SkIDentity ... Trusted Identities for the Cloud

Trusted Cloud

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages

Umsetzung der DSGV am Beispiel SkIDentity – Herausforderungen, Erfahrungen und Ausblick

Dr. Detlef Hühnlein, ecsec GmbH

Deutschland Land der Ideen Ausgezeichneter Ort 2013/14

SecurITy made in Germany

TeleTrusT Quality Seal www.teletrust.de/itsmig

Deutschland Land der Ideen Ausgezeichneter Ort 2015

Agenda

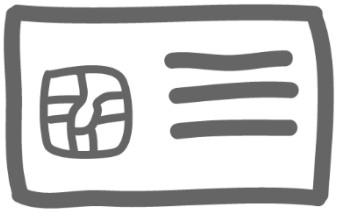
- **Einleitung**
- SkIDentity
- Umsetzung der DSGVO am Beispiel SkIDentity
- Zusammenfassung und Ausblick

ecsec GmbH – Kernkompetenzen

IT-Sicherheit

Identitätsmanagement

Elektronische Signaturen

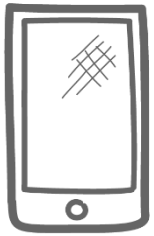


Chipkartentechnologie

Cloud Services

Open Source

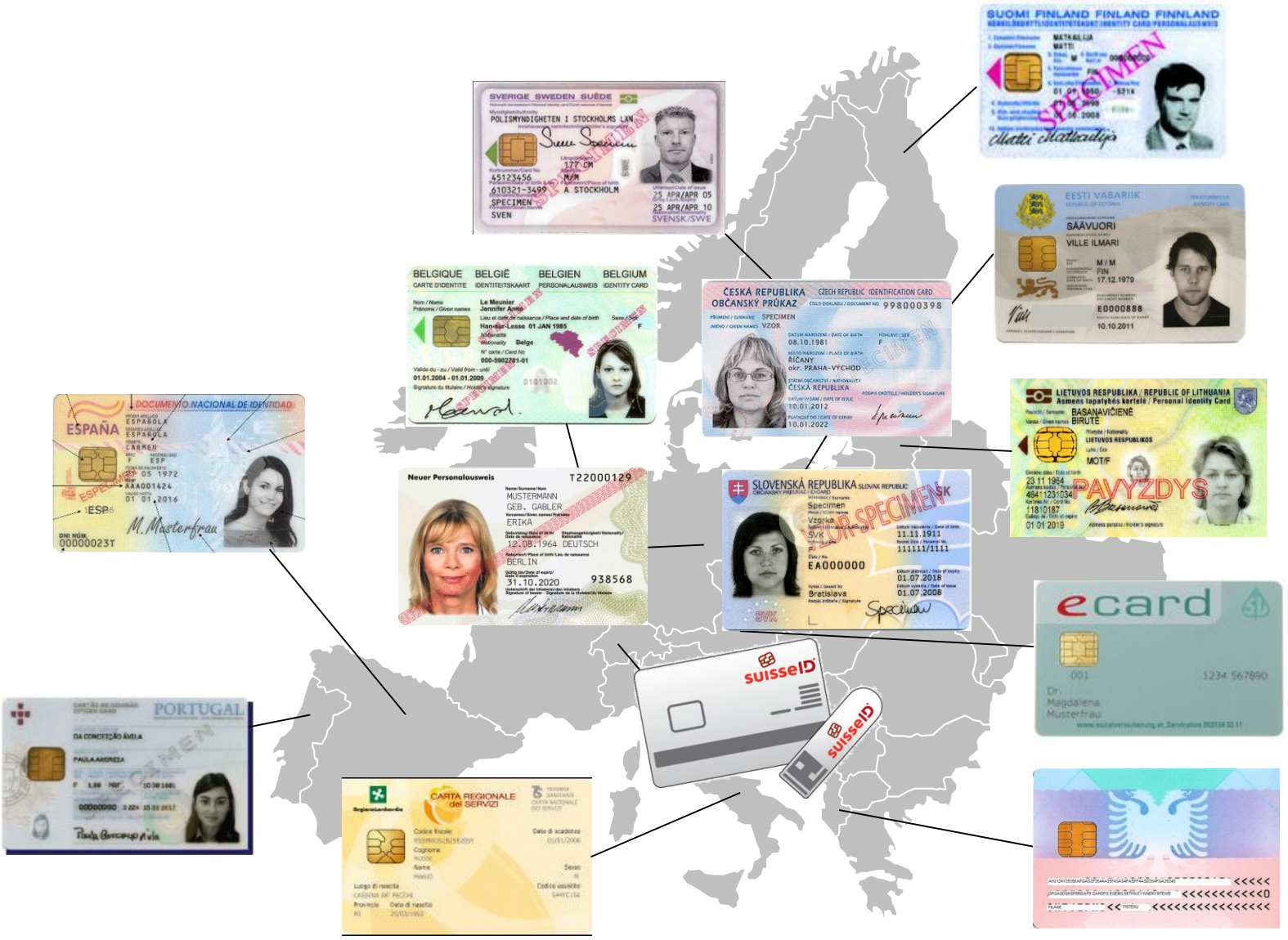
Sicherheitsmanagement



Mobile Lösungen

eGovernment

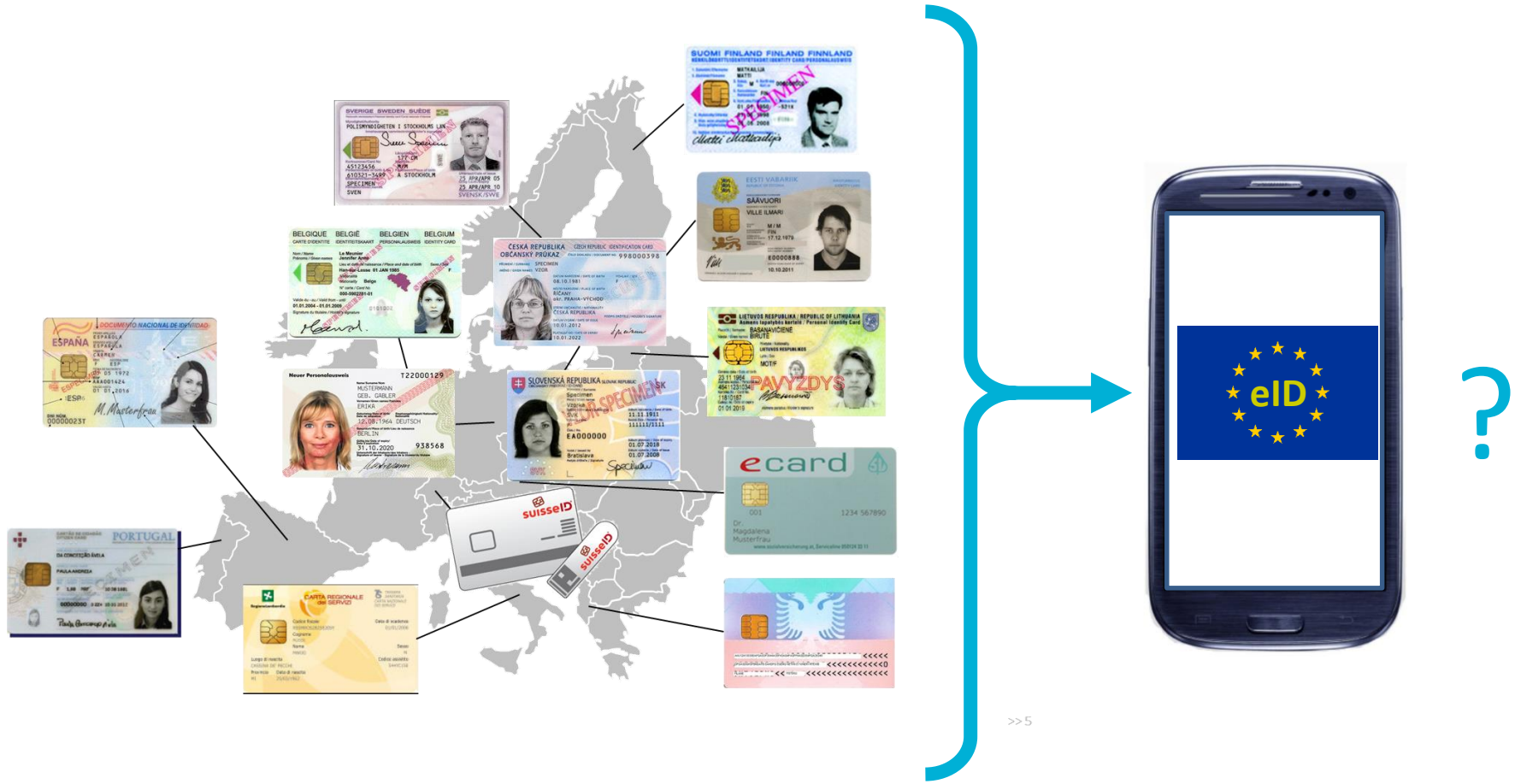
Elektronische Ausweise (eID) in Europa



Mobile eID in Europa

MOBIIL-ID

Mobile Nutzung elektronischer Ausweise?



>> 5

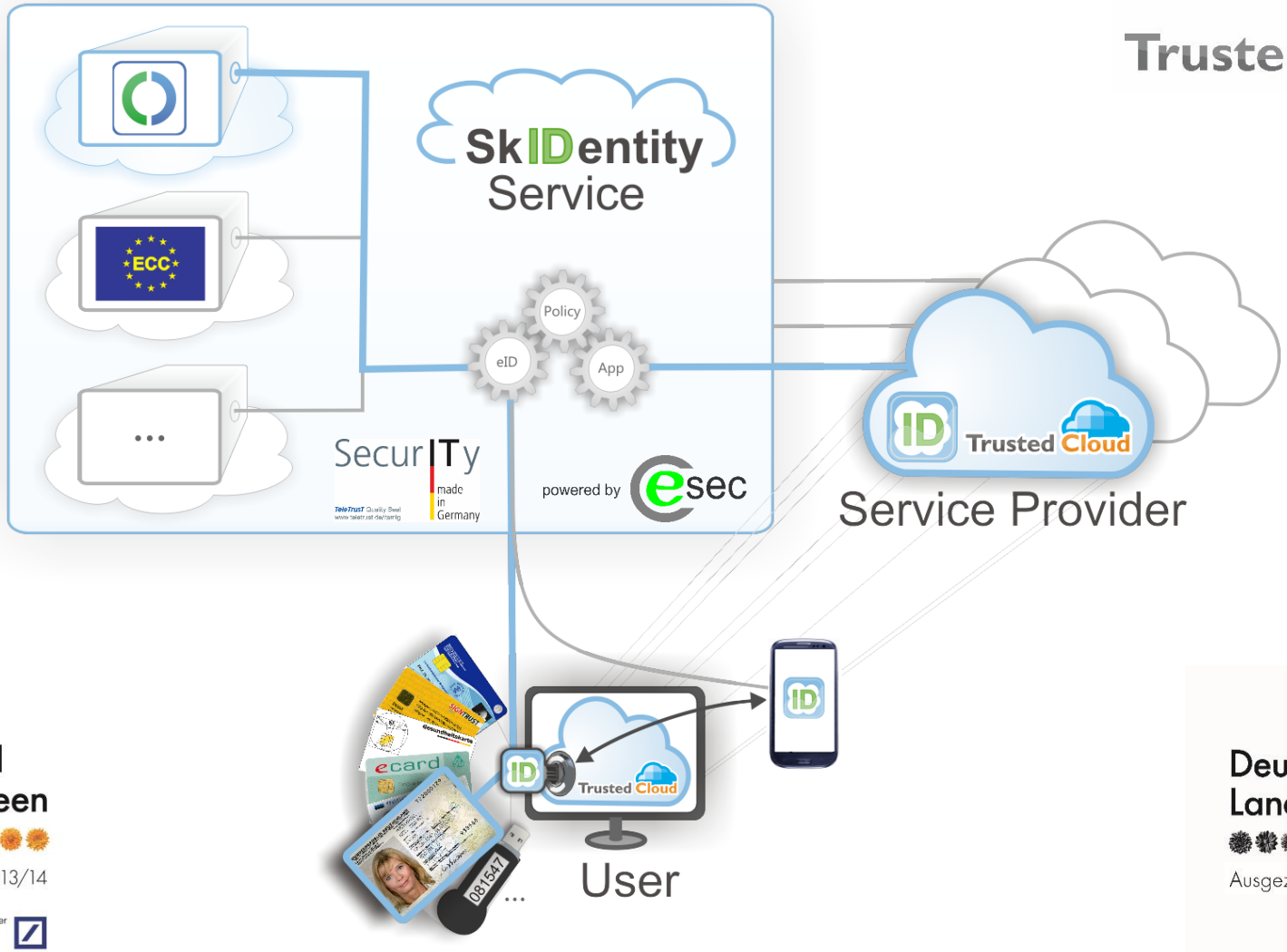
Agenda

- Einleitung
- **SkIDentity**
- Umsetzung der DSGVO am Beispiel SkIDentity
- Zusammenfassung und Ausblick

SkIDentity – Mobile eID as a Service

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

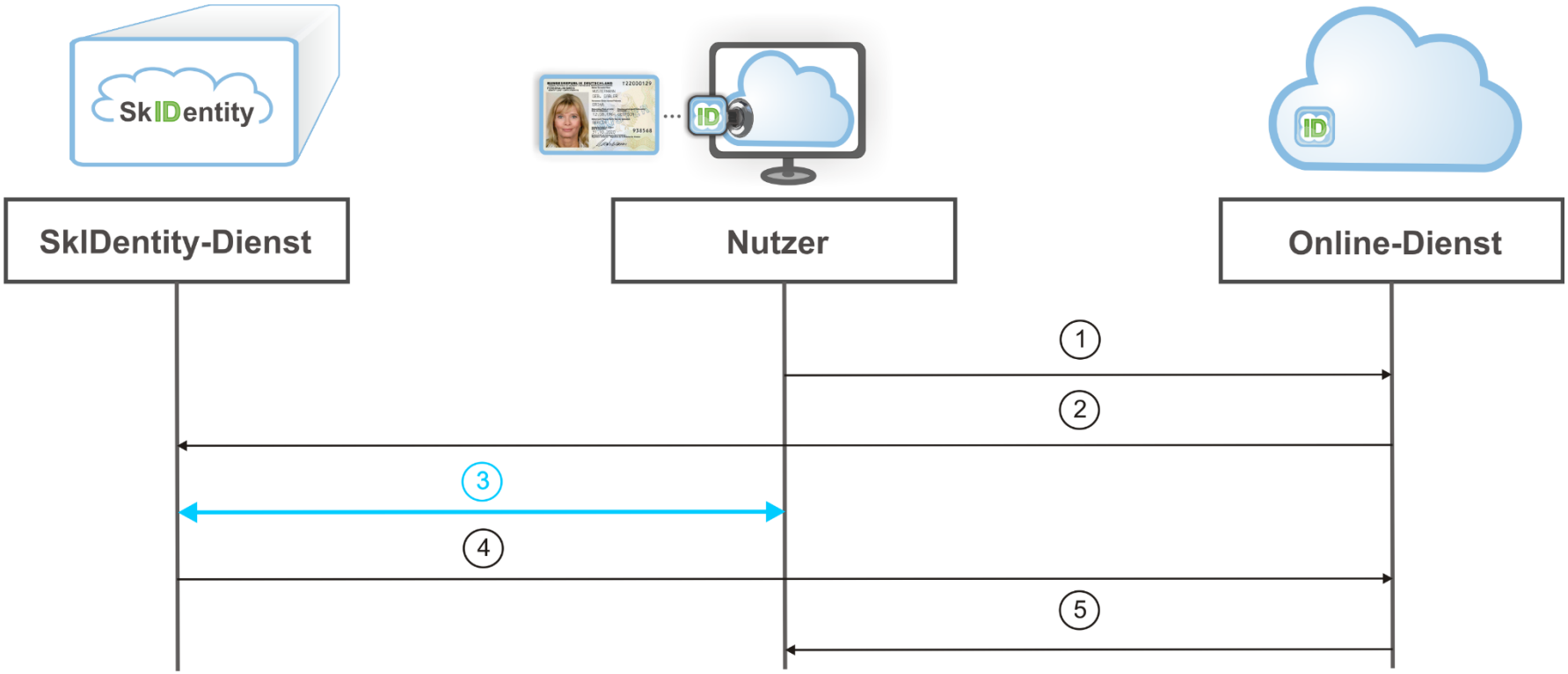
Trusted Cloud



Deutschland Land der Ideen
Ausgezeichneter Ort 2013/14
Nationaler Förderer Deutsche Bank

Deutschland Land der Ideen
Ausgezeichneter Ort 2015
Nationaler Förderer Deutsche Bank

