TQSLCert-Deutsche Hilfe

Inhaltsverzeichnis

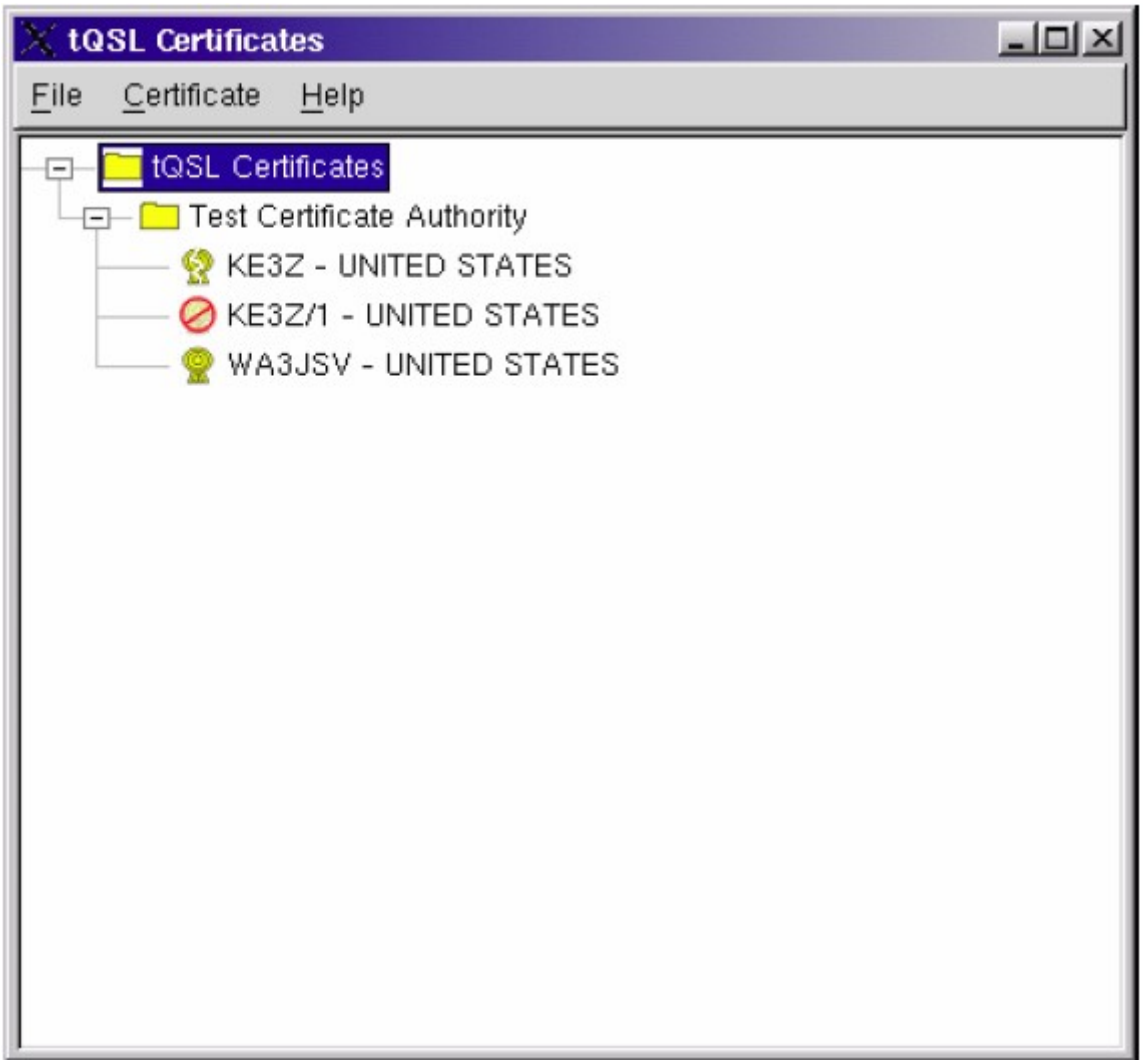
1 Überblick

TrustedQSL (=die sichere QSL) und Systeme, die es verwenden, wie das Welt-Logbuch der ARRL (***LOTW***=Logbook of the World) basieren auf digitalen Sicherheits-Zertifikaten. Das Programmpaket ***TrustedQSL*** besteht aus zwei Teilen, dem Programm ***tqslcert.exe*** zur Anforderung eines Zertifikats und dem TQSL-Dienstprogramm ***tqsl.exe*** zum Absenden eines Logs an das LOTW.
Um an dem TrustedQSL) – System teilnehmen zu können, müssen Sie sich ein Zertifikat beschaffen, dass vom dem System akzeptiert wird. Das Programm ***tQSL cert*** wird benutzt, um ein digitales Zertifikat anzufordern und die erhaltetenen Zertifikate abzuspeichern.
Sie müssen so vorgeben, um ein Zertifikat zu erhalten :

- Nutzen Sie ***tQSLCert*** um eine Anfrage für ein Zertifikat zu erzeugen.
- Senden Sie diese Anfrage an die Organisation, die ein Zertifikat für ihr System ausgibt

- Nehmen Sie das vom Ausgeber erzeugte Zertifikat in Empfang und laden Sie es in ***tQSL cert***

Im Hauptfenster von ***tQSLCert*** sehen Sie, welche Zertifikate Ihnen zur Verfügung stehen. Haben Sie bereits eine Anfrage für ein Zertifikat abgeschickt, aber noch kein vom Ausgeber erwartetes Zertifikat erhalten und geladen, dann steht hinter dem Rufzeichen das Icon 
Gibt es ein Problem mit einem schon geladenen Zertifikat, steht dahinter das Icon  für eine gebrochene Verbindung :



Wenn Sie auf den Eintrag für das Zertifikat mit der linken Maustaste klicken und den Eintrag ***Eigenschaften*** (**Properties)** wählen, sehen Sie diese Liste :

Im Menü Zertifikat (***Certificate***) können Sie mit ***Save*** das Zertifikat abspeichern.

