

CR220N-Fernwartung über ein DSL-Modem

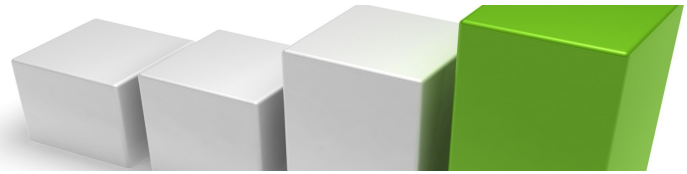
1. Allgemeines

In der Internet-Fernwartung wird es immer wichtiger, nicht nur einzelne IP-Adressen anzusprechen, sondern ein ganzes IP-Subnetz fernzuwarten. Der VPN-Router CR220N stellt ein solches Fernwartungs-Subnetz auf seinem LAN1-Interface zur Verfügung. Alle Netzwerkteilnehmer, die mit diesem Interface verbunden sind, nehmen an der Fernwartung teil. Es handelt sich um ein Klasse-C-Subnetz, das heißt, es können bis zu 252 Netzwerkteilnehmer ferngewartet werden. Das Fernwartungs-Subnetz ist frei konfigurierbar, indem die LAN1-IP-Adresse durch den Anwender konfiguriert wird.

Es können alle IP-Protokolle verwendet werden, also nicht nur TCP, sondern beispielsweise auch UDP und ICMP. Das ist für die Inbetriebnahme hilfreich, da somit alle fernzuwartenden Netzwerkteilnehmer auch per „ping-Befehl“ erreicht werden können.

Als Fernwartungs-Client dient ein PC, der ebenfalls mit dem Internet verbunden wird. Die Fernwartungs-Verbindung zwischen PC und CR220N ist durch einen OpenVPN-Tunnel gesichert. Damit ist die Übertragung der Anwenderdaten nach dem neuesten Stand der Technik gegen Fremdzugriffe geschützt. Als VPN-Vermittler arbeitet, für den Anwender unsichtbar, ein schneller OpenVPN-Server im Internet, der „ISK-CRASER“. Für eine komfortable Subnetz-Fernwartung nach heutigem technischen Stand ist die Vermittlung über den „ISK-CRASER“ unumgänglich. Dafür sprechen 3 gewichtige Gründe:

1. CRASER ist 24h Online und hat die Leistungsfähigkeit moderner Serversysteme. Dadurch wird eine gleichzeitige und sichere Kommunikation mit sehr vielen Clients möglich.
2. CRASER ist ein Open-VPN-Server mit einer festen IP-Adresse: Sowohl der Fernwartungs-PC als auch der Fernwartungsrouter melden sich als VPN-Client an. Damit ist weder beim Fernwartungs-PC noch beim Fernwartungsrouter eine public IP-Adresse bzw. eine feste IP-Adresse erforderlich.
3. CRASER kann Open-VPN-Verbindungen routen: Das bedeutet, der Fernwartungs-PC kann mit einer einzigen Open-VPN-Verbindung auch Fernwartungs-Subnetze mehrerer CR220N/CR230U gleichzeitig erreichen und die Fernwartungs-Subnetze mehrerer CR220N/CR230U können auch untereinander kommunizieren. Bei Bedarf sind mehrere Fernwartungs-PCs mit unterschiedlichen Zertifikaten möglich. Maximal 64 Fernwartungs-Subnetze lassen sich nach diesem Prinzip gleichzeitig durch den CRASER vermitteln. Die Zugriffsrechte aller Clients können variiert werden.



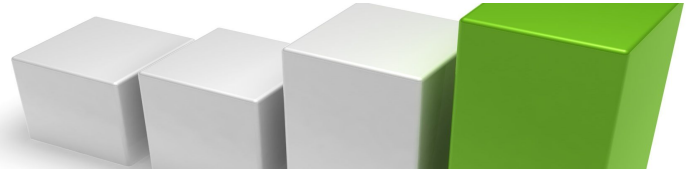
2. Aufgabenstellung

Der VPN-Router CR220N soll mit dem DSL-Modem AM100 verbunden werden und den Aufbau einer Internetverbindung über das Modem steuern. Die ISP-Zugangsdaten sollen im CR220N konfiguriert werden, das Modem AM100 verbleibt in der Werkseinstellung.

