

## **Manuel utilisateur**

### **HIP secEMAIL**

Date:	11.05.2017
Version:	1.1
Auteur:	Pascal von Ow
Etat:	En cours
Classification:	Aucune
Destinataires:	HIP

**Contrôle des modifications et validation**

<b>Vers.</b>	<b>Date</b>	<b>Nom</b>	<b>Remarques</b>	<b>Validation (visa)</b>
0.1	18.10.2016	Martin Zurbrügg	Version initiale	
0.2	17.11.2016	Pascal von Ow	Extension, captures d'écran	
0.3	08.12.2016	Pascal von Ow	Complément certificat racine	
0.4	25.10.2017	Pascal von Ow	autorités fédérales	
1.0	10.02.2017	Pascal von Ow	Screenshots	
1.1	11.05.2017	Martin Page	Sreenshots	

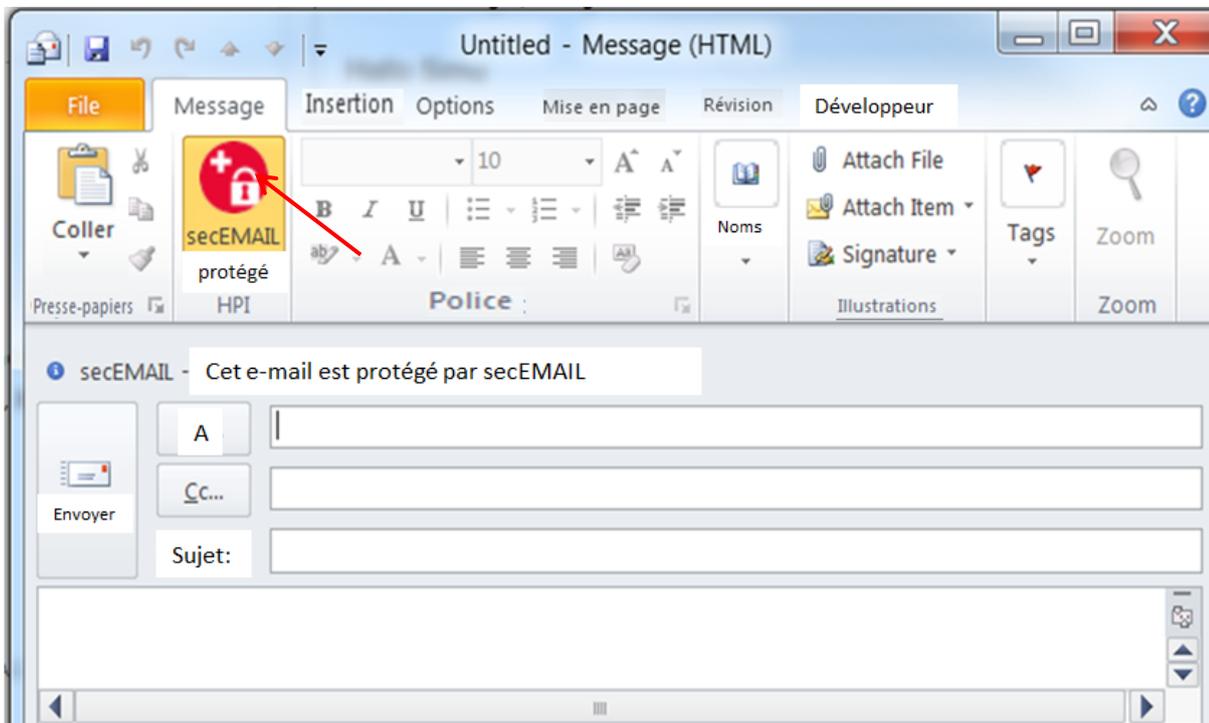
## Table des matières

1	Envoyer des messages avec secEMAIL .....	4
1.1	Microsoft Outlook.....	4
1.2	Téléphone mobile .....	4
1.3	Caractérisation des messages.....	5
2	Groupes de destinataires.....	5
2.1	Corps de police.....	5
2.2	Autorités fédérales.....	5
2.3	Tiers .....	5
2.3.1	WebMail (standard) .....	5
2.3.2	Acheminement direct avec un certificat S/MIME / PGP.....	7
2.3.3	Passage à S/MIME ou PGP.....	7
3	FAQ.....	9
3.1	Message: Votre certificat n'a pas été accepté ou n'est pas digne de confiance .....	9
3.2	Message: Problèmes de signature. Cliquez sur le bouton Signature pour afficher les détails. 10	
4	Autres informations et assistance .....	13
5	Annexe .....	14
5.1	E-mails d'information aux tiers .....	14

# 1 Envoyer des messages avec secEMAIL

## 1.1 Microsoft Outlook

Cliquer sur le bouton «secEMAIL»



Votre message est transmis de manière sécurisée.