2 Anfrage für ein Zertifikat erzeugen (Generating a Certificate Request)

Zum Start einer Anfrage gehen Sie zum Menüpunkt ***File > New Certificate Request***

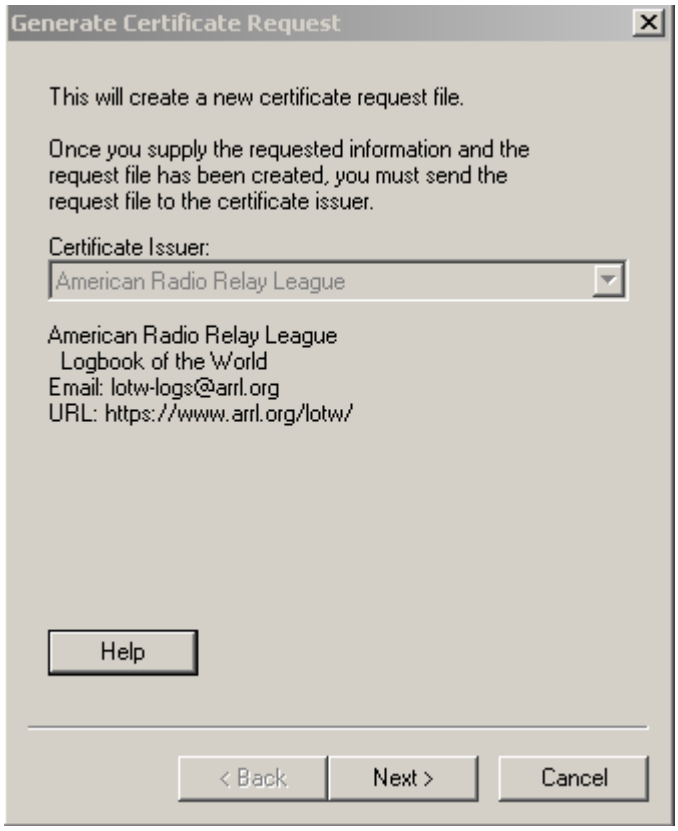
Für die Anfrage müssen Sie folgende Informationen eintragen ::

- Die Bezeichnung des Ausgebers des Zertifikates (ARRl-LOTW ist vorgegeben)
- Das Rufzeichen, für das das Zertifikat gelten soll
- Ihre DXCC-Entity, für die die QSOs zählen sollen
- Ihr Name und Postanschrift
- Ihre Email-Adresse

Wenn Sie schon ein bestätigtes Zertifikat haben, können Sie damit damit eine Anfrage für ein weiteres Zertifikat unterschreiben.

Für die Erzeugung der Anfrage steht Ihnen ein Werkzeug ("wizard") zur Verfügung, mit dem die Eingaben Schritt für Schritt abgefragt werden.

Im ersten Schritt werden Sie gefragt, für welchen Zertifkat-Ausgeber Sie die Anfrage starten wollen. Im Moment ist nur ein Ausgeber, hier die ARRL-LOTW, eingetragen und nicht änderbar.



