

Installationsanleitung für Zertifikate zur Nutzung der ISBJ-Portale

 Autor:
 V E 21

 Datum:
 27.02.2024

 Version:
 3.0





1 Inhaltsverzeichnis

Einleitung	3
Mozilla Firefox	4
Google Chrome	. 10
Microsoft Edge	. 15
Apple Safari	. 19
	Einleitung Mozilla Firefox Google Chrome Microsoft Edge Apple Safari



1 Einleitung

Dieses Dokument beschreibt die Installation eines Zertifikats zur Nutzung der ISBJ Portale für Träger und Einrichtungen. Die Installationsanleitung gilt für die Browser Mozilla Firefox, Google Chrome, Microsoft Edge und Safari.

Von der Nutzung des Internet Explorers raten wir aus Sicherheitsgründen ab.

Um sich in einem der Portale anmelden zu können, muss jeder Benutzer einen Benutzernamen und ein Kennwort besitzen. Der Benutzername und das Kennwort werden nach Einrichtung durch den Administrator über das BNV-Portal an die hinterlegte E-Mailadresse des Benutzers versendet. Außerdem benötigt der Benutzer ein Zertifikat, das ihm sein Administrator zusammen mit dem Kennwort für die Installation zur Verfügung stellt. Das Zertifikat gehört zum Administrator und ist für alle ihm zugeordneten Benutzer gleich.

Jeder Benutzer, der ein gültiges Zertifikat verwendet, hat einen - seinen Rechten entsprechenden -Zugriff auf alle ISBJ-Portale.



2 Mozilla Firefox

Das ISBJ Trägerportal unterstützt generell den Mozilla Firefox ab der Version 25. Im Folgenden wird die Installation des Zertifikats exemplarisch anhand des Mozilla Firefox Version 102.14.0esr dargestellt.

1. Speichern Sie die Zertifikatsdatei aus der Email (Betreff: Zertifikat fuer Zugang zum ISBJ Portal) zunächst lokal auf Ihrem Rechner ab.

2. Starten Sie Mozilla Firefox und wählen Sie im Menü "Extras" den Punkt "Einstellungen" aus. Alternativ können Sie auch über die Menüschaltfläche am rechten Rand die Einstellungen aufrufen. Wählen Sie nun links "Datenschutz und Sicherheit" aus und klicken ganz unten auf "Zertifikate anzeigen".

Allgemein	
Startseite	Sicherheit
 Q Suche Datenschutz & Sicherheit Q Sync 	Schutz vor betrügerischen Inhalten und gefährlicher Software Gefährliche und betrügerische Inhalte blockieren Gefährliche Downloads blockieren Vor unerwünschter und ungewöhnlicher Software warnen
Erweiterungen & Themes	Zertifikate Wenn eine Website nach dem persönlichen Sicherheitszertifikat verlangt Automatisch eins wählen Jedes Mal fragen ✓ Aktuelle Gültigkeit von Zertifikaten durch Anfrage bei OCSP-Server bestätigen lassen Kryptographie-Module

3. Der Assistent zur Organisation von Zertifikaten öffnet sich. Wechseln Sie in den Reiter "Ihre Zertifikate".

		Zertifikatve	rwaltung	×
Ihre Zertifikate	Personen	Server	Zertifizierungsstellen	

<u>Wir empfehlen zunächst alle abgelaufenen ISBJ Zertifikate zu löschen. ISBJ Zertifikate erkennen</u> <u>Sie daran, dass in der Spalte "Ausgestellt von" ISBJ Zertifizierungsinstanz angegeben ist.</u>



4. Klicken Sie hier zunächst auf die Schaltfläche "Importieren".

		Zertifikatver	waltung			>
Ihre Zertifikate	Personen	Server	Zertifizierun	gsstellen		
ie haben Zertifikate	dieser Organis	ationen, die S	ie identifiziere	n:		
Zertifikatsname	Krypt	ographie-Mo	dul	Seriennummer	Gültig bis	
Ansohon Si	chorp All	a cicharn	Incorporations	l ässhan		

5. Es öffnet sich ein Fenster zur Auswahl der zu importierenden Zertifikatsdatei. Wählen Sie nun die zuvor heruntergeladene Zertifikatsdatei aus.

Bestätigen Sie die Auswahl über die Schaltfläche "Öffnen".