## 1.2 Téléphone mobile

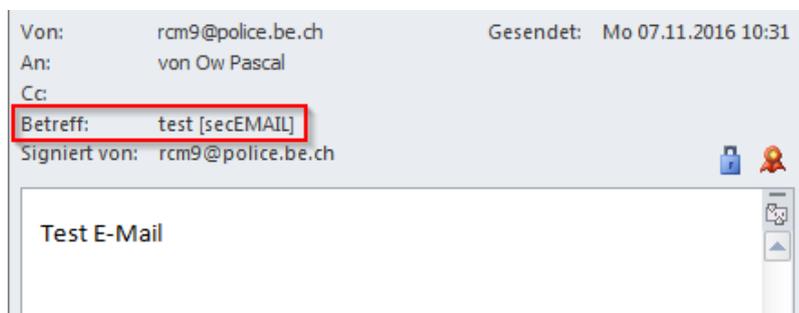
Au début de l'objet de l'e-mail, saisissez les caractères suivants: //



Votre message est transmis de manière sécurisée.

### 1.3 Caractérisation des messages

Pour tous les messages envoyés avec secEMAIL, [secEMAIL] apparaît dans l'objet de l'e-mail chez le destinataire:



Cela signifie également que les réponses seront automatiquement cryptées. Si l'e-mail doit être renvoyé ultérieurement de manière normale, l'utilisateur doit modifier l'objet en conséquence.

## 2 Groupes de destinataires

Le système sélectionne automatiquement le groupe de destinataires approprié à l'aide de l'adresse e-mail du destinataire. Les groupes de destinataires suivants sont configurés:

### 2.1 Corps de police

Les e-mails protégés par secEMAIL adressés aux corps de police utilisateurs sont transmis de manière sécurisée, peuvent être lus directement par le destinataire et sont compatibles avec les appareils portables.

### 2.2 Autorités fédérales

Les e-mails protégés par secEMAIL adressés aux autorités fédérales, par exemple au Corps des gardes-frontières ou à fedpol, sont transmis de manière sécurisée. Toutefois, le destinataire ne peut décrypter l'e-mail qu'avec son certificat Admin-PKI personnel. L'e-mail est compatible avec les appareils portables.

En vertu des directives de sécurité de la Confédération, il est possible que votre certificat Admin-PKI personnel soit requis pour décrypter la réponse à l'e-mail.

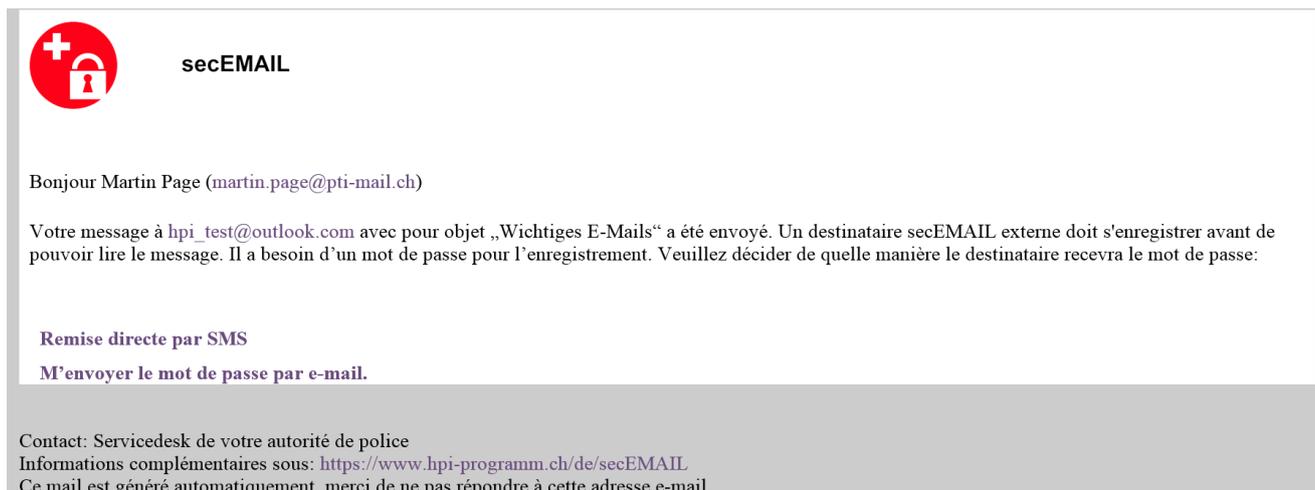
### 2.3 Tiers

Les e-mails protégés par secEMAIL adressés à des tiers sont d'abord conservés sur la passerelle secEMAIL. Le destinataire reçoit automatiquement un e-mail (cf. chapitre 4 en annexe) avec des informations pour la transmission du message.

