


**besonderes
elektronisches
Anwaltspostfach beA**



einfach. digital. kaputt.

Markus Drenger / Felix Rohrbach



```
public static void main(final String[] args) throws  
InterruptedException {  
    final StartDaShit shitty = new StartDaShit();  
    new PCardListener(shitty, null);  
    ...  
}
```



Was wir heute tun

- Was ist das beA?
- was wir getan haben
- was wir nicht getan haben
- Informationen sammeln
- Analyse
- Reporting
- Q&A



Chaos Darmstadt e.V.

- Markus Drenger
 - Twitter: @reg_nerd
 - md@darmstadt.ccc.de
- Felix Rohrbach
 - Twitter: @fxrh
 - fxrh@darmstadt.ccc.de



Chaos Darmstadt e.V.

Hochschulgruppe an der TUD und h_da

Hackspace in der Wilhelminenstr 17

offenes Chaos dienstags & freitags ab 19 Uhr

Capture-The-Flag-Team mittwochs 19 Uhr

infos: chaos-darmstadt.de



beA

- BeA ist das **b**esondere **e**lektronische **A**nwaltspostfach
- Kommunikation zwischen Anwaltschaft und Gerichten (sicher)
- Quasi „De-Mail“



was wir getan haben

wir haben Spezifikationen angeschaut

wir haben uns die Webseite angeschaut

wir haben uns die frei verfügbare
Clientsoftware angeschaut



was wir getan haben

wir haben schlechte Spezifikationen gefunden

wir haben Probleme im Webserver gefunden

wir haben eine angreifbare Clientsoftware gefunden



was wir nicht gemacht haben

wir haben das beA nicht „gehackt“

wir haben uns die Server nicht angeschaut

wir haben „die Krypto“ nicht geknackt



was wir nicht gemacht haben

wir haben das beA nicht „gehackt“

wir haben uns die Server nicht angeschaut

wir haben „die Krypto“ nicht geknackt

wir haben „die Krypto“-Implementierung nicht angeschaut



was wir nicht gemacht haben

wir haben kein vollständiges Code-Audit von Client- und Serverkomponenten gemacht

-> selbst wenn alle von uns gemeldeten Probleme behoben werden, garantiert dies nicht die Sicherheit

beA - ist das sicher?





FragDieBRAK

- Anfrage an den Datenschutzbeauftragten nach einem Verzeichnissesverzeichnis
- Anfrage nach dem Informationsfreiheitsgesetz



IFG

- Verträge mit Atos
- Lasten- und Pflichtenhefte
- Mängel- und Fehlerlisten
- Sicherheitsüberprüfungen / Audits

„Zu den Mängel- und Fehlerlisten sowie den Sicherheitsüberprüfungen/Audits

Atos hat kontinuierlich im Rahmen der Softwareentwicklung Tests der beA-Software durchgeführt. Die BRAK hat **vor Abnahme der Software eigene Tests durchgeführt. Bei den in diesem Zusammenhang geführten Fehlerlisten handelt es sich wiederum um Betriebs- und Geschäftsgeheimnisse von Atos und der BRAK i. S. d. § 6 Satz 2 IFG, deren Offenlegung Atos nicht zugestimmt hat.**“

IFG

„Atos hat im Dezember 2015 eine externe **Sicherheitsüberprüfung** der beA-Webanwendung durch die Firma **Sec Consult** durchführen lassen. Zudem hat Atos im April 2016 einen **Penetrationstest** der Kanzleisoftware-Schnittstelle des beA durchgeführt. Die Testberichte hierzu sind **ebenfalls** Betriebs- oder **Geschäftsgeheimnisse** von Atos im Sinne von § 6 Satz 2 IFG. Auch hier hat Atos einer Offenlegung nicht zugestimmt.“



readthedocs

- egvp.de
- OSCI 1.2 Spezifikation
- Xjustiz, Handbücher, Präsentationen...
- Anforderungen an egvp-Drittprodukte

Teilnahme von Drittanwendungen₁ am OSCI-gestützten
elektronischen Rechtsverkehr

Anforderungen



beA < EGVP

Teilnahme von Drittanwendungen₁ am OSCI-gestützten
elektronischen Rechtsverkehr

Anforderungen



Sicherheit: Clientseitig?