Login mit SkIDentity



Cloud Identität

Auszeichnungen

Deutschland
Land der Ideen

Ausgezeichneter Ort 2013/14

Nationaler Förderer
Deutsche Bank

Ausgezeichneter Ort im Land der Ideen 2013/14

kuppingercole
eic 2015
EUROPEAN IDENTITY & CLOUD CONFERENCE

European Identity & Cloud Award 2015

EuroCloud
AWARD 2015

EuroCloud
DEUTSCHLAND | eco

EuroCloud Germany Award 2015

Trusted Cloud

Trusted Cloud Award 2011

SkIDentity

Ausgezeichneter Ort im Land der Ideen 2015

innovationspreis
Bayern 2016

Bayerischer Innovationspreis 2016

EuroCloud
AWARD 2015

EuroCloud
EuroCloud Forum 2015

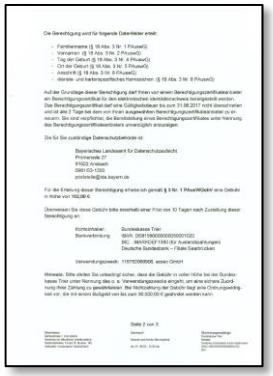
EuroCloud Europe Award 2015

Siegel und Zertifikate

SecurITy made in Germany

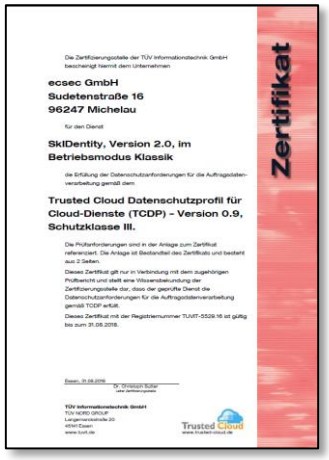
TeleTrusT Quality Seal
www.teletrust.de/itsmig

esec seit 2014

Berechtigungszertifikate
gemäß § 21 PAuswG

BSI TR-03124 Zertifikat
für Open eCard App 2015

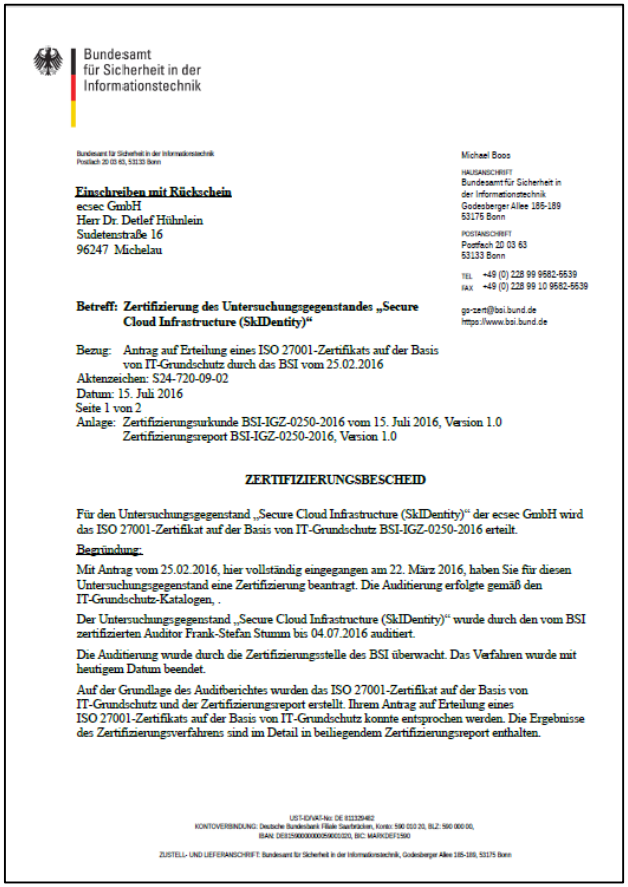


SkIDentity

„Trusted Cloud Datenschutz Profil“ (TCDP)
für „SkIDentity 2.0 “

ISO 27001 auf Basis von IT-
Grundschutz für „Secure Cloud
Infrastructure (SkIDentity)“ (BSI-
IGZ-250)

BSI-IGZ-0250 „Secure Cloud Infrastructure (SkIDentity)“



Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn

Einschreiben mit Rückschein
ecsec GmbH
Herr Dr. Detlef Hühnlein
Sudetenstraße 16
96247 Michelau

Michael Boos
HAUSANSCHRIFT
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn
POSTANSCHRIFT
Postfach 20 03 63
53133 Bonn
TEL +49 (0) 228 99 9582-5539
FAX +49 (0) 228 99 10 9582-5539
gs-zert@bsi.bund.de
https://www.bsi.bund.de

Betreff: Zertifizierung des Untersuchungsgegenstandes „Secure Cloud Infrastructure (SkIDentity)“

Bezug: Antrag auf Erteilung eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz durch das BSI vom 25.02.2016
Aktenzeichen: S24-720-09-02
Datum: 15. Juli 2016
Seite 1 von 2
Anlage: Zertifizierungsurkunde BSI-IGZ-0250-2016 vom 15. Juli 2016, Version 1.0
Zertifizierungsreport BSI-IGZ-0250-2016, Version 1.0

ZERTIFIZIERUNGSBESCHEID

Für den Untersuchungsgegenstand „Secure Cloud Infrastructure (SkIDentity)“ der ecsec GmbH wird das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz BSI-IGZ-0250-2016 erteilt.

Begründung:

Mit Antrag vom 25.02.2016, hier vollständig eingegangen am 22. März 2016, haben Sie für diesen Untersuchungsgegenstand eine Zertifizierung beantragt. Die Auditierung erfolgte gemäß den IT-Grundschutz-Katalogen, .

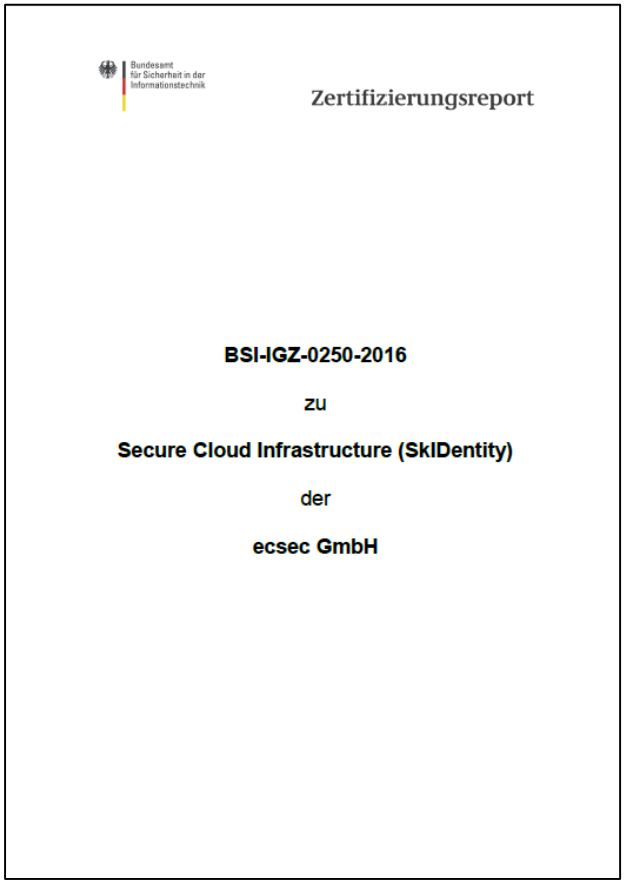
Der Untersuchungsgegenstand „Secure Cloud Infrastructure (SkIDentity)“ wurde durch den vom BSI zertifizierten Auditor Frank-Stefan Stumm bis 04.07.2016 auditiert.

Die Auditierung wurde durch die Zertifizierungsstelle des BSI überwacht. Das Verfahren wurde mit heutigem Datum beendet.

Auf der Grundlage des Auditberichtes wurden das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz und der Zertifizierungsreport erstellt. Ihrem Antrag auf Erteilung eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz konnte entsprochen werden. Die Ergebnisse des Zertifizierungsverfahrens sind im Detail in beiliegendem Zertifizierungsreport enthalten.

UST-ID/VAT-No: DE 812329462
KONTOVERBINDUNG: Deutsche Bundesbank Filiale Saarbrücken, Konto: 590 010 20, BLZ: 590 000 00,
IBAN: DE81590000000059001020, BIC: MARKDEF1590

ZUSTELL- UND LIEFERANSCHRIFT: Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185-189, 53175 Bonn



Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-IGZ-0250-2016

zu

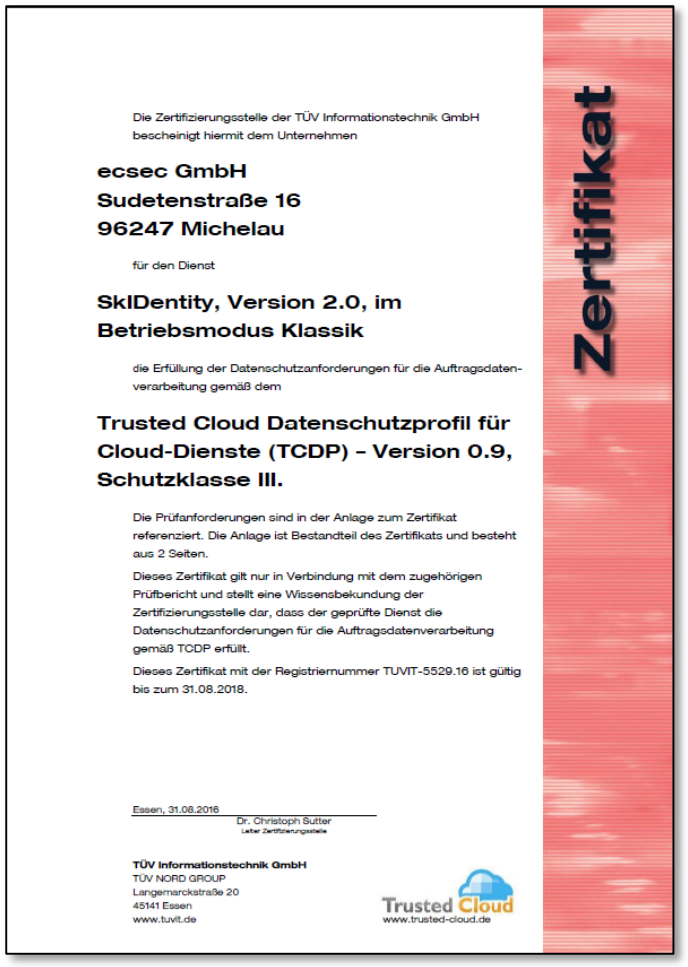
Secure Cloud Infrastructure (SkIDentity)

der

ecsec GmbH

https://skidentity.de/zertifiziert-nach-iso27001-und-tcdp

Trusted Cloud Datenschutzprofil für Cloud-Dienste (TCDP)



Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

ecsec GmbH
Sudetenstraße 16
96247 Michelau

für den Dienst

SkIDentity, Version 2.0, im Betriebsmodus Klassik

die Erfüllung der Datenschutzanforderungen für die Auftragsdatenverarbeitung gemäß dem

Trusted Cloud Datenschutzprofil für Cloud-Dienste (TCDP) – Version 0.9, Schutzklasse III.

Die Prüfanforderungen sind in der Anlage zum Zertifikat referenziert. Die Anlage ist Bestandteil des Zertifikats und besteht aus 2 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem zugehörigen Prüfbericht und stellt eine Wissensbekundung der Zertifizierungsstelle dar, dass der geprüfte Dienst die Datenschutzanforderungen für die Auftragsdatenverarbeitung gemäß TCDP erfüllt.

Dieses Zertifikat mit der Registriernummer TUVIT-5529.16 ist gültig bis zum 31.08.2018.

Essen, 31.08.2016
Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstraße 20
45141 Essen
www.tuvit.de

Trusted Cloud
www.trusted-cloud.de

http://tcdp.de/

https://skidentity.de/zertifiziert-nach-iso27001-und-tcdp

Nach TCDP zertifizierte Dienste

Home TCDP Zertifizierung Hintergrund Dokumente Über uns English

Nach TCDP zertifizierte Dienste

Hier finden Sie Cloud-Dienste, die bereits nach TCDP zertifiziert wurden und damit datenschutzkonform eingesetzt werden können.

Dienst	Anbieter	nach	bis	durch
Authentisierungsservice	VDG Versicherungswirtschaftlicher Datendienst GmbH	TCDP 0.9	31.03.2018	TÜViT
Bürgerportal	regio IT	TCDP 0.9	31.08.2018	TÜViT
iDGARD	Uniscon GmbH	TCDP 0.9	31.03.2018	TÜViT
SkIDentity	ecsec GmbH	TCDP 0.9	31.08.2018	TÜViT
Dynamic Services for Infrastructure with vCloud (DSI vCloud)	T-Systems International GmbH	TCDP 1.0	08.08.2020	DEKRA Certification GmbH
Open Telekom Cloud				

http://www.tcdp.de/index.php/zertifizierung/zertifizierte-dienste

Agenda

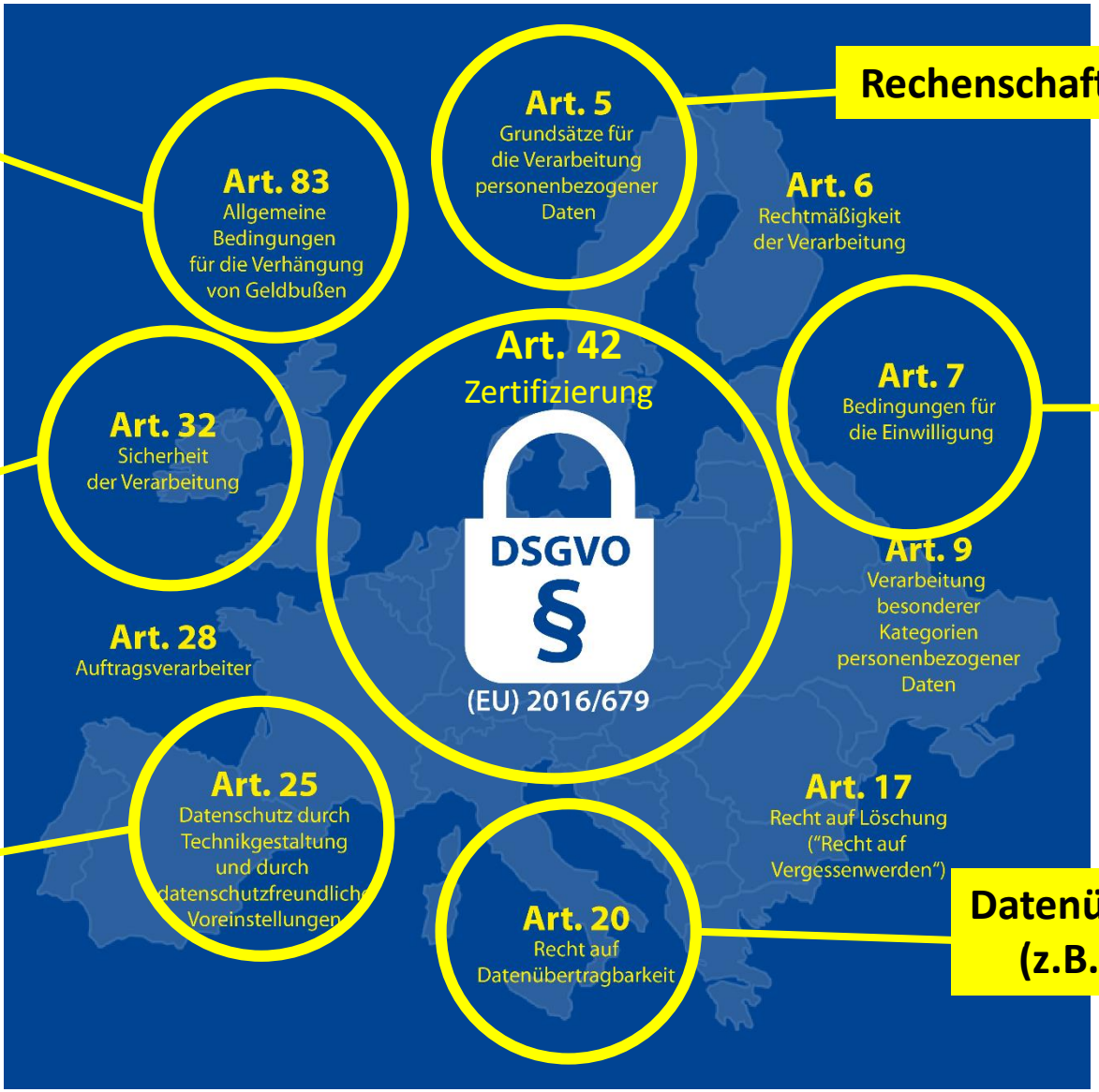
- Einleitung
- SkIDentity
- **Umsetzung der DSGVO am Beispiel SkIDentity**
- Zusammenfassung und Ausblick

Einige Artikel der DSGVO im Überblick

Bußgelder bis zu **20 Mio €** (oder **4% des Umsatzes**)

Sicherheit nach dem Stand der Technik

Privacy by Design & Default



Rechenschaftspflicht

Einwilligung

Datenübertragbarkeit (z.B. XML, JSON)

Einwilligung

Anmeldung SkIDentity für Service Provider DE | EN

Diensteanbieter	ecsec GmbH
Internetadresse	https://sp.skidentity.de
Datenschutz	https://sp.skidentity.de/privacy_de.pdf

Identitätsattribute auswählen

Erforderliche Attribute:

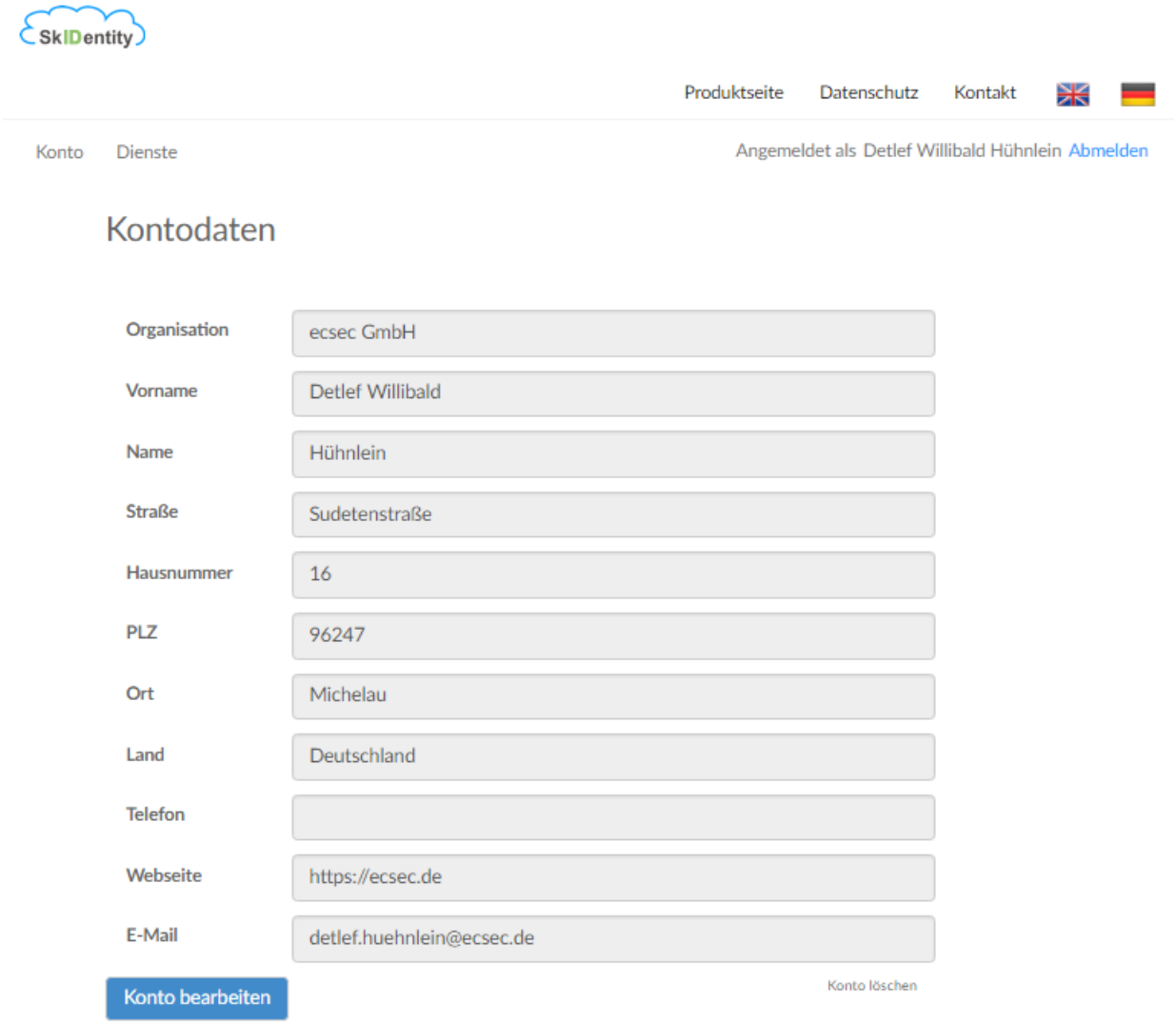
Vorname	☑	Pseudonym	☑
Nachname	☑		

Optionale Attribute:

Geburtsdatum	☐	Ort	☐
Straße	☐	Postleitzahl	☐
Hausnummer	☐	Land	☐
		Alle auswählen	☐

Zurück | Daten übertragen | Abbrechen

Datenübertragbarkeit



117 Mio. (01.06.16)

LinkedIn-Hack: 117 Millionen Passwort-Hashes zum Download aufgetaucht

01.06.2016 15:39 Uhr – Uli Ries, Fabian A. Scherschel vorlesen

Die Angebote mit riesigen Passwort-Hash-Listen im Netz häufen sich: 117 Millionen LinkedIn-Hashes, 360 Millionen MySpace-Konten und 65 Millionen Tumblr-Hashes befeuern die Algorithmen der Cracker. Alle stammen aus alten Hackerangriffen von 2012 und 2013.

Nachdem vor gut zwei Wochen die beim Hack im Jahr 2012 abgesaugte Nutzerdatenbank des Business-Netzwerks LinkedIn zum Kauf im Netz angeboten wurde, stehen jetzt die Hashwerte der Kennwörter frei zugänglich zum Download. Insgesamt 117 Millionen verschiedene SHA1-Hashes stehen der weltweiten Knackergemeinde damit als Übungsmaterial zur Verfügung. Gut 4,5 Gigabyte groß ist die Textdatei, die seit kurzem beim Filehoster mega.nz zum Download steht. Inhalt: 117 Millionen verschiedene Hashwerte der Passwörter von LinkedIn-Nutzern.

https://www.heise.de/security/meldung/LinkedIn-Hack-117-Millionen-Passwort-Hashes-zum-Download-aufgetaucht-3224212.html

SkIDentity

171 Mio.
(06.06.16)

Nach LinkedIn, Tumblr und MySpace: 171 Millionen VKontakte-Passwörter im Netz

06.06.2016 15:37 Uhr – Fabian A. Scherschel

vorlesen

Das VK.com-Hauptquartier im Singer-Haus in Sankt Petersburg (Bild: Pavlikhin, CC BY-SA 3.0)

Ende 2012 bis Anfang 2013 muss eine gute Zeit für Hacker gewesen sein. Nun wurde ein viertes Datenleck von damals bekannt. Diesmal hat es das russische soziale Netz VK.com erwischt. Besondes bitter: Es handelt sich wohl um Klartext-Passwörter.

Der Verkäufer, der in den vergangenen Tagen immer wieder hunderte Millionen Passwort-Hashes großer Webseiten im Netz angeboten hatte, hat nachgelegt. Jetzt bietet der Kriminelle mit dem Pseudonym peace_of_mind 100 Millionen Klartext-Passwörter und dazugehörige Nutzernamen des russischen sozialen Netzes VK.com (früher VKontakte) an. Insgesamt will er 171 Millionen Passwörter erbeutet haben.

https://www.heise.de/security/meldung/Nach-LinkedIn-Tumblr-und-MySpace-171-Millionen-VKontakte-Passwoerter-im-Netz-3227916.html

127 Mio. (07.06.16)

Dating-Seite Badoo: 127 Millionen Passwort-Hashes im Netz

07.06.2016 14:54 Uhr – Fabian A. Scherschel

vorlesen

(Bild: Badoo)

Eine Nutzerdatenbank der Dating-Plattform zirkuliert im Netz. Die Passwörter der Accounts scheinen als ungesalzene MD5-Hashes gespeichert worden zu sein und sind entsprechend leicht knackbar.

Die Reihe der im Netz veröffentlichten Nutzerdatenbanken reißt nicht ab. Jetzt ist ein Datensatz von über 127 Millionen Nutzern des Dating-Portals Badoo aufgetaucht. Neben Benutzernamen sind MD5-gehashte Passwörter enthalten, berichtet Vice. Die Nachrichtenseite hat nach eigenen Angaben 30.000 Datensätze zur Probe erhalten.

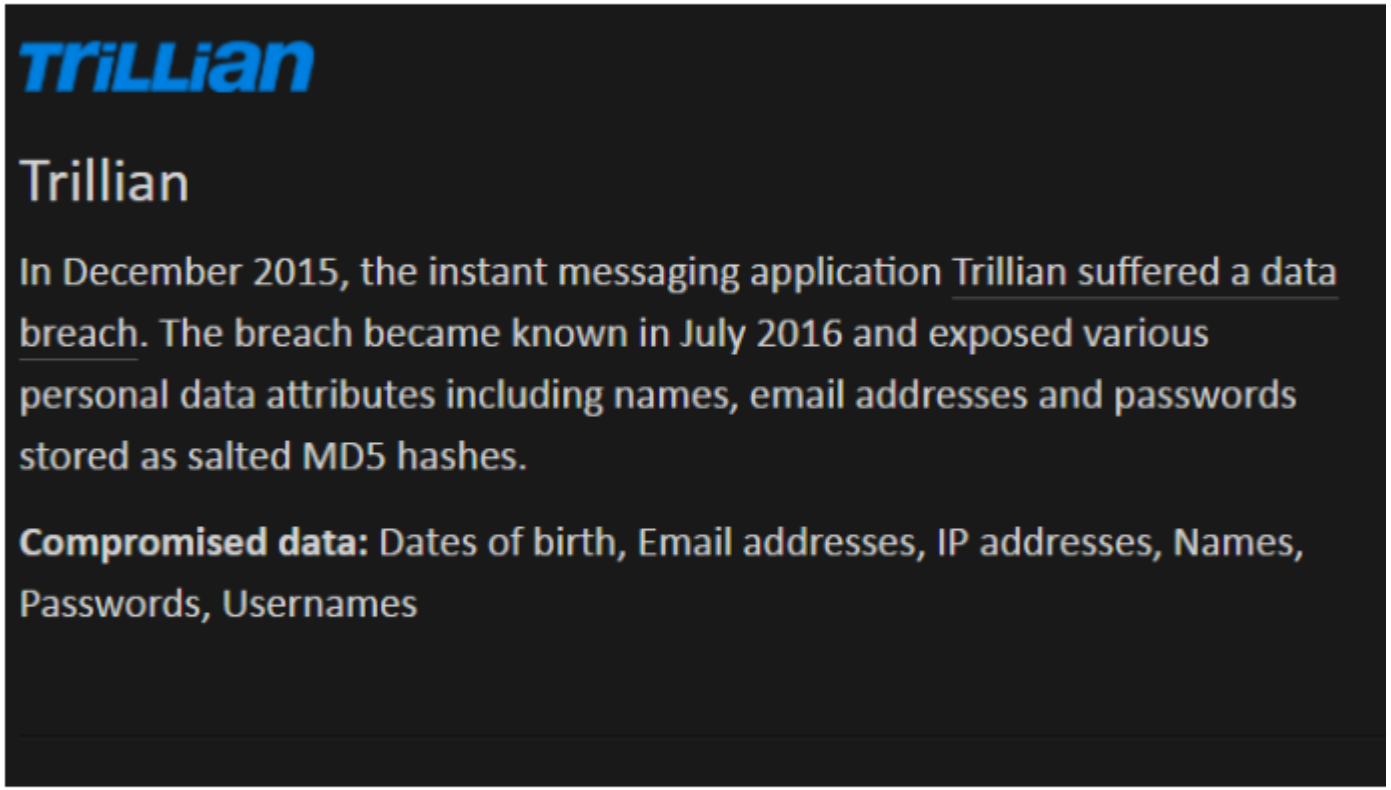
https://www.heise.de/security/meldung/Dating-Seite-Badoo-127-Millionen-Passwort-Hashes-im-Netz-3228893.html