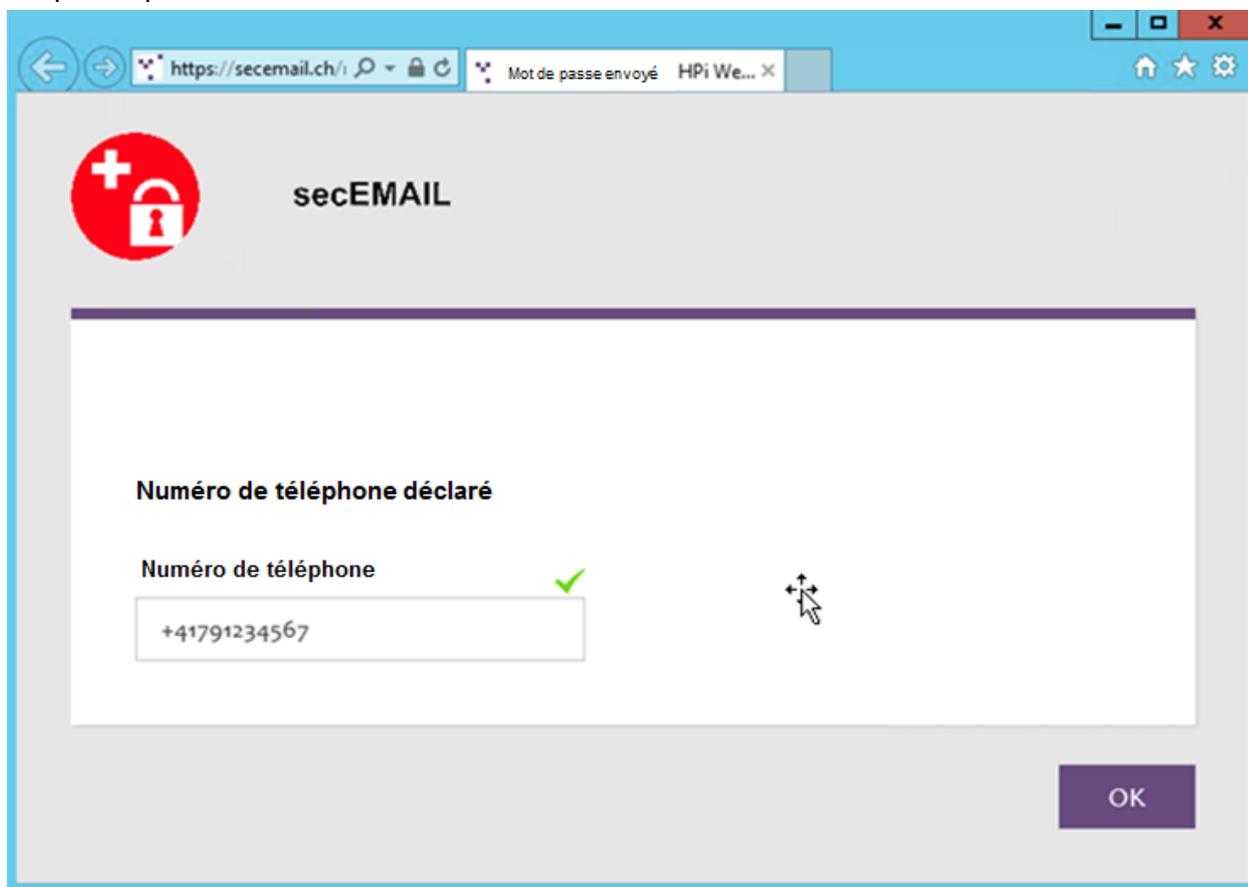
Le destinataire peut choisir entre deux options: afficher le message dans WebMail (standard), utiliser un certificat S/MIME ou une clé PGP.

#### 2.3.1 WebMail (standard)

Pour s'enregistrer, le destinataire a besoin d'un mot de passe à usage unique. Vous recevez alors l'e-mail suivant:



Cliquez sur «Saisir un numéro de téléphone portable», si vous êtes en possession du numéro de téléphone portable du destinataire. Saisissez le numéro sur le site Internet suivant:



Le mot de passe initial est transmis automatiquement par SMS au destinataire. Vous pouvez également sélectionner dans l'e-mail «Envoyer le mot de passe par e-mail». Vous recevez alors un e-mail avec le mot de passe initial, comme dans l'exemple ci-dessous:



Communiquer le mot de passe oralement au destinataire. Ne transmettez en aucun cas le mot de passe par e-mail! Vous pouvez transmettre le mot de passe par téléphone ou par SMS.

Une fois que le tiers a effectué son seul et unique enregistrement, l'e-mail conservé sur la passerelle lui est automatiquement transmis. Vous recevez alors une confirmation:



Le destinataire n'a ensuite plus besoin de s'enregistrer pour recevoir les e-mails suivants. Il reçoit seulement un e-mail l'informant qu'un nouveau message est arrivé pour lui dans WebMail (cf. chapitre 4 en annexe).

Les messages stockés dans WebMail sont supprimés au plus tard après 60 jours.

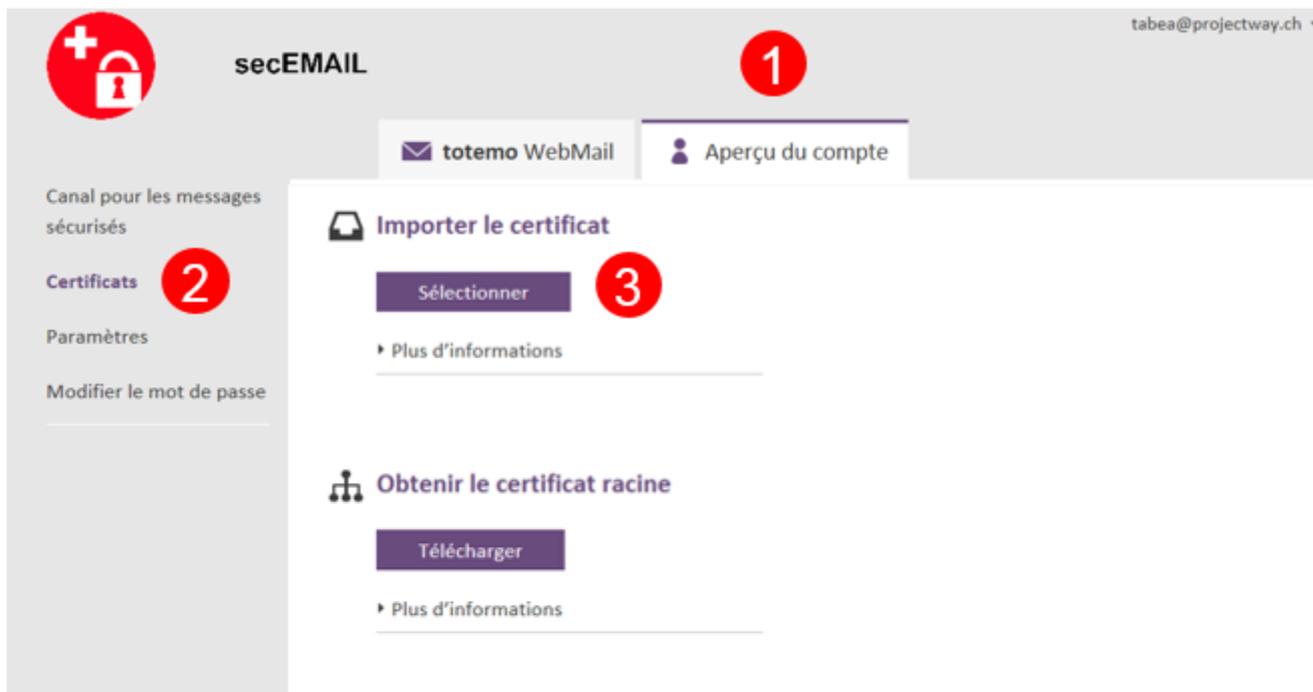
### 2.3.2 Acheminement direct avec un certificat S/MIME / PGP

Si le tiers dispose déjà d'un certificat S/MIME, il peut répondre à l'e-mail, avec les informations complémentaires, et signer sa réponse avec son certificat S/MIME personnel. L'e-mail conservé sur la passerelle secEMAIL est alors transmis directement. Le mot de passe à usage unique n'est pas nécessaire dans ce cas. L'accès à WebMail est alors désactivé et n'est plus disponible.

Si l'utilisateur souhaite utiliser une clé PGP personnelle ou passer ultérieurement de WebMail à S/MIME, le tiers doit procéder à la configuration nécessaire sur le portail Web. Le prochain chapitre fournit des informations à ce sujet. Vous recevez également une confirmation si l'e-mail a été acheminé crypté par S/MIME ou PGP.

### 2.3.3 Passage à S/MIME ou PGP

Des certificats personnels ou des clés PGP peuvent être téléchargés sur le portail Web, sous «Certificats».



The screenshot shows the 'secEMAIL' interface. At the top right, the user 'tabea@projectway.ch' is logged in. A red circle '1' highlights the 'Aperçu du compte' tab. On the left sidebar, a red circle '2' highlights the 'Certificats' menu item. The main content area shows the 'Importer le certificat' section with a red circle '3' highlighting the 'Sélectionner' button. Below it is the 'Obtenir le certificat racine' section with a 'Télécharger' button.

### Certificats



The dialog box shows the 'Importer le certificat' step 4. It includes a progress indicator '1 2', the instruction 'Télécharger le certificat (S/MIME ou OpenPGP).', and buttons for 'Annuler' and 'Importer' (highlighted with a red circle '4'). A 'Plus d'informations' link is also present.

### Zertifikate



The dialog box shows the 'Zertifikat importieren' step 5. It includes a progress indicator '✓ 2', the instruction 'Importieren Sie das Zertifikat. pascal.vonow@bedag.ch.cer', buttons for 'Abbrechen' and 'Importieren' (highlighted with a red circle '5'), and a 'Mehr Informationen' link.

Une fois l'importation terminée, les certificats enregistrés et leurs options d'utilisation s'affichent dans un aperçu.

