Documentation : Installation manuelle des logiciels BEWAN RPV avec Admin PKI

Sommaire

1. Introduction

Le canton de Berne utilise une technologie RPV fondée sur Cisco qui permet à un-e agent-e cantonal-e de se connecter à BEWAN. L'authentification de l'utilisateur final est réalisée à l'aide d'un certificat numérique qui est enregistré sur un jeton USB protégé par un numéro d'identification personnel (NIP). Le jeton USB (fabriqué par la société Aladdin) et le certificat qu'il contient sont établis et fournis par la société Connectis. Le certificat utilisateur est signé numériquement avec un certificat racine de Connectis. Le certificat racine utilisé pour la signature expirera le 16 septembre 2009, de sorte que tous les certificats (certificats utilisateur, machine et routeur) signés avec celui-ci perdront aussi leur validité à cette date.
En conséquence, ces certificats ne permettront plus d'établir la connexion RPV à partir du 16 septembre 2009.
Techniquement, il n'est pas possible de prolonger le certificat racine sans remplacer tous les certificats signés avec celui-ci, ce qui implique qu'il faut aussi échanger tous les jetons USB contre de nouveaux.
De ce fait, il a été décidé de remplacer les certificats de Connectis par des certificats ADMIN PKI.

2. Situation technique actuelle

La connexion RPV à BEWAN est établie par l'intermédiaire du client RPV Cisco.
Pour réaliser l'authentification sur le concentrateur RPV de BEWAN, le client RPV a besoin du certificat utilisateur qui est enregistré sur le jeton USB de la société Aladdin.

Le tableau ci-dessous décrit les composants logiciels qui sont nécessaires sur un ordinateur portable ou de bureau. Dans le canton de Berne, les logiciels sont distribués par l'intermédiaire de Reno. Les progiciels utilisés dans Reno sont indiqués dans le tableau.

Logiciel	Version	Description	Nom du progiciel Reno
Cisco VPN Client	4.0.4	Client RPV de la société Cisco	E_VPN_CISCO_4.0.4D
Aladdin eToken	3.65 ou 4.0	Intergiciel et pilote pour le jeton USB de la société Aladdin. Régit l'accès du client Cisco aux certificats stockés sur le jeton USB.	M_VPN_ALADDIN_RTE_3.65_KTBE M_VPN_ALADDIN_RTE_4.00_KTBE
VPN Konfiguration KTBE	1.0	Configure le client Cisco pour la connexion RPV à Bewan et contient le certificat racine de la société Connectis pour la vérification du certificat utilisateur stocké sur le jeton USB.	E_VPNCONF_KTBE_STD
VPN Uninstall	4.0.4	Désinstalle complètement le logiciel Cisco Client 4.0.4. Ce progiciel est utilisé uniquement pour la désinstallation. Il n'est pas fourni en standard.	E_VPN_UNINSTALL_4X

3. Situation technique cible

La connexion RPV à BEWAN est établie par l'intermédiaire du client RPV Cisco.
Pour réaliser l'authentification sur le concentrateur RPV de BEWAN, le client RPV a besoin du certificat utilisateur qui est enregistré sur le jeton USB ou sur la carte à puce de la société Safenet.

La communication est établie de la même manière qu'avec l'ancienne solution, à une exception près : les certificats de la société Connectis sont remplacés par ceux de la Confédération (ADMIN PKI). Ces certificats ne sont plus stockés sur un jeton électronique Aladdin (jeton USB), mais sur un jeton ou une carte à puce Safenet.

Le changement des supports de stockage (jeton USB ou carte à puce) nécessite des adaptations dans les logiciels utilisés. Les nouveaux composants logiciels nécessaires sont décrits dans le tableau ci-dessous et dans les chapitres qui suivent.
Dans le canton de Berne, les logiciels sont distribués par l'intermédiaire de Reno. Le tableau ci-dessous indique les progiciels utilisés dans Reno.

Logiciel	Version	Description	Nom du progiciel Reno
Cisco VPN Client	5.0	Client RPV de la société Cisco	E_VPN_CISCO_5.0_NOKONF_KTBE

Safenet Borderles Security Client	7.0.2	Intergiciel et pilote pour le jeton USB de la société Safenet. Régit l'accès du client Cisco aux certificats stockés sur le jeton USB.	E_VPN_Safenet_7.02_KTBE
VPN Konfiguration KTBE	2.0	Configure le client Cisco pour la connexion RPV à Bewan et contient le certificat racine pour ADMIN PKI destiné à la vérification du certificat utilisateur stocké sur le jeton USB.	E_VPNCONF_KTBE_ADMINPKI
SCKI	2.1.0.6.	Logiciel utilisé pour renouveler le certificat client.	D_SCKI_2.1

3.1 Cisco VPN Client V. 5.0

Ce logiciel sert à établir la connexion et la communication cryptée (IPSec) avec BEWAN. Du côté de BEWAN (Connectis), la connexion cryptée est terminée sur le concentrateur RPV Cisco et reroutée dans BEWAN.