SkIDentity

3 Mio.
(16.07.16)

Alter Trillian-Forumsserver gehackt, gut drei Millionen Nutzerdatensätze abgegriffen

heise Security 16.07.2016 13:36 Uhr – Jan Schüßler vorlese



(Bild: Screenshot haveibeenpwned.com)

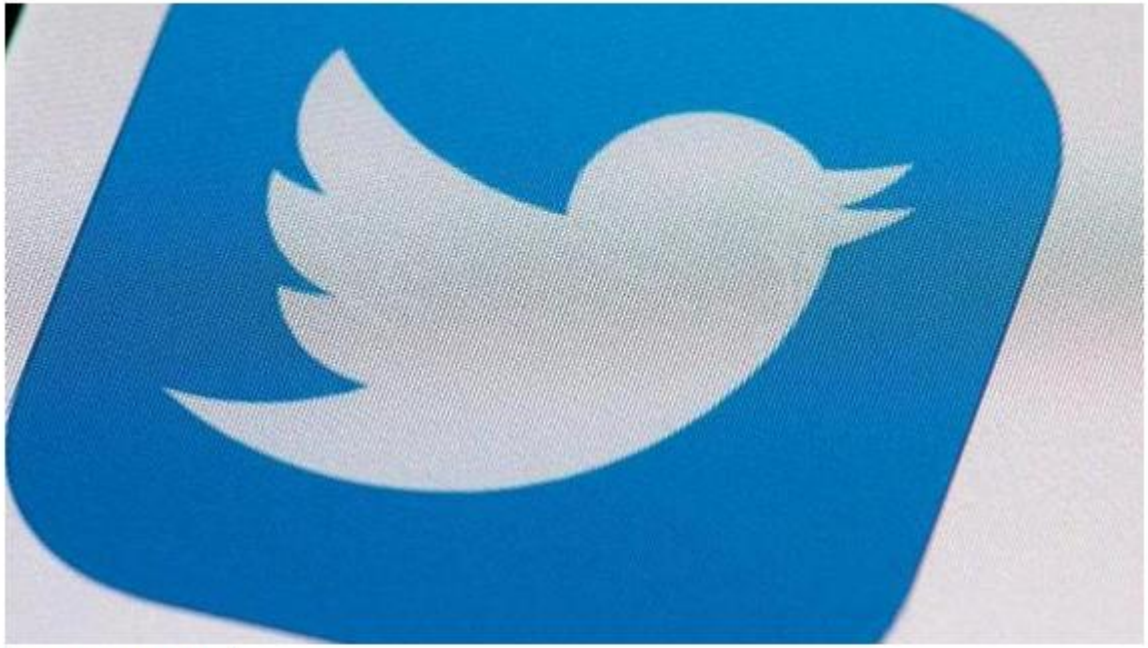
Bei den Betreibern des Instant Messengers Trillian ist ein Server gehackt worden, der zu Archivzwecken Support-Forum und Blog hostete. Ein paar Millionen Nutzerdaten sind dabei in fremde Hände gelangt. Der eigentliche Messenger-Dienst ist nicht betroffen.

https://www.heise.de/newsticker/meldung/Alter-Trillian-Forumsserver-gehackt-gut-drei-Millionen-Nutzerdatensaetze-abgegriffen-3269058.html

33 Mio.
(09.06.16)

33 Millionen Twitter-Passwörter kursieren angeblich im Netz

09.06.2016 11:47 Uhr – Axel Kannenberg vorlesen



(Bild: dpa, Arno Burgi)

Und noch ein mutmaßlicher Millionenleak – diesmal sollen es 33 Millionen Passwörter von Twitter-Accounts sein. Twitter behauptet aber, nicht gehackt worden zu sein.

Nach Linkedin, Tumblr, Myspace und Vk gesellt sich nun auch Twitter in die Reihe der Millionenleaks: Fast 33 Millionen Passwörter von Nutzeraccounts sollen derzeit im Netz verfügbar sein, schreiben die Macher der auf solche Leaks spezialisierten Suchmaschine Leakedsource. Die Datenbank stammt, genau wie bei den vorherigen Fällen, von einem Kriminellen mit dem Pseudonym "peace_of_mind".

https://www.heise.de/security/meldung/33-Millionen-Twitter-Passwoerter-kursieren-angeblich-im-Netz-3233021.html

SkIDentity

68 Mio.
(31.08.16)

Gestohlene Dropbox-Passwörter offenbar echt

31.08.2016 13:37 Uhr – Jürgen Schmidt

vorlesen

(Bild: dpa, Armin Weigel/Archiv)

Die jetzt aufgetauchten Dropbox-Passwörter sind anscheinend echt; ein Test verrät, ob das eigene dabei war. Wer in den letzten Jahren sein Passwort für den Cloud-Speicherdienst nicht geändert hat, sollte das schleunigst tun.

Die kürzlich aufgetauchten Dropbox-Passwörter sind offenbar echt, wie Selbst-Tests von Betroffenen zeigen. Mitte 2012 waren Dropbox rund 68 Millionen Passwörter abhanden gekommen. Zum Glück hatte der Cloud-Dienstbetreiber die Passwörter nur als Hashes gespeichert.

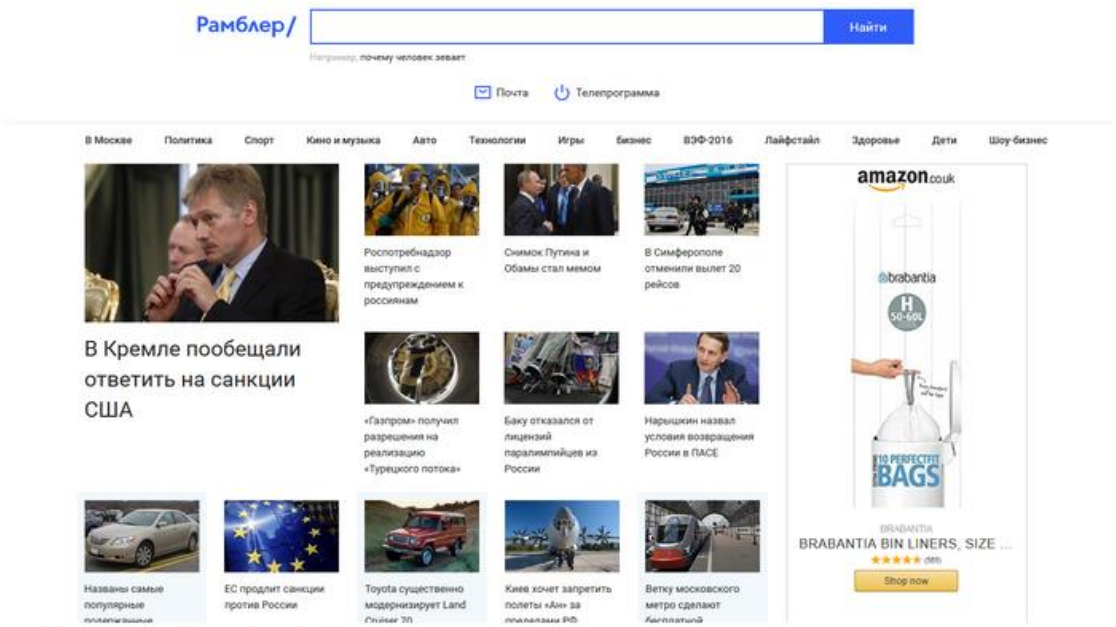
https://www.heise.de/security/meldung/Gestohlene-Dropbox-Passwoerter-offenbar-echt-3310017.html

Fast 100 Millionen Klartextpasswörter von russischem Web-Portal Rambler im Netz

heise Security 07.09.2016 17:25 Uhr – Fabian A. Scherschel vorlesen

98 Mio.

(07.09.16)



Rambler.ru ist das "russische Yahoo"

Das Web-Portal Rambler, welches ebenfalls E-Mail-Dienste bereitstellt und als "russisches Yahoo" gilt, wurde im Jahr 2012 gehackt. Die Passwörter der Nutzer waren unverschlüsselt gespeichert.

