

Installation der Zertifikate für Mozilla[®] Firefox^{®1}

¹ Alle Screenshots wurden mit *Firefox Version 92.0.1* erstellt. Mozilla und Firefox sind eingetragene Marken der Mozilla Foundation.

(Weitere Informationen zu Mindestanforderungen und unterstützten Browser-Versionen finden Sie hier: <u>e-Card System Browser</u> und <u>ELGA Browser</u>.) Wesentliche Änderungen zur Vorversion sind gelb markiert.





Installation der Zertifikate

Die Zertifikate finden Sie unter folgendem Link:

→ <u>Download-Zertifikate</u>

(Alternativ navigieren Sie auf <u>www.chipkarte.at</u> zum Bereich "Gesundheitsdiensteanbieter" \rightarrow dann im linken Menü: Security & Kompatibilität \rightarrow Sichere Kommunikation im e-card System (HTTPS) \rightarrow Zertifikate: Download (Produktionsumgebung)

Unter dem Punkt "Zertifikate: Download (Produktionsumgebung)" stehen zwei Zertifikatdateien zum Download zur Verfügung. (Die .cer Dateiversionen sind im Regelfall die richtige Wahl.)

Schritt 1:

Starten Sie die Installation durch einen Klick mit der linken Maustaste auf die Datei "Zert_CA_Root_V02_Prod.cer".

Schritt 2:

Es öffnet sich folgendes Fenster (siehe Abbildung 1). Hier wählen Sie den Punkt "**Datei** speichern" und anschließend "**OK**".

Öffnen von Zert_CA_Root_V02_Prod.cer	×
Sie möchten folgende Datei öffnen:	
Zert_CA_Root_V02_Prod.cer	
Vom Typ: cer File (1,3 KB)	
Von: https://www.chipkarte.at	
Wie soll Firefox mit dieser Datei verfahren?	
○ <u>Ö</u> ffnen mit <u>D</u> urchsuchen	
Datei speichern	
<u>F</u>ür Dateien dieses Typs immer diese Aktion ausführen	
OK Abbrecher	١

Abbildung 1: Auswahl der Option "Datei speichern"





Schritt 3:

Das Zertifikat wird nun im voreingestellten Download-Ordner Ihres Browsers gespeichert. Um diesen Ordner zu öffnen, klicken Sie bitte auf das Pfeil-Symbol im rechten oberen Rand Ihres Browser-Fensters. Es öffnet sich eine Liste mit Ihren zuletzt heruntergeladenen Dateien. Der oberste Eintrag sollte nun Ihr Zertifikat sein.

Wie in Abbildung 2 gezeigt, wählen Sie als Nächstes bitte das kleine Ordner-Symbol rechts neben Ihrem Zertifikat aus.



Abbildung 2: Öffnen des Download-Ordners

Es erscheint das in Abbildung 3 gezeigte Fenster.

Merken Sie sich bitte das Verzeichnis!

🕹 🕑 📙 🖛 D	lownloads					-	×
Datei Start	Freigeben Ansicht						~ 🕐
$\leftrightarrow \rightarrow \checkmark \uparrow$	> Dieser PC > Downloa	ds		*	ට 🔎 "Downloads" durchsuchen		
🕹 Cabaallaumili	Nar	ne		Änderungsdatum	Тур	Größe	
Schneilzügnin	V He	eute (1)					
OneDrive		Zert_CA_Root_V02_Prod.cer		07.10.2021 14:11	Sicherheitszertifikat		2 KB
💻 Dieser PC			•				
💣 Netzwerk							

Abbildung 3: Speicherort der Zertifikatdatei





Schritt 4:

Anschließend öffnen Sie bitte erneut *Mozilla Firefox* und wählen Sie rechts oben den Menüpunkt "**Einstellungen**" (siehe Abbildung 4).