🕹 Zu importierende Zertifik	at-Datei	Annual and Add in Females,		-	X
Sibliother Sibliother	eken 🕨	Dokumente 🕨 ISBJ-Zertifikat 🛛 👻	49	ISBJ-Zertifikat durchsuch	en 🔎
Organisieren 🔻 Neue	er Ordner	r			1 🕐
★ Favoriten ■ Desktop 0 Downloads		Bibliothek "Dokumente" ISBJ-Zertifikat		Anordnen nach: Ordr	ner 🔻
🔄 Zuletzt besucht	=	adm_penkuhbn.p12			
Bilder					
🎝 Musik 📑 Videos					
I톺 Computer	-				
Date	i <u>n</u> ame:	adm_penkuhbn.p12	•	PKCS12-Dateien (*.p12;*.p Öffnen 🚽 Abbr	fx) ▼ echen

Hinweis: Im Beispiel wurde das Zertifikat zuvor unter "Dokumente" in einem separat erstellten Ordner namens "ISBJ-Zertifikat" gespeichert. Sofern Sie keinen anderen Ort ausgewählt haben, wird das Zertifikat standardmäßig unter "Downloads" gespeichert.



6. Geben Sie das Kennwort für die Installation des Zertifikats aus dem Brief im entsprechenden Feld

ein. Klicken Sie auf "OK".

Passwort	erforderlich X
?	Bitte geben Sie das Passwort ein, das zur Verschlüsselung dieses Zertifikatbackups verwendet wurde:
	•••••
	OK Abbrechen

7. Das Zertifikat erscheint jetzt in der Liste Ihrer Zertifikate.

	Zertifikatverwaltung		:
Ihre Zertifikate	Personen Server Zertifizieru	ingsstellen	
Sie haben Zertifikate	dieser Organisationen, die Sie identifizier	ren:	
Zertifikatsname	Kryptographie-Modul	Seriennummer	Gültig bis
∽ ISBJ			
202001010245	das Software-Sicherheitsmodul	20:20:01:01:02:45	Donnerstag, 13. Ja
202001010243	uas sontware-sichemensmodul	20.20.01.01.02.43	Donnerstag, 15. Ja
Ansehen Sid	thern Alle sichern Importieren	löschen	

7. Klicken Sie im Zertifikatsmanager auf den Reiter "Authentifizierungsentscheidungen".

	Zertifikat	verwaltung		
Ihre Zertifikate	Authentifizierungs-Entscheidungen	Personen	Server	Zert



8. Falls hier bestehende Einträge vorhanden sind, die unter Host "verwalt-berlin.de" enthalten, klicken Sie diese mit der linken Maustaste an und klicken unten auf "Löschen."

Beispiele: portal.isbj.verwalt-berlin.de bnvportalp.isbj.verwalt-berlin.de stportal.isbj.verwalt-berlin.de

8. Wechseln Sie im Zertifikats-Manager auf den Reiter "Zertifizierungsstellen".

Ihre Zertifikate Personen Server Zertifizierungsstellen

9. Suchen Sie in der Liste nach ISBJ und markieren Sie den Eintrag "ISBJ Zertifizierungsinstanz mit der linken Maustaste. Klicken Sie danach auf "Vertrauen bearbeiten".

∽ ISBJ			
ISBJ Zertifizierungsinstanz	das S	oftware-Sicherhe	itsmodul
∽ IZENPE S.A.			
Izenpe.com	Builti	n Object Token	
✓ Japan Certification Services, Inc.			
Ansehen Vertrauen <u>b</u> earbeiten	Importieren	Exportieren	Löschen oder Vertrauen

Es öffnet sich das Pop-Up "CA-Zertifikat-Vertrauenseinstellungen bearbeiten". Markieren Sie bitte die Vertrauenseinstellung "Dieses Zertifikat kann Websites identifizieren", und bestätigen Sie mit "OK".





Kontrolle des Fingerabdrucks:

10. Wechseln Sie im Zertifikats-Manager auf den Reiter "Zertifizierungsstellen". Suchen Sie in der Liste nach ISBJ und markieren Sie den Eintrag "ISBJ Zertifizierungsinstanz". Klicken Sie anschließend auf die Schaltfläche "Ansehen..."

	Zertifikatve	erwaltung		×
Ihre Zertifikate Personen	Server	Zertifizie	rungsstellen	
Sie haben Zertifikate gespeichert,	die diese Zerti	fizierungsst	ellen identifiziere	n:
Zertifikatsname		Kryp	tographie-Modu	I
✓ Internet Security Research Gro	up			
ISRG Root X1		Builtin	n Object Token	
Let's Encrypt Authority X3		das S	oftware-Sicherhei	itsmodul
∽ ISBJ				
ISBJ Zertifizierungsinstanz		das S	oftware-Sicherhei	itsmodul
→ IZENPE S.A.				
Izenpe.com		Builti	n Object Token	
 Japan Certification Services, Inc 	ε.			
Ansehen Vertrauen bearb	eiten Imp	ortieren	Exportieren	Löschen oder Vertrauen

Hinweis: Alternativ kann unter "Kryptographie-Modul" auch "OS Client Cert Token" stehen.

