Informationsblatt zu Client-Zertifikaten und secuTrial

Voraussetzungen:
Der Arbeitsplatzrechner benötigt:

- Internetverbindung (Test: https://st03.mi.med.uni-goettingen.de/cgi-bin/WebObjects/productive-DataCapture.woa/wa/choose?customer=DZHK)
- Microsoft Internet Explorer ab Version 8, Firefox ab Version 27 oder Chrome ab Version 30 unter (mind.) Windows 7
- Die Ausführung von JavaScript muss im Browser aktiviert sein
- Hinsichtlich der zum Einsatz kommenden Verschlüsselungsverfahren für die Datenübertragung per Web-Browser sind Vorgaben der Datenschutzbeauftragten umzusetzen: Die Nutzung von TLS 1.2 ist erforderlich. Ob der zu verwendende Browser diese Verschlüsselungstechnik unterstützt kann der TLS1.2 Test gemacht werden (Siehe FAQ-Bereich: http://dzhk.de/das-dzhk/klinische-dzhk-studien/3-wissenschaftliche-infrastruktur-des-dzhk/faq/).

Installationsanweisung für ein Client-Zertifikat:
Nachdem das Client-Zertifikat beantragt wurde, prüft die THS den Antrag und verschickt das Zertifikat an den Antragsteller. Zur Installation des Zertifikates wird ein Passwort benötigt, welches sie in einer separaten E-Mail erhalten.

Für die Installation des Client-Zertifikats in den Browsern Internet Explorer oder Chrome haben Sie folgende Optionen:

- die Installation über die Zertifikatverwaltung (certmgr.msc). Eine Anleitung dafür finden Sie unter http://windows.microsoft.com/de-de/windows/import-export-certificates-private-keys#1TC=windows-7;
- die Installation durch den Zertifikatimport-Assistenten. Der Assistent öffnet sich automatisch, sobald Sie auf das erhaltene Client-Zertifikat einen Doppelklick ausgeführt haben. Hinweis: Wenn Sie im Zertifikatimport-Assistenten auf Durchsuchen klicken, um das Client-Zertifikat zu suchen, werden im Dialog Öffnen standardmäßig nur X.509-Zertifikate angezeigt. Möchten Sie einen anderen Zertifikattyp installieren, müssen Sie diesen im entsprechenden Auswahlfeld auswählen.

Hinweis: Bitte beachten Sie, dass sich die Darstellung der Icons in Abhängigkeit von der Browserversion unterscheiden kann.

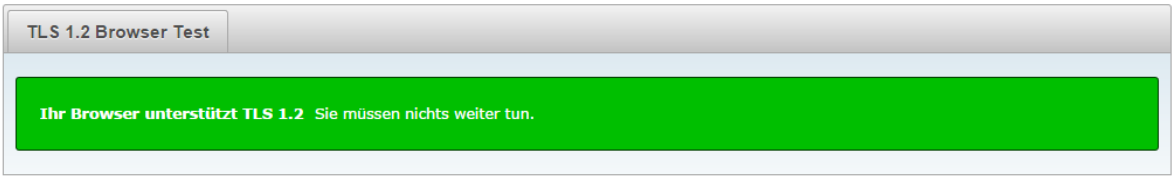
Da der Mozilla Firefox Browser nicht den Zertifikatsspeicher von Windows benutzt, ist eine Firefox-spezifische Verfahrensweise zur Installation des Client-Zertifikates notwendig. Unter nachfolgendem Link finden Sie eine Installations- und Importanweisung: http://security.ag-nbi.de/Projekte/XMLSicherheitsdienste/Demonstrator/de/InstallCertFirefox.html

Testung des Client-Zertifikats:

Öffnen Sie den Browser, für den das Zertifikat eingerichtet wurde, und führen Sie die nachfolgenden Schritte aus.

1.https://browser-test.med.uni-greifswald.de/

Wenn Sie folgenden Hinweis angezeigt bekommen, war der Test erfolgreich:



Hinweis: Für Browser wie dem Internet Explorer 10 muss die Internet-Verschlüsselung TLS 1.2 manuell aktiviert werden. Der nachfolgenden Link beschreibt die Vorgehensweise: http://www.guntiahoster.de/blog/2013/allgemein/tls-12-im-browser-aktivieren/

2. Rufen Sie in ihren Webbrowser folgende Webseite für die Überprüfung des Client-Zertifikates auf: https://test.ths.dzhk.med.uni-greifswald.de/dzhk/html/authenticated.xhtml

Wenn Sie folgenden Hinweis angezeigt bekommen, war der Test erfolgreich: