.html

Sperrbestätigungsnummer? 🤔



🤨

Self-Service / Login bei KUNO:

1.) IBAN (steht auf nahezu jeder Girocard)

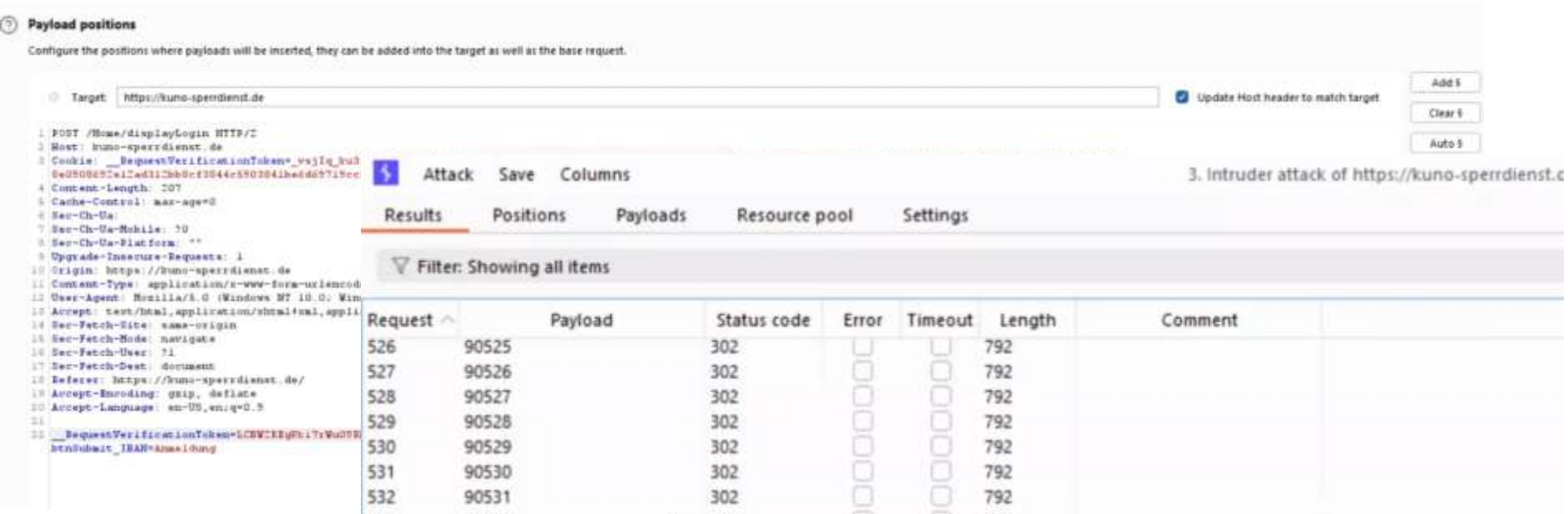
2.) Sperrbestätigungsnummer (5-stellig)

Die haben doch bestimmt Rate-Limits, oder? 😕

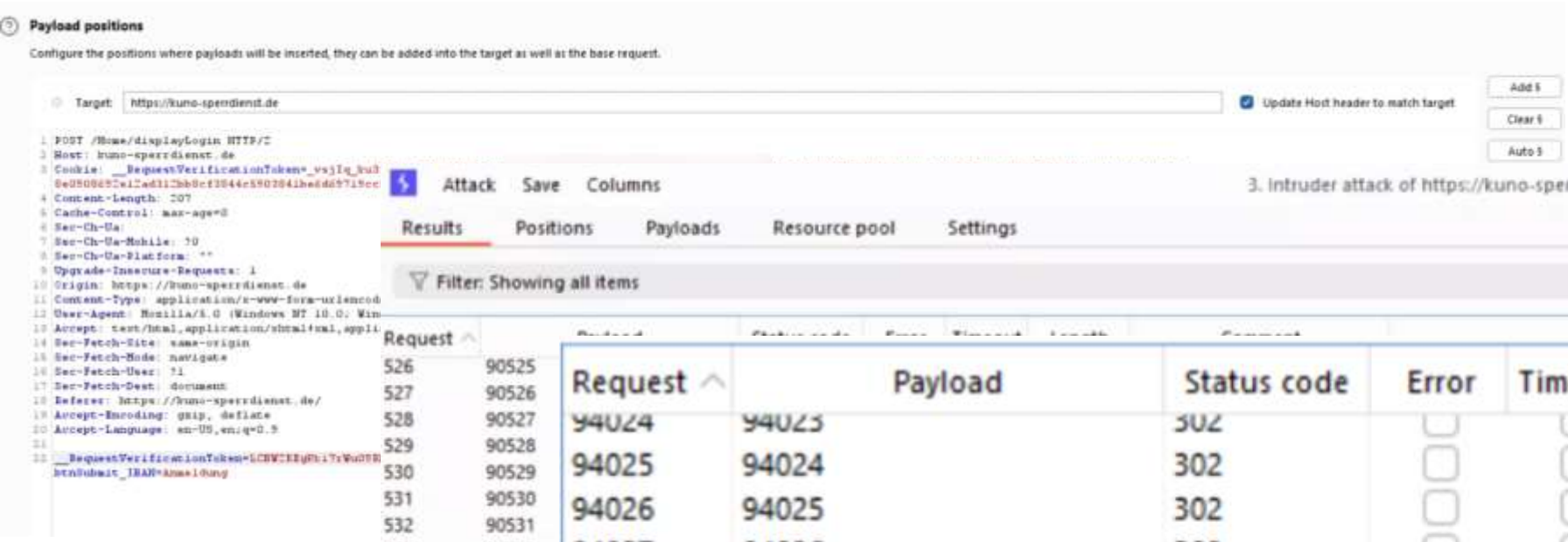
POST /Home/displayLogin HTTP/2
Host: www.kuno-sperrdienst.de
[…]
__RequestVerificationToken=zEEY0_okO0jV[…]mookW7INGdon8e-ZuX03i0J7S7kWDXglH0gX6jdpEPe0TrxNrwXI-_pxGchznb5blUywDP_uzp1n3XXQE28V-eBZok1
&I_B_A_N=DEXXXXXXXXXXX
&SpeBesNum=11111
&btnSubmit_IBAN=Anmeldung

Die haben doch bestimmt Rate-Limits, oder? 😕

Die haben doch bestimmt Rate-Limits, oder? 😕



Die haben doch bestimmt Rate-Limits, oder? 😕



Request	Payload	Status code	Error	Timeout	Length	Comment
94024	94023	302			800	
94025	94024	302			800	
94026	94025	302			800	
94027	94026	302			800	
94028	94027	302			800	
94029	94028	302			800	
94030	94029	302			800	
94031	94030	302			800	
94032	94031	302			800	
94033	94032	302			780	
94034	94033	302			800	
94035	94034	302			800	
94036	94035	302			800	

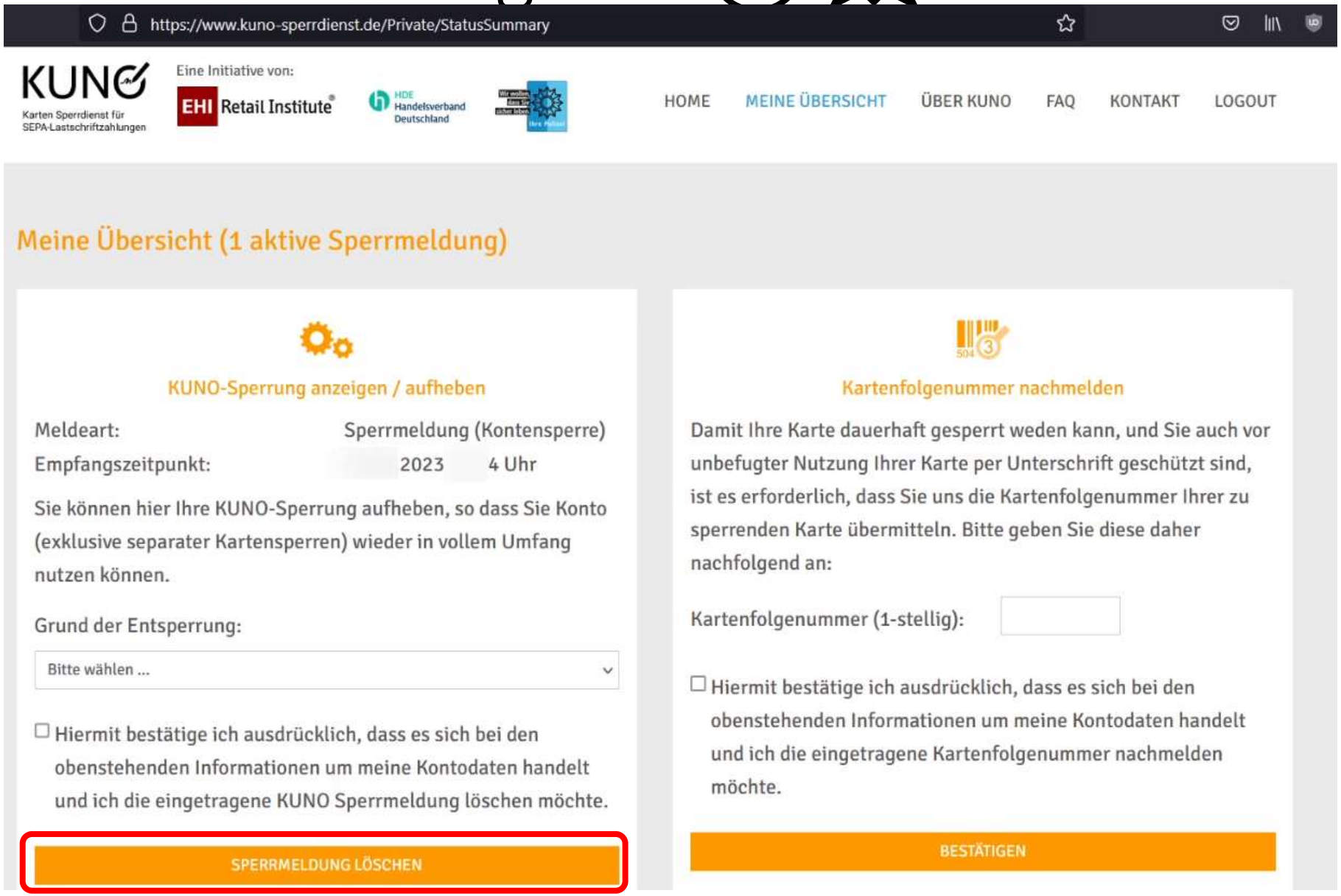
😮

Bereit für den Login … 😉

Self-Service / Login bei KUNO:

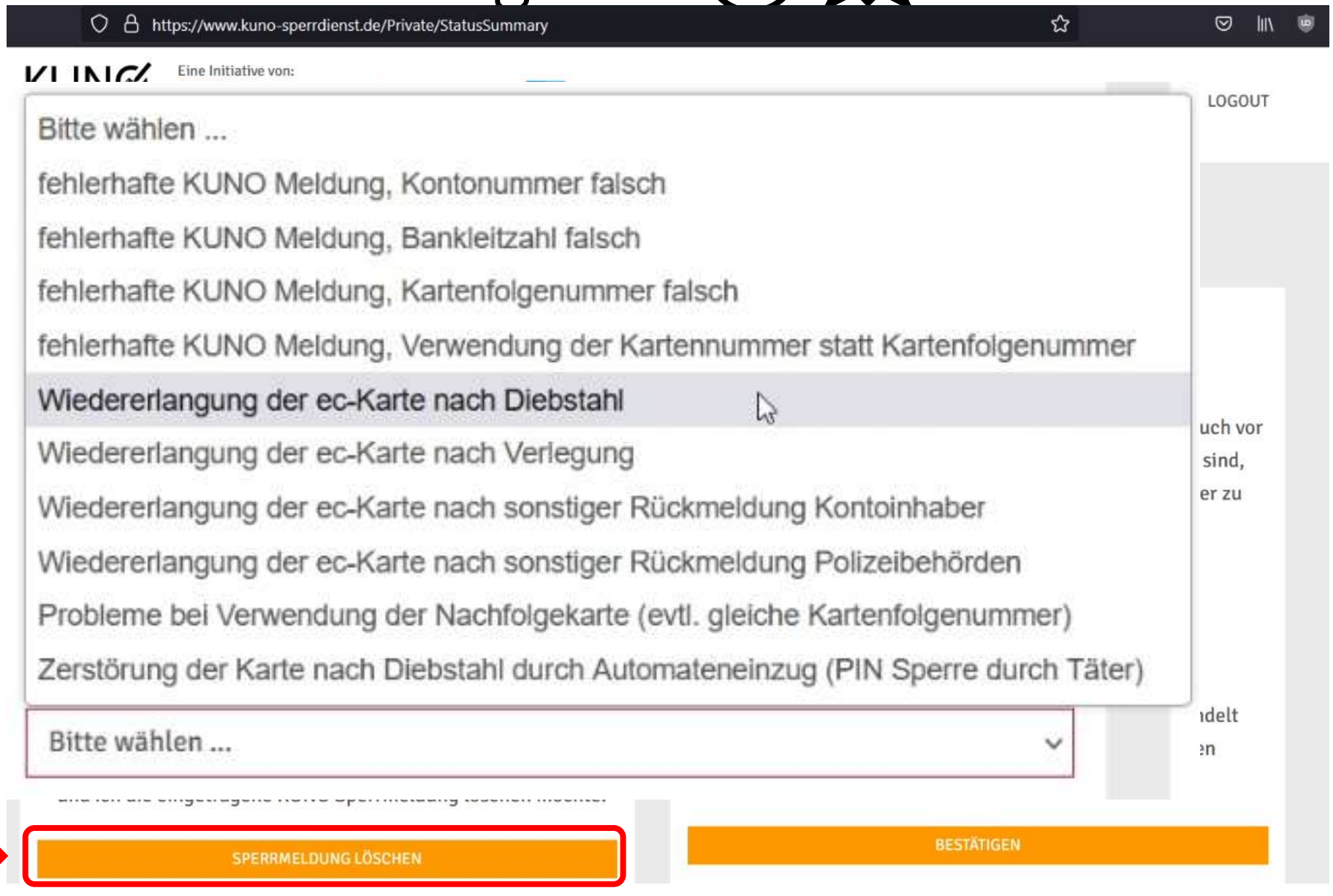
- ☑ 1.) IBAN (steht auf nahezu jeder Girocard)
- ☑ 2.) Sperrbestätigungsnummer (5-stellig)

Hinter dem Login … 😑💥



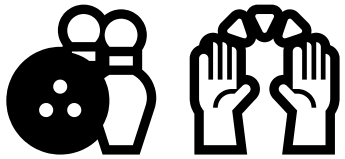
😮

Hinter dem Login … 😑💥



😮

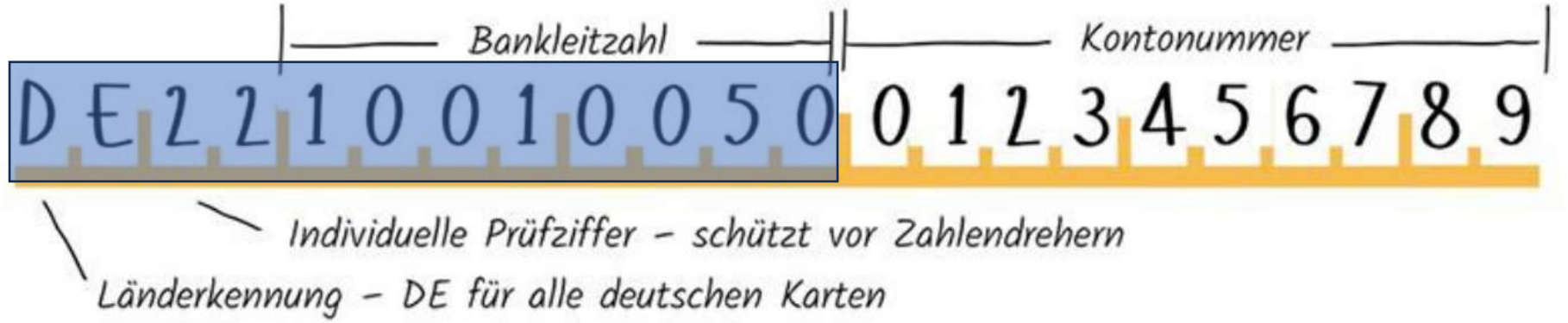
Damit wäre SEPA-Lastschrift für dieses Konto/Karte **unlocked***



* Rollout der Sperr-Datei in der Regel nach 24 Stunden oder früher …

Ausweitung denkbar …

Statt „nur“ Bruteforce auf Sperrbestätigungsnummer …
auch Bruteforce der IBAN (maximal 100.000 Requests notwendig)



ISO 13616-1:2020 sieht u.a. 34-stellige IBANs vor
Deutschland: 22-stellige IBANs

Vorgehen zur Entsperrung aller Karten …

Versuchsnummer	IBAN (abgetrennte BLZ und Kontonummer)	Sperrbestätigungsnummer
1	DE94|10050000|6600046463	00000
2	DE94|10050000|6600046463	00001
3	DE94|10050000|6600046463	00002
[…]	DE94|10050000|6600046463	[…]
100.000	DE94|10050000|6600046463	99999
100.001	DE94|10050000|66000464644	00000
100.002	DE94|10050000|66000464644	00001
100.003	DE94|10050000|66000464644	00002
[…]	DE94|10050000|66000464644	[…]
200.000	DE94|10050000|66000464644	99999
200.001	DE94|10050000|66000464655	00000
200.002	DE94|10050000|66000464655	00001
[…]	[…]	[…]

Das Vorgehen ist eher theoretisch und würde für alle IBANs in Deutschland mehrere Wochen dauern.

Kosten für einen „KUNO-Check“

https://media3.payone.com/f/64176/x/5c33c0e5ba/preis-leistungsverzeichnis-e-com_de.pdf

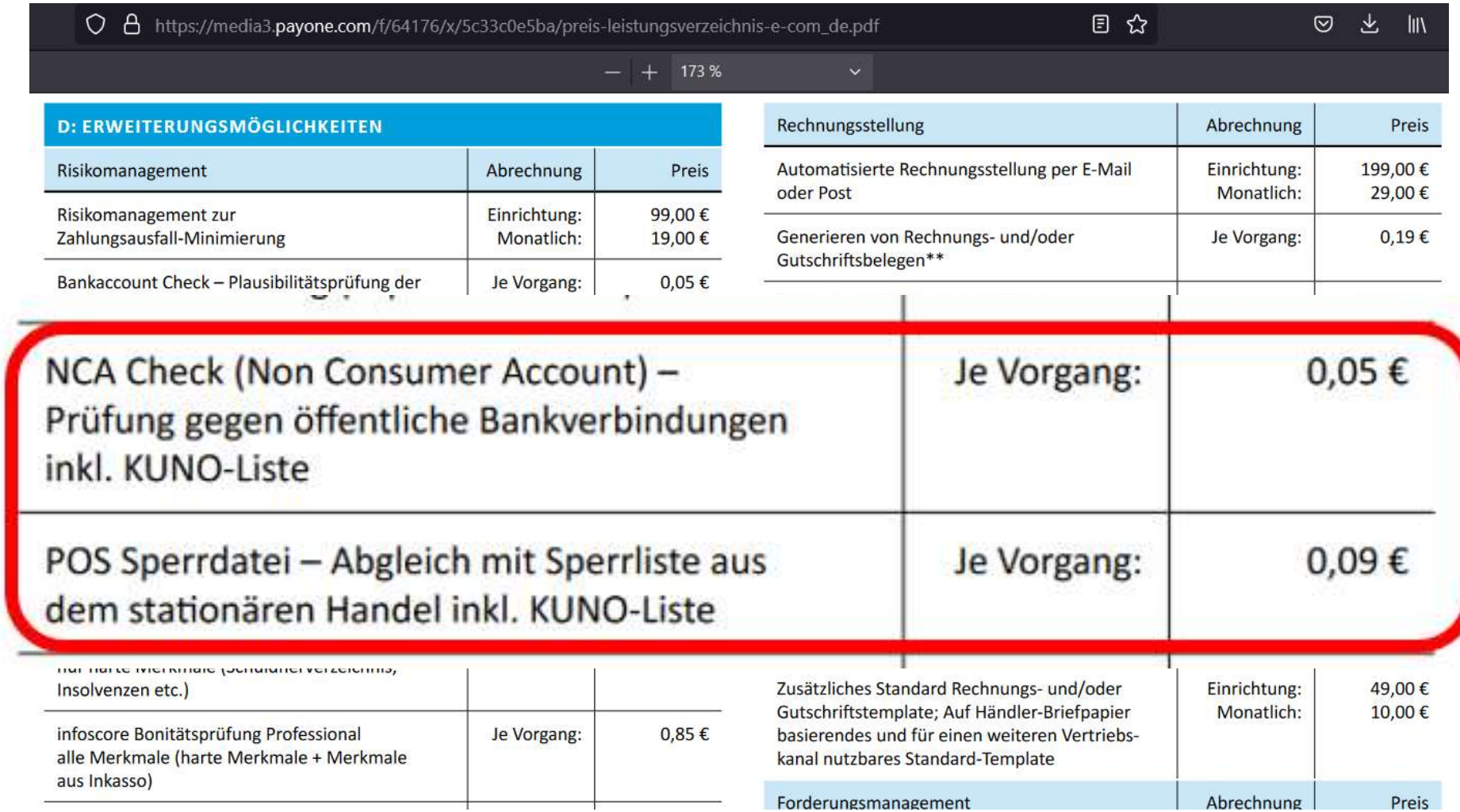
173 %

D: ERWEITERUNGSMÖGLICHKEITEN		
Risikomanagement	Abrechnung	Preis
Risikomanagement zur Zahlungsausfall-Minimierung	Einrichtung: Monatlich:	99,00 € 19,00 €
Bankaccount Check – Plausibilitätsprüfung der Kontoverbindung (separater Aufruf)	Je Vorgang:	0,05 €
NCA Check (Non Consumer Account) – Prüfung gegen öffentliche Bankverbindungen inkl. KUNO-Liste	Je Vorgang:	0,05 €
POS Sperrdatei – Abgleich mit Sperrliste aus dem stationären Handel inkl. KUNO-Liste	Je Vorgang:	0,09 €
Address Check Basic – Adressprüfung auf Existenz in 20 Ländern	Je Vorgang:	0,15 €
Address Check Person – Namens- und Adressprüfung auf Postzustellbarkeit (nur DE)	Je Vorgang:	0,19 €
infoscore Bonitätsprüfung Basic nur harte Merkmale (Schuldnerverzeichnis, Insolvenzen etc.)	Je Vorgang:	0,45 €
infoscore Bonitätsprüfung Professional alle Merkmale (harte Merkmale + Merkmale aus Inkasso)	Je Vorgang:	0,85 €

Rechnungsstellung	Abrechnung	Preis
Automatisierte Rechnungsstellung per E-Mail oder Post	Einrichtung: Monatlich:	199,00 € 29,00 €
Generieren von Rechnungs- und/oder Gutschriftsbelegen**	Je Vorgang:	0,19 €
Versand von Rechnungs- und/oder Gutschriftsbelegen per E-Mail		kostenlos
Versand von Rechnungs- und/oder Gutschriftsbelegen per Post (einseitig, s/w, Deutschland, zzgl. Porto)	Je Vorgang:	0,44 €
Versand von Rechnungs- und/oder Gutschriftsbelegen per Post (einseitig, Farbe, Deutschland, zzgl. Porto)	Je Vorgang:	1,40 €
Versand von Rechnungs- und/oder Gutschriftsbelegen über kundeneigenen Mailserver via SMTP	Einrichtung: Monatlich:	99,00 € 19,00 €
Standard Rechnungs- und/oder Gutschriftstemplate		kostenlos
Zusätzliches Standard Rechnungs- und/oder Gutschriftstemplate; Auf Händler-Briefpapier basierendes und für einen weiteren Vertriebskanal nutzbares Standard-Template	Einrichtung: Monatlich:	49,00 € 10,00 €
Forderungsmanagement	Abrechnung	Preis

Quelle: Payone Preis-/Leistungsverzeichnis (Zugriff: 20.12.2023)
https://media3.payone.com/f/64176/x/5c33c0e5ba/preis-leistungsverzeichnis-e-com_de.pdf

Kosten für einen „KUNO-Check“



Quelle: Payone Preis-/Leistungsverzeichnis (Zugriff: 20.12.2023)
https://media3.payone.com/f/64176/x/5c33c0e5ba/preis-leistungsverzeichnis-e-com_de.pdf

Datenschutzbestimmungen KUNO-Sperrsystem

Quelle: https://kuno-sperrdienst.de/Home/displayDataProtection

alt (< November 2023)

Informationen zum Datenschutz

Das EHI möchte Ihre personenbezogenen Daten schützen. Personenbezogene Daten sind alle Daten, die in Zusammenhang mit Ihrem Namen gespeichert sind. Mit der Anzeige bei der Polizei und der Meldung an die KUNO-Plattform erhalten wir lediglich die Informationen zu Ihrer Kontoverbindung inkl. Kartenfolgenummer. Weitere personenbezogene Daten, wie Name oder Adresse, werden nicht gespeichert.