La version 5.0 du client est impérativement nécessaire pour réaliser la nouvelle solution.
Le chapitre 3.3 décrit le profil de configuration du client Cisco.

3.2 Safenet Borderless Security V. 7.0.2

Le client « Safenet Borderless Security » est nécessaire en tant que logiciel de liaison entre le jeton USB ou la carte à puce et le client RPV Cisco ; d'autre part, il installe le pilote pour tous les jetons USB et les cartes à puce Safenet.

Sans l'intergiciel Safenet, le client Cisco ne peut pas accéder au jeton USB ou à la carte à puce et, par conséquent, aux certificats qui y sont stockés, afin de réaliser l'authentification RPV.

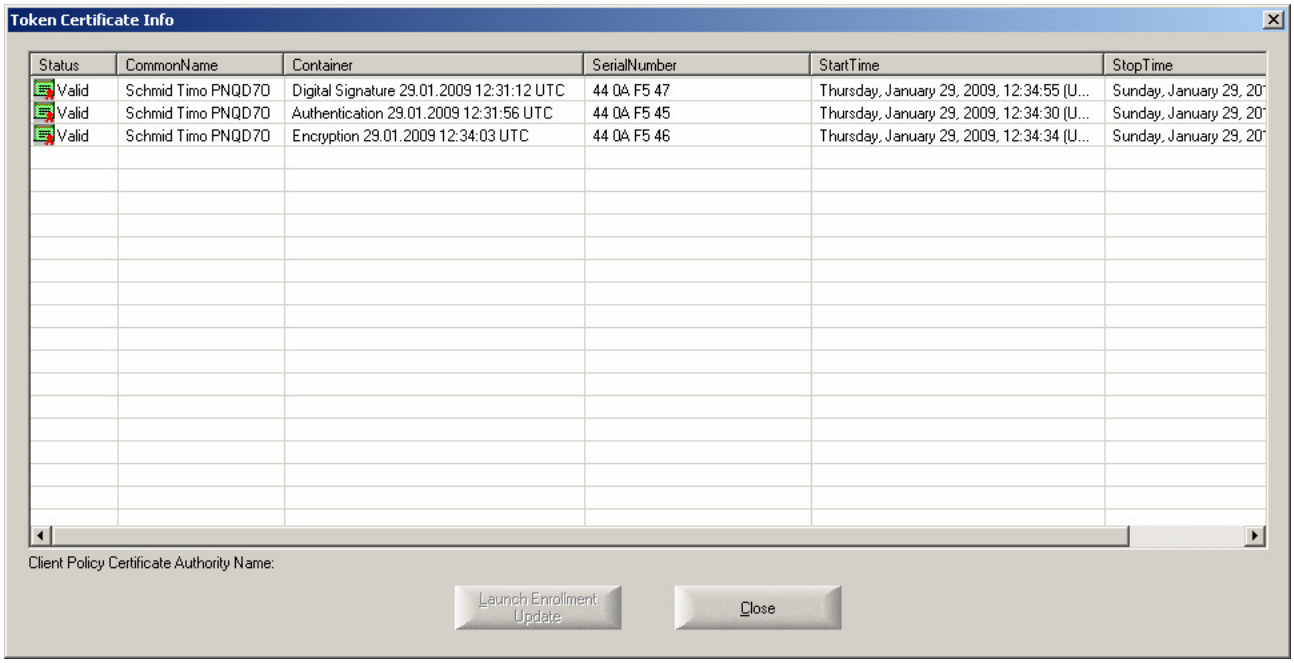
Après l'installation de ce logiciel, une de ces deux icônes apparaît dans la barre des tâches :

icône de jeton USB

ou

icône de carte à puce

En cliquant sur cette icône, vous pouvez visualiser les certificats enregistrés sur le jeton USB ou sur la carte à puce correspondante.



3.3 VPN Konfiguration KTBE

Ce progiciel de configuration permet de générer ou d'importer le profil de connexion RPV et le certificat racine dans le client Cisco.

Le certificat racine est nécessaire à la vérification du certificat utilisateur.

4. Installation manuelle

Cette opération consiste à installer un à un les trois composants logiciels.

Remarque :
Pour réaliser l'installation et la désinstallation de ces composants, il faut disposer des droits d'administrateur local.

