Anleitung zur Anpassung der beA-Konfiguration

Stand 27.12.2017

Einleitung

Nachdem wir am 21.12.2017 informiert wurden, dass ein für die Funktion der beA-Endgerätesoftware (Client Security) notwendiges Zertifikat ausgetauscht werden musste, wurde durch die Firma Atos ein Ersatzzertifikat (**bealocalhost.de**) bereitgestellt. Die entsprechende Anleitung wurde mit dem beA-Sondernewsletter am 22.12.2017 und auf der WEB-Seite bea.brak.de veröffentlicht.

Später am 22.12.2017 wurde die BRAK darüber informiert, dass dieses Ersatzzertifikat fehlerhaft und dadurch potentiell unsicher ist. Die BRAK hat sich daraufhin entschieden, die beA-Anwendung vom Netz zu nehmen. Wir bitten Sie dringend, dieses Zertifikat wieder zu entfernen. Haben Sie das Zertifikat "**bealocalhost.de**" nicht manuell installiert, so brauchen Sie auch keine weiteren Maßnahmen durchzuführen.

Das durch das Zertifikat "bealocalhost.de" verbundene Risiko ist:

"Mit Hilfe dieses Zertifikats könnte ein Angreifer eigene Webseiten als vertrauenswürdig präsentieren. Derselbe Angreifer könnte anschließend einen weiteren IT-Sicherheitsangriff (sog. "DNS-spoofing" oder "cache poisoning") durchführen. Schließlich könnte er Anwenderinnen und Anwender auf seine eigenen Webseiten umleiten und ihre Rechner über diese Webseiten mit Schadsoftware infizieren."

Obwohl nur eine sehr geringe Wahrscheinlichkeit besteht, dass diese Schwachstelle ausgenutzt wird, bitten wir Sie nachdrücklich darum, dieses Zertifikat zu entfernen.

Die Bundesrechtsanwaltskammer (BRAK) wird die Plattform beA vorerst weiter offline lassen. Die Ende-zu-Ende-Verschlüsselung war von dem potentiell unsicheren Zertifikat nicht betroffen. Die Vertraulichkeit der Datenübertragungen war zu jedem Zeitpunkt gesichert. Es handelt sich um ein Zugangs- bzw. Verbindungsproblem, das der Technologieentwickler des beA-Systems bislang nicht gelöst hat.

Die BRAK wird daher das beA-System erst wieder bereitstellen, wenn der technologische Dienstleister die Störungen vollständig behoben hat und einen sicheren Zugang gewährleisten kann.

Allen Rechtsanwältinnen und Rechtsanwälten, die entsprechend der ursprünglichen Empfehlung vom 22.12.2017 das ersatzweise bereitgestellte Sicherheitszertifikat installierten, rät die BRAK dringend zur Deinstallation, um sich aus dem Zertifikat möglicherweise ergebende Sicherheitsrisiken für die individuelle PC-Umgebung auszuschließen. Eine Anleitung finden Sie nachfolgend:

Inhalt

beA Zertifikat entfernen	3
Microsoft Internet Explorer unter Windows	4
Firefox (gilt für Windows ebenso wie Linux und macOS)	6
Safari (gilt für Linux und macOS)	9
Chrome (gilt für Windows ebenso wie Linux und macOS)	10

beA Zertifikat entfernen

Wenn Sie das Zertifikat **bealocalhost.de** installiert haben, so führen Sie bitte – je nach eingesetztem Browser – die nachfolgenden Schritte durch.

Sollten im Rahmen der Durchführung Fragen oder Probleme auftreten, so wenden Sie sich bitte an den beA-Service Desk der Firma Atos unter **+49 30 520009444** oder **bea-servicedesk@atos.net**.

Die notwendigen Schritte zur Entfernung des Zertifikats sind beschrieben für:

- 1. Microsoft Internet Explorer unter Windows
- 2. Firefox (gilt für Windows ebenso wie für Linux und MacOS)
- 3. Safari (gilt für Linux und MacOS)
- 4. Chrome (gilt für Windows ebenso wie für Linux und MacOS)

Microsoft Internet Explorer unter Windows

Um das Zertifikat zu entfernen, führen Sie bitte die folgenden Schritte durch:



Klicken Sie im Internet Explorer auf das Zahnradsymbol. Es erscheint ein Pop-up-Menü.