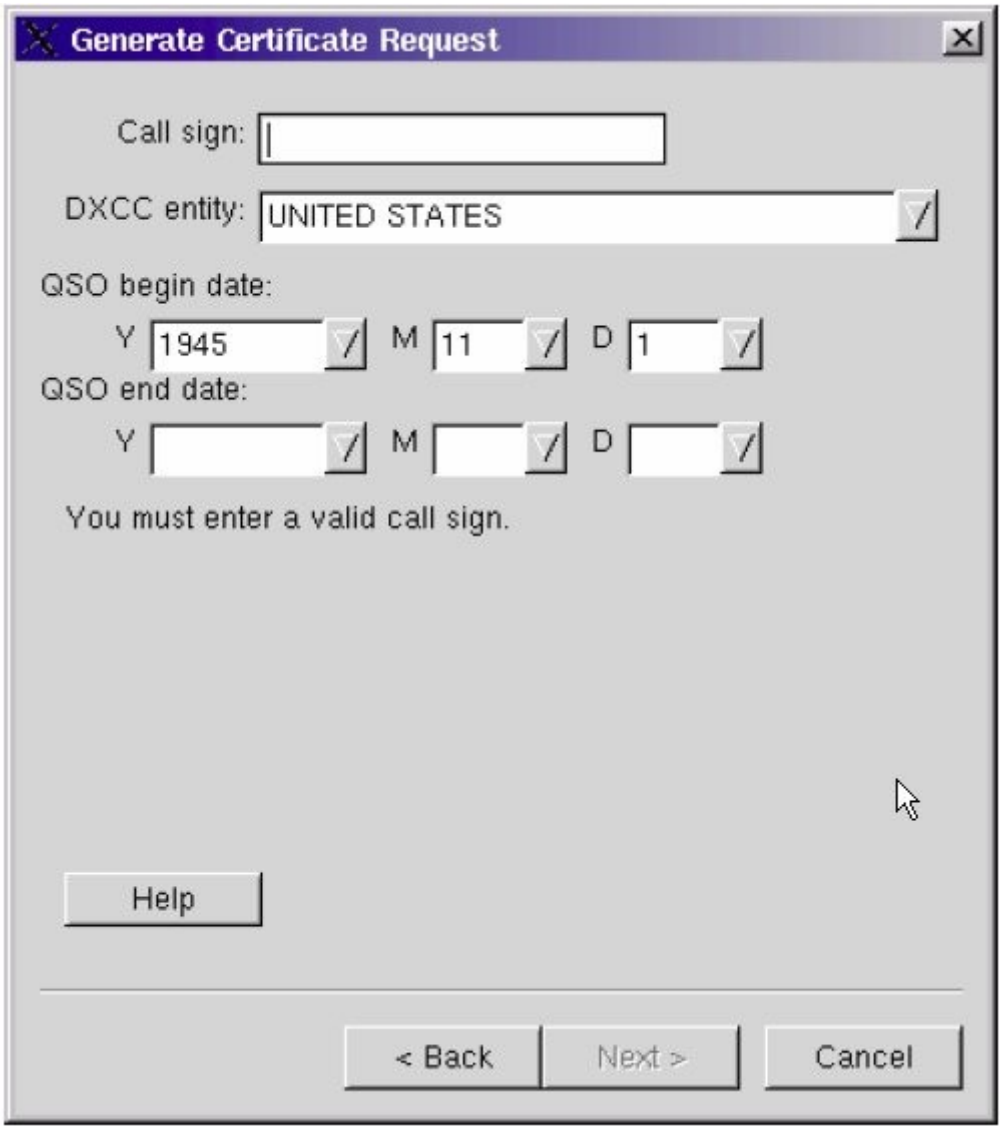
2.1 Rufzeichen, Land und QSO-Daten (Call, DXCC and QSO Dates)

Mit ***> Next*** kommen Sie zur nächsten Seite. Hier tragen Sie Ihr Rufzeichen, Ihre DXCC-Entity und den Zeitbereich für Ihre QSOs ein.

> *Hinweis DM3ML* : Sie müssen für jedes Rufzeichen ein neues Zertifikat beantragen. DM3ML ist nicht gleich DM3ML/P oder PA/DM3ML.
> Als DXCC-Entity müssen DL-Stationen nach dem 3.10.1990 den Eintrag ***Federal Republic of Germany (ADIF-Nummer 230)*** wählen. *Germany* und German *Democratic Republic* sind „deleted countries“, sie sind nur dann zu wählen, wenn QSOs vor dem 3.10.1990 nach LOTW transportiert werden sollen. Mein Call DM3ML von 1962 bis 1964 (DXCC-Entity : Germany) ist nicht identisch mit DM3ML ab Oktober 1998 (DXCC-Entity : Federal Republic of Germany) oder dem Clubrufzeichen DM3ML September 1973 bis Dezember 1979 (DXCC-Entity : German Democratic Republic).
> Nachsatz (22.08.07) auf Anregung von Andre, DL3DUE : Wollen Sie QSOs unter einem Y-Rufzeichen ab dem 3.10.1990 bis zur Ausgabe der D-Rufzeichen Ende Oktober 1991 an das LoTW melden, müssenSie ein getrenntes Zertifikat mit der Landesbezeichnung ***Federal Republic of Germany (ADIF-Nummer 230)*** beantragen.