IMPORTANT :
Avant l'installation des nouveaux logiciels, il faut supprimer/désinstaller les composants suivants :

Logiciel	Version
Cisco VPN Client	4.0.4
Aladdin eToken	3.65 ou 4.0

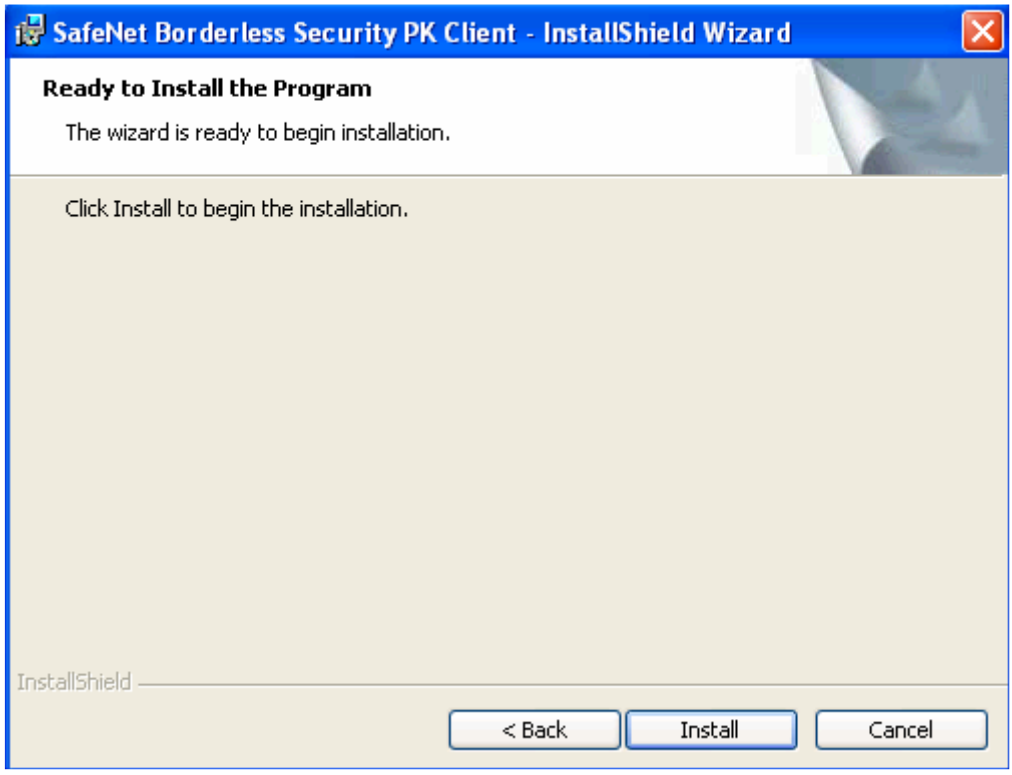
Après la suppression de ces composants, vous devez réinitialiser l'ordinateur.

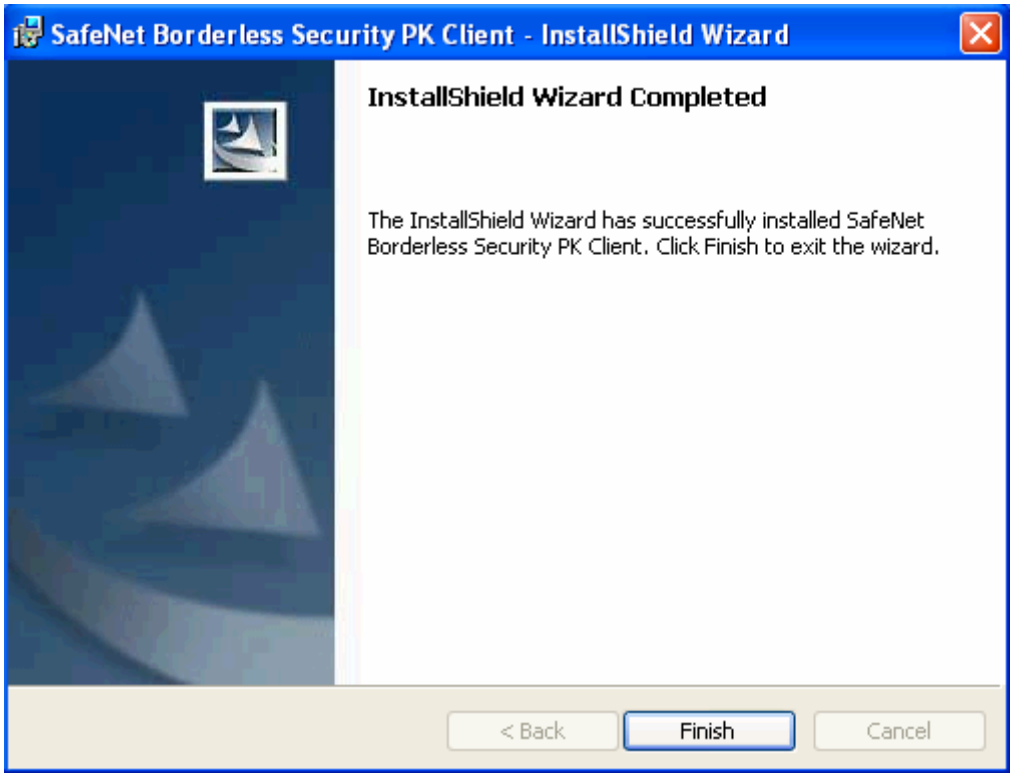
L'installation des composants doit être réalisée dans l'ordre suivant :