### Certificats

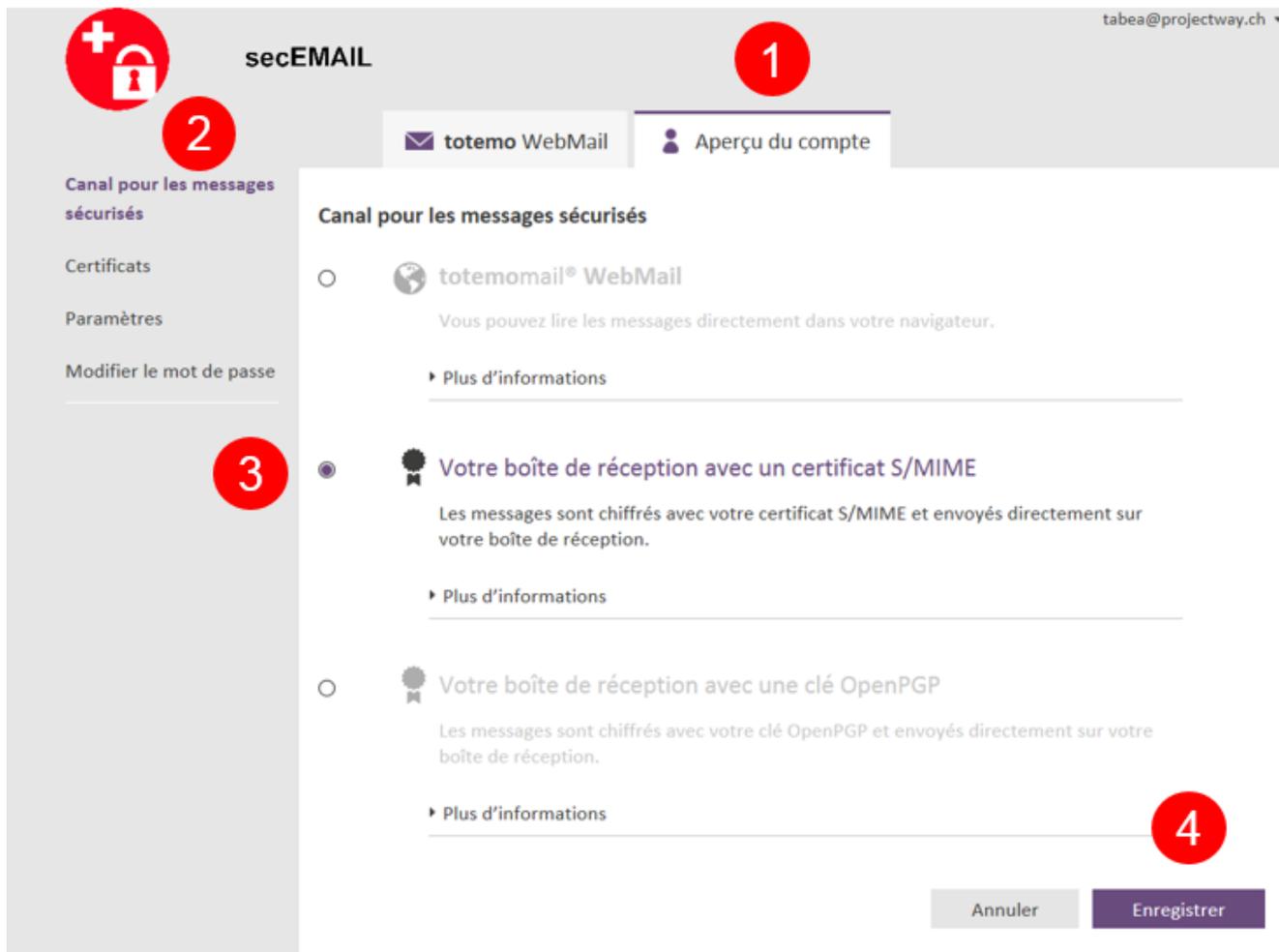
#### Importation du certificat réussie

Le certificat importé se trouve dans la liste ci-après.

Emetteur	Délivré pour	Valable j...			Type	Trier ▾
SwissSign Perso...	tabea@projectway.ch	14-févr.-2...			Certificat S/MIME	

### Importer le certificat

Si le certificat ou la clé PGP doivent également être utilisés pour des messages ultérieurs, cela doit être configuré dans les préférences.



The screenshot shows the 'secEMAIL' interface for user 'tabea@projectway.ch'. It features a sidebar on the left with a red circle '2' next to 'Canal pour les messages sécurisés'. The main content area has a red circle '1' above the 'Aperçu du compte' tab. Below this, there are three radio button options for the security channel. The second option, 'Votre boîte de réception avec un certificat S/MIME', is selected and has a red circle '3' next to it. At the bottom right, there are 'Annuler' and 'Enregistrer' buttons, with a red circle '4' next to 'Enregistrer'.

Remarque: la modification concerne uniquement les nouveaux messages. Les autres messages sont conservés dans WebMail.

## 3 FAQ

### 3.1 Message: Votre certificat n'a pas été accepté ou n'est pas digne de confiance

Si l'autorité qui délivre les certificats (AC) ne figure pas encore dans la liste des instances dignes de confiance, le tiers reçoit le message suivant:

**secEMAIL**

□

Bonjour Tabea Page ([tabea@projectway.ch](mailto:tabea@projectway.ch))

**Votre certificat doit encore être sécurisé manuellement par le service secEMAIL.**

En raison de notre politique de sécurité, le certificat que vous utilisez n'a pas pu être validé automatiquement. Cette tâche doit être exécutée manuellement.

