## **3.5 tlsca** (*required for* **TLS**)

**xrd.tlsca noverify** | {**certdir** | **certfile**} *path* [*options*]

*options*: [**crlcheck** {**all** | **external** | **last**}]

[**log** {**failure** | **off**}] [[**no**]**proxies**]

[**refresh** *rint*[**h**|**m**|**s**]] [**verdepth** *vdn*]

**Function**

Configure client certificate verification for transport layer security (**TLS**).

**Parameters**

**noverify**

Disables client certificate verification. All subsequent parameters, if any, are ignored.

**certdir** *path*

*S*pecifies the absolute path of the directory containing trusted **C**ertificate **A**uthority certificates that can be used to verify client certificates. Each file in the directory may only contain a single certificate in **PEM** format. Naming conventions are those required by the version of **OpenSSL** being used. The directory may only be written to by the owner of the directory.

**certfile** *path*

Specifies the absolute path to the file containing one or more trusted **C**ertificate **A**uthority certificates that can be used to verify client certificates. The certificates in the specified file are used first before an attempt is made to find an appropriate certificate in **certdir**, if specified. The file must be in **PEM** format. The file may only be written to by the owner of the file.

**crlcheck**

Specifies the **c**ertificate **r**evocation **l**ist (**crl**) is to be handled. Choose one of the following:

**all** - apply **crl** checking to the complete certificate chain.

**external *-*** **crl** application is handled by an external plug-in (the default).

**last** -apply **crl** checking only to the last certificate in the chain.

**log**Specifies logging requirements. Logging messages are written to the log file. Choose one of the following:

**failure** - log failed verifications (the default).

**off *-*** verification failures are not to be logged.

*vdn* Specifies the verification depth. Should the client present a certificate chain, up to the last *vdn* certificates are verified. Specify a value between 1 and 256, inclusive. The default is 9.

*rint* Specifies the refresh interval. Suffix the value with **h** for hours, **m** for minutes, or **s** for seconds (the default). The default is **8h** (eight hours).

**Defaults**

**xrd.tlsca crlcheck external log failure proxies refresh 8h verdepth 9**

**Notes**

1. You may specify both a directory and a file. The certificates in the **certfile** will be searched before any certificates in **certdir**.
2. If *all* the loaded protocols use strong authentication (e.g. **Kerberos**, **GSI**, or **SSS**) client certificate verification is not necessary as the client will be verified using a strong authentication mechanism and the client’s certificate will only be used to establish a **TLS** connection.
3. Certain protocols require certificate verification (e.g. **HTTPS**). If you enable one of these protocols you should enable verification overall to avoid specifying protocol specific directives that duplicate ones that could be specified using the **tlsca** directive.
4. In the absence of strong authentication, you should always verify client certificates. Generally, you should always verify client certificates. This is why the directive requires that you make an explicit choice.
5. All of the certificates in the directory, as well as the file, must in a format that is recognized by the version of **OpenSSL** being used.
6. If you use a **certdir** be aware that **OpenSSL** requires that the **c\_rehash** utility be run after the certificates in the directory are updated. This introduces a race condition between refreshes and updates to the directory and may produce verification failures should a refresh occur while the directory is being updated. You can avoid this problem by making sure that changes to the directory are visibly done in an atomic fashion.

**Example**

**xrd.tlsca certfile /etc/security/xrootd/cacerts.pem**