	Neuer Tab	× +		- 🗆 ×
\leftarrow	→ C	Q Mit Google suchen oder Adresse eingeben		⊗ ⊻ ≡
		S	Daten synchronisieren und speichern	Anmelden
		1	Neuer Tab	Strg+T
		,	Neues Fenster	Strg+N
		1	Neues privates Fenster	Strg+Umschalt+P
		L	Lesezeichen	>
			Chronik	>
		ſ	Downloads	Strg+J
		F	asswörter	
			Add-ons und Themes	Strg+Umschalt+A
		c.	Drucken	Strg+P
		s	seite speichern unter	Strg+S
		- I	n Seite suchen	Strg+F
		2	Zoom –	100% 🛨 🎽
		E	Einstellungen	
			Weitere Werkzeuge	>
		,	Hilfe	>
		E	Beenden	Strg+Umschalt+Q

Abbildung 4: Aufruf des Menüpunktes "Einstellungen" zum Zertifikatimport

Schritt 5:

Klicken Sie auf den Punkt "**Datenschutz & Sicherheit**" im linken Menü, scrollen Sie nach unten bis zum Bereich "Sicherheit" und wählen Sie den Button "**Zertifikate anzeigen…**" (siehe Abbildung 5).

SVC

ecard

	Neu	er Tab	×	😵 Einstellungen × +		_		×
\leftarrow	\rightarrow	C	单 Firefox	about:preferences#privacy	\$	\bigtriangledown	$ \pm $	≡
	ゆ の の の の	Allgemein Startseite Suche Datenschutz & Sicherheit Synchronisation]	 Nicht gesendete Absturzberichte automatisch von Firefox senden lassen Sicherheit Schutz vor betrügerischen Inhalten und gefährlicher Software Gefährliche und betrügerische Inhalte blockieren Weitere Informationen Gefährliche Downloads blockieren Vor unerwünschter und ungewöhnlicher Software warnen 	¹ In Einstellungen suchen Weitere Informationen	I		^
	ப் ூ	Erweiterungen & 1 Hilfe für Firefox	Themes	Zertifikate Aktuelle <u>G</u> ültigkeit von Zertifikaten durch Anfrage bei OCSP-Server bestätigen lassen Nur-HTTPS-Modus	Zertifikate anzei <u>K</u> ryptographie-Moo	gen]	
	-			HTTPS bietet eine sichere, verschlüsselte Verbindung zwischen Firefox und de Websites. Die meisten Websites unterstützen HTTPS und wenn der Nur-HTTP	en von Ihnen besuchten S-Modus aktiviert ist wir	·d		~

Abbildung 5: Menüpunkt "Datenschutz & Sicherheit" → "Sicherheit" → "Zertifikate anzeigen…"

Schritt 6:

Hier sind die verschiedensten Stammzertifizierungsstellen (CA) eingetragen. Achten Sie bitte darauf, dass Sie sich auf dem richtigen Reiter **"Zertifizierungsstellen"** befinden (siehe Abbildung 6). Klicken Sie dann auf **"Importieren"**.

Zertifikatverwaltung				
Ihre Zertifikate Authentifizierungs-Entscheidu	ngen Personen S	erver Zertifizierungsstellen		
ie haben Zertifikate gespeichert, die diese Zertifizieru	ngsstellen identifizieren:			
Zertifikatsname	Kryptographie-Mo	dul I		
✓ AC Camerfirma S.A.				
Chambers of Commerce Root - 2008	Builtin Object Token			
Global Chambersign Root - 2008	Builtin Object Token			
✓ AC Camerfirma SA CIF A82743287				
Camerfirma Chambers of Commerce Root	Builtin Object Token			
Camerfirma Global Chambersign Root	Builtin Object Token			
Ansehen Vertrauen <u>b</u> earbeiten Imp	ortieren Exportiere	n Lösche <u>n</u> oder Vertrauen entziehen		

Abbildung 6: Übersicht über die Stammzertifizierungsstellen und Möglichkeit zum Import neuer Zertifikate





Schritt 7:

Navigieren Sie zu dem Ordner, in dem Sie ihr Zertifikat zwischengespeichert haben. Wählen Sie es aus und klicken Sie auf "**Öffnen**" (siehe Abbildung 7).