Veillez tenir compte de délais pour la distribution de votre message.

Contact: Martin Page ([martin.page@pti-mail.ch](mailto:martin.page@pti-mail.ch))

Informations complémentaires (actuellement ne disponibles qu'en allemand) sous: <https://www.hpi-programm.ch/de/secEMAIL>

Ce mail est généré automatiquement, merci de ne pas répondre à cette adresse e-mail.

Bedag, en tant qu'exploitant, reçoit également le message et ajoute l'autorité digne de confiance à la liste. Après la validation de l'autorité, l'e-mail est acheminé comme prévu.

### 3.2 Message: Problèmes de signature. Cliquez sur le bouton Signature pour afficher les détails.

Le message suivant, ou un message similaire, s'affiche dans Outlook:

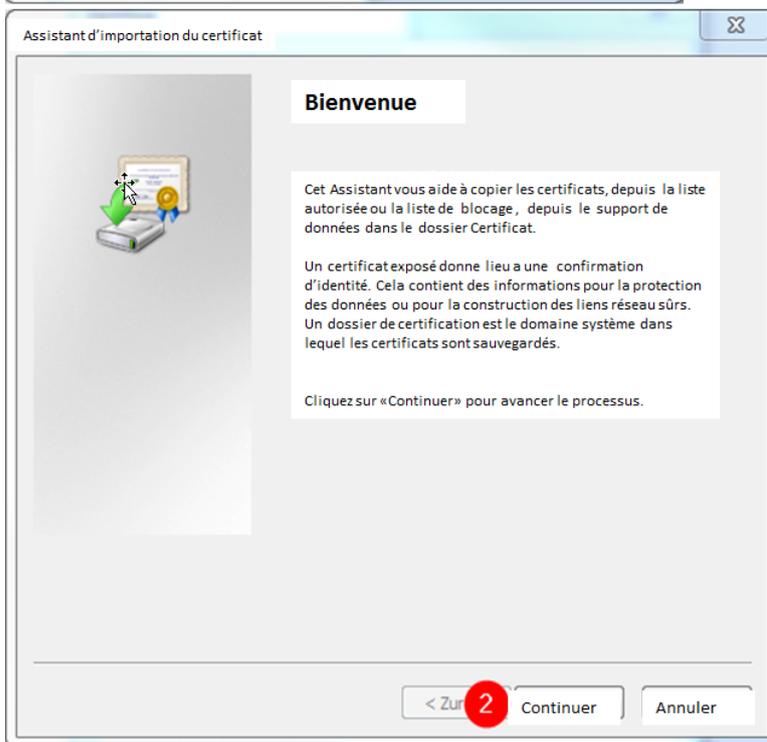
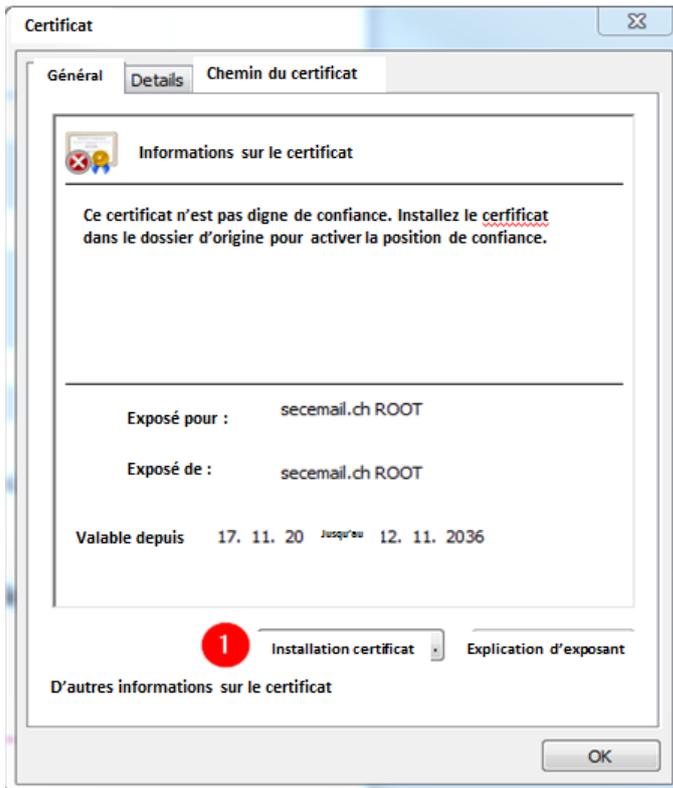
Signiert von: Probleme mit der Signatur. Klicken Sie auf die Signaturschaltfläche, um Details anzuzeigen.

