DZHK
DEUTSCHES ZENTRUM FÜR
HERZ-KREISLAUF-FORSCHUNG E.V.

Information Sheet

# Client Certificate and secuTrial

Within the DZHK, the secuTrial web application allows a data-protection-compliant transmission of personally identifiable information (IDATs) to the DZHK's Independent Trusted Third Party (TTP), as well as an automatic adoption of pseudonyms generated there. Due to the high security requirements for this data transmission, it is necessary that

(1) the public IP address of the workstation PC or, if applicable, the internet proxy used at the TTP is registered once, and that
(2) a Client Certificate is installed in the browser.

**Validity:**

One Client Certificate is valid for one workstation computer and one study. If a user works at multiple workstation computers, a Client Certificate needs to be requested for each of these computers. A Client Certificate is always valid for one computer no matter how many individuals use this computer. If an alternative workstation computer already has a Client Certificate, this one can also be used by the same user after processing request, review, and release by the TTP. Together with the request for secuTrial user accesses, the Client Certificate is a requirement for using secuTrial. How to use secuTrial?, see the secuTrial manual.

**Requirements:**
The workstation computer needs:

- Internet connection (test: https://st03.mi.med.uni-goettingen.de/cgi-bin/WebObjects/productive-DataCapture.woa/wa/choose?customer=DZHK)
- Microsoft Internet Explorer version 8 or later, Firefox version 27 or later or Chrome version 30 or later running on Windows 7 (or later)
- JavaSkript execution must be enable in the browser
- Regarding the encryption methods used for data transmission via web browser, specifications of the data protection officers must be met: The use of TLS 1.2 is required. To determine whether the browser to be used supports this encryption method, you can perform the TLS 1.2 test (see FAQ-Bereich: http://dzhk.de/das-dzhk/klinische-dzhk-studien/3-wissenschaftliche-infrastruktur-des-dzhk/faq/).

**Instructions for installing a Client Certificate:**
Once the Client Certificate has been requested, the TTP will review the request and send the certificate to the requester. The installation of the certificate requires a password, which has to be obtained from the TTP by phone (+49 (0)3834 / 86-7588). You will only receive this information if the phone number on the request form matches the caller's phone number and if the requester is calling himself. Please note that the password must be entered during the installation routine.

For installation of the Client Certificate in the browsers Internet Explorer or Chrome, you have the following options:

- Installation via certificate management (certmgr.msc). Instructions are available under: http://windows.microsoft.com/de-de/windows/import-export-certificates-private-keys#1TC=windows-7;
- Installation using the certificate import wizard. The wizard will open automatically when you double-click the received Client Certificate. Note: If you click “Durchsuchen” (Browse) in the certificate import wizard in order to browse for the Client Certificate, the dialogue “Öffnen” (Open) will only show X.509 certificates by default. If you want to install another type of certificate, you must select it in the corresponding selection field.

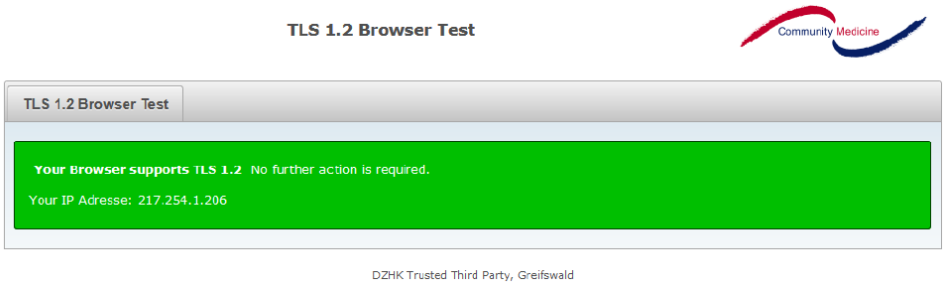
Note: Please note that depending on the browser version, the icons may be displayed differently.

As the Mozilla Firefox browser does not use the Windows certificate memory, a Firefox-specific procedure is necessary to install the Client Certificate. Under the following link, you will find instructions for installation and import: http://security.ag-nbi.de/Projekte/XMLSicherheitsdienste/Demonstrator/de/InstallCertFirefox.html

**Testing the Client Certificate:**

Open the browser for which the certificate has been set up and complete the following steps:

- Open the following website in your web browser to test the encrypted transmission: https://browser-test.med.uni-greifswald.de/
  If you see the following note, the test was successful:




  Note: For browsers such as Internet Explorer 10, internet encryption TLS 1.2 must be enabled manually. The procedure is available under the following link: http://www.guntiahoster.de/blog/2013/allgemein/tls-12-im-browser-aktivieren/
- Open the following website in your web browser to test the Client Certificate: https://test.ths.dzhk.med.uni-greifswald.de/dzhk/html/authenticated.xhtml
  If you see the following note, the test has been successful: