Single Sign On

Bundesinstitut
für Arzneimittel
und Medizinprodukte

BfArM Dienstsitz Köln
Waisenhausgasse 36-38a
50676 Köln

Tel.: +49 228 99 307-0
Fax: +49 228 99 307-5207
www.dimdi.de

Ansprechpartner:
Helpdesk Technik
Tel: +49 22899307-4949
helpdesk-technik@bfarm.de

FAQ zu Nutzung der Zertifikate

Inhalt

Im Geschäftsbereich des

Bundesministerium
für Gesundheit

Benötigt jeder Benutzer ein eigenes Zertifikat?

Ja, es dient dem Nachweis der Identität.

Können mehrere Zertifikate auf demselben Rechner installiert sein?

Ja, wenn mehrere Personen mit dem gleichen Rechner arbeiten, benötigt jeder sein eigenes Zertifikat.

Kann das gleiche Zertifikat auf mehreren unterschiedlichen Rechnern genutzt werden?

Ja, wenn eine Person von verschiedenen Rechnern arbeitet, so kann sie auf jedem dieser Rechner das gleiche Zertifikat installieren.

Kann man ein Zertifikat ausprobieren?

Ja, unter: https://portal.dimdi.de/ruben/faces/CheckCertificatePage.xhtml (reiner Upload-Test) kann das Zertifikat ausprobiert werden.

Könnten Sie uns einen Anbieter nennen, bei dem solche Zertifikate zu erwerben sind?

In der Anleitung (Anleitung zur Nutzung der Zertifikate) sind einige Zertifizierungsstellen aufgelistet, die digitale X.509-User-Zertifikate ausstellen. Die aufgeführte Liste dient ausschließlich dem Zweck, einige Beispiele zu geben und ist keinesfalls als Verweis oder Empfehlung zum Kauf der Produkte der genannten Unternehmen zu verstehen. Nicht alle der dort aufgelisteten Aussteller können das benötigte Zertifikat zur Client-Authentifizierung ausstellen.

Können auch Zertifikate von alternativen Anbietern/Resellern erworben werden?

Sogenannte Reseller (z.B. https://icertificate.eu) bieten Zertifikate verschiedener Hersteller an. Die ausgestellten Zertifikate unterscheiden sich nicht in der „Qualität“, sondern im Drumherum (z. B. Schnelligkeit der Ausstellung, Preis, Support usw.).

Ist das PKI Zertifikat der Firma xyz das richtige?

Eine Empfehlung dürfen wir aus rechtlichen Gründen nicht aussprechen.

Informationen zu X.509-Zertifikaten

bei SwissSign: https://www.swisssign.com/de/produkte/personenzertifikate

SwissID geht wohl nur für Schweizer, weil es eine „face to face“-Identitätsprüfung bei der Schweizerischen Post vorsieht (quasi Post-Ident auf Schwyzerdütsch).

„Personal Gold-Id“ ist das Richtige.

bei GlobalSign: https://www.globalsign.com/de-de/personalsign/vergleichen.html

Aussteller von Zertifikaten, die bisher bei uns hochgeladen wurden:

- GlobalSign PersonalSign 2 CA – SHA256 – G2 (4x)
- SwissSign Personal Gold CA 2008 – G2 (4x)
- GlobalSign PersonalSign 1 CA – SHA256 – G2 (1x)
- GlobalSign PersonalSign 2 CA – G2 (1x)
- AlphaSSL CA – G2 (→ GlobalSign) (1x)
- GlobalSign PersonalSign 1 CA - G2 (DIMDI Zertifikate)

Wofür steht "Extended Key Usage"?

Diese Erweiterungen können einem Zertifikat hinzugefügt werden. Ursprünglich waren Zertifikate nur dazu geeignet, um etwas zu signieren, z. B. eine E-Mail oder ein Dokument. Wenn man es außerdem auch noch als "Ausweis" für eine Zugangskontrolle nutzen möchte, muss in der Erweiterung ein entsprechender Eintrag sein. In den Erweiterungen gibt es eine ganze Reihe von Möglichkeiten, die beim Erstellen des Zertifikates eingefügt werden können. Wir brauchen eben diese "Client Authentication", damit das Zertifikat den User "Ausweisen" kann.

Besteht die Möglichkeit, das Zertifikat über PEI oder DIMDI zu beziehen?

Nein, nur über die in der Anleitung (Anleitung zur Nutzung der Zertifikate) genannten Aussteller.

Aber: Nicht alle dort genannten Hersteller bieten notwendigerweise den richtigen Typ von Zertifikat an.

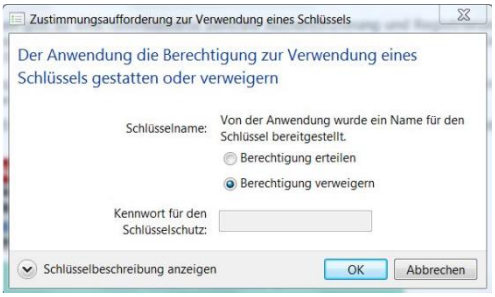
Die DIMDI-User-Administration hat mein Zertifikat „repariert“, aber es geht trotzdem nicht.

Browser neu starten oder zu Fuß im Browser Cookies und aktive Logins löschen (Tastenkombination STRG + SHIFT + ENTF)

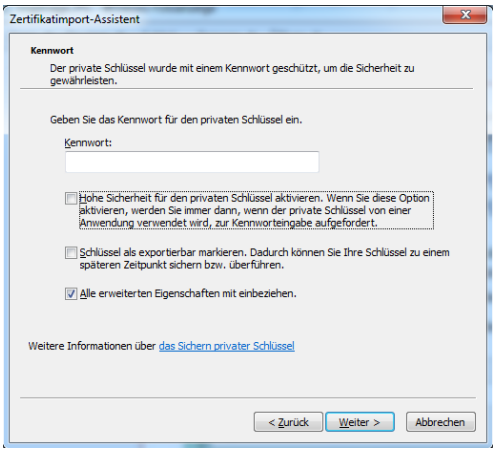
Nach Eingabe von Benutzernamen und Passwort erscheint nur eine leere Seite.

Wahrscheinlich hat der Nutzer noch nicht sein Zertifikat im Browser importiert.

Nach dem Aufruf einer hochabgesicherten Anwendung mit dem Internet Explorer erscheint zunächst das Fenster zur Zertifikatsbestätigung und anschließend noch ein weiteres Fenster "Zustimmungsaufforderung zur Verwendung eines Schlüssels" (evtl. noch mit Kennworteingabe)



Dieses zweite Fenster erscheint, wenn man beim Importieren eines Zertifikats in den IE die Option "Hohe Sicherheit für den privaten Schlüssel aktivieren" anklickt. Bei einigen Anwendern ist diese Option anscheinend durch den System-Administrator unveränderbar voreingestellt. Die Zustimmungsaufforderung erfolgt dann bei jedem SSO-Login und muss erteilt werden (ggf. durch Eingabe eines Passwortes).



Ich habe bei der Benutzer-Identifikationsanfrage durch den Browser das falsche Zertifikat ausgewählt oder auf den "Abbrechen"-Knopf geklickt. Jetzt erhalte ich beim Aufruf der Anwendung immer die Fehlermeldung "401: No client certificate chain in this request".

Der Browser merkt sich die erste Entscheidung des Nutzers und stellt die Benutzer-Identifikationsanfrage, also die Auswahl des Zertifikats, fortan nicht mehr. Erst wenn man die aktiven Logins im Browser löscht, erscheint die Abfrage erneut.

Vorgehensweise: Tastenkombination STRG + SHIFT + ENTF drücken, "Aktive Logins" (bzw. "Temporäre Internetdateien" im IE) auswählen und auf den Lösch-Button klicken. Manchmal hilft auch nur ein Neustart des Browsers.

Ich kann in RuBen unter „Meine Daten“ mein Zertifikat nicht einsehen.

Wenn ich im Abschnitt „Zertifikat“ auf den Button „ansehen“ klicke, sollte sich ein Dialog-Fenster öffnen, die Option „Öffnen mit“ ist selektiert und daneben gibt es einen „Durchsuchen“-Button. In diesem Fall reicht „ok“ und das Zertifikat wird mit dem Zertifikate-Viewer angezeigt.

Falls die Anzeige nicht so läuft oder nicht funktioniert, hilft Folgendes:

im Windows-Explorer auf einem Zertifikat (xyz.der) mit *__rechte Maustaste__* → Öffnen mit → Standardprogramm auswählen → Krypto-Shellerweiterungen wählen → ok, danach sollte in RuBen das Zertifikat automatisch mit diesem Programm geöffnet werden.

Der Nutzer erhält die Meldung "Das hochgeladene Zertifikat konnte nicht als Nachfolgezertifikat des bisher hinterlegten Zertifikats erkannt werden und muss daher erneut vom zuständigen Administrator geprüft werden."

Wenn das Zertifikat nicht als Nachfolgezertifikat erkennbar war, muss die Identität des Inhabers des Zertifikats, das aus technischer Sicht valide ist und alle Anforderungen erfüllt, vom Administrator bestätigt werden.

Für welche (Fach-) Anwendungen brauche ich ein Zertifikat?

Anwendungen, welche mit einem hohen Schutzbedarf eingestuft wurden, erfordern eine Zwei-Faktor-Authentifizierung. Hierfür ist ein Nutzerzertifikat mit entsprechenden Merkmalen (X.509-Standard, „Extended Key Usage“) notwendig.

Zum gegenwärtigen Zeitpunkt erfüllen folgende Anwendungen diesen Schutzbedarf:

- PharmNet.Bund „Sunset Clause“
- PharmNet.Bund „elektronische Änderungsanzeigen“
- PharmNet.Bund „Lieferengpassmeldungen“
- PharmNet.Bund „Chargenprüfung“ (PEI-CR)
- Samenspenderregister
- RuBen (hier: Benutzerverwaltung)

Weitere Informationen erhalten Sie auf den Webseiten des BfArM: https://www.bfarm.de/DE/Arzneimittel/Arzneimittelzulassung/ZulassungsrelevanteThemen/eSubmission/AMIS-Gesamtabl%C3%B6sung.html.

Wer braucht alles ein Zertifikat?

Alle Nutzer, die auf eine Anwendung mit hohen Schutzbedarf zugreifen.

Darunter zählen unter anderem sogenannte „Superuser“. Dieser stellt im engeren Sinne ein Hauptnutzer (OrgaAdmin) eines pharmazeutischen Unternehmens dar, der bspw. für die Eingabe von Änderungsanzeigen verantwortlich ist und diesen Prozess administriert.

Der Hauptnutzer kann ebenso weitere Nutzer (User) anlegen, die dann bspw. für das unter dem Hauptnutzer registrierte Unternehmen Änderungsanzeigen eingeben kann.

Werden Gruppenzertifikate akzeptiert?

Nein. Ein Zertifikat muss genau einer natürlichen Person zugeordnet sein.

Die Zertifizierungsstellen bieten mehrere Optionen zur Identitätsprüfung an (Validierung anhand der E-Mail-Adresse, Validierung inkl. Ausweisprüfung usw.). Welche ist nun die richtige Wahl?

Das Zertifikat muss für eine TLS-WWW-Client-Authentifizierung ausgestellt und SHA-2 signiert sein und das Attribut „Extended-Key-Usage für Client-Authentifizierung“ besitzen.

Wie Sie in Ihrem Unternehmen die Legitimation bei Beantragung eines Zertifikats durchführen, bleibt in Ihrem Ermessen. Unseres Wissens sollte die Validierung nach der E-Mail-Adresse ausreichen und mit der übereinstimmen, welche bei der Nutzerkennung eingetragen worden ist.

Es dürfen hierbei keine unspezifischen Angaben (bspw. Funktions-E-Mail-Adresse à la „info@...“ usw.) gemacht werden. Es muss genau einer natürlichen Person zugeordnet sein.

Kann eine Registrierung bzw. Anmeldung, welche auf eine natürliche Person mit entsprechendem Zertifikat ausgestellt ist, auch von weiteren Personen aus dessen unmittelbaren Kollegenkreis genutzt werden?

Dieses Szenario ist zwar aus technischer Sicht möglich, wenn Sie denselben Account nutzen. Die Benutzerverwaltung lässt es aber nicht zu, mehreren Teilnehmern dasselbe Zertifikat zu vergeben.

Da die Nutzerkennungen personengebunden sind, ist die Verantwortung zur nachfolgenden Nutzung der Datenbankanwendungen höchstpersönlich: d. h. eindeutig und ausschließlich einer natürlichen Person zuzuordnen.

Die Weitergabe der Nutzer- bzw. Anmeldedaten würden im konkreten Fall gegen das Urheberrecht verstoßen, weil Rechte ohne Ermächtigung des Urhebers eingeräumt wurden.

Ich betreue mehrere pharmazeutische Unternehmen, welche jeweils unter einer eigenen PNR registriert sind. Brauche ich für jedes dieser Registrierungen (Nutzerkennungen) ein separates Zertifikat?

Eigentlich nicht. Sofern Sie als Bevollmächtigter unter den jeweiligen Nutzerkennungen eindeutig identifizierbar sind, Sie bspw. bei jeder Ihrer Nutzerkennungen unter derselben E-Mail-Adresse registriert und erreichbar sind, ist es ausreichend, wenn Sie für sich ein einziges Zertifikat von einer Zertifizierungsstelle ausstellen lassen.

Sie müssten uns informieren, unter welcher Nutzerkennung Sie ein Zertifikat erstmalig hochgeladen haben. Dieses Zertifikat können wir dann auf die weiteren, von Ihnen zu betreuenden Nutzerkennungen übertragen. Bitte teilen Sie uns hierzu ebenso alles weiteren Nutzerkennungen mit.