Das EHI nutzt Ihre Daten ausschließlich, um diese an die an KUNO angeschlossenen (Handels-) Unternehmen weiterzuleiten. In diesem Zusammenhang werden auch Ihre Zugriffe auf die KUNO-Plattform protokolliert und Ihre Kontodaten in einer Datenbank über einen klar definierten Zeitraum abgespeichert. Die Kommunikation zwischen der Polizei und der KUNO-Plattform sowie zwischen der KUNO-Plattform und den angeschlossenen Händlern verläuft dabei signiert und verschlüsselt.

Das EHI verkauft Ihre personenbezogenen Daten nicht an Dritte.

Datenschutzerklärung

neu (> Dezember 2023)

Informationen zum Datenschutz

Das EHI möchte Ihre personenbezogenen Daten schützen. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen (Art. 4 Nr. 1 DSGVO). Mit der Anzeige bei der Polizei und der Meldung an die KUNO-Plattform erhalten wir die Informationen zu Ihrer Kontoverbindung inkl. Kartenfolgenummer. Weitere personenbezogene Daten, wie Name oder Adresse, werden nicht gespeichert.

Das EHI nutzt Ihre Daten ausschließlich, um diese an die an KUNO angeschlossenen (Handels-) Unternehmen weiterzuleiten. In diesem Zusammenhang werden auch Ihre Zugriffe auf die KUNO-Plattform protokolliert und Ihre Kontodaten in einer Datenbank über einen klar definierten Zeitraum abgespeichert. Die Kommunikation zwischen der Polizei und der KUNO-Plattform sowie zwischen der KUNO-Plattform und den angeschlossenen Händlern verläuft dabei signiert und verschlüsselt.

Datenschutzhinweise

Datenschutzbestimmungen KUNO-Sperrsystem

Quelle: https://kuno-sperrdienst.de/Home/displayDataProtection

alt (< November 2023)

Informationen zum Datenschutz

Das EHI möchte Ihre personenbezogenen Daten schützen. Personenbezogene Daten sind alle Daten, die in Zusammenhang mit Ihrem Namen gespeichert sind. Mit der Anzeige bei der Polizei und der Meldung an die KUNO-Plattform erhalten wir lediglich die Informationen zu Ihrer Kontoverbindung inkl. Kartenfolgenummer. Weitere personenbezogene Daten, wie Name oder Adresse, werden nicht gespeichert.

Das EHI nutzt Ihre Daten ausschließlich, um diese an die an KUNO angeschlossenen (Handels-) Unternehmen weiterzuleiten. In diesem Zusammenhang werden auch Ihre Zugriffe auf die KUNO-Plattform protokolliert und Ihre Kontodaten in einer Datenbank über einen klar definierten Zeitraum abgespeichert. Die Kommunikation zwischen der Polizei und der KUNO-Plattform sowie zwischen der KUNO-Plattform und den angeschlossenen Händlern verläuft dabei signiert und verschlüsselt.

Das EHI verkauft Ihre personenbezogenen Daten nicht an Dritte.

Datenschutzerklärung

neu (> Dezember 2023)

Informationen zum Datenschutz

Das EHI möchte Ihre personenbezogenen Daten schützen. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen (Art. 4 Nr. 1 DSGVO). Mit der Anzeige bei der Polizei und der Meldung an die KUNO-Plattform erhalten wir die Informationen zu Ihrer Kontoverbindung inkl. Kartenfolgenummer. Weitere personenbezogene Daten, wie Name oder Adresse, werden nicht gespeichert.

Das EHI nutzt Ihre Daten ausschließlich, um diese an die an KUNO angeschlossenen (Handels-) Unternehmen weiterzuleiten. In diesem Zusammenhang werden auch Ihre Zugriffe auf die KUNO-Plattform protokolliert und Ihre Kontodaten in einer Datenbank über einen klar definierten Zeitraum abgespeichert. Die Kommunikation zwischen der Polizei und der KUNO-Plattform sowie zwischen der KUNO-Plattform und den angeschlossenen Händlern verläuft dabei signiert und verschlüsselt.

Datenschutzhinweise

Kein Verkauf von Daten? 🤔

Quelle: https://kuno-sperrdienst.de/Home/displayDataProtection
& https://kuno-sperrdienst.de/Home/displayFAQ

Datenschutzerklärung

Das EHI verkauft Ihre personenbezogenen Daten nicht an Dritte.

Ansonsten erfolgt keine Weitergabe und kein Verkauf Ihrer personenbezogenen Daten an Dritte. Das EHI trifft bestmögliche Vorkehrungen für die Sicherheit Ihrer Daten.

vs.

Händler FAQ

4. Was kostet mich die KUNO-Anbindung als Händler?

Bei einem jährlichen Außenumsatz von bis zu 75 Mio. Euro berechnen wir für Ihre Teilnahme eine **feste Jahrespauschale von 120,00 Euro netto**. Bei einem höheren Außenumsatz verwenden wir einen Kostenumlageschlüssel, der jährlich neu kalkuliert wird. Genauere Informationen hierzu können Sie über unser Kontaktformular anfordern.

Auszug aus dem KUNO FAQ für Händler

2. Nutze ich KUNO vielleicht bereits?

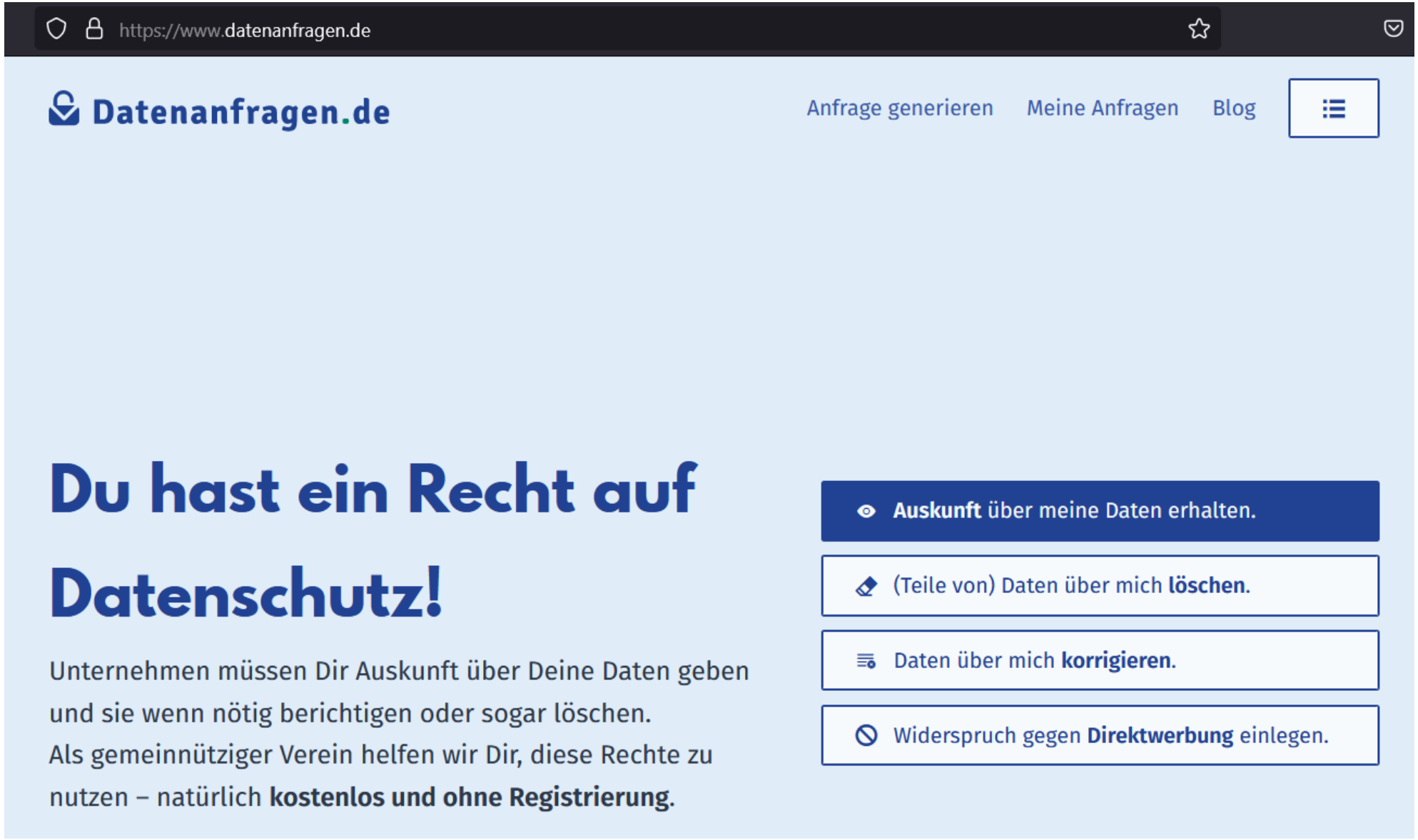
Die unten aufgeführten Netzbetreiber/Finanzdienstleister haben sich bereits der zentralen Meldestelle des EHI angeschlossen und gleichen somit ihre Zahlungstransaktionen mit KUNO-Daten ab. Wenn Sie Kunde der hier aufgeführten Dienstleister sind, brauchen Sie sich nicht mehr separat beim EHI als Empfänger registrieren, dies hat dann bereits der Dienstleister übernommen.