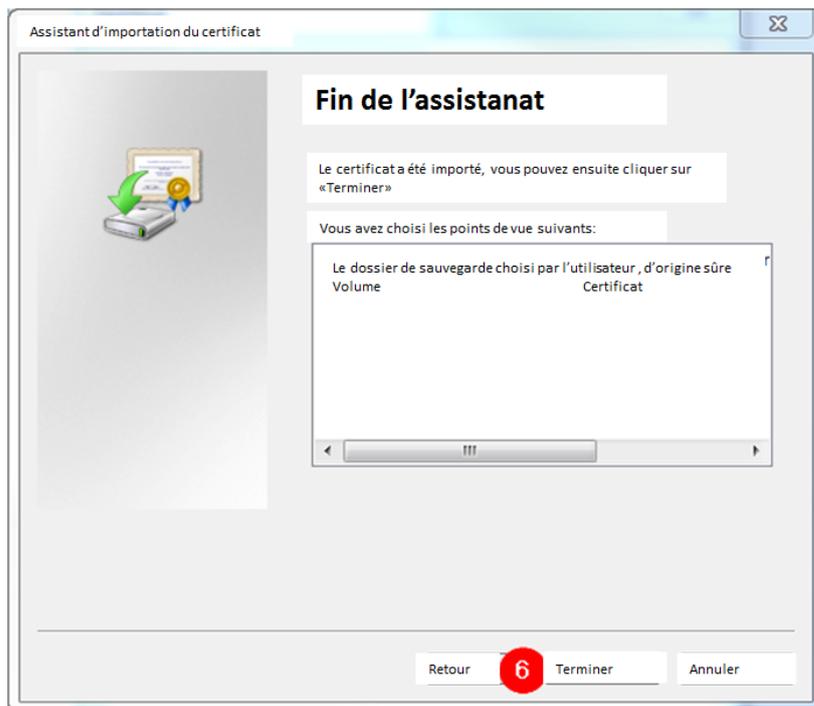
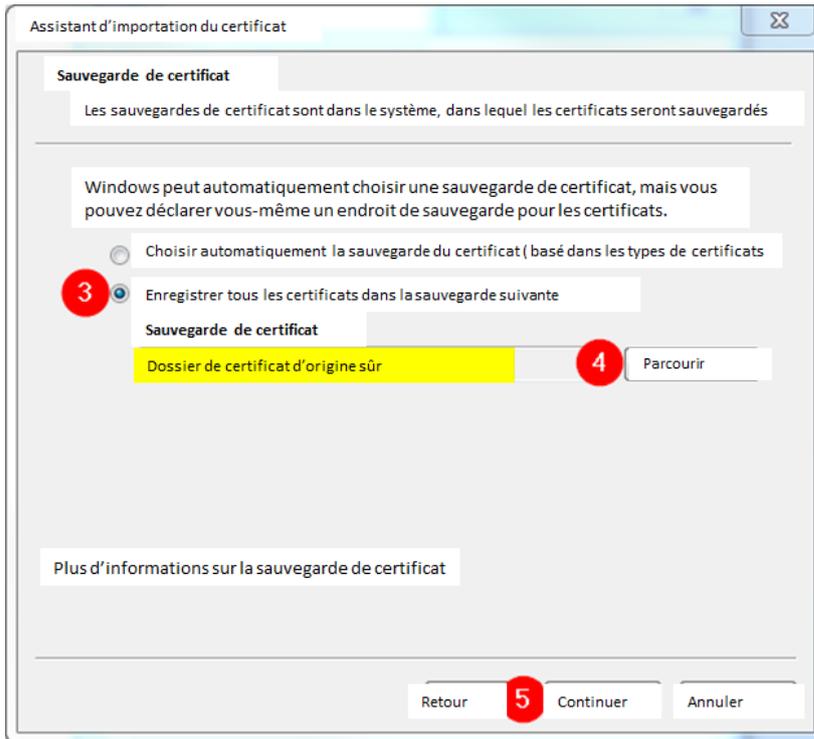


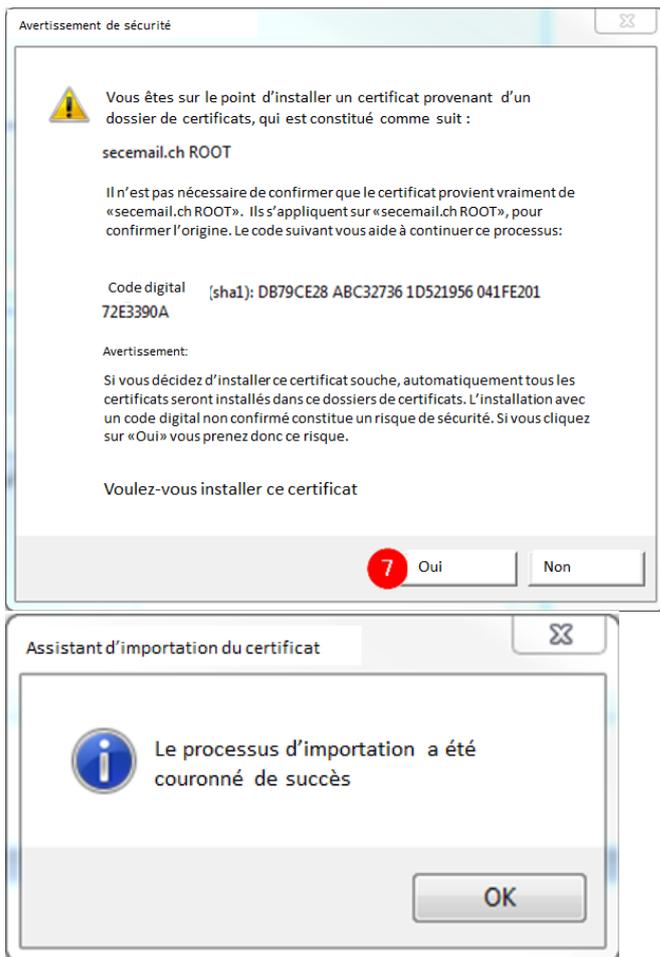
Avec la variante d'acheminement B des organisations utilisatrices, les certificats sont délivrés par une propre autorité de certification. Celle-ci doit par conséquent être enregistrée comme autorité de certification racine digne de confiance.