11. Vergleichen Sie bitte in dieser Ansicht den SHA1-Fingerabdruck mit dem Fingerabdruck aus dem per Post geschickten Brief mit dem Installationskennwort für das Zertifikat.

Falls Sie mehrere ISBJ Zertifizierungsinstanzen haben, prüfen Sie bitte die jeweils aktuellste.



11.1 Stimmen die Daten überein, kann das installierte Zertifikat genutzt werden. Bitte klicken Sie auf "Schließen"



11.1.1 Klicken Sie im Anschluss im Fenster der Einstellungen auf "OK", um die Installation des Zertifikats abzuschließen.

11.2 Stimmen die Fingerabdrücke <u>nicht</u> überein, muss das Zertifikat wieder deinstalliert werden.Bitte klicken Sie auf "Schließen".

11.2.1 Wechseln Sie in den Reiter "Ihre Zertifikate".

11.2.2 Wählen Sie das importierte Zertifikat aus der angezeigten Liste aus und klicken Sie auf "Löschen".

	Zertifikatverwaltung		
Ihre Zertifikate	Personen Server Zertifizie	rungsstellen	
Sie haben Zertifikate	dieser Organisationen, die Sie identifiz	ieren:	
Zertifikatsname	Kryptographie-Modul	Seriennummer G	ültig bis
∽ ISBJ			
202001010245	das Software-Sicherheitsmodu	l 20:20:01:01:02:45 Do	nnerstag, 13. Ja
202001010245	das Software-Sicherheitsmodu	l 20:20:01:01:02:45 Do	nnerstag, 13. Ja

11.2.4 Das Zertifikat wird aus der Liste entfernt. Klicken Sie im folgenden Fenster auf "OK".

11.2.5 Sie können nun die Einstellungen schließen.

11.2.6 Bitte melden Sie nicht übereinstimmende Fingerabdrücke sofort an: traeger-service@senbjf.berlin.de



3 Google Chrome

Das ISBJ Trägerportal unterstützt generell Google Chrome ab der Version 33. Im Folgenden wird die Installation des Zertifikats exemplarisch anhand der Google Chrome Version 97 dargestellt.

1. Speichern Sie die Zertifikatsdatei aus der Email (Betreff: Zertifikat fuer Zugang zum ISBJ Portal) zunächst lokal auf Ihrem Rechner ab.

2. Starten Sie Google Chrome und wählen Sie über die Menüschaltfläche oben rechts den Punkt "Einstellungen" aus. Auf der linken Seite klicken Sie nun auf die Kategorie "Sicherheit und Datenschutz" und wählen dann "Sicherheit" aus. Scrollen Sie hier etwas nach unten und wählen den Punkt "Zertifikate verwalten".

Einstellungen	Q. In Einstellungen suchen
Google und ich Automatisches Ausfüllen	Kein Schutz (nicht empfohlen) O Sie werden nicht vor schädlichen Websites, Downloads und Erweiterungen geschützt. Sofern verfügbar, sind Sie in anderen Google-Diensten, wie Gmail und der Google Suche, durch Safe Browsing geschützt.
Sicherheit und Datenschutz Darstellung Suchmaschine Standardhrawser	Erweitert Immer sichere Verbindungen verwenden Aufrufe von Websites auf HTTPS umstellen und warnen, bevor Websites geladen werden, die das Protokoll nicht unterstützen
Standardbrowser Standardbrowser Beim Start Enweitert	Sicheres DNS verwenden Legt fest, wie Websites über eine sichere Verbindung aufgerufen werden Mit Ihrem aktuellen Dienstanbieter Sicheres DNS ist möglicherweise nicht immer verfügbar
Erweiterungen 🗾 Über Google Chrome	O Mit Benutzerdefiniert Benutzerdefinierten Anbieter eingeben
	Zertifikate verwalten HTTPS/SSL-Zertin ate und -Einstellungen verwalten
	Erweitertes Sicherheitsprogramm von Google Schützt private Google-Konten jeglicher Nutzer vor gezielten Angriffen

3. Der Assistent zur Organisation von Zertifikaten öffnet sich. Wechseln Sie in den Reiter "Eigene Zertifikate".

<u>Wir empfehlen zunächst alle abgelaufenen ISBJ Zertifikate zu löschen. ISBJ Zertifikate erkennen</u> <u>Sie daran, dass in der Spalte "Ausgestellt von" ISBJ Zertifizierungsinstanz angegeben ist.</u>



4. Um das neue Zertifikat zu installieren, klicken Sie nun auf die "Importieren" Schaltfläche um den

Zertifikatsimport-Assistenten zu öffnen.