- Real inform GmbH
- AFC Rechenzentrum GmbH
- arvato infoscore Consumer Data GmbH
- Ingenico Payment Services GmbH
- HIT Hanseatische Inkasso-Treuhand GmbH
- Hobex AG
- ICP GmbH
- InterCard AG
- montrada GmbH

Viele bieten auch „Bonitätsprüfungen“ an

Quelle: https://kuno-sperrdienst.de/Home/displayFAQ

Artikel 15 DSGVO: Recht auf Auskunft



Guten Tag,
ich bitte hiermit um Auskunft gemäß Art. 15 DSGVO. Bitte bestätigen Sie mir, ob Sie mich betreffende personenbezogene Daten verarbeiten (vgl. Art. 4 Nr. 1 und 2 DSGVO).

Falls dem so sein sollte, stellen Sie mir bitte im Sinne des Art. 15 Abs. 3 DSGVO eine Kopie sämtlicher personenbezogener Daten, die Sie zu meiner Person verarbeiten, einschließlich eventueller mich betreffender pseudonymisierter Daten im Sinne des Art. 4 Nr. 5 DSGVO, zur Verfügung. Weiterhin bitte ich Sie in diesem Fall im Sinne des Art. 15 Abs. 1 DSGVO um Auskunft über:
1. die Verarbeitungszwecke;
2. die Kategorien personenbezogener Daten, die verarbeitet werden;
3. die Empfänger und Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden;
4. falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
5. wenn die personenbezogenen Daten nicht bei mir erhoben wurden, alle verfügbaren Informationen über die Herkunft der Daten;
6. falls zutreffend, das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO und – sofern gegeben – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für meine Person.

Falls Sie mich betreffende anonymisierte Daten verarbeiten, bitte ich Sie darum, mir das nicht nur mitzuteilen, sondern auch das verwendete Verfahren verständlich zu erläutern.

Sofern Sie meine personenbezogenen Daten an ein Drittland oder an eine internationale Organisation übermitteln, bitte ich über die geeigneten Garantien gemäß Art. 46 DSGVO im Zusammenhang mit der Übermittlung unterrichtet zu werden.

Meine Anfrage schließt explizit auch sämtliche weiteren Angebote und Unternehmen ein, für die Sie Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO sind.

Die Auskunft ist nach Art. 12 Abs. 3 DSGVO unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang der Anfrage zu erteilen. Sie hat nach Art. 15 Abs. 3 DSGVO kostenlos zu erfolgen.

Guten Tag,
ich bitte hiermit um Auskunft gemäß Art. 15 DSGVO. Bitte bestätigen Sie mir, ob Sie mich betreffende personenbezogene Daten verarbeiten (vgl. Art. 4 Nr. 1 und 2 DSGVO).

Falls dem so sein sollte, stellen Sie mir bitte im Sinne des Art. 15 Abs. 3 DSGVO eine Kopie sämtlicher personenbezogener Daten, die Sie zu meiner Person verarbeiten, einschließlich eventueller mich betreffender pseudonymisierter Daten im Sinne des Art. 4 Nr. 5 DSGVO, zur Verfügung. Weiterhin bitte ich Sie in diesem Fall im Sinne des A
1. die Verarb
2. die Kateg
3. die Empfä aten
offengelegt
4. falls mögl der, falls dies
nicht möglic
5. wenn die tionen über die
Herkunft de
6. falls zutre ling gemäß
Art. 22 Abs. lvierte Logik
sowie die Tr e Person.

Falls Sie mic r mitzuteilen,
sondern auc

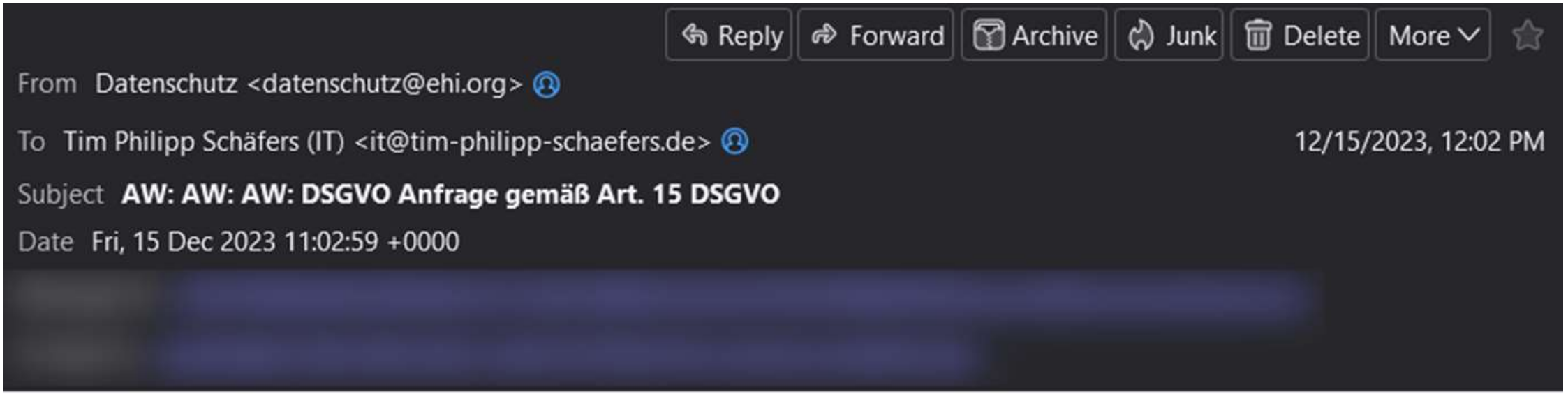
Sofern Sie m sation
übermitteln, b mit der
Übermittlung unterrichtet zu werden.

Meine Anfrage schließt explizit auch sämtliche weiteren Angebote und Unternehmen ein, für die Sie Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO sind.

Die Auskunft ist nach Art. 12 Abs. 3 DSGVO unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang der Anfrage zu erteilen. Sie hat nach Art. 15 Abs. 3 DSGVO kostenlos zu erfolgen.

TL;DR
Welche Daten speichert ihr über mich?
Wer hat meine Daten erhalten?