- Spam
- DoS
- ...



Spamschutz

A13:

„Es darf nicht möglich sein, eine Nachricht mit ein und demselben Bedienschritt an mehrere Gerichte und/oder Staatsanwaltschaften zu versenden.“



Spamschutz

- Kleine Gerichte haben 2 mbit/s-Anbindung an Landesverwaltungsnetze



Spamschutz

- Kleine Gerichte haben 2 mbit/s-Anbindung an Landesverwaltungsnetze
- 100 mbit/s = 50 lahmgelegte Gerichte

Clientseitiges Rate-Limit

A2:

„Die Drittanwendung darf auf Dienste und Server der EGVP-Infrastruktur nur in solchen Intervallen zugreifen, welche keine Störungen des Betriebs verursachen. Es werden Zeitabstände von mindestens 15 Minuten empfohlen.“



Browser

Pop-up-Fenster:
Sie dürfen Pop-up-Fenster des
beA nicht blockieren.



Datenvolumen

- Die Clientsoftware soll Nachrichten auf maximal 30 MB begrenzen
- Bei größeren Nachrichten kann ein Transport nicht garantiert werden



Datenvolumen

- Die Clientsoftware soll Nachrichten auf maximal 30 MB begrenzen
- Bei größeren Nachrichten kann ein Transport nicht garantiert werden
- beA laut BRAK bis zu 60 MB (Vermutung: Spezifikation auf egvp.de veraltet)



Betriebssysteme

„beA unterstützt **aktuelle Versionen** von Windows, Mac OS und Linux. Ein regelmäßiger Test erfolgt für die Betriebssysteme **Mac OS 10.11** El Capitan und Windows Vista, 7, 8 und 8.1, **Linux openSUSE 13.2.**“



Betriebssysteme

- OpenSuse 13.2
 - **End of life seit Januar 2017**
- OSX 10.11
 - **Extended support endet im Herbst 2018**

Ende zu Ende- Verschlüsselung

- „[...] Übermittlungsweg **mit sogenannter Ende-zu-Ende-Verschlüsselung.**“

(Bundesverfassungsgericht, 22.12.2017)

- „Die über das beA versandten Nachrichten **werden Ende-zu-Ende verschlüsselt.**“

(Bundesregierung, 17.10.2016 BT-Drs.
18/9994)



„Umschlüsselung“

- Was macht man, wenn man nicht alleine arbeitet?



„Umschlüsselung“

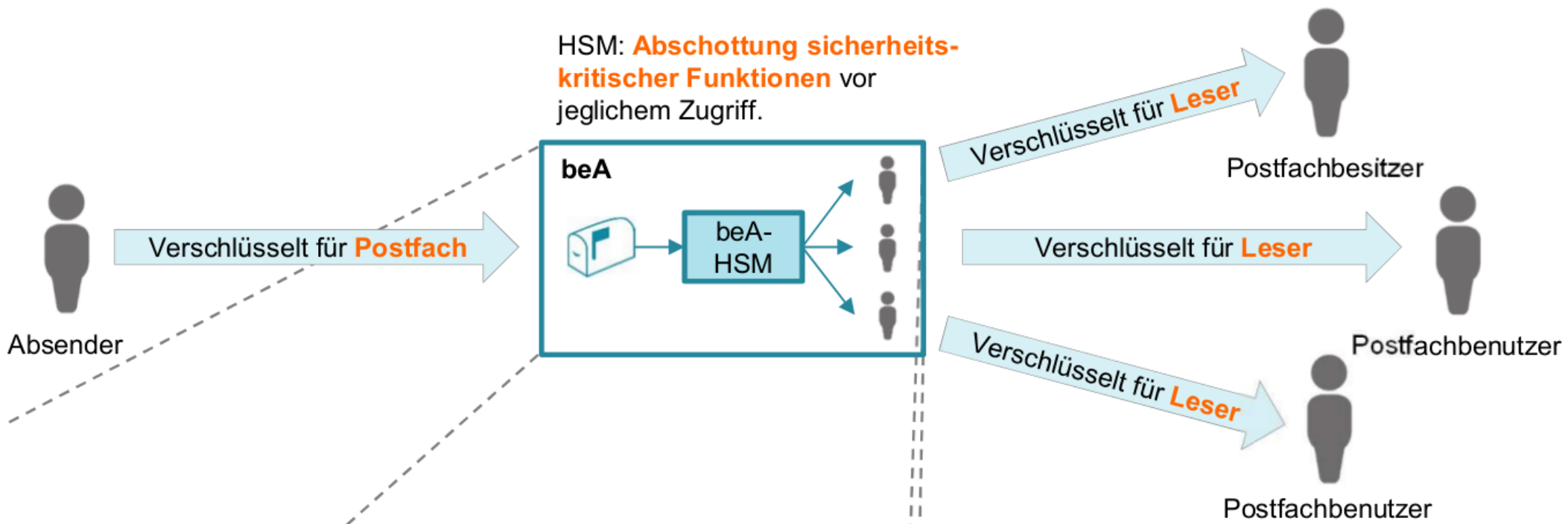
- Wenn MitarbeiterInnen oder PartnerInnen auf die Nachrichten zugreifen sollen?