Allem Anschein nach hatten die kriminellen Hacker im Jahr 2012 alle Hände voll zu tun. In den letzten Monaten sind immer wieder riesige Passwortlecks bekannt geworden, die alle ihren Ursprung im Jahr 2012 haben. Auch der jetzt bekannt gewordene Fall des russischen Web-Portals Rambler passt in dieses Muster. Laut der Suchmaschine LeakedSource, die geklaute Datensätze sammelt und gegen ein Entgelt durchsuchbar macht, sind Rambler die Passwörter von mehr als 98 Millionen Nutzern abhanden gekommen.

https://www.heise.de/newsticker/meldung/Fast-100-Millionen-Klartextpasswoerter-von-russischem-Web-Portal-Rambler-im-Netz-3315622.html

500 Mio.
(22.09.16)

Rekordhack bei Yahoo: Daten von halber Milliarde Konten kopiert

heise Security 22.09.2016 22:03 Uhr – Daniel AJ Sokolov vorlesen

Mindestens 500 Millionen Opfer dürften Weltrekord sein. (Bild: dpa, Michael Nelson)

Bei Yahoo wurden Ende 2014 Daten von 500 Millionen Usern abgegriffen. Diesen GAU gestand Yahoo am Donnerstag ein. Das Unternehmen vermutet einen "staatlich finanzierten" Angreifer dahinter.

"Wir haben bestätigt, dass Ende 2014 eine Kopie bestimmter Nutzerkontoinformationen aus dem Netzwerk der Firma gestohlen wurde", beichtet Yahoos Sicherheitschef Bob Lord in einer aktuellen Mitteilung. Mindestens 500 Millionen Konten seien betroffen. Damit handelt es sich, gemessen an der Zahl der Opfer, um einen der größten bekannt gewordenen Hacks der IT-Geschichte. Namen, E-Mail-Adressen, Telefonnummern, Geburtsdaten, und Passwort-Hashes sind nun in falschen Händen.

Bald gehört der Problemfall Yahoo zu Verizon.

http://www.heise.de/newsticker/meldung/Rekordhack-bei-Yahoo-Daten-von-halber-Milliarde-Konten-kopiert-3330083.html

SkIDentity

43 Mio.
(21.10.16)

Hacker erbeuten 43 Millionen Daten von Nutzern des Web-Baukastens Weebly

heise Security 21.10.2016 14:26 Uhr – Dennis Schirrmacher vorlesen

Der Werbespruch auf der Startseite von Weebly ist nicht ironisch gemeint.

Die Betreiber von Weebly haben bestätigt, dass Angreifer Millionen Kunden-Daten abgezogen haben. Neben E-Mail-Adressen umfasse die Beute auch Passwörter. Davon soll aber ein Großteil effektiv geschützt sein.

Bereits im Februar dieses Jahres sind unbekannte Hacker in die Server des Web-Baukastens Weebly eingedrungen und haben Nutzer-Daten von mehr als 43 Millionen Kunden kopiert. Das teilt das Unternehmen in einem Statement mit.

https://www.heise.de/security/meldung/Hacker-erbeuten-43-Millionen-Daten-von-Nutzern-des-Web-Baukastens-Weebly-3356684.html

SkIDentity

87 Mio.
(06.12.16)

DailyMotion anscheinend gehackt: 87,6 Millionen Nutzer betroffen

06.12.2016 10:59 Uhr – Dennis Schirrmacher vorlesen

(Bild: Katy Levinson, CC BY 2.0)

Unbekannte Hacker sollen in das Server-System die Videoportals eingestiegen sein und neben E-Mail-Adressen auch geschützte Passwörter kopiert haben.

Beim Videoportal DailyMotion hat es allem Anschein nach ein Datenleck gegeben und Hacker konnten eine Datenbank mit mehr als 87,6 Millionen Accountdaten abziehen. Das geht aus einem Datenbank-Eintrag des Leaking-Portals Leakedsource.com hervor. Eine offizielle Stellungnahme von DailyMotion steht aktuell noch aus.

https://www.heise.de/security/meldung/Hacker-erbeuten-43-Millionen-Daten-von-Nutzern-des-Web-Baukastens-Weebly-3356684.html

SkIDentity

1 Mrd.
(15.12.16)

Yahoo muss erneut Massenhack beichten: Eine Milliarde Opfer

UPDATE

15.12.2016 05:31 Uhr – Daniel AJ Sokolov

vorlesen

Yahoos Europazentrale in Dublin (Bild: Daniel AJ Sokolov)

Im September hatte Yahoo einen Hack von über einer halben Milliarde Nutzerkonten bekanntgegeben. Den Rekord hat Yahoo nun gebrochen. Diesmal geht es um über eine Milliarde Konten. Dazu kommen gezielte Attacken mittels Cookies.

https://www.heise.de/security/meldung/Yahoo-muss-erneut-Massenhack-beichten-Eine-Milliarde-Opfer-3570674.html

SkIDentity

BKA findet eine halbe Milliarde ausgespähte Zugangsdaten

08.07.2017 12:34 Uhr – Thomas Hoffmann

vorlesen

500 Mio.

(08.07.17)

(Bild: dpa, Oliver Berg/Illustration)

Das Bundeskriminalamt hat in einer Underground-Economy-Plattform eine riesige Sammlung ausgespähter Zugangsdaten gefunden. Mit einem Tool können Sie überprüfen, ob Ihre Daten betroffen sind.

https://www.heise.de/newsticker/meldung/BKA-findet-eine-halbe-Milliarde-ausgespaehte-Zugangsdaten-3767465.html

SkIDentity

143 Mio.
(08.09.17)

Hacker-Jackpot: Credit Bureau Equifax gehackt UPDATE

08.09.2017 07:48 Uhr – Daniel AJ Sokolov

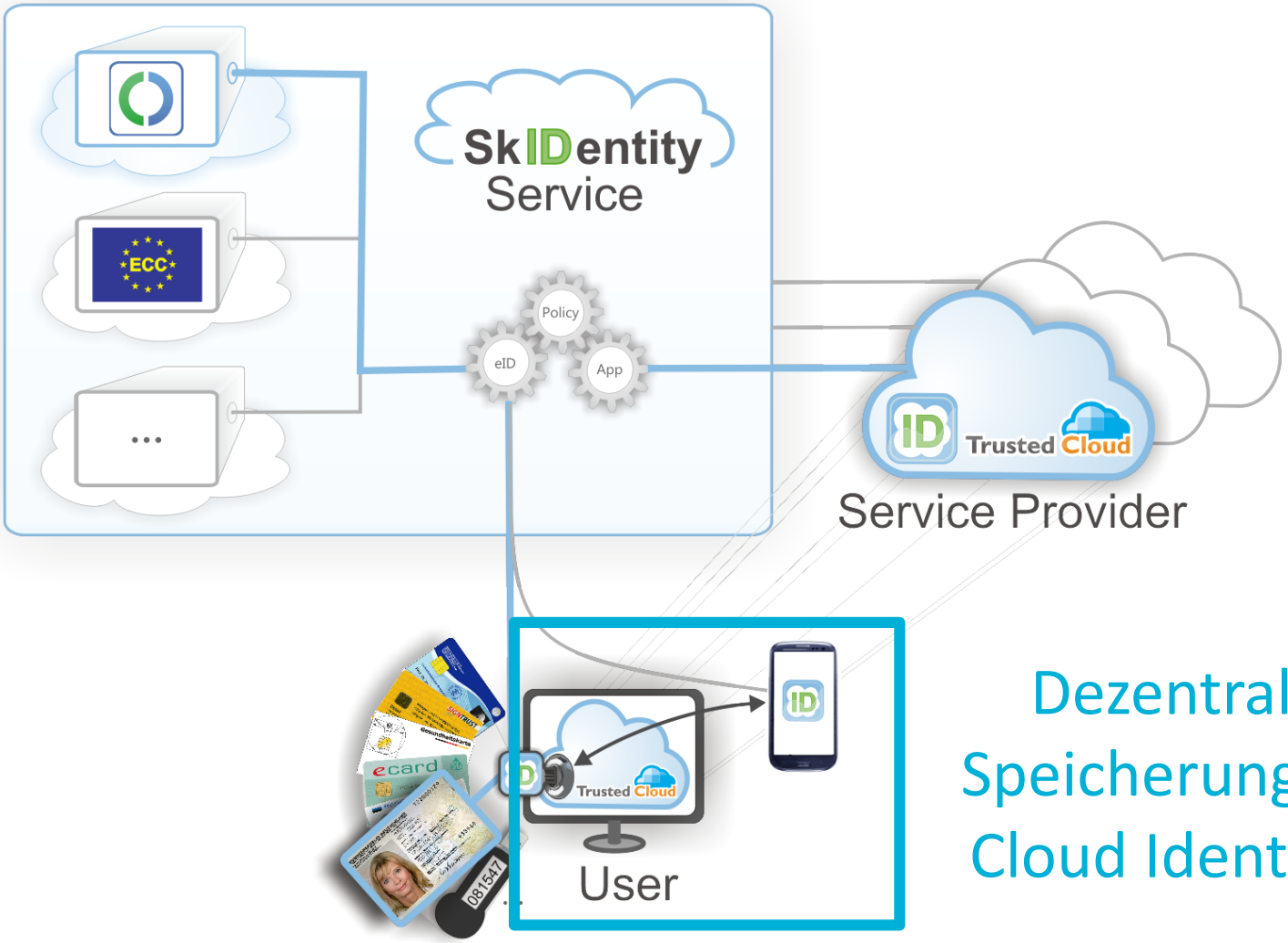
vorlesen

(Bild: gemeinfrei)

Kreditkarten-, Sozialversicherungs- und Ausweisnummern von mehr als Hundert Millionen US-Amerikanern sind in falsche Hände gelangt, als Equifax monatelang gehackt war. Dazu kommen weitere Opfer in Kanada und dem Vereinigten Königreich.

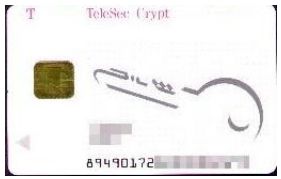
https://www.heise.de/newsticker/meldung/Hacker-Jackpot-Credit-Bureau-Equifax-gehackt-3824607.html

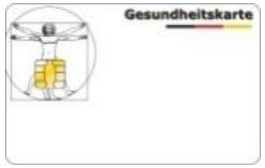
Privacy by Design & Default

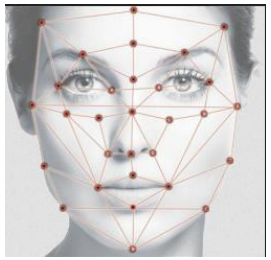


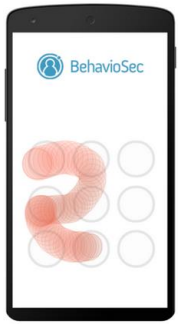
Dezentrale Speicherung der Cloud Identität!

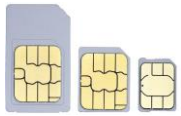
Starke Authentisierung – jetzt!



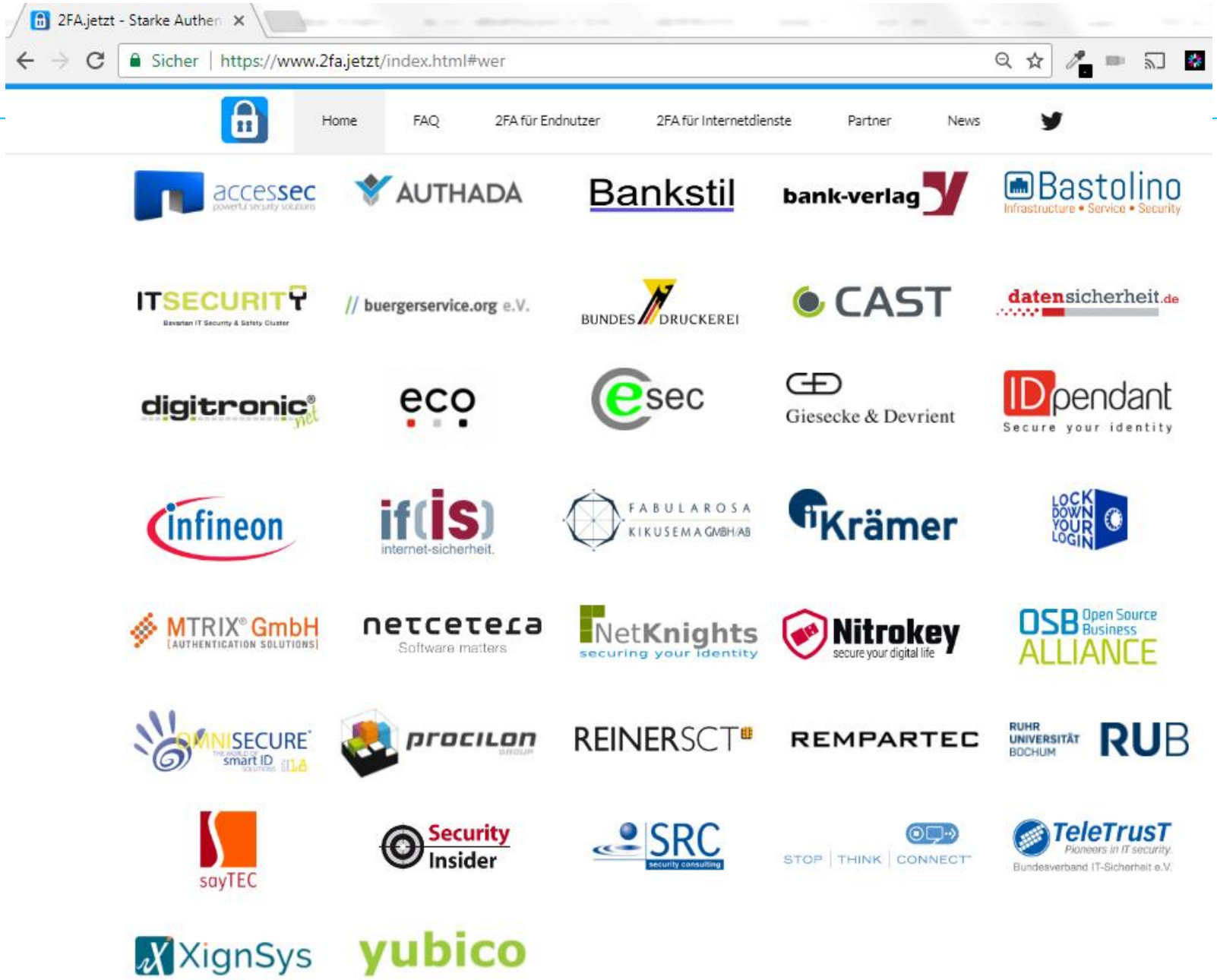









2FA.jetzt - Starke Authen
Sicher
https://www.2fa.jetzt/index.html
Home
FAQ
2FA für Endnutzer
2FA für Internetdienste
Partner
News
fido
TAN
Starke Authentisierung - jetzt!
FAQ
2FA für Endnutzer
2FA für Internetdienste
Partner


2FA.jetzt - Starke Authen
Sicher | https://www.2fa.jetzt/index.html#wer
Home
FAQ
2FA für Endnutzer
2FA für Internetdienste
Partner
News
accessec
powerful security solutions
AUTHADA
Bankstil
bank-verlag
Bastolino
Infrastructure • Service • Security
ITSECURITY
Bavarian IT Security & Safety Cluster
// buergerservice.org e.V.
BUNDESDRUCKEREI
CAST
datensicherheit.de
digitronic net
eco
esec
Giesecke & Devrient
IDpendant
Secure your identity
infineon
if(is)
internet-sicherheit.
FABULAROSA
KIKUSEMA GMBH/AB
iKrämer
LOCK DOWN YOUR LOGIN
MTRIX® GmbH
[AUTHENTICATION SOLUTIONS]
netceteca
Software matters
NetKnights
securing your identity
Nitrokey
secure your digital life
OSB Open Source Business ALLIANCE
OMNISECURE
smart ID
procilon
REINERSCT
REMPARTEC
RUHR UNIVERSITÄT BOCHUM
RUB
sayTEC
Security Insider
SRC
security consulting
STOP | THINK | CONNECT
TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.
XignSys
yubico

AUDITOR
(European Cloud Service Data Protection Certification)

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Konsortium

- UNIKASSEL VERSITÄT – ITeG Wissenschaftliches Zentrum für Informationstechnik-Gestaltung
- CLOUD&HEAT
- datenschutz cert
- DIN
- esec
- EuroCloud DEUTSCHLAND | eco
- eco VERBAND DER INTERNETWIRTSCHAFT – WIR GESTALTEN DAS INTERNET. GESTERN. HEUTE. ÜBER MORGEN.
- UNIKASSEL VERSITÄT provet – ITeG Wissenschaftliches Zentrum für Informationstechnik-Gestaltung

Assoziierte Partner

- Bundesamt für Sicherheit in der Informationstechnik
- HORNETSECURITY
- SCOPE EUROPE
- Trusted Cloud
- TÜVIT – TÜV NORD GROUP
- ULD – Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
- VOICE – Bundesverband der IT-Anwender e.V.

Zusammenfassung

- SkIDentity ermöglicht Mobile eID as a Service
- DSGVO – ein Meilenstein für den Datenschutz!
- Umfassendes Rahmenwerk mit diversen Änderungen im Vergleich zum „alten BDSG“
- „Datenschutzdefizite“ werden durch DSGVO-Screening erkennbar – und werden richtig teuer!
- Umgekehrt „belohnt“ DSGVO datenschutz-freundliches Design und gute Praktiken

Keine Angst vor der DSGVO
– aber bitteschön den nötigen Respekt!

Deutschland Land der Ideen
Ausgezeichneter Ort 2013/14
Nationaler Förderer Deutsche Bank

Herzlichen Dank für Ihre Aufmerksamkeit!

Deutschland Land der Ideen
Ausgezeichneter Ort 2015
Nationaler Förderer Deutsche Bank

Kontakt

ecsec ... being secure made easy

ecsec GmbH
Sudetenstr. 16
96247 Michelau
Telefon + 49 9571 604 8014
Mobil + 49 171 9754980
detlef.huehnlein@ecsec.de
http://www.ecsec.de

Dipl.-Inform. (FH)
Dr. Detlef Hühnlein
Geschäftsführer