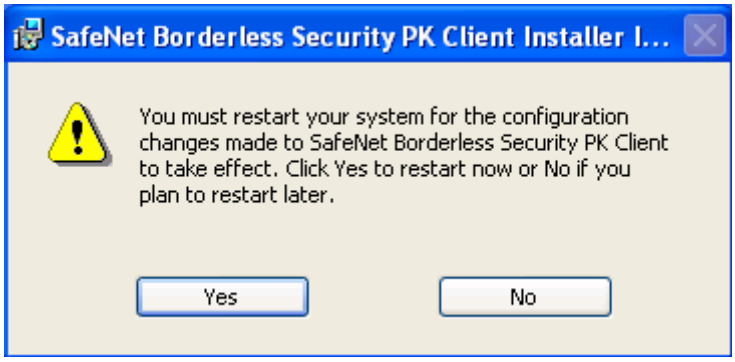
1. Safenet Borderless Security Client 7
2. Cisco VPN Client 5
3. VPN Konfiguration KTBE

4.1 Installation de Safenet Borderless Security

Accédez au dossier « 1_Safenet Borderless Security 7 », puis exécutez le fichier « Setup.msi ».







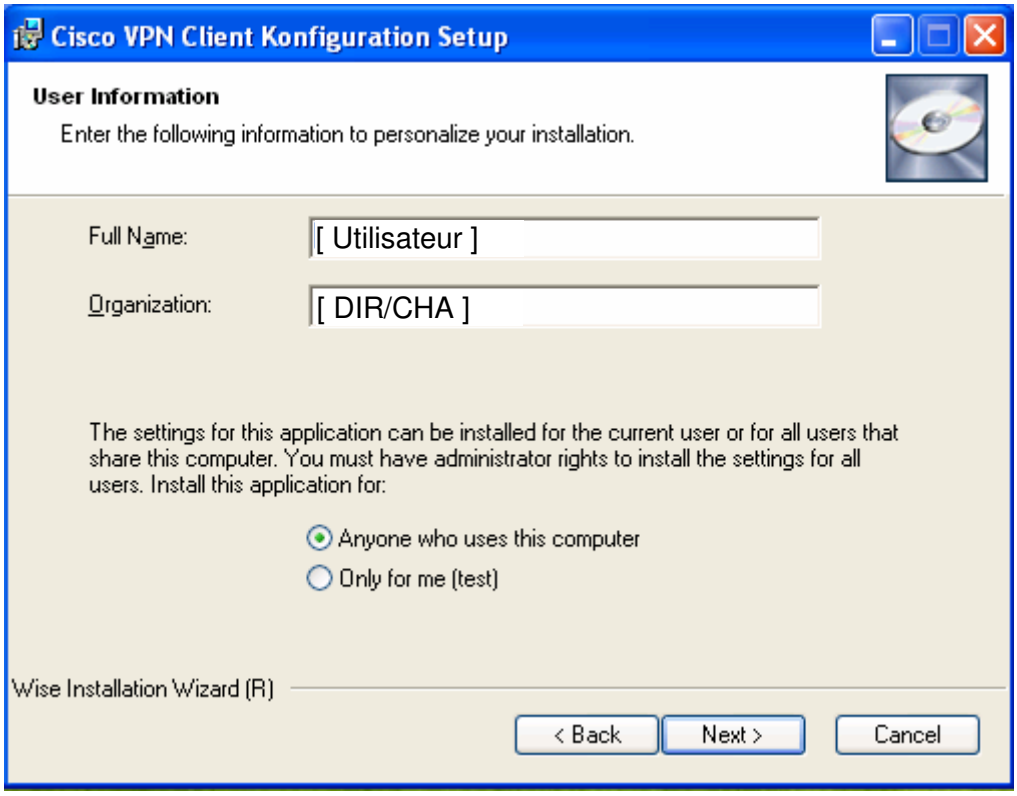
Une fois l'installation terminée, vous devez réinitialiser le système.

4.2 Installation de Cisco VPN Client 5.0

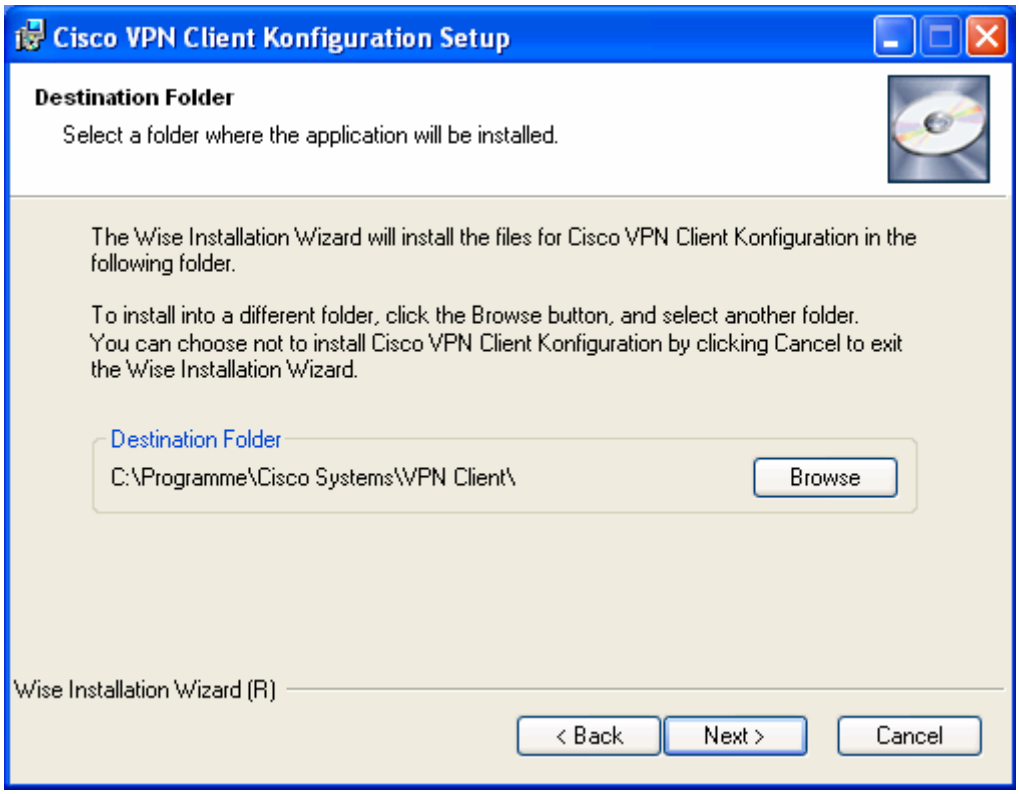
Accédez au dossier « 2_CiscoVPN5.0 » et exécutez le fichier « install.exe ».
L'installation se déroule totalement en arrière-plan.
Une fois qu'elle est terminée, le système exécute **automatiquement** une réinitialisation.

4.3 Installation de VPN Konfiguration KTBE

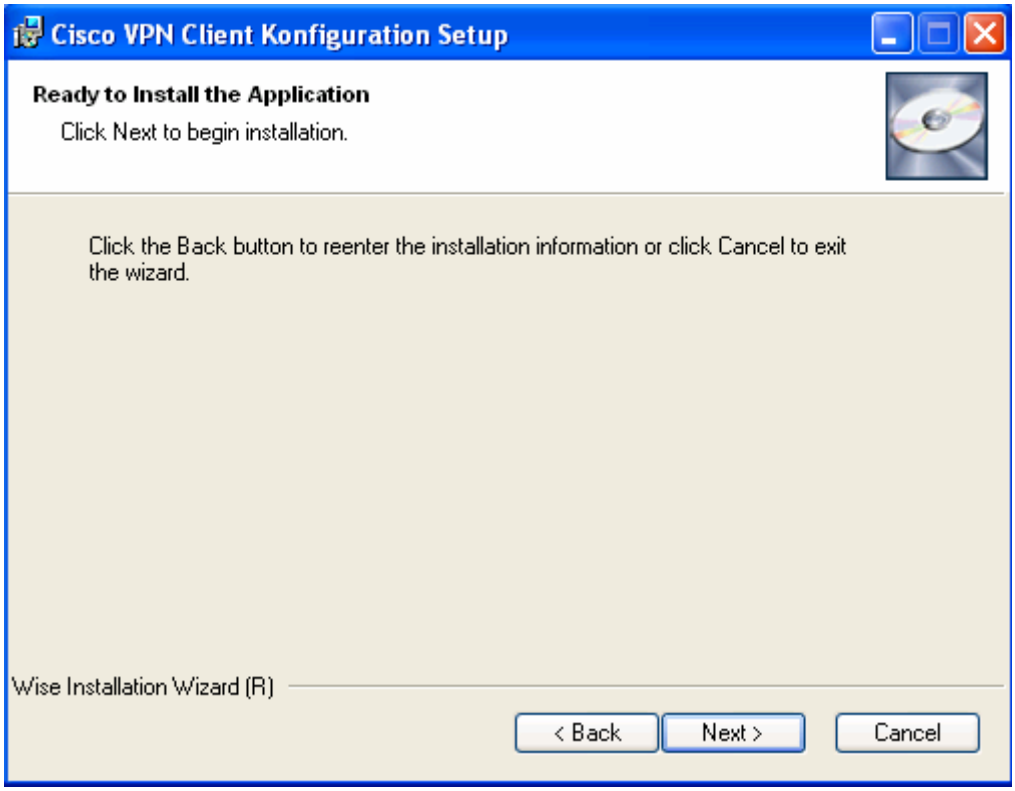
Accédez au dossier « 3_VPN Konfig KTBE », puis exécutez le fichier « VPN_Konfig.msi ». Vous pouvez reprendre les configurations standard. Cliquez sur « Next » pour continuer l'installation.



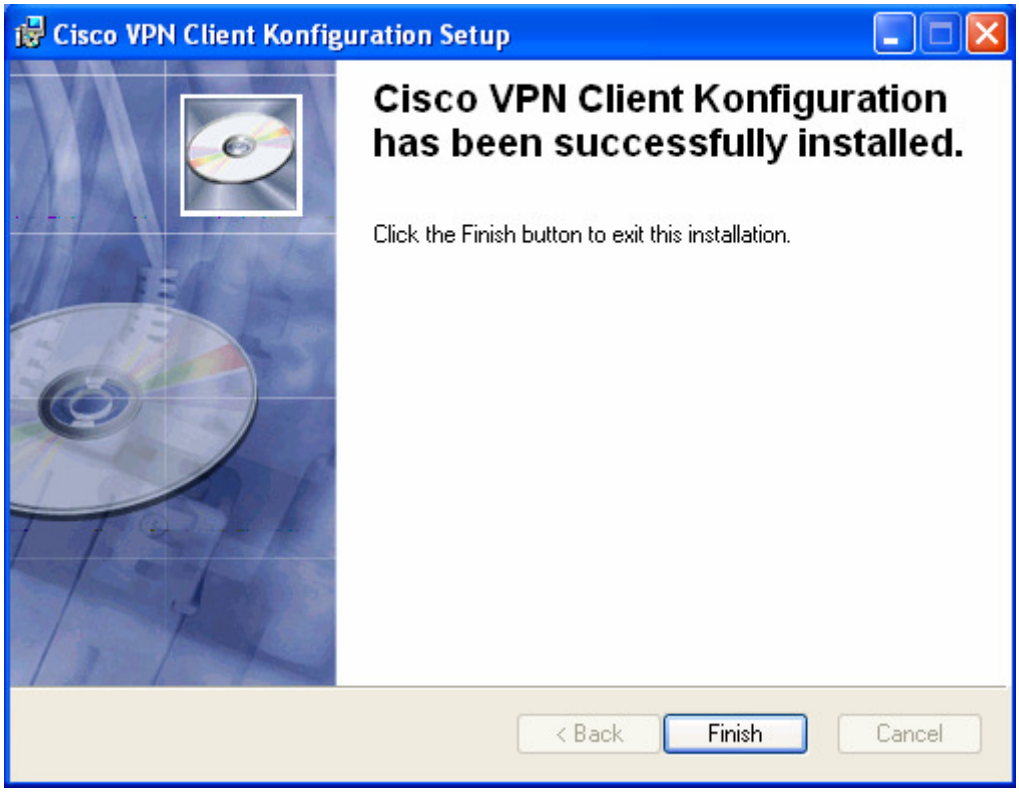
Cliquez sur « Next » pour continuer.



Cliquez sur « Next » pour continuer.



Cliquez sur « Next » pour continuer.



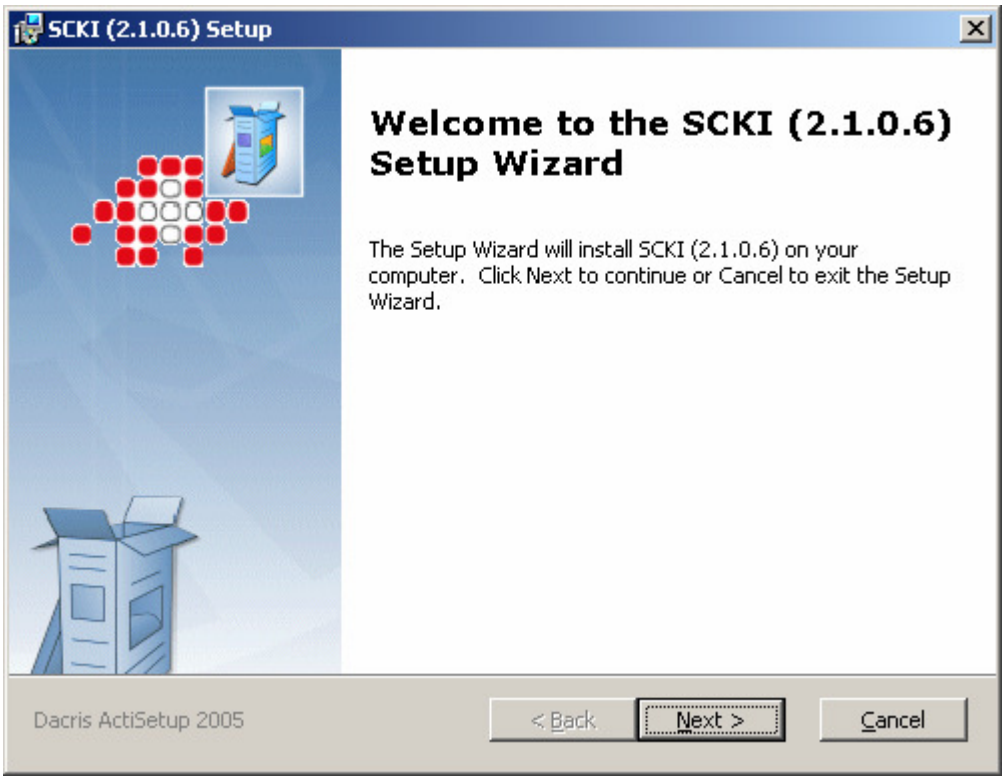
L'installation prend fin lorsque vous cliquez sur « Finish ».