Klicken Sie im Pop-up-Menü auf die Option **Internetoptionen**.



Klicken Sie auf die Registerkarte Inhalte.

Klicken Sie dort auf die Schaltfläche Zertifikate.

Ausgestellt für	Ausgestellt von	Ablaufda	Anzeigename	^
🔄 AddTrust External	AddTrust External CA	30.05.2020	The USERTrust	
Baltimore CyberTru	Baltimore CyberTrust	13.05.2025	DigiCert Baltimor	
boskg-CA01	boskg-CA01	23.01.2018	<keine></keine>	
boskg-CA01	boskg-CA01	23.01.2018	<keine></keine>	
Certum Trusted Ne	Certum Trusted Netw	31.12.2029	Certum Trusted	
Class 3 Public Prima	Class 3 Public Primary	02.08.2028	VeriSign Class 3	
COMODO RSA Cert	COMODO RSA Certific	19.01.2038	COMODO SECU	
Copyright (c) 1997	Copyright (c) 1997 Mi	31.12.1999	Microsoft Timest	
Deutsche Telekom	Deutsche Telekom Ro	10.07.2019	Deutsche Teleko	
mportieren Exportierer	n Entfernen		Erweite	ert
eabsichtigte Zwecke des Ze	rtifikats			
eabsichtigte Zwecke des Ze	n Entfernen		Erweite	ert

Es wird das Dialogfenster für die Zertifikatsverwaltung geöffnet.

Wechseln Sie auf die Registerkarte Vertrauenswürdige Stammzertifizierungsstellen.

Mit sehr hoher Wahrscheinlichkeit sehen sie etliche weitere Zertifikate in der angezeigten Liste. Stellen Sie sicher, dass Sie kein anderes Zertifikat versehentlich löschen! Markieren Sie das Zertifikat "bealocalhost.de" durch einfaches Klicken.

Betätigen Sie die Schaltfläche **Entfernen**. Bestätigen Sie die folgende Warnung. Das Zertifikat ist entfernt.

Prüfen Sie vorsichtshalber, ob das Zertifikat "bealocalhost.de" noch an anderen Stellen installiert ist, indem Sie in der Zertifikatsverwaltung auch die übrigen Registerkarten anklicken. Sollten das Zertifikat an anderen Stellen installiert sein, löschen Sie es auch dort.

Löschen Sie schließlich "**bealocalhost.de**" an dem Ort, an dem Sie es durch das Herunterladen zwischengespeichert haben (z. B. auf dem Desktop).

Firefox (gilt für Windows ebenso wie Linux und MacOS)

Um das Zertifikat zu entfernen, führen Sie bitte die folgenden Schritte durch:



Klicken Sie auf das **Optionensymbol** (i.d.R. oben rechts ganz außen neben der Adressleiste). Es erscheint ein Pop-up-Menü.