	Andere	Persone	n Zwische	enzertifizierungsstellen	Vertrauenswürdige	St.
Ausgestell	Ausgestell	АЫ	Anzeige	la.		
= <mark>5b167e5</mark>	5b167e54	25.0	Microso			
M						

5. Klicken Sie hier auf "Weiter". Sie werden nun aufgefordert ein Zertifikat auszuwählen. Klicken Sie dazu auf die "Durchsuchen" Schaltfläche.



6. Wählen Sie nun die zuvor heruntergeladene Zertifikatsdatei aus. Bestätigen Sie die Auswahl über die Schaltfläche "Öffnen" und klicken Sie dann auf "Weiter".

Öffnen					×
$\leftrightarrow \rightarrow \checkmark \uparrow 4$	> Dieser PC > Downloads >		~ C		
Organisieren - Neue	r Ordner			a ·	• • •
🗸 💻 Dieser PC	Name	Ānderungsdatum	Тур		Größe
> 🛃 Bilder	adm_schnemii.p12	14.01.2022 10:40	Privater Inf	ormationsaustausch	5 KB
> 🔜 Desktop	Ablage	14.01.2022 10:36	Dateiordne		
> 📔 Dokumente					
> 🛓 Downloads					
Datein	ame:			X.509-Zertifikat (*.c	er;*.crt)*.cer;' ~
				Öffnen	Abbrechen



7. Geben Sie das Kennwort für die Installation des Zertifikats im entsprechenden Feld ein. Klicken

Sie auf "Weiter".

F Zertifikatimport-Assistent

D	z un den privaten schrusser er private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu ewährleisten.
G	eben Sie das Kennwort für den privaten Schlüssel ein.
Ke	innwort:
	Kennwort anzeigen
In	iportoptionen:
	Hohe Sicherheit für den privaten Schlüssel aktivieren. Wenn Sie diese Option aktivieren, werden Sie immer dann, wenn der private Schlüssel von einer Anwendung verwendet wird, zur Kennworteingabe aufgefordert.
	Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einen späteren Zeitpunkt sichern bzw. überführen.
	Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen (nicht exportierbar)
	SAlle erweiterten Eigenschaften mit einbeziehen

8. Markieren Sie im Fenster "Zertifikatspeicher" die Option "Zertifikatspeicher automatisch

auswählen". Bestätigen Sie mit "Weiter".

Lerunnalspeicher	
Zertifikatspeicher sind Systembereiche, in denen	Zertifikate gespeichert werden.
Windows kann automatisch einen Zertifikatsneich	er auswählen, oder Sie können einen
Speicherort für die Zertifikate angeben	er auswanien, oder sie konnen einen
O Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)
Alle Zertifikate in folgendem Speicher spei	chern
Zertifikatspeicher:	
Eigene Zertifikate	Durchsuchen.



9. Klicken Sie auf "Fertig stellen", um den Zertifikatimport abzuschließen.

Das Zertifikat wird im	iportiert, nachdem Sie auf "Fertig stellen" geklickt haben.
Sie haben folgende E	instellungen ausgewählt:
Gewählter Zertifikat:	peicher Auswahl wird vom Assistenten automatisch festgelegt
Inhalt	PFX

Kontrolle des Fingerabdrucks:

10. Eine Sicherheitswarnung mit Informationen zur Zertifizierungsinstanz und dem Hinweis zur Kontrolle des Fingerabdrucks erscheint. Überprüfen Sie den SHA1-Fingerabdruck mit dem Fingerabdruck aus dem per Post geschickten Brief mit dem Installationskennwort für das Zertifikat.