ڬ Wählen Sie die Datei mit dem	oder den zu importierenden CA-Zertifikat(en)			×
\leftarrow \rightarrow \checkmark \uparrow \blacklozenge > Dieser $𝔅$	PC > Downloads	Ŷ	, <u>ර</u> "Dov	nloads" durchsuchen
Organisieren 👻 Neuer Ord	ner			::: • 🔳 ?
📌 Schnellzugriff	Name V Heute (1)	Änderungsdatum	Тур	Größe
OneDrive	Zert_CA_Root_V02_Prod.cer	07.10.2021 14:11	Sicherheitszertifikat	2 KB
📃 Dieser PC				
Netzwerk				
Dateiname	E Zert_CA_Root_V02_Prod.cer		✓ Zertifikat-Öffner	Dateien (*.p7b;*.crt;*. ∨ Abbrechen

Abbildung 7: Auswahl des zu importierenden Zertifikats aus dem Verzeichnis

Schritt 8:

Beim Import werden Sie gefragt, welchen Zweck dieses Zertifikat erfüllt. Wählen Sie hier "**Dieser CA vertrauen, um Websites zu identifizieren**" (siehe Abbildung 8) und klicken Sie anschließend auf "**OK**".



Abbildung 8: Vertrauen des Zertifikats als Zertifizierungsstelle





Schritt 9:

Danach gelangen Sie wieder zum Fenster "Zertifikateverwaltung". Wenn Sie in dieser Liste zum Herausgeber navigieren, sollten Sie nun Ihr installiertes Zertifikat sehen können (siehe Abbildung 9). Mit einem Klick auf "**OK**" beenden sie die "Zertifikateverwaltung".

Hinweis: Es kann sein, dass das Fenster nach dem Import erneut geöffnet werden muss, um die Zertifikate in der Liste zu sehen.

	Zertifikatverwaltung					
Ihre Zertifikate	Authentifizierungs-Entsch	eidungen Pers	onen	Server	Zertifizierungsstellen	
ie haben Zertifikate	e gespeichert, die diese Zertifi	izierungsstellen ident	ifizieren:			
Zertifikatsname		Krypt	tographie-M	odul		E
 Hauptverband o 	esterr. Sozialvers.					^
Hauptverban	d oesterr. Sozialvers.	das So	ftware-Siche	rheitsmoo	dul	
∨ Hellenic Academ	nic and Research Institutions C	Cert. Authori				
Hellenic Acad	lemic and Research Institution	s RootCA 2 Builtin	Object Toker	ı		
Hellenic Acad	lemic and Research Institution	s ECC Root Builtin	Object Toker	ı		
Hellenic Acad	lemic and Research Institution	s RootCA 2 Builtin	Object Toker	ı		
<u>A</u> nsehen	Vertrauen <u>b</u> earbeiten	Importieren	E <u>x</u> portie	ren	Lösche <u>n</u> oder Vertrauen entz	ziehen
						ок
	Abbildung	9: Zertifikateve	erwaltung	ı – Koni	trolle	

Anschließend ist die **Installation beendet**.

Der gesamte Vorgang muss auch für das Zertifikat "Zert_CA_ECS_V02_Prod.cer" wiederholt werden.

Für die Verwendung der Testumgebung müssen die Zertifikate "Zert_CA_Root_V02_Test" und "Zert_CA_ECS_V02_Test" installiert werden. Zusätzlich ist auch das "Zert_CA_Root_V02_Prod" für die Testumgebung notwendig. Für Gesundheitsdiensteanbieter ohne Zugang zum Testsystem ist diese Funktionalität irrelevant.

In Firefox gibt es keine spezielle Zuordnung der Zertifikate.