Vous trouverez de plus amples informations sur l'utilisation du client RPV BEWAN dans le document « 02_Benutzeranleitung Konfiguration BEWAN VPN mit Admin PKI_V3.doc ».

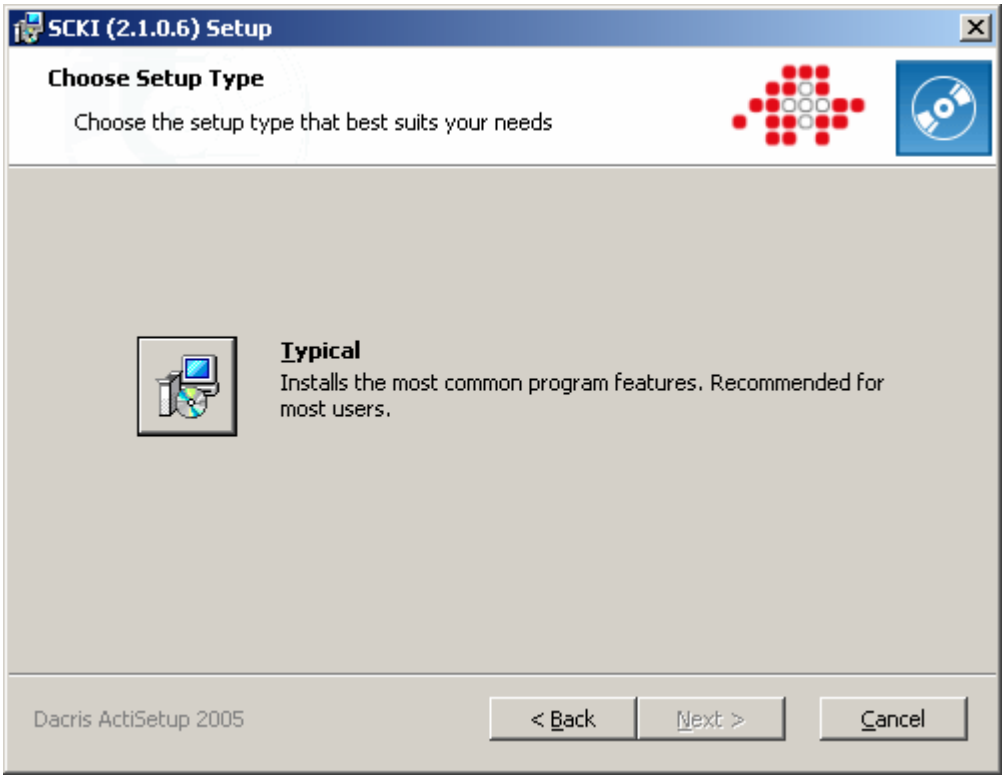
5. Renouvellement du certificat ADMIN PKI

Le certificat ADMIN PKI expire au bout de trois ans. Avant la date d'expiration, un responsable LRA rappelle à l'utilisateur que son certificat va bientôt expirer. Il faut alors suivre la procédure décrite ci-après afin de renouveler le certificat pour trois années supplémentaires.