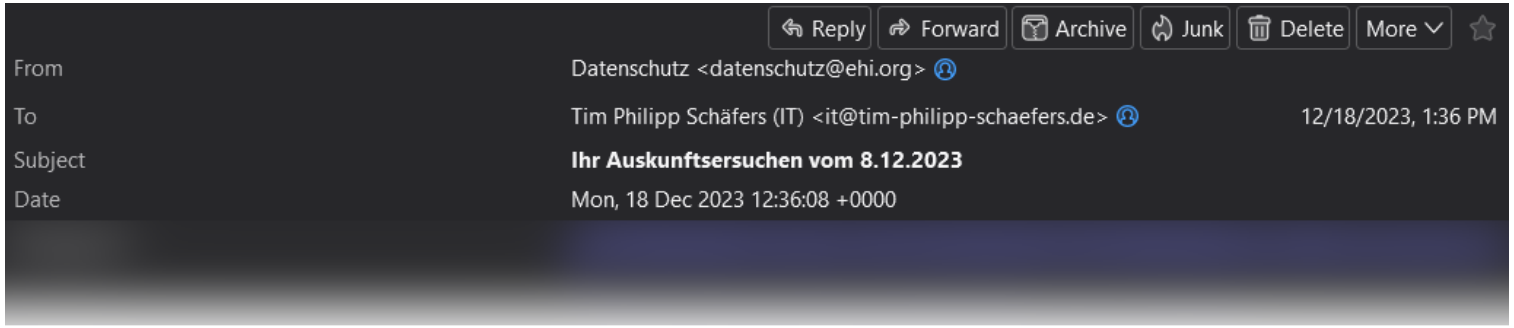
(Betroffenenrecht nach Artikel 15 DSGVO)



Guten Tag Herr Schäfers,

um sicherzustellen, dass Sie der berechtigte Kontoinhaber der von Ihnen angegebenen Kontodaten sind, müssten Sie uns einmal zur Identifizierung die letzten zwei Ziffern Ihrer Sperrbestätigungsnummer mitteilen.

🤨 ¯_(ツ)_/¯



Guten Tag Herr Schäfers,

mit Ihrem Auskunftsersuchen vom 8.12.2023 haben Sie uns gebeten, Ihnen Auskunft darüber zu geben, welche personenbezogenen Daten wir von Ihnen zu welchem Zweck verarbeiten. Wie besprochen erhalten Sie die gewünschte Auskunft im Anhang als PDF.

Zu Ihren weiteren Fragen kann ich Ihnen folgende Antworten geben:

Unternehmen können sich für eine Gebühr von 120,00€ im Jahr dem KUNO-Projekt anschließen. Die Gebühr erfolgt aufgrund der technischen Umsetzung und den Kosten, die damit verbunden sind. Die Kontodaten werden ohne Namen an die angeschlossenen Handelsunternehmen bzw. deren Zahlungsdienstleister/ Netzwerkbetreiber weitergegeben, sodass Zahlungen mit den als gestohlen gemeldeten Karten beim Bezahlvorgang abgelehnt werden können. Der Zweck ist klar eingeschränkt und auf die Nutzung zur Kartensperrung begrenzt und vertraglich festgehalten.

Im Zuge Ihres Auskunftsersuchens finden Sie die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind im Anhang. Aus Sicherheitsgründen, um eine betrügerische Verwendung zu verhindern, können wir Privatpersonen nicht über die Namen der angeschlossenen Händler informieren. Rechtsgrundlage der Datenverarbeitung ist unser berechtigtes Interesse an der Datensicherheit und dem Schutz vor betrügerischen Verwendungen und Missbrauch der Daten gemäß Art. 6 (1)(f) DSGVO.

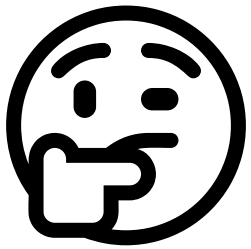
Das EHI Retail Institute ist keine Behörde. Das EHI ist ein wissenschaftliches Institut des Handels mit rund 800 Mitgliedern und über 70 Jahre Erfahrung. Im Vordergrund steht der Austausch mit der Handelsbranche und eine praxisrelevante Forschung. Das KUNO-Projekt ist in Zusammenarbeit mit Polizeibehörden und Wirtschaft entstanden und soll ein einfaches, aber wirkungsvolles Sperrsystem darstellen, um Zahlungen per Debitkarte im elektronischen Lastschriftverfahren – also mit Unterschrift – sicherer zu gestalten. Der Name KUNO ist die Abkürzung für „Kriminalitätsbekämpfung im unbaren Zahlungsverkehr unter Nutzung nichtpolizeilicher Organisationsstrukturen“.

Antwort auf die DSGVO Artikel 15 Anfrage:
Ja – wir haben deine Daten gespeichert und geben sie weiter (sinngemäß).

„Aus Sicherheitsgründen, um eine betrügerische Verwendung zu verhindern, können wir Privatpersonen nicht über die Namen der angeschlossenen Händler informieren.“

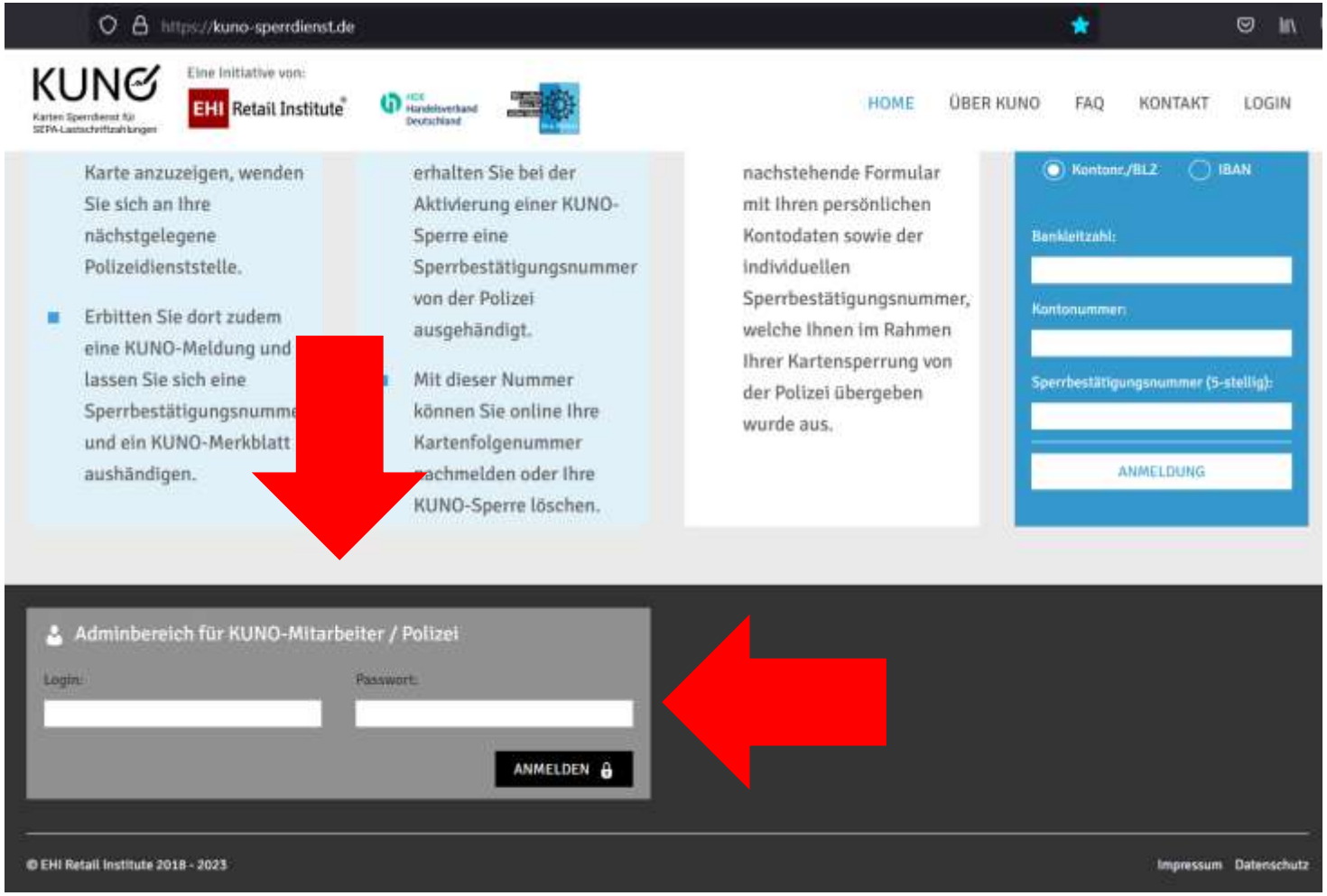
Datenschutz – EHI Retail Institute GmbH
E-Mail vom 18.12.2023 ¯_(ツ)_/¯