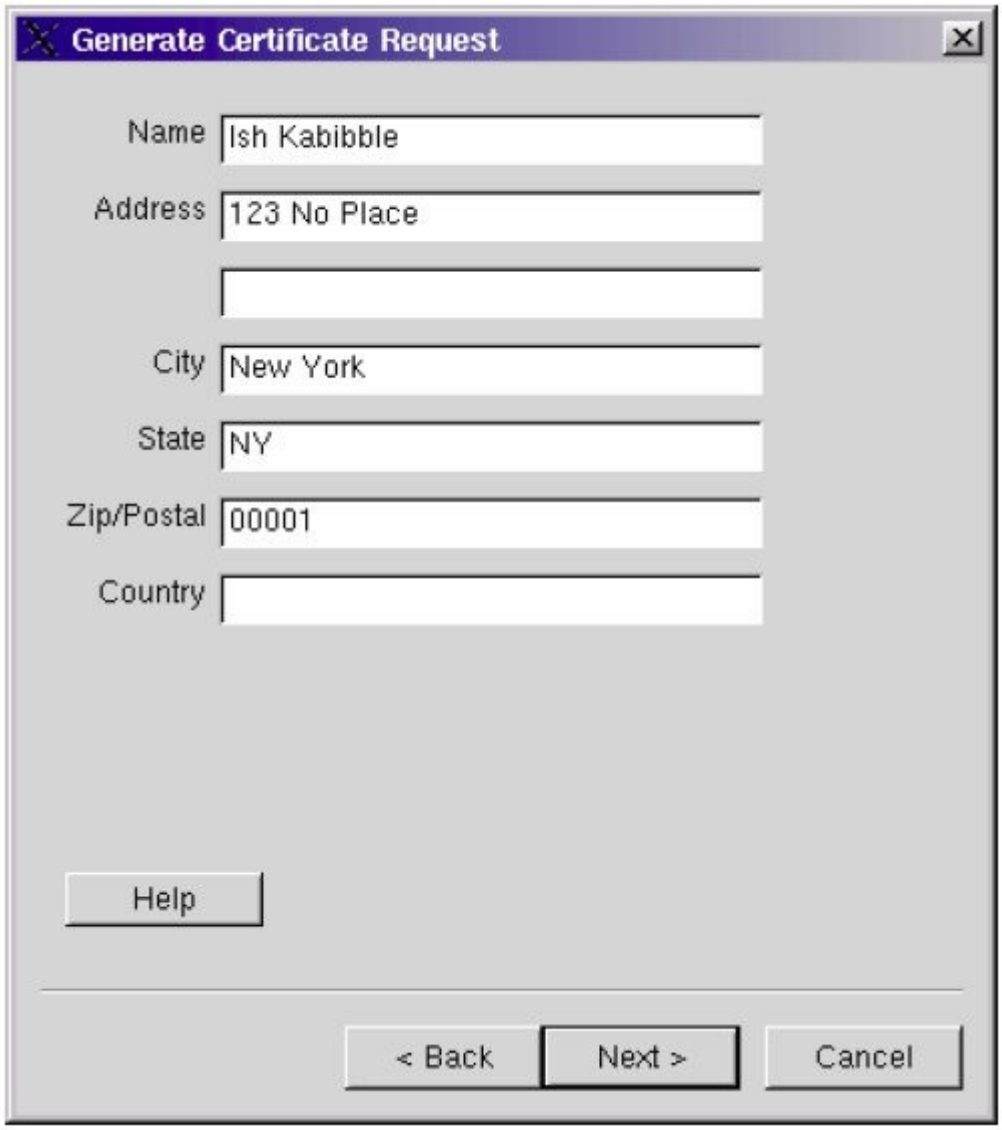
Üblicherweise tragen Sie für ***QSO begin date*** den Tag der Lizenzausgabe für Ihr Rufzeichen ein. Unter ***QSO end date*** brauchen Sie in aller Regel nichts einzutragen, es sei denn, Sie wissen schon wann Ihre Lizenz ausläuft oder wenn Sie eine Lizenz nur eine befristete Zeit in Ihrem Besitz hatten.

Hinweis DM3ML : Ihre abgeschickten Logs dürfen nicht älter als ***QSO begin date*** sein, brauchen aber nicht so weit zurück reichen.



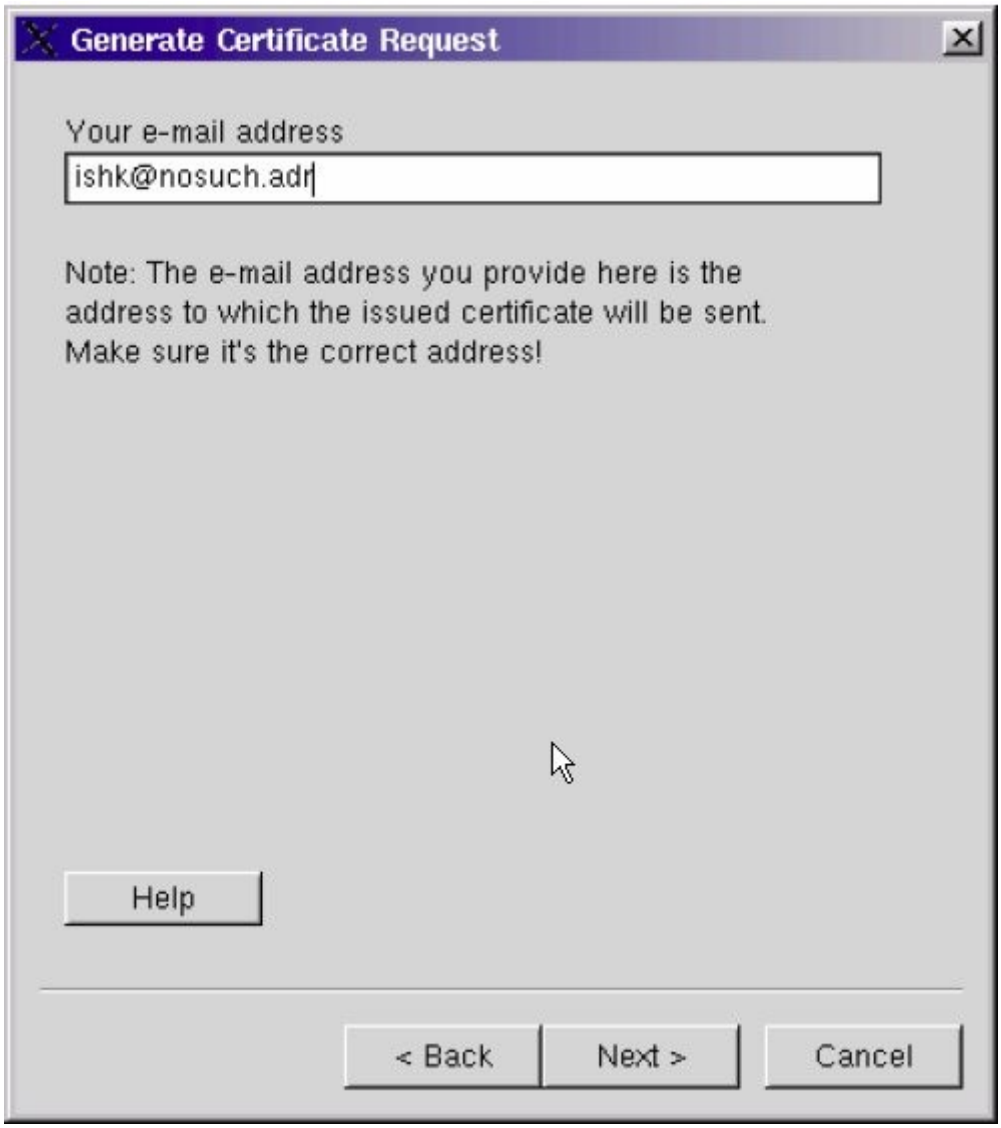
2.2 Name und Adresse (Name and Address)