Klicken Sie in dem Pop-up-Menü auf die Option **Einstellungen.**





Ihre Zettifikate Personen Server Zettifikierungsstellen Andere ice haben Zettifikate gespeichert, die diese Zettifizierungsstellen identifizieren: Kryptographie-Modul Zettifikatsname Kryptographie-Modul Semen Internet CA VLD das Softwar-Sichetheitsmodul Telsées ServerBas CA 2 das Softwar-Sichetheitsmodul Verton Namis Surdserver CA G14-SHA2 das Softwar-Sichetheitsmodul Verton Namis Surdserver CA G14-SHA1 das Software-Sichetheitsmodul Verton Assist Statt das Software-Sichetheitsmodul Notation Constatt Builtin Object Token Bayass Clask S Root CA Builtin Object Token Agueshen				Zertifikatverwaltu	ing	
ie haben Zertifikate gespeichert, die diese Zertifizierungsstellen identifizieren: Zertifikatsmane kryptographie-Modul Siemen Internet CA V1.0 da Software-Sichenheitsmodul Telese: ServerPas CA 2 das Software-Sichenheitsmodul Verton Akama SureSever CA G14-SHA2 das Software-Sichenheitsmodul Verton Akama SureSever CA G14-SHA1 das Software-Sichenheitsmodul Bugas Class Z Soct CA Builtin Object Token Bugas Class Z Root CA Builtin Object Token Bugas Class Z Root CA Builtin Object Token Bugas Class Z Root CA Builtin Object Token	Ihre Zertifi	ikate Personen	Server Zert	ifizierungsstellen	Andere	
Zertifikatsname Kryptographie-Modul Semen Internet CA YLD das Schware-Schehnetsmodul TeleSee ServePasc CA 2 das Schware-Schehnetsmodul Verton Alatin SureServer CA G14-SHA2 das Schware-Schehnetsmodul Verton Alatin SureServer CA G14-SHA1 das Schware-Schehnetsmodul Verton Alatin SureServer CA G14-SHA1 das Schware-Schehnetsmodul Verton Rubin SureServer CA G14-SHA1 das Schware-Schehnetsmodul Bugsas Class 2 Root CA Builtin Object Token B	ie haben Zer	rtifikate gespeichert, die	diese Zertifizierur	ıgsstellen identifiziere	en:	
Siemen Internet CA V1.0 das Software-Sicherheitsmodul Telésice ServerPass CA 2 das Software-Sicherheitsmodul Verston Auka Server CA G14-5H42 das Software-Sicherheitsmodul Verston Auka Server CA G14-5H42 das Software-Sicherheitsmodul Verston Aukami SureServer CA G14-5H42 das Software-Sicherheitsmodul bealocalhoxte Verston Aukami SureServer CA G14-5H42 das Software-Sicherheitsmodul bealocalhoxte Bugass Cass 2 Root CA Builtin Object Token Bugass Class 2 Root CA Builtin Object Token Ansehen	Zertifikatsna	ime		Kryptogra	aphie-Modul	1 3
Telésce Serve/Ras CA 2 das Software-Sicheheitsmodul Verton Akama SureServer CA G14-SHA2 das Software-Sicheheitsmodul Verton Akama SureServer CA G14-SHA2 das Software-Sicheheitsmodul Verton Akama SureServer CA G14-SHA1 das Software-Sicheheitsmodul Verton Ve	Siemens Inte	rnet CA V1.0		das Software-	Sicherheitsmodul	
Vertion Ablici Surdivere CA G14-SHA2 das Software-Sicheheitsmodal Vertion Ablania Surdivere CA G14-SHA1 das Software-Sicheheitsmodal Bugeas Cass 2 Root CA Builtin Object Token Bugeas Class 3 Root CA Builtin Object Token Agnsehn Vertrauen bearbeiten Ipportieren Esportieren	TeleSec Serve	erPass CA 2		das Software-	Sicherheitsmodul	
Verizon Akamai SureServer CA G14-SHA2 das Software-Sicheheitsmodul Verizon Akamai SureServer CA G14-SHA1 das Software-Sicheheitsmodul Vostone (Frozonsze Roman 2009) das Software-Sicheheitsmodul bealsocalhost.de das Software-Sicheheitsmodul bealsocalhost.de das Software-Sicheheitsmodul begass Class 2 Root CA Builtin Object Token Buypass Class 3 Root CA Builtin Object Token Ansehen Vertrauen bearbeiten Importieren	Verizon Publi	ic SureServer CA G14-SHA2		das Software	Sicherheitsmodul	
Vertron Akamal SueSever CA (SI 45:414) das Software-Schecheitsmodul Voldrone (Forenzule Forenzie Forezu Forenzie Forenzie Forenzie Forenzie Forenzie For	Verizon Akan	mai SureServer CA G14-SHA2		das Software-	Sicherheitsmodul	
Vokatore (Cronoste Donain 2019) das Software-Sicheheitsmodul bealicationst.de bealicationst.de Bealicationst.de Buypass Class 2 Root CA Builtin Object Token Buypass Class 3 Root CA Builtin Object Token Ansehen	Verizon Akan	mai SureServer CA G14-SHA1		das Software	Sicherheitsmodul	
beslocalhost.de beslocalhost.de beslocalhost.de des Software-Sicherheitsmodul Bugsas A.Seg115327 Bugsas Class 2 Root CA Builtin Object Token Bugsas Class 2 Root CA Builtin Object Token Ansehen	Vodafone (C	orporate Domain 2009)		das Software	Sicherheitsmodul	
beskpoints/be das Software-Skribententsmodul Burgeais XA-9831633277 Burgeais Class 32 Root CA Burlisin Object Token Burgeass Class 32 Root CA Burlisin Object Token American Class 22 Root CA Ansehen Vertrauen bearbeiten Importieren Exportieren Löschen oder Vertrauen entziehen	bealocalhost.de	e				
Bugpars A5-98316327 Bugpars Class 2 Root CA Builtin Object Token Bugpars Class 3 Root CA Builtin Object Token Ansehen	bealocalhost	t.de		das Software	Sicherheitsmodul	
Bugnass Class 2 Root CA Builtin Object Token Bugnass Class 3 Root CA Builtin Object Token Ansehen Vertrauen bearbeiten Importieren Exportieren Löschen oder Vertrauen entziehen	Buypass AS-98:	3163327				
Buypass Class 3 Root CA Builtin Object Token Ansehen Vertrauen bearbeiten Importieren Exportieren Löschen oder Vertrauen entziehen	Buypass Clas	is 2 Root CA		Builtin Object	Token	
Ansehen Vertrauen bearbeiten Importieren Exportieren Löschen oder Vertrauen entziehen	Buypass Clas	s 3 Root CA		Builtin Object	Token	
	Ansehen	Vertrauen bearbeite	n Importierer	Exportieren	Löschen oder Vertrauen entziehen	
OK						OK

Wählen Sie unter Einstellungen links den Bereich **Datenschutz & Sicherheit** aus.

Scrollen Sie bitte ganz nach unten. Klicken Sie auf die Schaltfläche Zertifikate anzeigen.

Wählen Sie im oberen Bereich die Registerkarte Zertifizierungsstellen.

Mit sehr hoher Wahrscheinlichkeit sehen sie etliche weitere Zertifikate in Ihrer Zertifikatverwaltung. Stellen Sie sicher, dass Sie kein anderes Zertifikat versehentlich löschen! Markieren Sie das Zertifikat "**bealocalhost.de**".

Wählen Sie unten die Schaltfläche Löschen oder Vertrauen entziehen....

C	A-Zertifikate löschen oder Vertrauen entziehen
	Sie haben um ein Löschen dieser CA-Zertifikate angefragt. Für eingebaute Zertifikate wird alles Vertrauen entzogen, was den gleichen Effekt hat. Sollen diese CA-Zertifikate wirklich gelöscht oder ihr Vertrauen entzogen werden?
	bealocalhost.de
	Wenn Sie ein Zertifizierungsstellen(CA)-Zertifikat löschen oder sein Vertrauen entziehen, vertraut die Anwendung keinen Zertifikaten mehr, die von dieser CA ausgestellt wurden.
	OK Abbrechen

Bestätigen Sie den folgenden Warnhinweis mit **OK**.

Das Zertifikat ist entfernt.

Prüfen Sie vorsichtshalber, ob das Zertifikat "**bealocalhost.de**" noch an anderen Stellen installiert ist, indem Sie in der Zertifikatsverwaltung auch die übrigen Registerkarten anklicken. Sollten das Zertifikat an anderen Stellen installiert sein, löschen Sie es auch dort.

Löschen Sie schließlich "**bealocalhost.de**" an dem Ort, an dem Sie es durch das Herunterladen zwischengespeichert haben (z. B. auf dem Desktop).