„Sicherheitsgründe“ vs. Betroffenheitsrechte nach Artikel 15 DSGVO



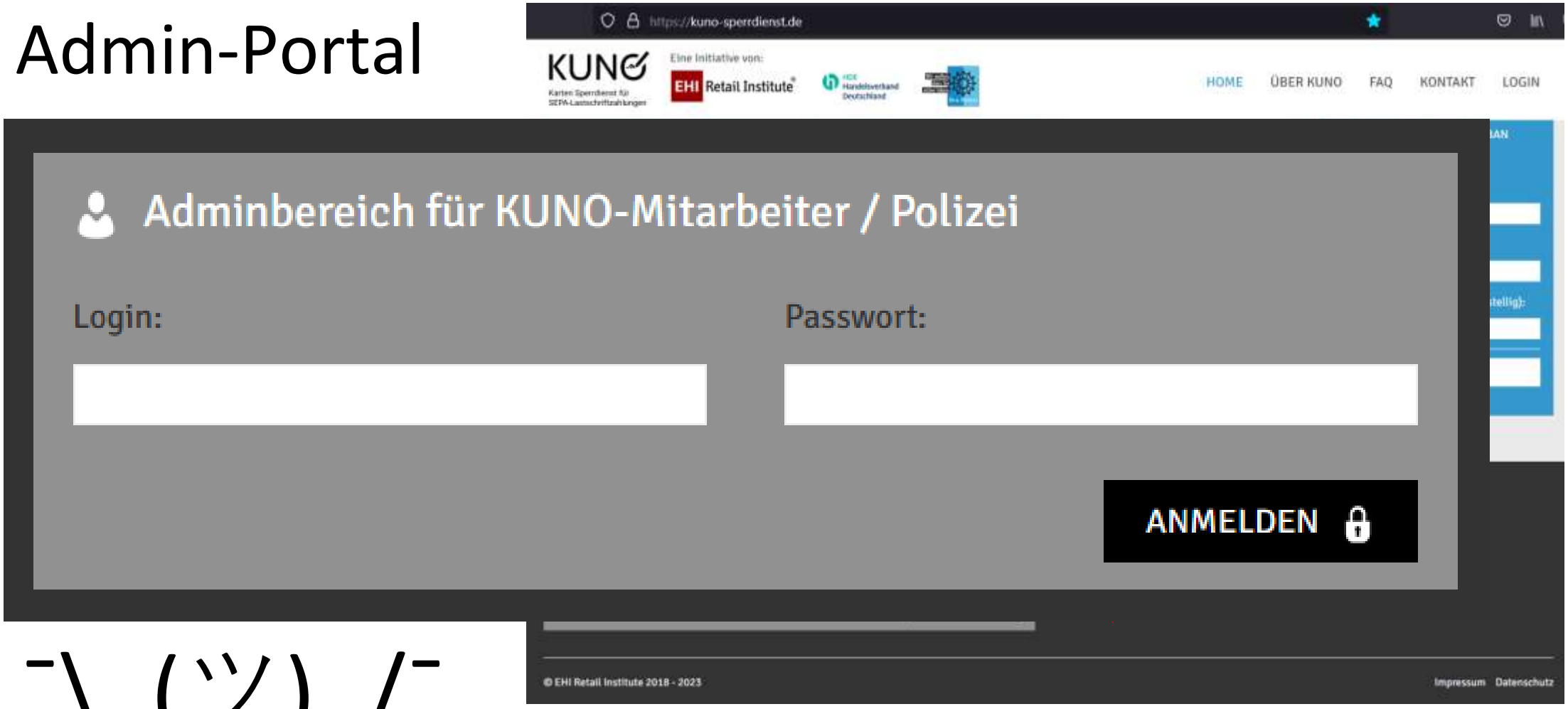
Es gibt ggfs. noch mehr zu „entdecken“ 😉

- Admin-Portal



Es gibt ggfs. noch mehr zu „entdecken“ 😉

- Admin-Portal



¯_(ツ)_/¯

Es gibt ggfs. noch mehr zu „entdecken“ 😉

- Übermittlung der Sperrdatei

Es gab zahlreiche weitere „Problemchen“

CVE-2016-10735, CVE-2018-14040, CVE-2018-14041, CVE-2018-14042, CVE-2019-8331, CVE-2019-11358, CVE-2020-11022, CVE-2020-11023, CVE-2020-23064, CVE-2021-21252, CVE-2021-43306, CVE-2022-31147

HTTP Server Header (inkl. Versionsnummern) exposed

Weitere Management Ports offen

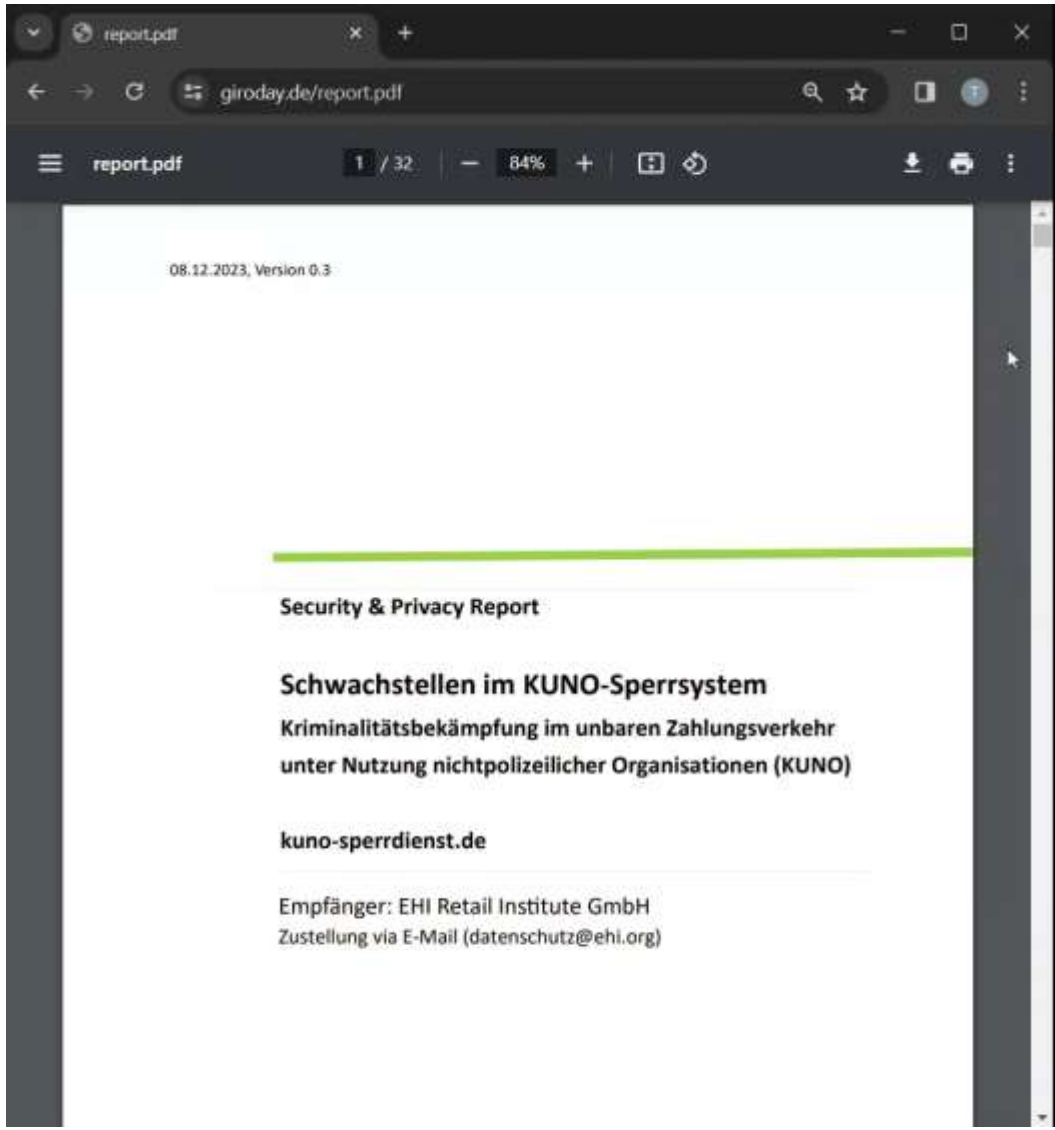
HSTS-Header nicht in Benutzung

Weitere Herausforderungen im Bereich Datenschutz

…

giroday

giroday.de



Giroday != Zeroday

Danke an Rico, Niklas und Tim für den Support und die Idee zum Namen

Herzlichen Dank ❤

- Professioneller Umgang mit der Meldung
- Schnelle Schließung der (meisten) Lücken
- Grundsätzlich funktionierendes Sperrsystem

Funfact 😉

Buchungen werden folgendermaßen vermerkt:

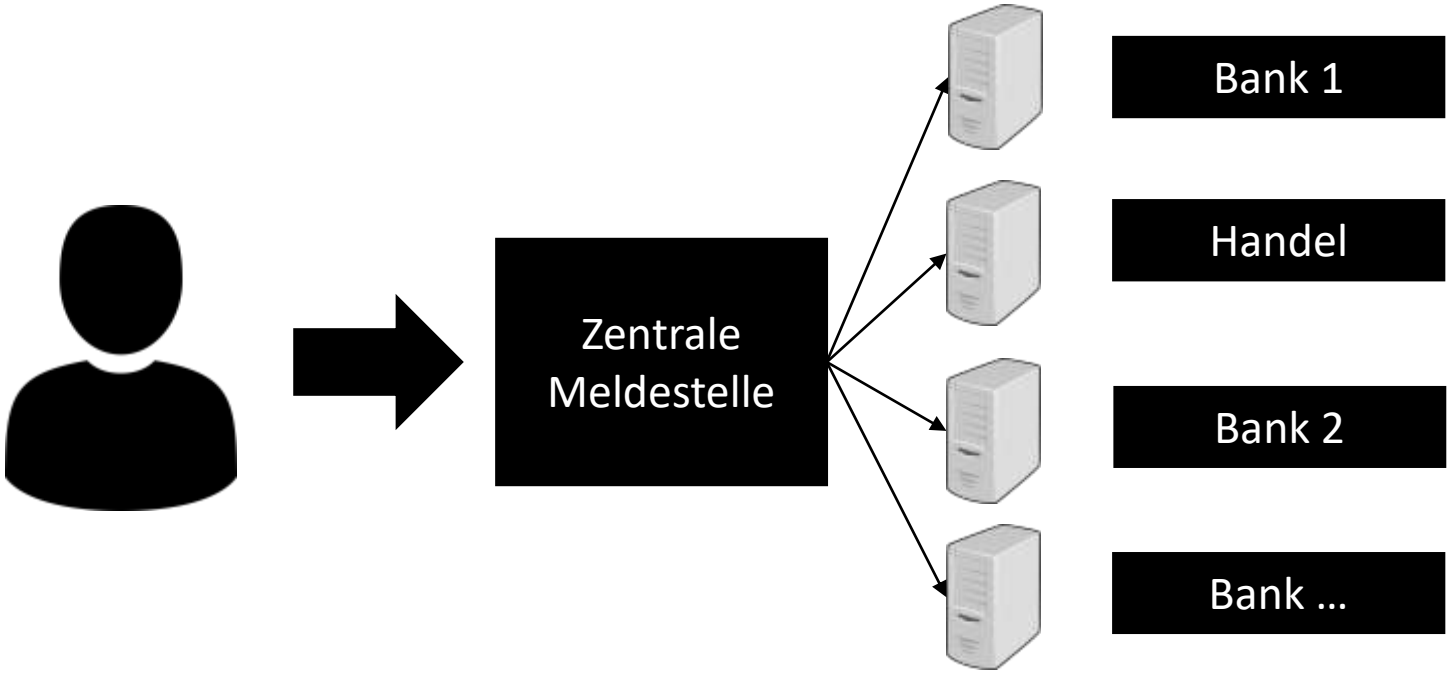
ELV68197325 26.04 18.07 ME0
EC 68197325 260410180710OC0

Zahlungsart,Terminal-ID,Datum,Uhrzeit, Autorisierung
Kartenfolgenummer

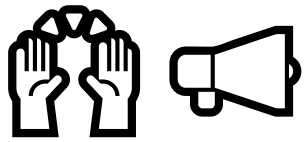
➔ Wenn man >10x die Karte verliert, dann sind alle Kombinationen gesperrt 😉

Quelle: https://de.wikipedia.org/wiki/Girocard#Autorisierungsmerkmal

Vision / Forderungen

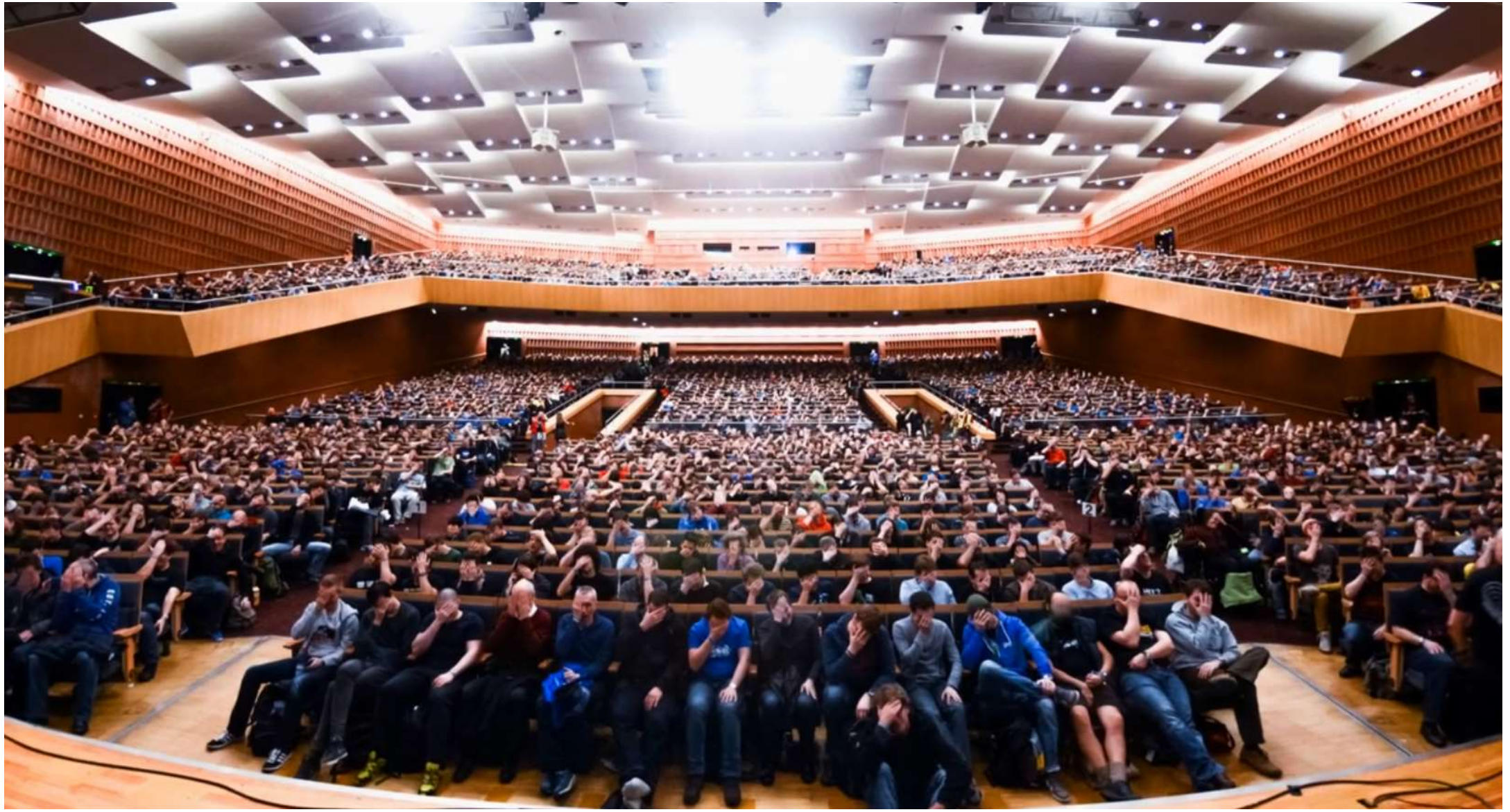


- <u>Eine zentrale Sperrstelle für alle Zahlarten</u>
- Transparent & nachvollziehbar (Open-Source)
- Finanzierung nachvollziehbar
- „Sicher“ und auditierbar

Call to Action 

- Informiert andere, damit ALLE Methoden gesperrt werden …
- Lasst uns gemeinsam daran arbeiten, dass Sperrungen mittelfristig besser durchgeführt werden können.
- Ein paar Wikipedia Artikel bräuchten mal ein Update 😉
- Nutzt Zugriffe auf Systeme, um diese zu verbessern …

Vielen Dank!



Quelle: Fnord Show 30c3

Herzlichen Dank!

Falls es Fragen gibt oder jemand meine Karte findet 😉

it@tim-philipp-schaefers.de

Weitere 1nfos & Folien: giroday.de