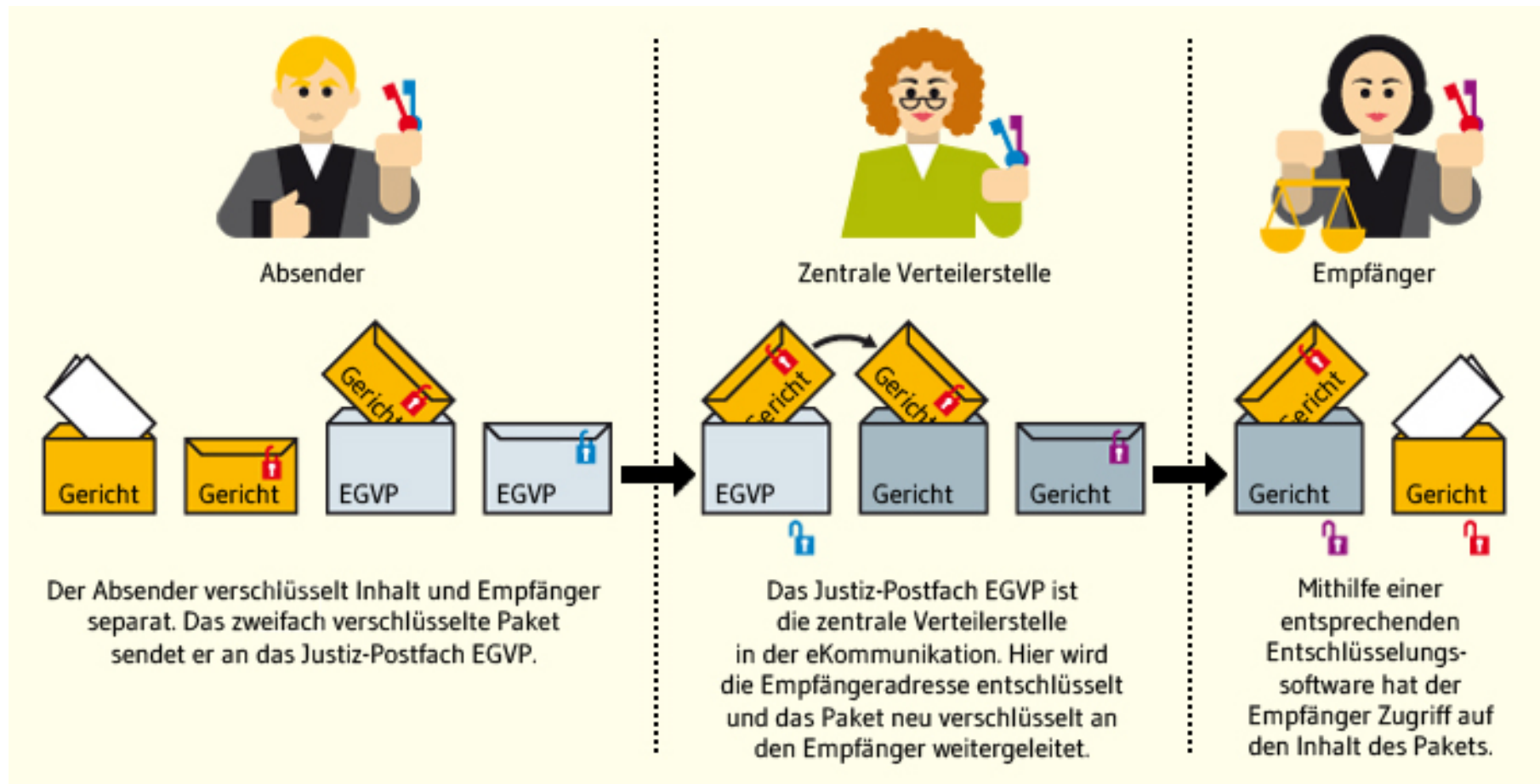
„Umschlüsselung“

- Weiterleitungsfunktion im beA:
Umschlüsselung

Grafik HSM



OSCI





Umschlüsselung

- Private Postfachschlüssel **aller Teilnehmer** werden **zentral gespeichert**
- Nachrichtenkeys werden **entschlüsselt**
- Für Zielempfänger **neu verschlüsselt**



Analyse der Software

- frei zum Download verfügbar
- In Java geschrieben
- Wir haben uns den Linux-Client angeschaut



Funktionsweise

- Client läuft als Daemon im Hintergrund
 - lauscht auf Port 9998
- Anwender öffnet bea-brak.de im Browser
- Webseite verbindet sich per WebSocket zum Client
- Client öffnet Login-Fenster