Cela s'effectue de la manière suivante

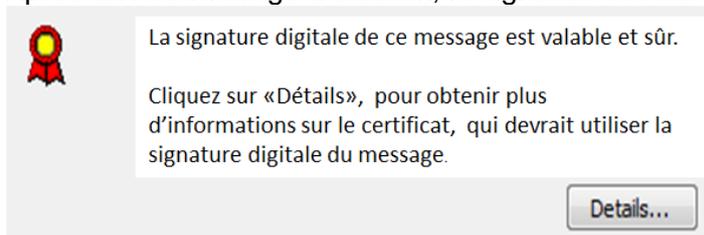
1. Téléchargement du certificat depuis le site Internet <https://www.hpi-programm.ch/de/secEMAIL>
2. Double clic sur le fichier secemail-RootCA.cer
3. Installation du certificat:







4. Après un redémarrage d'Outlook, la signature est classée comme digne de confiance



## 4 Autres informations et assistance

Vous trouverez d'autres informations et des réponses aux questions fréquemment posées sur <https://www.hpi-programm.ch/fr/secEMAIL>.

En cas de problèmes techniques, adressez-vous au service d'assistance.

## 5 Annexe

### 5.1 E-mails d'information aux tiers

E-mail d'information aux tiers qui reçoivent pour la première fois un message sécurisé via secEMAIL:



[Deutsch](#) [Français](#) [Italiano](#) [English](#)

#### Français

Bonjour [tabea@projectway.ch](mailto:tabea@projectway.ch)

Martin Page ([martin.page@pti-mail.ch](mailto:martin.page@pti-mail.ch)) souhaite vous transmettre un message dont le contenu est confidentiel. C'est pourquoi le message est envoyé de manière sécurisée.

Pour pouvoir lire ou recevoir ce message confidentiel, vous disposez de deux possibilités. Veuillez sélectionner l'option de votre choix et suivre les instructions correspondantes:

#### Option 1: lire l'e-mail sur le webmail sécurisé

Vous pouvez lire le e-mail en toute sécurité dans votre navigateur web en cliquant sur le lien suivant: [Webmail sécurisé](#). L'e-mail est conservé pendant 60 jours sur le serveur, puis il est supprimé.

Vous n'avez besoin de vous enregistrer qu'une seule fois, vous recevez le mot de passe nécessaire de l'expéditeur du message. Ensuite, vous êtes invité(e) à créer un mot de passe personnel. Celui-ci doit comporter au moins 8 caractères et être composé de lettres et de chiffres.

#### Option 2: vous disposez d'un certificat S/MIME

Vous devez exécuter les étapes suivantes:

- Répondez à ce message avec un e-mail signé électroniquement.
- Vous recevrez aussitôt le message crypté de l'expéditeur.
- Si la signature des e-mails suivants n'est pas fiable, veuillez installer le certificat racine conformément au site web suivant <https://www.hpi-programm.ch/de/secEMAIL>.

**Remarque:** Si vous disposez d'un certificat S/MIME auto-signé ou d'une clé PGP, vous pouvez les télécharger à tout moment sur le webmail.

En cas d'incertitudes, veuillez vous rendre sur le site web ou contacter Martin Page ([martin.page@pti-mail.ch](mailto:martin.page@pti-mail.ch)). Il vous aidera à accéder au service d'assistance. Informations complémentaires sur: <https://www.hpi-programm.ch/de/secEMAIL>.

E-mail d'information aux utilisateurs de WebMail déjà enregistrés (tiers), lors de la réception d'un nouveau message:

**secEMAIL**

Bonjour Tabea Page ([tabea@projectway.ch](mailto:tabea@projectway.ch))

Martin Page ([martin.page@pti-mail.ch](mailto:martin.page@pti-mail.ch)) vous a envoyé un secEMAIL. Veuillez vous connecter sous le lien suivant: [secEMAIL](#).

Contact: Martin Page ([martin.page@pti-mail.ch](mailto:martin.page@pti-mail.ch))  
Informations complémentaires sous: <https://www.hpi-programm.ch/de/secEMAIL>  
Ce mail est généré automatiquement, merci de ne pas répondre à cette adresse e-mail.