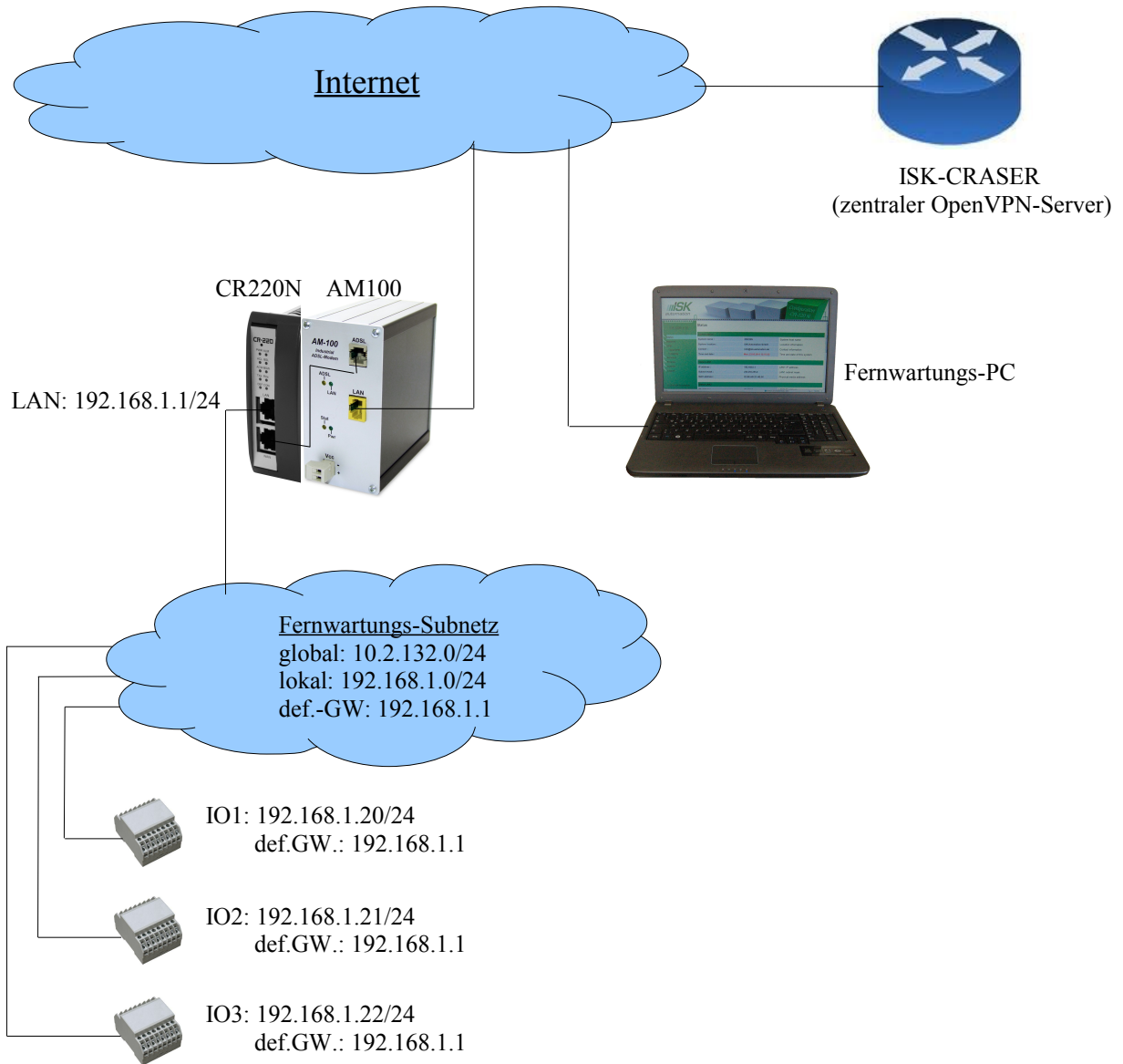
Daraufhin soll eine Verbindung zwischen einem Fernwartungs-PC und dem Fernwartungs-Subnet des CR220N über das Internet in Betrieb genommen werden. Diese Inbetriebnahme erfolgt in 6 Schritten:

1. Kabelverbindungen vorbereiten.
2. Fernwartungs-Subnetz (LAN1) auf eine zur Anwendung passende IP-Adresse konfigurieren und DSL-Betriebsart für LAN2 aktivieren.
3. WAN-Interface für DSL konfigurieren.
4. OpenVPN auf dem CR220N aktiv schalten und Verbindung zum CRASER herstellen.
5. Fernwartungs-PC konfigurieren und eine OpenVPN-Verbindung zum CRASER aufbauen.
6. Fernwartungs-Subnetz durch ping-Kommandos von der Konsole des Fernwartungs-PCs testen.

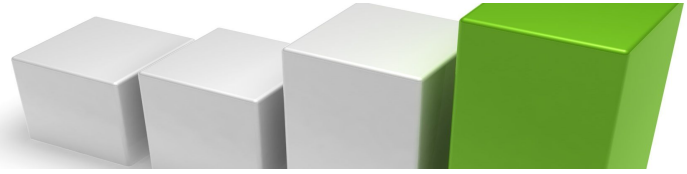
Werfen wir zunächst einen Blick auf die Netzwerkstruktur unserer Anwendung, bevor wir die 6 Schritte zur Inbetriebnahme abarbeiten:



3. Netzwerkstruktur der Fernwartung mit Beispieladressen



Testzugriffe: PC → CR220N: ping 10.2.132.1 (globaler Zugriff)
 PC → IO1: ping 10.2.132.20 (globaler Zugriff)
 PC → IO2: ping 10.2.132.21 (globaler Zugriff)
 PC → IO3: ping 10.2.132.22 (globaler Zugriff)
 IO1 → IO2: ping 192.168.1.21 (lokaler Zugriff)



Tipp1: Ein globaler Zugriff ist ein Zugriff auf ein Fernwartungs-Subnetz über das Internet.
Ein lokaler Zugriff ist ein Zugriff innerhalb eines Fernwartungs-Subnetzes.

Tipp2: Die globale IP-Adresse Ihres Fernwartungs-Subnets ist für jeden am CRASER arbeitenden Router einmalig und ist bereits auf Ihrem Router vorkonfiguriert (siehe Routerkonfigurationsmenü: VPN → OpenVPN → p12-certificate).

Tipp3: So finden Sie die Zieladresse für einen globalen Zugriff auf den Teilnehmer „IO1“ Ihres Fernwartungs-Subnetzes:

globale Adresse des Fernwartungs-Subnetzes:	10.2.132.0/24
gesuchte Zieladresse:	→ 10.2.132.20
lokale Adresse des Teilnehmers IO1:	192.168.1.20/24

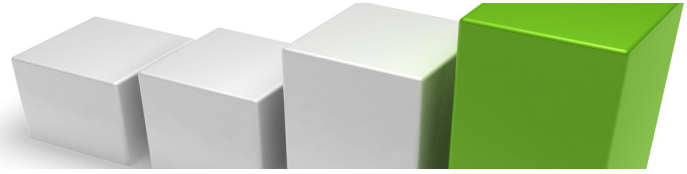
Tipp4: Durch die Zuordnung der globalen IP-Adresse zur lokalen IP-Adresse des Fernwartungs-Subnetzes können Sie die lokale IP-Adresse frei konfigurieren, ohne Rücksicht auf später hinzukommende Fernwartungs-Subnetze nehmen zu müssen.