Download

```
algorithm_catalog-4.1.0.8.jar
algorithm_identifier-1.0.0.9.jar
authentCommon-3.9.0.0.jar
authentRequester-3.9.0.0.jar
base64-1.2.2.3.jar
bcmail-1.46.jar
bcprov-1.46.jar
bctsp-1.46.jar
BeaPayload-2.1.4.0.jar
BeaToolkit-2.1.4.0.jar
cadestoolbox-1.5.0.0.jar
challengeResponseClient-3.9.0.0.jar
ci-1.11.1.5.jar
client_ca_certs-57.jar
ClientSecurity-2.1.4.0.jar
commons-cli-1.2.jar
commons-compress-1.4.1.jar
commons-io-2.4.jar
commons-lang3-3.0.jar
commons-logging-1.2.jar
commons-mimetype-1.4.8.0.jar
ComponentInfo-1.0.3.jar
config_produkativ.jar
dtos-2.1.4.jar
ecard-model-2.1.2.1.jar
fontbox-1.8.8-GOV.jar
freemarker-2.3.23.jar
gcf-businesscard-3.6.3.5.jar
gcf-observable-server-3.6.3.5.jar
gcf-verification-3.6.3.5.jar
gov_crypto_provider-1.3.0.6.jar
govServerUtils-3.8.jar
http-core-2.4.0.14.jar
ISOCountryCodeType-V2006-2.jar
itext-1.4.8.jar
jackson-core-asl-1.9.13.jar
jackson-mapper-asl-1.9.13.jar
javax.servlet-3.0.0.v201112011016.jar
jcl-over-slf4j-1.7.9.jar
jetty-http-9.0.3.v20130506.jar
jetty-io-9.0.3.v20130506.jar
jetty-server-9.0.3.v20130506.jar
jetty-util-9.0.3.v20130506.jar
log4j-1.2.17.jar
mcard-1.25.0.2-HF1.jar
oasis-dss-core-schema-v1.0-os-1.0.4-Streaming.jar
oasis-sstc-saml-schema-assertion-1.1-1.0.4-Streaming.jar
osci-bibliothek-1.6.1.jar
padestoolbox-1.5.3.4.jar
PCard-2.1.4.0.jar
pdfbox-1.8.8-GOV.jar
SignerToolBox-2.1.4.0.jar
slf4j-api-1.7.9.jar
slf4j-log4j12-1.7.9.jar
ts_102231v020000_xsd-1.0.4-Streaming.jar
vi-framework-3.7.1.9.jar
vi-output-html-3.7.1.9.jar
vi-output-xml-3.7.1.9.jar
vi-plugin-cades-3.7.1.9.jar
vi-plugin-cms-3.7.1.9.jar
vi-plugin-osci-3.7.1.9.jar
vi-plugin-pades-3.7.1.9.jar
vi-plugin-x509-3.7.1.9.jar
vi-plugin-xades-3.7.1.9.jar
vi-util-ades-3.7.1.9.jar
vi-util-xmlsignature-3.7.1.9.jar
websocket-api-9.0.3.v20130506.jar
websocket-client-9.0.3.v20130506.jar
websocket-common-9.0.3.v20130506.jar
websocket-server-9.0.3.v20130506.jar
websocket-servlet-9.0.3.v20130506.jar
XAdES-1-3-2-1.0.4-Streaming.jar
xadestoolbox-1.5.3.4.jar
xenc-schema-1.0.4-Streaming.jar
xkms20-1.0.4-Streaming.jar
XKMSExtensionsPEPPOL_v2.2-1.0.4-Streaming.jar
xml-1.jar
xmldsig-core-schema-1.0.4-Streaming.jar
xmlsec-1.4.4.jar
```

Das neueste vom Neuen

- Auftrag: 2014
- Veraltete Libraries:
 - „javax.servlet-3.0.0.v**2011**12011016.jar“
 - „jetty-server-9.0.3.v**2013**0506.jar“
 - „log4j-1.2.17“
 - **End of Life** seit 5. August 2015
 - ...

Der WebSocket

- Versionsabfrage:

```
{  
    "command": "getVersion",  
    "payload": "{}"  
}
```

- Alle anderen Anfragen benötigen Session-ID die mit bea-brak.de ausgehandelt wird
 - benötigen einen Account

WebSocket - Command

- **IdentifyYourSelf**

Session-ID:

„base64(**"IdentifyYourSelf"**)“

- **killCurrentInstance**

Session-ID:

„base64(**"UN33dT0K1IIY0urS3If"**)“



Denial of Service

- Locke Anwalt auf Webseite
- Webseite versucht regelmäßig, sich zum Client zu verbinden
- Wenn erfolgreich -> beende Client



Das SSL-Dilemma

- User verbinden sich per https zu bea-brak.de
- Damit nur SSL-Websockets möglich
- Clientsoftware muss API per SSL anbieten



Die „Lösung“

- bealocalhost.de -> 127.0.0.1
- SSL-Zertifikat für bealocalhost.de gekauft
- Private Key für Zertifikat in Keystore im Client
- Hard-coded Passwort im Client



Website

„da geht was“

Dank an Alexander Druffel für Hinweis auf
XSS

Website

```
//restrict the length to prevent script-injection
if (windowId != null && windowId.length() > this.maxWindowIdLength)
{
    windowId = windowId.substring(0, this.maxWindowIdLength);
}
return windowId;
```



CVE-2017-17837

Website hat nur einen Parameter

erlaubt 10 Zeichen XSS



Reporting

Wer ist für was zuständig?



Reporting

Wer ist für was zuständig?

Auftraggeber: BRAK

Aufsichtsbehörde: BMJV

Softwarehersteller: Atos

Betrieb: Atos

EGVP: ??