Sie müssen Ihren vollen Namen und Ihre Adresse eintragen. Anhand der von Ihnen einzusendenden Dokumente überprüft ARRL-LOTW Ihre Identität. Für US-Funkamateure wird die Übereinstimmung mit der FCC-Datenbank überprüft.



2.3 Email-Adresse (Email Address)

Sie erhalten das Zertifikat und Ihr Zugangspasswort zum LOTW per Email. Die Email wird an die Adresse geschickt, die Sie bei der Anfrage eingeben, NICHT an die Email-Adresse, von der sie die Anfrage abschicken. Eine korrekte Email-Adresse ist Voraussetzung dafür, dass Sie das Zertifikat erhalten :



2.4 Passwort (Password)

Sie können den privaten Schlüssel (private key) für die Anfrage für das Zertifikat mit einem Passwort schützen. Jedesmal, wenn Sie das erhaltene Zertifikat für die Kodierung eines Logs als digitale Unterschrift nutzen wollen, werden Sie dann nach dem Passwort gefragt.. Wir empfehlen Ihnen, das Zertifikat durch ein Passwort zu schützen, damit niemand der direkt oder über ein Netzwerk Zugriff zu Ihrem Rechner hat, Ihr Zertifikat missbrauchen kann.
Sichern Sie das Wort an einem sicheren Ort. Es gibt keine Möglichkeit, dass Passwort wiederherzustellen, wenn Sie es vergessen haben. Das Passwort bleibt dem Ausgeber des Zertifikats verborgen und er kann Ihnen bei einem Verlust des Passworts nicht helfen.
Lassen Sie die Eingabefelder frei, wenn Sie kein Passwort verwenden wollen.

2.5 Anfrage unterschreiben (Signing)

Ihre erste Anfrage ist ***Unsigned*** . Haben Sie schon ein Zertifikat, können Sie es als Unterschrift (***Signed***) für weitere eigene Rufzeichen als verwenden***.***

Ausgeber können verlangen, das zusätzliche Zertifikate für die gleiche Person von dieser unterschrieben werden müssen. Beim ARRL-Welt-Logbuch LOTW werden dadurch keine weiteren Dokumente benötigt. Der Zugriff zu der LOTW-Webseite kann für verschiedene Rufzeichen mit dem gleichen Passwort erfolgen.
Sie sollten daher, wenn Sie schon ein Zertifikat haben, dieses beim Beantragen weiterer Zertifikate als Unterschrift benutzen.
Wählen Sie als Unterschrift (***Signed***) durch einen Mausklick ein schon erteiltes Zertifikat. Haben Sie das Zertifikat mit einem Passwort geschützt, werden Sie nach dem Passwort gefragt.

3 Anfrage abschicken (Sending a Certificate Request)

Nach dem letzten Schritt des Wizards wird eine Datei ***<call>.tq5*** erzeugt. Diese Datei müssen Sie per Email an den Ausgeber des Zertifikats für ***TrustedQSL*** schicken. **tQSLCert** zeigt Ihnen ein Fenster mit der Adresse für die Anfrage nach einem Zertifikat.

> *Hinweis DM3ML* : Die Adresse lautet lotw-logs@arrl.org. Betreff und Text können freibleiben. Die Datei ***<call>.tq5*** ist als Anhang zu schicken.

Sie sollten die Datei gut aufheben und getrennt vom Rechner auf einer Diskette oder einer CD aufbewahren, da Sie sie für das eigentliche Zertifikat benötigen. Der Ausgeber des Zertifikat schickt Ihnen nach erfolgreicher Bearbeitung eine Datei **<call>.tq6**. Erst mit dieser Datei wird TQSL arbeitsfähig.

> *Hinweis DM3ML* : Ausländische Funkamateure müssen an die ARRL per Post eine Kopie Ihrer Lizenzurkunde und eine Kopie eines Ausweises (Reisepass, Personalausweis oder Fahrerlaubnis) schicken. Die Daten des Ausweises und

der Lizenzurkunde werden mit der Email-Anfrage abgeglichen. Die ARRL-Adresse lautet :

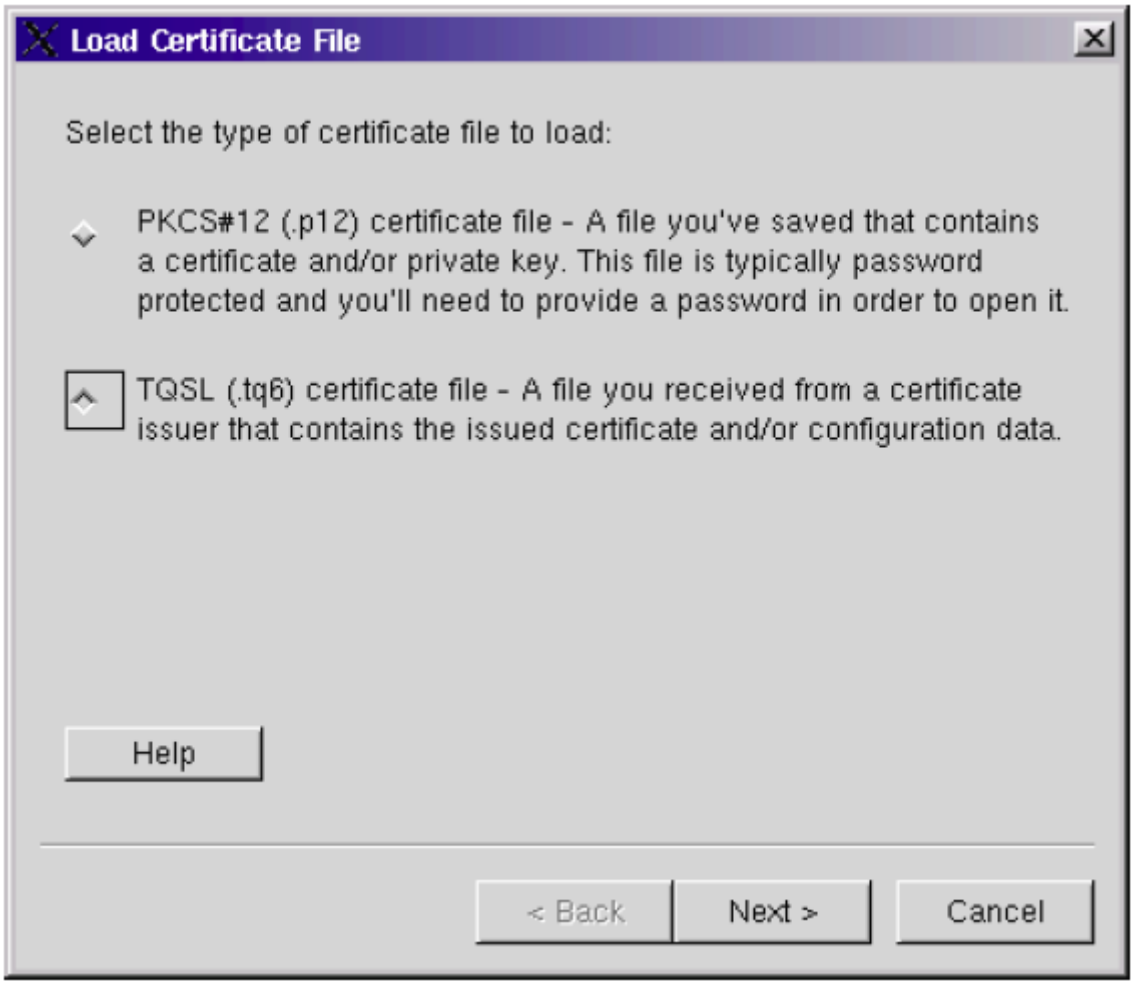
Logbook Administration
ARRL
225 Main Street
Newington, CT 06111
USA

Ich (DM3ML) habe eine Kopie meiner Fahrerlaubnis geschickt.. Nach etwa 14 Tagen kam eine Email mit meinem Passwort zum ***Logon*** in das LOTW und die Datei DM3ML.tq6.

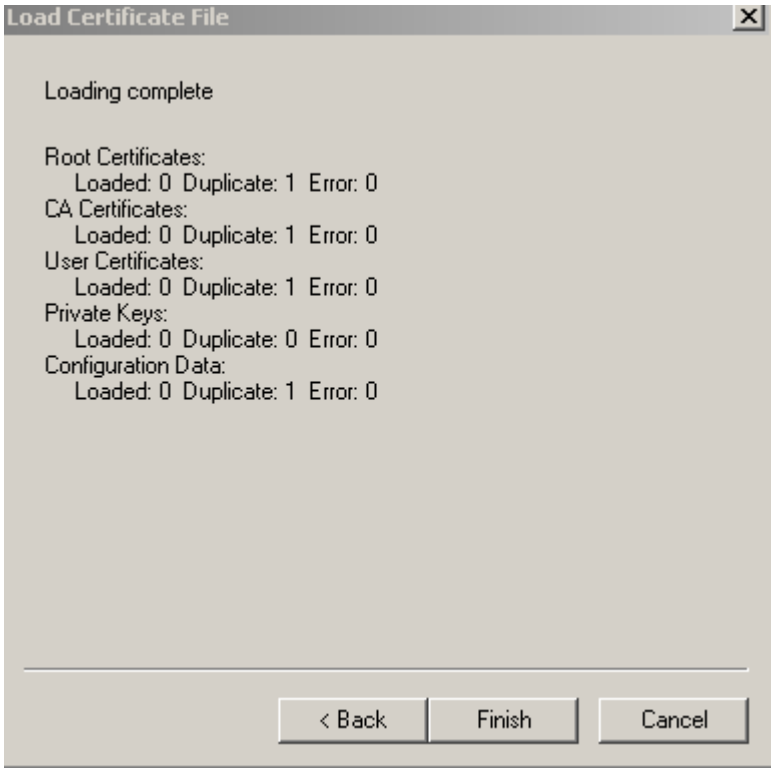
4 Zertifikate laden (Loading a Certificate File)

Haben Sie die Datei ***<call>.tq6*** erhalten, kopieren Sie sie in das Unterverzeichnis **Certificates** und gehen Sie zum Menü **File** > **Load Certificate File.** Mit diesem Menü können Sie zwei Arten von Dateien laden :

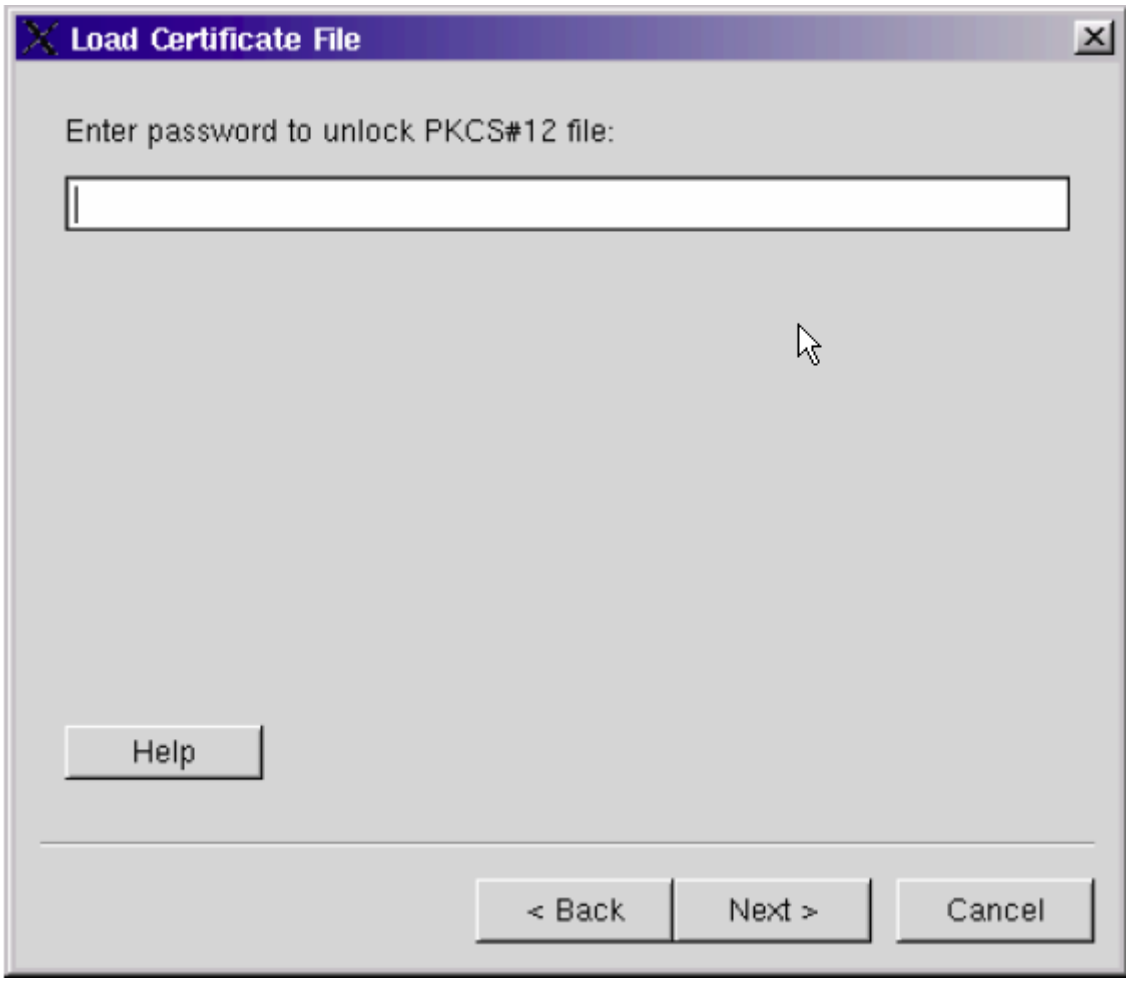
- PKCS#12 (.p12) certificate file : Diese Datei wird erzeugt, wenn Sie existierenden Zertifikate über das Menü ***Certificate > Save*** als Datei ***<call>.p12*** gesichert haben
- TQSL (.tq6) certificate file : Die Datei ***<call>.tq6*** erhalten Sie vom Ausgeber des Zertifikates als Email-Anhang als Antwort auf eine Email-Anfrage und erfolgter Authentifizierung (siehe oben)



Treffen Sie Ihre Wahl (beim Start die zweite Möglichkeit) und klicken Sie auf **Next.** . Wählen Sie aus der Verzeichnisübersicht das Unterverzeichnis ***Certificates*** und dort die Datei ***<call>.tq6***. Nach der Anwahl wird die Datei unmittelbar verarbeitet und das Ergebnis angezeigt (*hier ein zweiter Durchlauf (duplicate) bei DM3ML*). :



Eine PKCS#12 – Datei ist in der Regel durch ein Passwort geschützt. Haben Sie den Import einer PKCS#12 – Datei gewählt, werden Sie nach dem Passwort gefragt , ehe die Datei entschlüsselt (unlocked) werden kann. Sie müssen daher das richtige Passwort eingeben :