Tipp5: Die Teilnehmer des Fernwartungs-Subnets können das Internet benutzen. Eine Sperrung dieser Funktion ist durch Laden einer speziellen Firewalldatei möglich. Bei Bedarf stellen wir Ihnen diese Datei zur Verfügung.

4. Checkliste zur Inbetriebnahme eines Fernwartungs-CR220N über ein DSL-Modem

Ausgangszustand:

- ISK-Automation liefert einen für Fernwartungszwecke vorkonfigurierten CR220N. Das OpenVPN-Zertifikat und die Firewalldatei sind bereits installiert.
- ISK-Automation liefert die OpenVPN-Konfigurationsdateien für den Fernwartungs-PC. Für das Projekt2, PC1 der Firma ISK-Automation würde diese Datei „ISK-P2-PC1.zip“ heißen.



Inbetriebnahme des Fernwartungsrouters CR220N über ein DSL-Modem in 6 Schritten:

1. Vorbereitungen

- Das mit "LAN" bezeichnete Interface wird mit dem Fernwartungs-Subnetz verbunden.
- Das mit "WAN" bezeichnete Interface wird mit dem DSL-Modem verbunden.
- Die Alias-Adresse kann genutzt werden, um den CR220N während der Netzwerkkonfiguration ohne Umschaltung des PC-Subnets ansprechen zu können.
- Web-Konfiguration des "CR220N" aufrufen: <http://192.168.0.126:7777>
- login: admin

2. lokale Fernwartungs-Subnetzadresse konfigurieren: (siehe Bild1)

Network → LAN → LAN1:

- IP address: 192.168.1.1 (Beispiel, die lokale Fernwartungsadresse können Sie selbst festlegen)
- Subnet mask: 255.255.255.0 (die Subnetzmaske muss auf 255.255.255.0 konfiguriert werden).

Network → LAN → LAN2:

- Use device for DSL: aktivieren (ist in Werkseinstellung bereits aktiviert, also nur überprüfen).
- Apply-Schalter betätigen.

3. WAN-Interface konfigurieren. (siehe Bild2)

Network → WAN → DSL activation:

- DSL Enable/Disable: enable

Network → WAN → ISP settings:

- Login name: 001xxxxxxxxxxxxxxxxxxxxxxxx0001@t-online.de (Beispiel)
- Password: xxxxxxxx
- Confirm password: xxxxxxxx

Network → WAN → Connection settings:

- Connect type: System start, always reconnect
- Apply-Schalter betätigen.

4. OpenVPN-Client aktivieren. (siehe Bild3)

VPN → OpenVPN:

- Enable/Disable OpenVPN: aktivieren
- "Apply" betätigen
- die Verbindung zum CRASER baut sich nach einigen Sekunden auf. Während des Verbindungsaufbaus blinkt die CON-LED. Nachdem die Verbindung aufgebaut ist, leuchtet die CON-LED statisch.

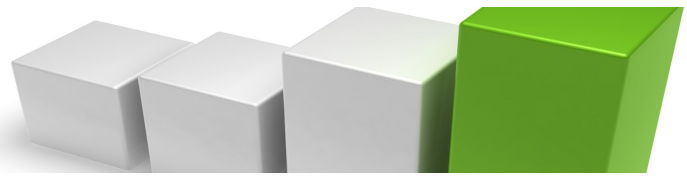
5. OpenVPN-Client auf dem Fernwartungs-PC konfigurieren und starten.

OpenVPN-Client nach unserer Anleitung „VPN_PC_Client_Install.pdf“ auf dem Fernwartungs-PC installieren und mit dem zu diesem Router gelieferten PC-Zertifikatpaket konfigurieren. Danach den OpenVPN-Client auf dem Fernwartungs-PC starten.

6. Subnet des CR220N vom Fernwartungs-PC her pingen:

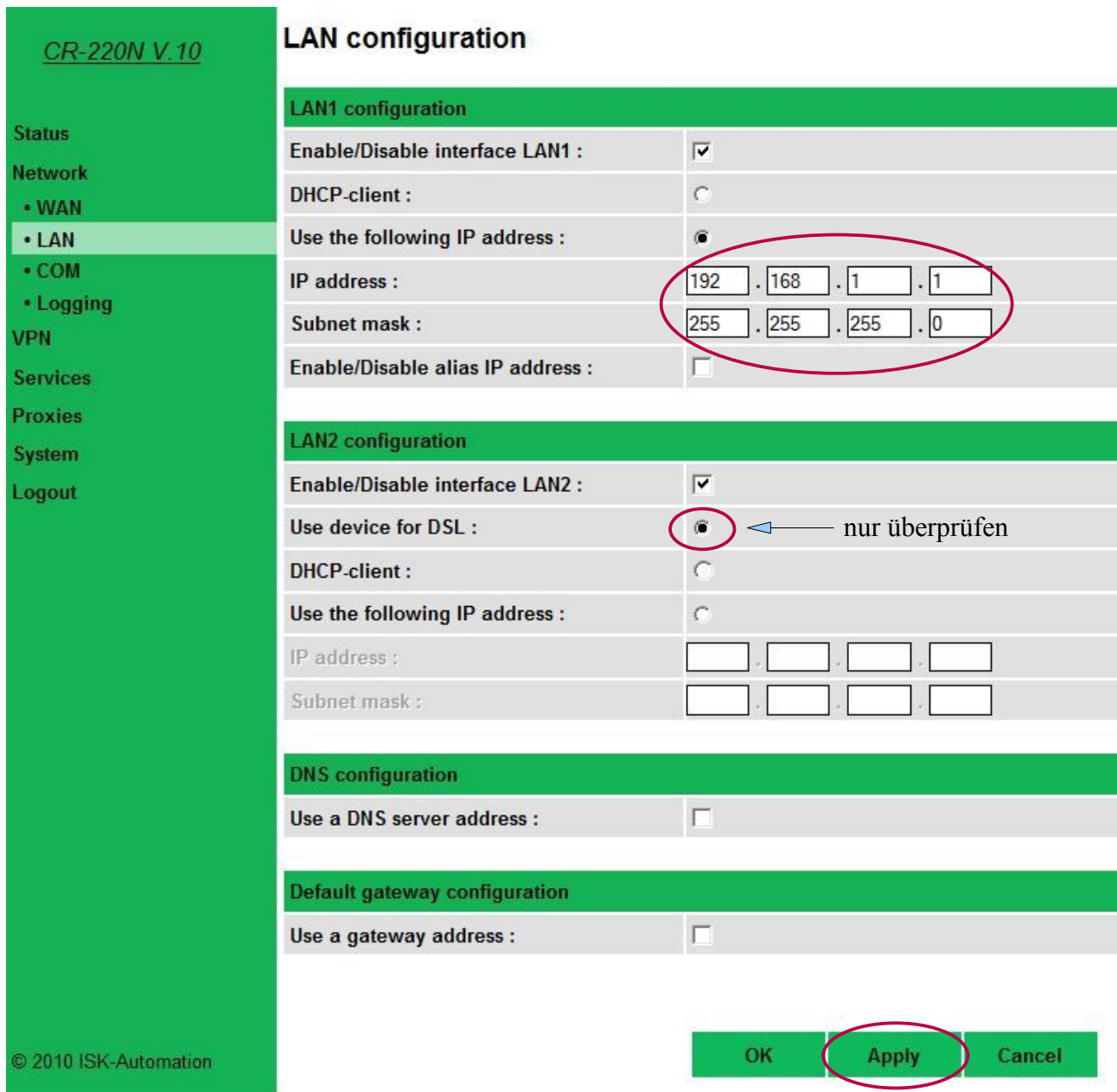
ping-Befehle siehe Kapitel 3 dieser Dokumentation.