Safari (gilt für Linux und MacOS)

Um das Zertifikat zu entfernen, führen Sie bitte die folgenden Schritte durch:

Klicken Sie hier, um de Schlüsselbunde Anmeldung Lokale Objekte System System-Roots	Sch n Schlüsselbund "Anmeldung" zu sperren. beA client internal (Root-Zertifizierungsinst Ablaufdatum: Mittwoch, © Dieses Zertifikat ist fr	Ilüsselbundverwaltung Ca Ianz , 22. Dezember 2027 um 15:53:19 M ür diesen Account als vertrauenswür	ttteleuropäische Normalzeit dig markiert.	Q Suchen
	Name	∧ Art	Verfällt	Schlüsselbund
Kategorie Alle Objekte L. Passwörter Sichere Notizen Meine Zertifikate Zertifikate				
	(I) (I) (Vanianaa)	1011	-	

Öffnen Sie die Schlüsselbundverwaltung. Es erscheint nebenstehendes Fenster.

Mit sehr hoher Wahrscheinlichkeit sehen sie etliche weitere Zertifikate in Ihrer Schlüsselbundverwaltung. Stellen Sie sicher, dass Sie kein anderes Zertifikat versehentlich löschen! Rechtsklicken Sie auf das Zertifikat "bealocalhost.de".

Wählen Sie im erscheinenden Kontextmenü

bealocalhost.de löschen.

Bestätigen Sie den folgenden Warnhinweis mit **Löschen**.

Im nun erscheinenden Dialog geben Sie im Eingabefeld den Namen eines **Benutzers** mit Administratorrechten und das entsprechende **Passwort** ein. Bestätigen Sie diese Angaben mit **Einstellungen aktualisieren**.

Das Zertifikat ist entfernt.

Chrome (gilt für Windows ebenso wie Linux und MacOS)

Neuer Tab	×	θ	×	Öffnen Sie das Menü über das Symbol
$\leftarrow \rightarrow C \land$		Neue Enveiterung hinzugefügt (Adobe Acrobat	* 🧕	rechts neben der Adressleiste und
Apps Platzieren	n Sie Ihre Lesezeichen hier in der Lesezeichenleiste, um schnell auf sie :	Neuer Tab Neues Fenster	Strg+T Strg+N	wählen Sie anschließend in der
		Neues Inkognito-Fenster	Strg+Umschalt+N	erscheinenden Liste Einstellungen.
		Verlauf Downloads	Strg+J	
		Lesezeichen Zoomen -	100 % + 53	
	Goo	Drucken	Strg+P	
		Streamen Suchen	Strg+F	
	Bei Google suchen oder URL eingeben	Weitere Tools Bearbeiten Ausschneiden Kopier	en Einfügen	
		Einstellungen	E	
	🔹 Williamman hai Chr. 🔤 Chrama Wah Stara	Hilte Beenden	Strg+Umschalt+Q	
	Weikkone to Orone	L		
			1	
			θ - Π	× Es orschoint das Monü
C Einstellungen	×			Finstellungen
€ → C @	Chrome chrome://settings		ŭ	
😑 Einstellu	ngen Q In Einstellungen suchen			
	Personen			
	Profil 1	IN CHROME AND	MELDEN	
	Melden Sie sich an, um Ihre Lesezeichen, Ihren Verlauf u zu sehen. Sie werden auch automatisch in Ihren Google-	ind Ihre anderen Einstellungen auf allen Ihren Ge Diensten angemeldet, Weitere Informationen	eräten	
	Andere Nutzer verwalten		•	
	Lesezeichen und Einstellungen importieren		•	
	Darstellung			
	Designs Chrome Web Store öffnen		Z	
	Schaltfläche "Startseite" anzeigen Deaktiviert			
	Lesezeichenleiste anzeigen			
	Schriftgröße	Mittel (empfohlen)		
	Schriftart anpassen		>	
	Seitenzoom	100%	*	
	Suchmaschine			
	In der Adressleiste verwendete Suchmaschine	Google	-	
	Suchmaschinen verwalten		>	
	Standardbrowser			*

Um das Zertifikat zu entfernen, führen Sie bitte die folgenden Schritte durch:

🗘 Einstellungen X	Θ	-		×
← → C Schrome chrome://settings/?search=zertifik			☆	•
≡ Einstellungen Q zertifik		8		
Sicherheit und Datenschutz				
Google Chrome verwendet möglicherweise Webdienste zur Verbesserung Ihrer Sucherfahrung. Sie haber Möglichkeit, diese Dienste zu deaktivieren. Weitere Informationen	n die			
Navigationsfehler mithilfe eines Webdienstes beheben				
Vervollständigung von Suchanfragen und URLs bei der Eingabe in die Adressleiste verwenden				
Vorhersagefunktion zum schnelleren Laden von Seiten verwenden				
Ich möchte automatisch einige Systeminformationen und Seiteninhalte an Google senden, um bei der Erfassung schädlicher Apps und Websites zu helfen				
Mich und mein Gerät vor schädlichen Websites schützen				
Nutzungsstatistiken und Absturzberichte automatisch an Google senden				
Mit Browserzugriffen eine 'Do Not Track'-Anforderung senden				
Rechtschreibfehler mithilfe eines Webdienstes korrigieren Intelligentere Rechtschreibprüfung, indem der im Browser eingegebene Text an Google gesendet wird				
Zertifikate verwalten HTTPS/SSL-Zertifikate und -Einstellungen verwalten	Ø			
Inhaltseinstellungen Festlegen, welche Informationen von Websites genutzt werden dürfen und welche Inhalte Websites präsentieren dürfen	•			
Browserdaten löschen Cache leeren sowie Verlauf, Cookies und andere Daten löschen	×			

Geben Sie im Feld **In Einstellungen suchen** den Begriff "Zertifikate" ein. Danach wählen Sie bitte den Listeneintrag **Zertifikate verwalten** aus.

Zwischenzertifizier	ungsstelle	N Vertrauenswürdige Sta	mmzertifizierun	igsstellen	Vertrauens	•
Ausgestellt für		Ausgestellt von	Ablaufda	Anzeigen	ame	^
AddTrust Ext	ternal	AddTrust External CA	30.05.2020	The USEF	RTrust	
Baltimore Cyl	berTru	Baltimore CyberTrust	13.05.2025	DigiCert B	Baltimor	
boskg-CA01		boskg-CA01	23.01.2018	<keine></keine>		
boskg-CA01		boskg-CA01	23.01.2018	<keine></keine>		
🔄 Certum Trust	ted Ne	Certum Trusted Netw	31.12.2029	Certum T	rusted	
Class 3 Public	: Prima	Class 3 Public Primary	02.08.2028	VeriSign (Class 3	
COMODO RS	A Cert	COMODO RSA Certific	19.01.2038	COMODO	SECU	
🔄 Copyright (c)	1997	Copyright (c) 1997 Mi	31.12.1999	Microsoft	Timest	
Deutsche Tel	ekom	Deutsche Telekom Ro	10.07.2019	Deutsche	Teleko	۷
importieren E	xportierer	n Entfernen			Erweite	rt
Beabsichtigte Zwei	cke des Ze	ertinkats				

Es wird das Dialogfenster für die Zertifikatsverwaltung geöffnet.

Wechseln Sie auf die Registerkarte Vertrauenswürdige Stammzertifizierungsstellen.

Mit sehr hoher Wahrscheinlichkeit sehen sie etliche weitere Zertifikate in der angezeigten Liste. Stellen Sie sicher, dass Sie kein anderes Zertifikat versehentlich löschen! Markieren Sie das Zertifikat "**bealocalhost.de**" durch einfaches Klicken. Betätigen Sie die Schaltfläche **Entfernen**. Bestätigen Sie die folgende Warnung.

Prüfen Sie vorsichtshalber, ob das Zertifikat "**bealocalhost.de**" noch an anderen Stellen installiert ist, indem Sie in der Zertifikatsverwaltung auch die übrigen Registerkarten anklicken. Sollten das Zertifikat an anderen Stellen installiert sein, löschen Sie es auch dort.

Löschen Sie schließlich "bealocalhost.de" an dem Ort, an dem Sie es durch das Herunterladen zwischengespeichert haben (z. B. auf dem Desktop).

Unter MacOS müssen Sie den Namen eines **Benutzers** mit Administratorrechten und das entsprechende **Passwort** eingeben. Bestätigen Sie diese Angaben mit **Einstellungen aktualisieren**. Das Zertifikat ist entfernt.