Sicherheit	swarnung	×
1	Sie sind im Begriff, ein Zertifikat von einer Zertifizierungsstelle zu installieren, die sich wie folgt darstellt:	
	ISBJ Zertifizierungsinstanz	
	Es wird nicht bestätigt, dass das Zertifikat wirklich von "ISBJ Zertifizierungsinstanz" stammt. Wenden Sie sich an "ISBJ Zertifizierungsinstanz", um die Herkunft zu bestätigen. Die folgende Zahl hift Ihnen bei diesem Prozess weiter:	
<	Fingerabdruck (sha1): 9B3FFE03 C9A3A622 BA6F5B68 89F2BAA5 D0498E21	
	Warnung: Wenn Sie dieses Stammzertifikat installieren, wird automatisch allen Zertifikaten vertraut, die von dieser Zertifizierungsstelle ausgestellt werden. Die Installation mit einem unbestätigten Fingerabdruck stellt ein Sicherheitsrisiko dar. Falls Sie auf "Ja" klicken, nehmen Sie dieses Risiko in Kauf.	
	Möchten Sie dieses Zertifikat installieren?	
	, la Nein	



10.1 Stimmen die Daten überein, kann das installierte Zertifikat genutzt werden. Bitte klicken Sie auf "Ja"

10.2 Stimmen die Fingerabdrücke <u>nicht</u> überein, sollte das Zertifikat nicht installiert werden. Bitte klicken Sie dazu einfach auf "Nein".

10.2.1 Bitte melden Sie nicht übereinstimmende Fingerabdrücke sofort an: traeger-service@senbjf.berlin.de



4 Microsoft Edge

Das ISBJ Trägerportal unterstützt generell jede offizielle Version von Microsoft Edge. Im Folgenden wird die Installation des Zertifikats exemplarisch anhand der Microsoft Edge Version 117.0.2045.60 (64 Bit) dargestellt.

1. Speichern Sie die Zertifikatsdatei aus der Email (Betreff: Zertifikat fuer Zugang zum ISBJ Portal) zunächst lokal auf Ihrem Rechner ab.

2. Starten Sie Microsoft Edge und wählen Sie über die Menüschaltfläche oben rechts den Punkt "Einstellungen" aus. Auf der linken Seite klicken Sie nun auf die Kategorie "Datenschutz suche und Dienste" und wählen dann unter der Überschrift "Sicherheit" die Schaltfläche "Zertifikate verwalten" aus.

Einstellungen	Erlauben Sie Microsoft, Ihre Browseraktivitäten wie Verlauf, Nutzung, Favoriten. Webinhalte und andere 👜 🔍 Browserdaten zu speichern, um Microsoft Edge und Microsoft-Dienste wie Anzeigen, Suche, Einkäufe und Nachrichten zu personalisieren.
Q Einstellungen durchsuchen	Deaktivieren Sie diese Einstellung, um diese Daten zurückzusetzen. Verwalten Sie zusätzliche Werbeeinstellungen auf dem <u>Microsoft-Datenschutz-</u> Dashboard
ම Profile	
Datenschutz, Suche und Dienste	
⑦ Darstellung	Sicherheit
Randleiste	Verwalten der Sicherheitseinstellungen für Microsoft Edge
Start, Startseite und neue Registerkarten	Zertifikate verwalten
🖄 Teilen, kopieren und einfügen	HTTPS-/SSL-Zertifikate und -Einstellungen verwalten

3. Der Assistent zur Organisation von Zertifikaten öffnet sich. Wechseln Sie in den Reiter "Eigene Zertifikate".

<u>Wir empfehlen zunächst alle abgelaufenen ISBJ Zertifikate zu löschen. ISBJ Zertifikate erkennen</u> <u>Sie daran, dass in der Spalte "Ausgestellt von" ISBJ Zertifizierungsinstanz angegeben ist.</u>

4. Um das neue Zertifikat zu installieren, klicken Sie nun auf die "Importieren" Schaltfläche um den Zertifikatsimport-Assistenten zu öffnen.





5. Klicken Sie hier auf "Weiter". Sie werden nun aufgefordert ein Zertifikat auszuwählen. Klicken Sie

dazu auf die "Durchsuchen" Schaltfläche.

Dateiname:				Durchsuchen
Syntaxstand Microsoft Se	lard kryptografischer rieller Zertifikatspeid	Meldungen - "PKCS #	7"-Zertifikate (.F	97B)

6. Wählen Sie nun die zuvor heruntergeladene Zertifikatsdatei aus. Bestätigen Sie die Auswahl über die Schaltfläche "Öffnen" und klicken Sie dann auf "Weiter".