Am Ende müssen folgende Zertifikate importiert sein:

- Zert_CA_Root_V02_Prod (Hauptverband oesterr. Sozialvers.)
- Zert_CA_ECS_V02_Prod (Prod ECS CA)

Für die Verwendung der Testumgebung müssen folgende Zertifikate importiert sein:

- Zert_CA_Root_V02_Test (Test Hauptverband oesterr. Sozialvers.)
- Zert_CA_ECS_V02_Test (Test ECS CA)
- Zert_CA_Root_V02_Prod (Hauptverband oesterr. Sozialvers.)

Die importierten Zertifikate werden nun unter dem Zertifikatnamen "Hauptverband österr. Sozialvers." gelistet (siehe Abbildung 10). Sie können so die korrekte Installation überprüfen.

		Zertifi	katverwaltung			>
Ihre Zertifikate	Authentifizierungs-Entsc	heidungen Per	sonen Server	Zertifizierungss	tellen	
Sie haben Zertifikat	e gespeichert, die diese Zerti	izierungsstellen iden	tifizieren:			
Zertifikatsname			Kryptographie-Mo	odul		C.
GDCA Trust/	AUTH R5 ROOT		Builtin Object Token		_	^
 Hauptverband 	oesterr. Sozialvers.					
Hauptverba	nd oesterr. Sozialvers.		das Software-Sicher	rheitsmodul		
Prod ECS CA	ł		das Software-Sicher	rheitsmodul		
✓ Hellenic Acade	mic and Research Institutions	Cert. Authority				
Hellenic Aca	demic and Research Institutio	ns RootCA 2011	Builtin Object Token			
Hellenic Aca	demic and Research Institutio	ns ECC RootCA 2015	Builtin Object Token			
Hellenic Aca	demic and Research Institutio	ns RootCA 2015	Builtin Object Token			
✓ Hongkong Pos	t					~
<u>A</u> nsehen	Vertrauen <u>b</u> earbeiten	Importieren	Exportieren	Lösche <u>n</u> oder V	ertrauen entziehen	
						ок

Abbildung 10: Liste der Zertifizierungsstellen nach erfolgreichem Zertifikatimport

Durch einen Doppelklick auf das jeweilige Zertifikat – oder auch durch ein Klicken auf "**Ansehen**" – wird dieses geöffnet und die Eigenschaften angezeigt. Hier sollten Sie die **Signatur (Fingerabdruck)** (grüne Umrandung) überprüfen:

- Hauptverband oesterr. Sozialvers. (siehe Abbildung 11)
- Prod ECS CA Hauptverband oesterr. Sozialvers. (siehe Abbildung 12)





Falls Sie einen Zugang zum Testsystem haben und die zugehörigen Zertifikate installiert haben:

- Test Hauptverband oesterr. Sozialvers.
- Test ECS CA
- Hauptverband oesterr. Sozialvers.

(siehe Abbildung 13) (siehe Abbildung 14) (siehe Abbildung 11)

Ausstellername

Land Organisation	AT Hauptverband oesterr. Sozialvers.
Gültigkeit Beginn Ende	Mon, 21 Sep 2009 08:08:05 GMT Tue, 21 Sep 2049 08:08:05 GMT

Öffentlicher Schlüssel -Informationen

Algorithmus	RSA
Schlüssellänge	4096
Exponent	65537
Modulus	C3:10:85:45:33:8E:68:81:1E:41:33:AC:DB:5A:AC:BD:D9:07:11:E8:4A:F9:9C:FA:06:44

Verschiedenes

Seriennummer	01:01:00:00:00:00:00:01:43:35:41:5A:AD:25:E7:E3
Signaturalgorithmus	SHA-256 with RSA Encryption
Version	3
Speichern	

Fingerabdrücke

SHA-25	6 9E:	A:C7:F6:C6:AC:3E:1A:1D:C1:72	:78:9A:D9:F6:5B:C7:F4:8F:30:4	1:D0:54:50:57:8D
SHA-	1 40:	36:FC:75:33:1B:CA:78:77:79:67:5	D:97:F1:4A:18:4E:37:7B:3A	

Abbildung 11: Signatur von "Hauptverband der oesterr. Sozialvers."