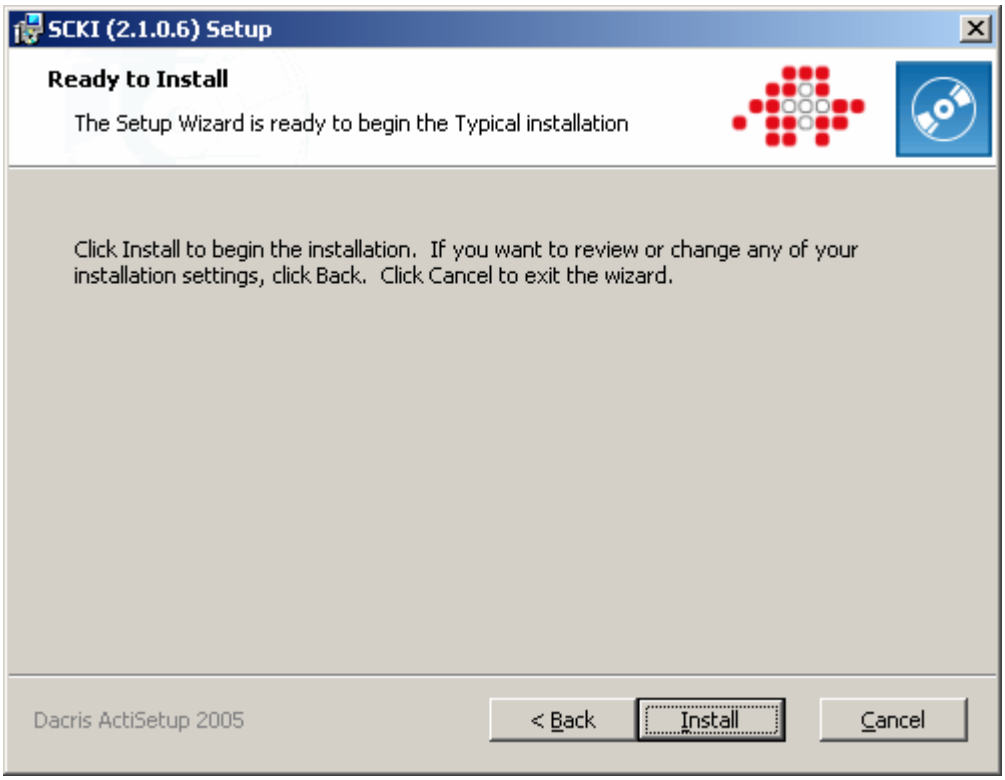
Accédez au dossier « 4_SCKI» et exécutez le fichier « SCKI_2.0.6a.msi».
Vous pouvez reprendre les configurations standard.



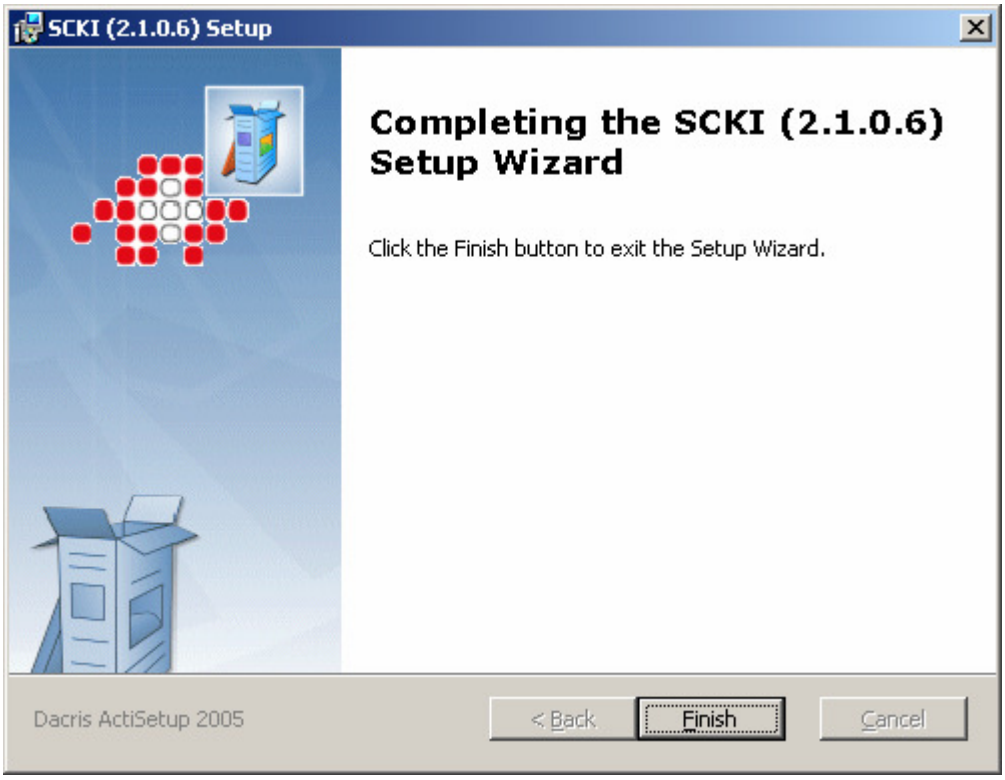
Cliquez sur « Next » pour continuer.



Sélectionnez « Typical » pour continuer.



Cliquez sur « Install » pour lancer l'installation.



L'installation prend fin lorsque vous cliquez sur « Finish ». Le document « 05_Benutzerhandbuch Certificate Renewal AdminPKI_V7.0.pdf» explique comment renouveler le certificat par l'intermédiaire d'une application Web.

6. Informations sur le document

Chemin d'accès:
Auteur: Timo Schmid

Contrôle des modifications

Version	Nom	Date	Remarques
0.1	Timo Schmid	11.03. 09	Version initiale
0.2	Esteban Bacariza	16.03.09	Remaniement
0.3	Esteban Bacariza	16.03.09	Remaniement

Vérification

Version	Service	Date	Visa	Remarques
0.6	KAIO	01.06.09	Bac	

Libération

Version	Service	Date	Visa	Remarques
0.6	KAIO	01.06.09	Bac	