7. Geben Sie das Kennwort für die Installation des Zertifikats im entsprechenden Feld ein. Klicken Sie auf "Weiter".

Sch	utz für den privaten Schlüssel
	Der private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu gewährleisten.
	Geben Sie das Kennwort für den privaten Schlüssel ein.
	Kennwort:
4	Kennwort weigen
	Importoptionen:
	Hohe Sicherheit f ür den privaten Schl üssel aktivieren. Wenn Sie diese Option aktivieren, werden Sie immer dann, wenn der private Schl üssel von einer Anwendung verwendet wird, zur Kennworteingabe aufgefordert.
	Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einen späteren Zeitpunkt sichern bzw. überführen.
	Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen (nicht exportierbar)
	Alle erweiterten Eigenschaften mit einbeziehen



8. Markieren Sie im Fenster "Zertifikatspeicher" die Option "Zertifikatspeicher automatisch auswählen". Bestätigen Sie mit "Weiter".

an annual personal		
Zertifikatspeicher sind Systembereiche, in denen 2	Zertifikate gespeichert	werden.
Windows kann automatisch einen Zertifikatspeiche Speicherort für die Zertifikate angeben	er auswählen, oder Sie	können einen
O Zertifikatspeicher automatisch auswählen (a	auf dem Zertifikattyp b	asierend)
O Alle Zertifikate in folgendem Speicher speic	:hern	
Zertifikatspeicher:		
Eigene Zertifikate		Durchsuchen

9. Klicken Sie auf "Fertig stellen", um den Zertifikatimport abzuschließen.





Kontrolle des Fingerabdrucks:

10. Eine Sicherheitswarnung mit Informationen zur Zertifizierungsinstanz und dem Hinweis zur Kontrolle des Fingerabdrucks erscheint. Überprüfen Sie den SHA1-Fingerabdruck mit dem Fingerabdruck aus dem per Post geschickten Brief mit dem Installationskennwort für das Zertifikat.

	uswamung
<u>^</u>	Sie sind im Begriff, ein Zertifikat von einer Zertifizierungsstelle zu installieren, die sich wie folgt darstellt:
	ISBJ Zertifizierungsinstanz
	Es wird nicht bestätigt, dass das Zertifikat wirklich von "ISBJ Zertifizierungsinstanz" stammt. Wenden Sie sich an "ISBJ Zertifizierungsinstanz", um die Herkunft zu bestätigen. Die folgende Zahl hilft Ihnen bei diesem Prozess weiter:
(Fingerabdruck (sha1): 9B3FFE03 C9A3A622 BA6F5B68 89F2BAA5 D0498E21
	Warnung: Wenn Sie dieses Stammzertifikat installieren, wird automatisch allen Zertifikaten vertraut, die von dieser Zertifizierungsstelle ausgestellt werden. Die Installation mit einem unbestätigten Fingerabdruck stellt ein Sicherheitsrisiko dar. Falls Sie auf "Ja" klicken, nehmen Sie dieses Risiko in Kauf.
	Warnung: Wenn Sie dieses Stammzertifikat installieren, wird automatisch allen Zertifikaten vertraut, die von dieser Zertifizierungsstelle ausgestellt werden. Die Installation mit einem unbestätigten Fingerabdruck stellt ein Sicherheitsrisiko dar. Falls Sie auf "Ja" klicken, nehmen Sie dieses Risiko in Kauf. Möchten Sie dieses Zertifikat installieren?

10.1 Stimmen die Daten überein, kann das installierte Zertifikat genutzt werden. Bitte klicken Sie auf "Ja"

10.2 Stimmen die Fingerabdrücke <u>nicht</u> überein, sollte das Zertifikat nicht installiert werden. Bitte klicken Sie dazu einfach auf "Nein".

10.2.1 Bitte melden Sie nicht übereinstimmende Fingerabdrücke sofort an:

traeger-service@senbjf.berlin.de



5 Apple Safari

Das ISBJ Trägerportal unterstützt generell Safari ab der Version 5.1.10. Im Folgenden wird die Installation des Zertifikats exemplarisch anhand des Safari 16.5 dargestellt.

Safari verwaltet selbst keine Zertifikate, sondern greift (ab Mac OS X) auf den so genannten Schlüsselbund (Keychain) des Betriebssystems zurück. Sie Importieren Ihr Zertifikat also in den Schlüsselbund.

1. Speichern Sie die Zertifikatsdatei zunächst lokal auf Ihrem Rechner ab.

2. Öffnen Sie das Programm "Schlüsselbundverwaltung". Sie finden es z.B. per Spotlight-Suche oder im Finder unter Programme/Dienstprogramme (Shift-Cmd-U).



