Client Zertifikate im Browser installieren

Um Webdienste sicherer zu gestalten können Client-Zertifikate eingesetzt werden. Ein Zertifikat ist dabei eine Datei, mit der sich ein Programm gegenüber dem Server ausweist. Diese Zertifikate sind personalisiert und ermöglichen einen Zugriff so zu gestalten, dass nur Personen mit gültigen Zertifikaten auf bestimmte Dienste zugreifen können.

Das kann beispielsweise eine Nextcloud-Instanz sein, in der sensible Daten liegen und bei der z.B. ein Zugriff nur über ein Passwort zu unsicher wäre. Ein Client-Zertifikat stellt einen zweiten Faktor dar: Ich muss für den Zugriff etwas wissen und etwas haben.

Voraussetzung für dieses Vorgehen ist eine sogenannte Public-Key-Infrastrutkur (PKI). Diese besteht aus einer zentralen Zertifikatsinstanz, die Zertifikate für Server und für einzelne Personen herausgibt. Mensch kennt das von Webseiten, die über https (ssl) verschlüsselt sind.

Sogenannte Client-Zertifikate (also solche, die für Personen ausgestellt werden) können für folgende Anwendungen verwendet werden:

- VPN (virtuelles privates Netzwerk)]]
- Client-Zertifikate für Webbrowser zum Zugriff auf bestimmte Webdienste
- Verschlüsseln und Signieren von E-Mails

JedeR, der/die Zertifikate einsetzen möchte, benötigt dafür einen eigenen Schlüssel in einer pkcs12-Datei sowie das Wurzelzertifikat der jeweiligen PKI seiner Organisation.

Installation der Zertifikate im Browser

Die Zertifikate werden in der Regel für einzelne Organisationen vom Datenkollektiv zur Verfügung gestellt. In der Regel ist das eine Datei wie

vorname.nachname@organisation.org.p12

In dieser sind privater Schlüssel, öffentlicher Schlüssel sowie der CA-Schlüssel schon enthalten. Sie ist mit einem Passwort gesichert und kann in verschiedenen Programmen importiert werden.

Client-Zertifikat installieren

Im Menü auf \rightarrow Bearbeiten \rightarrow Einstellungen gehen. Links "Datenschutz und Sicherheit" auswählen.

Last update: 2019/04/18 public:client_zertifikate_im_browser_installieren https://wiki.datenkollektiv.net/public/client_zertifikate_im_browser_installieren?rev=1555579020 11:17



Ganz unten findet sich dann eine Rubrik "Zertifikate"

Wenn eine Website nach dem persönlichen Sicherheitszertifikat verlangt

- Automatisch eins <u>w</u>ählen
- Jedes Mal fragen
- Aktuelle Gültigkeit von Zertifikaten durch Anfrage bei OCSP-Server bestätigen lassen

Ze	rtifika	te	anz	eiger	٦
				~	

Hier auf "Zertifikate anzeigen klicken

	Zertifika	tverwaltung		
Ihre Zertifikate Personen	Server Zertifizierungsstellen			
ie haben Zertifikate dieser Organis	ationen, die Sie identifizieren:			
Zertifikatsname	Kryptographie-Modul	Seriennummer	Gültig bis	
Incohen Statem March	there are a second to be a second to			
Ansehen Sichern Alle s	ichern Importieren Löschen			
Ansehen Schern Ale e	ichern Impartieren Löschen			
Ansehen Sichern Ale s	ichem Impertieren Löschen			0

Weiter im Tab \rightarrow Ihre Zertifikate Auf importieren klicken und das gespeicherte Zertifikat auswählen



An dieser Stelle muss das Passwort, mit dem das Zertifikat gesichert ist, eingegeben werden.

6	Passwort erforderlich		•	×	
di de la compositione de la comp	Bitte geben Sie das Passwort ein, das zur Verschlüsselun verwendet wurde:	g dieses Zertifikatbackups			
	••••••••••]	F
		Abbrechen	OK		
L					1.1

Anschließend ist das Zertifikat im Browser installiert

	Zertifikatverwaltung				
Ihre Zertifikate Personen Server Ze	ertifizierungsstellen				
ie haben Zertifikate dieser Organisationen, die Sie	identifizieren:				
Zertifikatsname	Kryptographie-Modul	Seriennummer	Goltig bis		
a second s	das Software-Sicherheitsmodul	60:78:5C:##	14. September 2028		
Broshen Schern Ale sichern Im	ogrtienen				
				OK	
				-	

Nach einem Neustart des Browsers sollte das Zertifikat installiert sein. Beim Zugriff auf eine per Client-Zertifikat abgesicherte Seite, erscheint dann eine Abfrage:

Last update: 2019/04/18 public:client_zertifikate_im_browser_installieren https://wiki.datenkollektiv.net/public/client_zertifikate_im_browser_installieren?rev=1555579020 11:17

• Privates Surfen	× +	
$\leftrightarrow \rightarrow \times \mathbf{\hat{\omega}}$	Q https://wiki	
	benutzer-Identifikationsanfrage	
	Diese Website verlangt, dass Sie sich mit einem Zertifikat identifizieren:	
	wiki.w443	
	Ausgestellt unter: "Let's Encrypt"	
	Wählen Sie ein Zertifikat, das als Identifikation vorgezeigt wird:	
	[46:E4:74:20:86:A4:24:84:50:07:30:7	:+ 0
	Details des gewählten Zertifikats:	IL S
	Ausgestellt auf: CN Seriennummer: 46:E4:74:2C:80:A4:24:6 Gültig vom 19. September 2016, 23:12:41 GMT+2 bis 17. September 2026, 23:12:41 GMT+2 Schlüsselgebrauch: unterzeichne,Schlüssel-Verschlüsselung E-Mail-Adressen: Ausgestellt von: CN= Gespeichert auf: das Software-Sicherheitsmodul	UN) ien, so
	✓Diese Entscheidung merken	Cooki
	Abbrechen OK	Temp
	• Lesezeichen	Down

From: https://wiki.datenkollektiv.net/ - **datenkollektiv.net**

Permanent link: https://wiki.datenkollektiv.net/public/client_zertifikate_im_browser_installieren?rev=1555579020

Last update: 2019/04/18 11:17