Ausstellername	
Ausstellername	
Land	AT
Organisation	Hauptverband oesterr. Sozialvers.
Gültigkeit	
Beginn	Wed, 06 Jul 2016 10:18:55 GMT
Ende	Fri, 06 Jul 2046 10:18:55 GMT
Öffentlicher Schlüssel -	
Informationen	
Algorithmus	RSA
Schlüssellänge	3072
Exponent	65537
Modulus	AF:2B:D2:62:96:47:09:79:29:A3:E2:78:B1:B9:3D:BE:F4:5D:3D:2B:14:6B:54:3D:82:D
Venekiedenee	
verschiedenes	
Seriennummer	01:01:00:00:00:00:23:86:E4:FD:37:79:36:9C:3C
Signaturalgorithmus	SHA-256 with RSA Encryption
Version	3
Speichern	
Fingerabdrücke	
SHA-256	73:70:4A:57:42:26:4A:98:7A:72:25:65:F7:B8:02:5F:46:EF:28:61:02:05:E9:4B:3E:D6:0
SHA-1	49:DF:19:F4:BF:1E:2E:B0:D5:09:8E:80:18:0F:5F:C7:B5:E7:E2:D0

Abbildung 12: Signatur von "PROD ECS CA – Hauptverband oesterr. Sozialvers."





Ausstellername	
Land	AT
Organisation	Test - Hauptverband oesterr. Sozialvers.
-	
Gültigkeit	
Beginn	Tue, 26 May 2009 12:28:37 GMT
Ende	Wed, 26 May 2049 12:28:37 GMT
Öffentlicher Schlüssel -	
Informationen	
Algorithmus	RSA
Schlüssellänge	4096
Exponent	65537
Modulus	BC:B9:A8:6C:91:82:49:45:59:27:C4:63:AA:39:B7:17:1F:19:A5:E8:7C:E9:C9:2E:71:FB:
Verschiedenes	
Seriennummer	01:01:00:00:00:00:0B:5D:BE:96:D3:2D:A1:00:8F
Signaturalgorithmus	SHA-256 with RSA Encryption
Version	3
Speichern	
Fingerabdrücke	
SHA-256	2E:9E:E1:6D:74:19:61:A6:AD:2E:97:D4:F5:B4:57:4D:AA:32:7B:99:4C:5F:86:3A:A2:B
SHA-1	36:9E:44:E6:AE:7D:35:BB:94:7E:C4:3C:3A:6D:DE:98:E4:E4:CE:C8

Abbildung 13: Signatur von "Test – Hauptverband oesterr. Sozialvers."





Ausstellername	
Land	AT.
Organisation	AI Test - Hauntverband gesterr Sozialvers
organisation	rest - nauptverband besten. Sozialvers.
Gültigkeit	
Beginn	Fri 10 Jun 2016 08:29:37 GMT
Ende	Sun 10 Jun 2046 08:29:37 GMT
Linc	Sun, 10 Jun 2010 00.23.37 Sinn
ör an eine eine	
Offentlicher Schlussel -	
Informationen	
Algorithmus	RSA
Schlüssellänge	3072
Exponent	65537
Modulus	87:41:FC:1A:1E:C9:66:EB:47:F4:D9:78:71:14:99:2D:5A:0B:11:BD:01:C4:5B:ED:36:5A
Verschiedenes	
Seriennummer	01-01-00-00-00-00-3E-9B-01-FR-F9-08-22-C8-FF
Signaturalgorithmus	SHA-256 with RSA Encryption
Version	3
Speichern	5
Spelenen	
Fingerabdrücke	
SHA-256	91:09:C4:E0:23:D0:B4:8C:AF:B9:10:1E:62:A1:57:91:BD:86:18:E4:EC:F7:27:3A:CA:17:
SHA-1	B6:6B:08:0F:F8:CA:DC:A7:8E:37:23:47:C4:23:DA:8F:A4:13:01:BA

Abbildung 14: Signatur von "Test ECS CA"