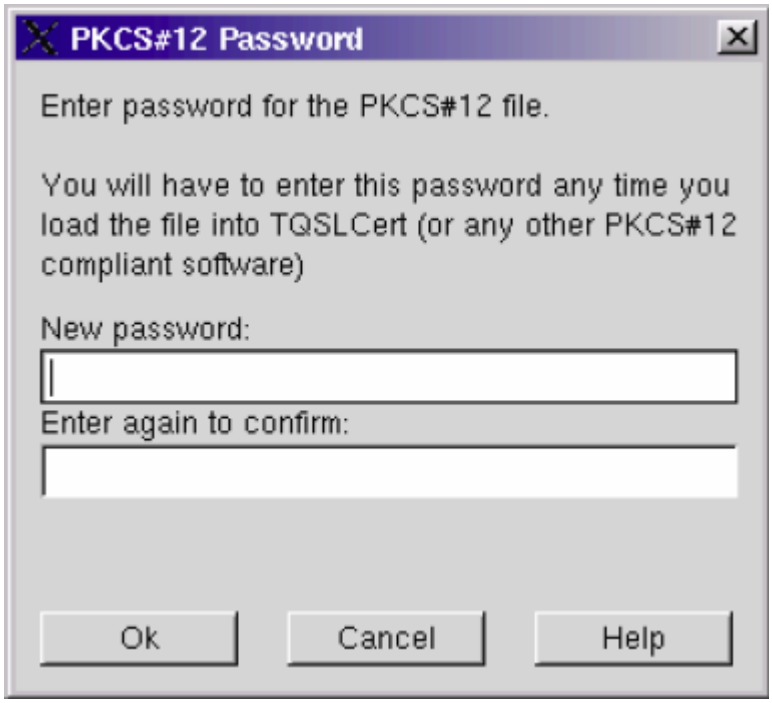
Falls die PKCS#12 – Datei einen privaten Schlüssel (private key) enthält, haben Sie die Möglichleit ein neues Passwort zum Schutz der Schlüssels zu setzen (***set a password***) . Sie können das Passwort mit dieser Eingabe ändern :

Es ist eine gute Idee einen privaten Schlüssel mit einem Passwort zu schützen, Sie müssen es aber nicht unbedingt tun. Wenn Sie die Eingabefelder freilassen und auf ***OK*** klicken, wird der Schlüssel ohne Passwort gespeichert. Im Ergebnis dieses Aktion wird dann ***results0*** als Ergebnis ausgegeben.

5 Zertifikat speichern (Save Certificate)

Sie können das/die Zertifikat(e) mit dem Menüpunkt **Certificate > Save** zusammen mit dem privaten Schlüssel in einer PKCS#12 – Datei (***<call.p12>***) speichern. Diese Datei kann unter **tQSLCert** mit dem Menüpunkt **File > Load Certificate File** wiederhergestellt werden. PKCS#12 ist ein Standardformat für digitale Zertifikate, das auch in andere kompatible Systeme wie Microsoft *Windows* geladen werden kann.

Mit diesem Menü können Sie das Passwort für die PKCS#12 – Datei ändern :



Wir empfehlen Ihnen ein Passwort zum Schutz Ihrer Identität und gegen Missbrauch. Sie können auch ohne Passwort arbeiten, sind aber in jedem Fall für den Missbrauch Ihres Zertifikats verantwortlich.

Hinweis : Falls der private Schlüssel für Zertifikat passwortgeschützt ist, müssen Sie zur Entsperrung ein Passwort eingeben, um das Zertifikat in einer PKCS#12 – Datei abspeichern zu können.

Hinweis : : Die abgespeicherte PKCS#12 – Datei entält jeweils ein einzelnes Zertifikat. Falls Sie mehr als ein Zertifikat haben, müssen Sie sie in getrennten PKCS#12 – Dateien ablegen.

Hinweis DM3ML : Heben Sie Ihre <call>.p12-Datei(en) gut auf. Wenn Sie TQSL auf einem neuen Rechner einrichten wollen, benötigen Sie diese Dateien. Eine

Neueinrichtung aus einer Kombination von <call>.tq5 mit der erhaltenen Datei <call>.tq6 funktioniert nicht.

6 Privatschlüssel öffnen (Unlock Private Key)

Ist der private Schlüssel passwortgeschützt, muss er mit dieser Eingabe für den Zugriff geöffnet werden :

Bei **tQSLCert** müssen Sie den privaten Schlüssel immer dann öffnen, wenn sie ein mit dem Schlüssel geschütztes Zertifikat sichern (***save***) wollen oder ein existierendes Zertifikat als Unterschrift verwenden wollen .

7 Stichwortverzeichnis (TrustedQSL Glossary)

ADIF (Amateur Data Interchange Format) : Format zum Datenaustausch zwischen Logprogrammen- Siehe http://www.hosenose.com/adif/ zu Details.

Cabrillo : Format für Contest-Logs. Siehe http://www.kkn.net/~trey/cabrillo/ zu Details .

Digital Certificate : Eine Datei mit einem einmaligen Satz von Schlüsseln zur Erzeugung von digitalen Signaturen

Digital Signature : Datenblock mit einer einmaligen Kombination eines Datenblocks aus Text und/oder Daten und eines digitalen Zertifikats. Das Programm von ***TrustedQSL*** kann sicherstellen, dass die eingeschickten Daten vom Inhaber des Zertifikats stammen und nach der digitalen Unterschrift (***signing***) nicht verändert wurden.

Signing : Erzeugen einer digitalen Signatur **(Digital Signature)** eines Datenblock aus Text und/oder Daten. Unter ***TrustedQSL*** werden die QSO-Daten signiert (**signed***)*.

Station Location : Beschreibt die Stationsdaten mit Rufzeichen, geographischer Lage, politischer und DXCC-Zuordnung. Zu einem Rufzeichen können bei mobil- oder portable-Betrieb mehrere ***Station Locations*** gehören.