Achtung: Benutzen Sie bei den ping-Befehlen die globale Subnetzadresse Ihres konkreten Fernwartungs-Subnetzes. Diese Adresse ist auf Ihrem Router schon vorkonfiguriert. Sie finden sie unter VPN → OpenVPN → p12 certificate.



5. Darstellung der zugehörigen Konfigurationsseiten zum Kapitel 4 dieser Doku

Bild 1 lokale Fernwartungs-Subnetadresse (LAN1) konfigurieren:



CR-220N V.10

Status

Network

- WAN
- LAN
- COM
- Logging

VPN

Services

Proxies

System

Logout

LAN configuration

LAN1 configuration

Enable/Disable interface LAN1 :

DHCP-client :

Use the following IP address :

IP address : 192 . 168 . 1 . 1

Subnet mask : 255 . 255 . 255 . 0

Enable/Disable alias IP address :

LAN2 configuration

Enable/Disable interface LAN2 :

Use device for DSL : ← nur überprüfen

DHCP-client :

Use the following IP address :

IP address : [] . [] . [] . []

Subnet mask : [] . [] . [] . []

DNS configuration

Use a DNS server address :

Default gateway configuration

Use a gateway address :

© 2010 ISK-Automation

OK Apply Cancel

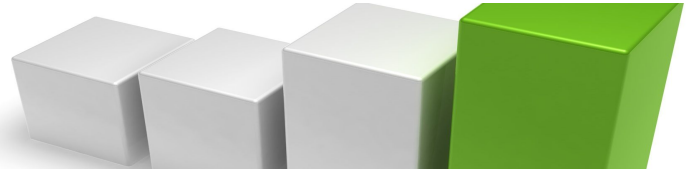


Bild 2 WAN-Interface konfigurieren:

CR-220N V.10 Status Network <ul style="list-style-type: none">• WAN• LAN• COM• Logging VPN Services Proxies System Logout	WAN configuration
	DSL activation
	DSL Enable/Disable: <input type="text" value="enable"/>
	ISP settings
	Login name : <input type="text" value="001xxxxxxxxxxxxxxxxxxxxxxxxxxxx0001@t-online.de"/>
	Password : <input type="password" value="....."/>
	Confirm password : <input type="password" value="....."/>
	DNS : <input type="text" value="Automatic"/>
	Gateway : <input type="text" value="Automatic"/>
	Connection settings
Connect type : <input type="text" value="System start, always reconnect"/>	
Manuell test : <input type="button" value="Connect"/> <input type="button" value="Disconnect"/>	
Connection State : Connected	
<input type="button" value="OK"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

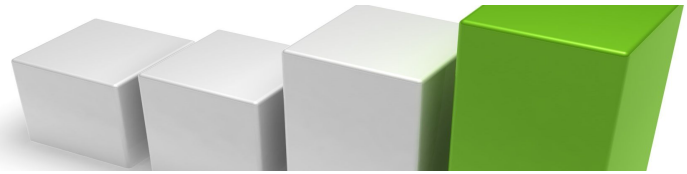


Bild 3 OpenVPN aktivieren:

CR-220N V.10

OpenVPN configuration

OpenVPN configuration	
Enable/Disable OpenVPN :	<input checked="" type="checkbox"/>
Work as :	<input type="radio"/> Server <input checked="" type="radio"/> Client
Status :	Running

OpenVPN client configuration

Server address :	<input type="text" value="83.169.44.109"/>
Protocol :	<input checked="" type="radio"/> UDP <input type="radio"/> TCP
Port :	<input type="text" value="1194"/>
VPN compression :	Enable ▾

OpenVPN certificates and keys

Authentication :	<input type="text" value="p12-Certificate"/>
P12-certificate :	<input type="text" value="ISK-P2-NET5(10.2.132.0).p12"/> <input type="button" value="Info"/>
Import p12-certificate :	<input type="text"/> <input type="button" value="Durchsuchen..."/> <input type="button" value="Import"/>

OK Cancel