OSCI: KoSIT (Koordinierungsstelle für IT-
Standards Bund und Länder)



Reporting

Muss man sich selbst schützen? (Hacking, Ausspähen, Dekompilierung, Urheberrecht)

Muss man Helfer schützen?

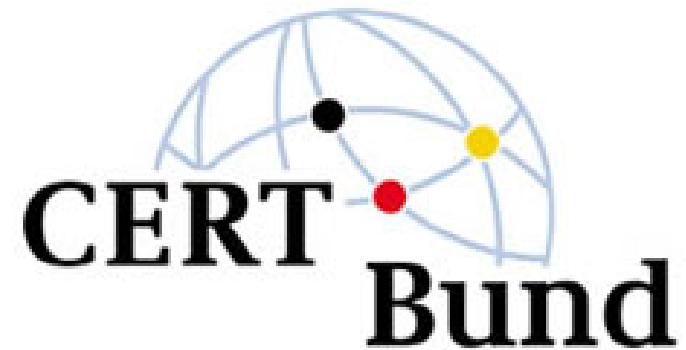
Gefährdet das Offenlegen von Lücken den Datenschutz oder die IT-Sicherheit von Dritten?

certbund@bsi.bund.de

CERT-Bund

CERT-Bund, das **C**omputer **E**mergency **R**esponse
Team für Bundesbehörden, ist die zentrale
Anlaufstelle für präventive und reaktive
Maßnahmen bei sicherheitsrelevanten Vorfällen in
Computer-Systemen.

Das Computer-Notfallteam





auch der CCC bietet sich als sicherer Proxy
oder Vertreter an, um mit Unternehmen oder
Behörden zu sprechen

Bundestrojaner

PC-Wahl

VDS-Gutachten



Presse


am besten Journalisten direkt anschreiben,
nicht info@

unterschiedliche Technikaffinität

c't / heise / golem / Zeit / FAZ / HR / Echo

nicht alle bieten Email-Verschlüsselung an

nicht in allen Fällen „hilfreich“ oder
angemessen



CA Browser Forum Baseline Requirements

„The CA SHALL revoke a Certificate **within 24 hours** if one or more of the following occurs:

[...]

3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;“



20.12.2017

- Information an
 - BRAK
 - CERTbund des BSI
 - T-Systems/Telesec
 - Apache Deltaspikes



21.12.2017

- Apache Deltaspikes patch



22.12.2017

- Bundesverfassungsgericht weist Klage gegen beA ab (aus den Nachrichten davon erfahren)



22.12.2017

- Bundesverfassungsgericht weist Klage gegen beA ab (aus den Nachrichten davon erfahren)
- T-Systems/Telesec sperrt Zertifikat
- Sondernewsletter der BRAK
 - Zertifikat sei „abgelaufen“
 - Softwareupdate und eigene Root-CA
 - Private Key der Root-CA wird per Update verteilt



23.12.2017

- Eigene Root-CA der BRAK wird gelöscht
- Pressemitteilung verschwindet von Webseite
- BRAK fordert Anwender auf, das Root-CA zu deinstallieren



27.12.

- Pressemitteilung Nr. 15 vom 27.12.
„Am Donnerstag, 21. Dezember 2017, zeigte eine **nicht zur Rechtsanwaltschaft zugelassene Person** an, dass sie in der Client-Security, dem Zugangsinstrument, um auf das beA-System zu gelangen, ein Zertifikat **kompromittiert habe.**“



status quo

- Gerichte können keine Dokumente an beA-Konten schicken
- Anwaltschaft kann beA nicht nutzen



status quo

„Wir können Ihnen den Zugang wieder gewähren[...]"



status quo

unter <http://schulung.bea-brak.de/> wird nach wie vor die Software inkl. root-ca angeboten

Installation des kompromittierten Zertifikats notwendig, um Schulungssystem zu nutzen



wie gehts weiter

wir als CCC DA sind nicht zuständig

wir wurden zu einem Gespräch eingeladen
(„beAthlon“)



Fragen