Sobald sich die Schlüsselbundverwaltung öffnet, sollten eventuell vorhandene alte Zertifikate gelöscht werden. Geben Sie dazu in die Suche der Schlüsselbundverwaltung "ISBJ" ein und löschen Sie alle Einträge der Art "Zertifikat" und "Identitätseinstellung"

3. Um das Zertifikat zu installieren wählen Sie zunächst auf der rechten Seite den Schlüsselbund "Anmeldung" aus und klicken Sie anschließend im Menü Ablage auf "Objekte importieren". (Shift-Cmd-I)

🗯 Schlüsselbund	verwaltung	Ablage Bearbeiter	n Darstellung	Fenster	Hilfe	Ō	()	.=	۹ 🛢
	Schlüssell	Neues Passwort Neue sichere Notiz		第 N 公第 N	2 Suchen				
Anmeldung	Alle Objekte	Neue Identitätseinste	allung		I Zertifikate				
☐ Lokale Obje	10	Objekte importieren		公第 1					
Systemschlüsselbuw	1	Objekte exportieren							
A System		Schlüsselbund hinzu	fügen						
System-Ro	Name					Verfällt			Schlüsselbu
	♀ <key></key>	Schließen							Anmeldung
	♀ <key></key>								Anmeldung
	Apple I	onconnen			:23				Anmeldung
	com.ar	Informationen			1, 05:12:59				Anmeldung
	/ com.ar				:15				Anmeldung
	/ com.ap	ple.assistant	Programmpasswort	Heute,	04:15				Anmeldung
	Com.ap	ple.assistant	Programmpasswort	Heute, I	04:19				Anmeldung
	/ com.app	ole.scookmarksagent.xpc	Programmpasswort	13.09.2	021, 05:13:46	- 14 - 1 - 14 - 14 - 14 - 14 - 14 - 14 - 14			Anmeldung



4. Wählen Sie nun die zuvor heruntergeladene Zertifikatsdatei aus und klicken Sie auf "Öffnen"



5. Geben Sie das Kennwort für die Installation des Zertifikats ein. Klicken Sie auf "OK".



6. Nach dem Import sollte Ihr persönliches Zertifikat in der Liste der Kategorie "Meine Zertifikate" des Schlüsselbundes "Anmeldung" angezeigt werden.

🔹 Schlüssell	oundverwaltung	Ablage	Bearbeiten	Darstellung	Fenster	Hilfe	Ō		q	8
• • •	Schlüsselbu	ndverwa	altung	G	3 (Ì	Q Suchen				
Standardschlüssell	Alle Objekte		Sichere Notia	en Meine Zertif	ikate Schl	üssel Zertifikate				
Anmeldung		latadatak	(avabain							
Cokale Obje Systemschlüsselbu	Al Al	rt: Progran ccount: rt: Metadat eändert: 1	nmpasswort taKeychain 3.09.2021, 05:1	3:28						
D Ourtern Dr	Name				Coën	lort	Marfällt		Coblin	alb
System-Ro	Name				Geand	iert.	verraiit		ocinus	seib
	20200101	02F2		Zertifikat			Gestern, 02:51		Anmelo	iunç
	t skaus k	5		Offernaner Schli	ùssel				Anmelo	lung
	₽ <key></key>			Privater Schlüsse					Anmelo	lung
	/ Apple Per	sistent Stat	te Encryption	Programmpasswo	ort Heute	, 04:23			Anmelo	iung
	/ com.apple	e.assistant		Programmpasswo	ort 13.09.	2021, 05:12:59			Anmelo	lung
	Com.apple	e.assistant		Programmpasswo	ort Heute	, 04:15			Anmelo	lunç
	/ com.apple	e.assistant		Programmpasswo	ort Heute	, 04:15			Anmelo	iung
	/ com.apple	e.assistant		Programmpasswo	ort Heute	, 04:15			Anmelo	iunç
	/ com.apple	e.assistant		Programmpasswo	ort Heute	, 04:19			Anmelo	iung
	/ com.apple	.scookma	arksagent.xpc	Programmpasswo	ort 13.09.	2021, 05:13:46			Anmelo	iung
	P ISBJ Nutz	er Zfikat 2	2020010102F2	Privater Schlüsse					Anmelo	jung
	ISBJ Zerti	ifizierungsi	nstanz	Zertifikat			15.04.2026, 04	:44:46	Anmelo	Jung



Kontrolle des Fingerabdrucks:

7. Klicken Sie nun im Schlüsselbund Anmeldung per Doppelklick auf den Eintrag "ISBJ-Zertifizierungsinstanz".

	Schlüsselbund	dverwaltung	Ablage	Bearbeiten	Darstellung Fe	enster	Hilfe	ý á	<u> </u>
•	• •	Schlüsselt	oundverwa	ltung	Ø	Ġ	Q Suchen		
		Alle Objekte	Passwörter	Sichere Notia	en Meine Zertifikat		issel Zertifikate		
പ്	Anmeldung								
്	Lokale Obje	Certificate	Root-Zertifizi	erungsinstanz Mittwoch 15	tanz	46 Norda	merikanische Wes	kiisten-Sommerzeit	
			Oleses Roo	t-Zertifikat ist	nicht vertrauenswurd	g.			
8	System								
O	System-Ro	Name			Art	Geänd	ert	Verfällt	Schlüsselb
		20200	10102F2		Zertifikat			Gestern, 02:51	Anmeldung
		♀ <key></key>			Öffentlicher Schlüsse				Anmeldung
		♀ <key></key>			Privater Schlüssel				Anmeldung
		Apple Persistent State Encryption			Programmpasswort	Heute,	04:23		Anmeldung
					Programmpasswort	13.09.3	2021, 05:12:59		Anmeldung
		/ com.ap	ple.assistant		Programmpasswort	Heute,	04:15		Anmeldung
		/ com.ap	ple.assistant		Programmpasswort	Heute,	04:15		Anmeldung
		/ com.ap	ople.assistant		Programmpasswort	Heute,	04:15		Anmeldung
		/ com.ap	ple.assistant		Programmpasswort	Heute,	04:19		Anmeldung
		/ com.ap	ple.scookma	rksagent.xpc	Programmpasswort	13.09.3	2021, 05:13:46		Anmeldung
		ISBJ NI	utzer Zfikat 2	020010102F2	Private, Cohlüssel				Anmeldung
		🗧 😿 ISBJ Zertifizierungsinstanz			Zertifikat			15.04.2026, 04:44:46	Anmeldung
		An Westerkeychain			2.Jarammpasswort	13.09.:	2021, 05:13:28		Anmeldung

8.Vergleichen Sie bitte in dieser Ansicht den SHA1-Fingerabdruck mit dem Fingerabdruck aus dem per Post geschickten Brief mit dem Installationskennwort für das Zertifikat.

	ISBJ Zertifizierungsinstanz
Allgemeiner Name	ISBJ Zertifizierungsinstanz
Seriennummer	20 16 04 00 00 00
Erweiterung	Alternativer Name des Inhabers (2.5.29.17)
Kritisch	NEIN
RFC 822 Name	lsbj-zertifikate@senbjs.verwalt-berlin.de
Erweiterung	Alternativer Name des Ausstellers (2.5.29.18)
Kritisch	NEIN
RFC 822 Name	lsbj-zertifikate@senbjs.verwalt-berlin.de
Erweiterung	Netscape-Zertifikatstyp (2.16.840.1.113730.1.1)
Kritisch	NEIN
Art des Zertifikats	SSL CA, S/MIME CA
Erweiterung	Netscape-Zertifikats-Kommentar (2.16.840.1.113730.1.13)
Kritisch	NEIN
Daten	ISBJ Zertifizierungsinstanz Zertifikat
Fingerabdrücke	
SHA-256	8C 70 CC 86 C1 37 34 D2 08 41 88 49 9A F5 A6 DB 2F 48
	TE 59 CE 6E 15 06 4F 4A 88 62 E6 D9 65 20
SHA-1	9B 3F FE 03 C9 A3 A6 22 BA 6F 5B 68 89 F2 BA A5 D0 49 8E 21 T



9. Wenn die Fingerabdrücke übereinstimmen, scrollen Sie im geöffneten Fenster der Zertifizierungsinstanz nach oben und klicken auf den kleinen Pfeil neben "Vertrauen", sodass sich das Menü ausklappt.



10. Wählen Sie nun unter "Bei Verwendung dieses Zertifikats" die Option "Immer vertrauen" aus und schließen Sie das Fenster. Das Zertifikat wurde erfolgreich installiert und Sie können die Schlüsselbundverwaltung schließen.

11. Stimmen die Fingerabdrücke nicht überein, muss das Zertifikat wieder deinstalliert werden. Klicken Sie hierzu das installierte Zertifikat an und wählen Sie über das Menü "Bearbeiten" den Punkt "Löschen" aus.

Bearbeiten	Darstellung	Fenster	Hilfe	
Widerrufe Wiederhol	n ien			¥Z o%Z
Ausschnei Kopieren Kennwort Einsetzen	iden In die Zwische	mablage k	opieren	жх жС ФжС жV
Löschen				(B)
Alles ausw	vählen			ЖА
Schlüsselt	oundliste			X. 36L

11.1 Bestätigen Sie den Löschvorgang mit "Löschen". Das Zertifikat wird aus der Liste entfernt.





11.1.2 Bitte melden Sie die nicht übereinstimmenden Fingerabdrücke sofort an traeger-service@senbjf.berlin.de.