

**SSI Université de Lille**

**CERTIFICATS  
ÉLECTRONIQUES  
PERSONNELS  
(Renater/TCS/Digicert V3)**

**Avril 2018**

# Constat

Nombreuses réceptions de mails usurpant une identité : l'émetteur n'est pas celui qu'il prétend être...

## Risques : confiance mal placée

- Diffusion de fausses informations (ex : report d'examen)
- Escroqueries diverses (« phishing »)

## Solutions possibles

- Vigilance constante (ex : ne pas hésiter à demander confirmation au prétendu émetteur)
- Moyens techniques : accroître le niveau de confiance en l'émetteur d'un mail à l'aide des « certificats électroniques personnels »
- Etc...

# Bénéficiaires

Tous les personnels ; service « TCS V3 » : marché RENATER / société DigiCert, via le réseau européen GEANT (anciennement TERENA) ; « gratuit » pour l'ESR

## Usage

- « Signature » du courrier électronique : le destinataire est assuré du **contenu** du mail et de **l'identité** de l'émetteur
- Chiffrement du courrier électronique : seul le destinataire peut déchiffrer le contenu du mail

## Principe de base

- Certificat = clefs de chiffrement asymétriques (clef privée, clef publique) + validation par un tiers de confiance
- Signature : l'émetteur « signe » avec son certificat
- Chiffrement : effectué avec le certificat du destinataire
- Voir [https://fr.wikipedia.org/wiki/Certificat\\_%C3%A9lectronique](https://fr.wikipedia.org/wiki/Certificat_%C3%A9lectronique)

# Prérequis

- Le demandeur doit être personnel de l'Université de Lille (au sens large) et avoir une adresse électronique en « `univ-lille.fr` » (ce qui exclut quelques personnels « invités » ou « vacataires »).

Le demandeur doit être **formellement identifié** : nécessite un rendez-vous avec le RSSI pour présentation d'un document d'identité officiel avec photo

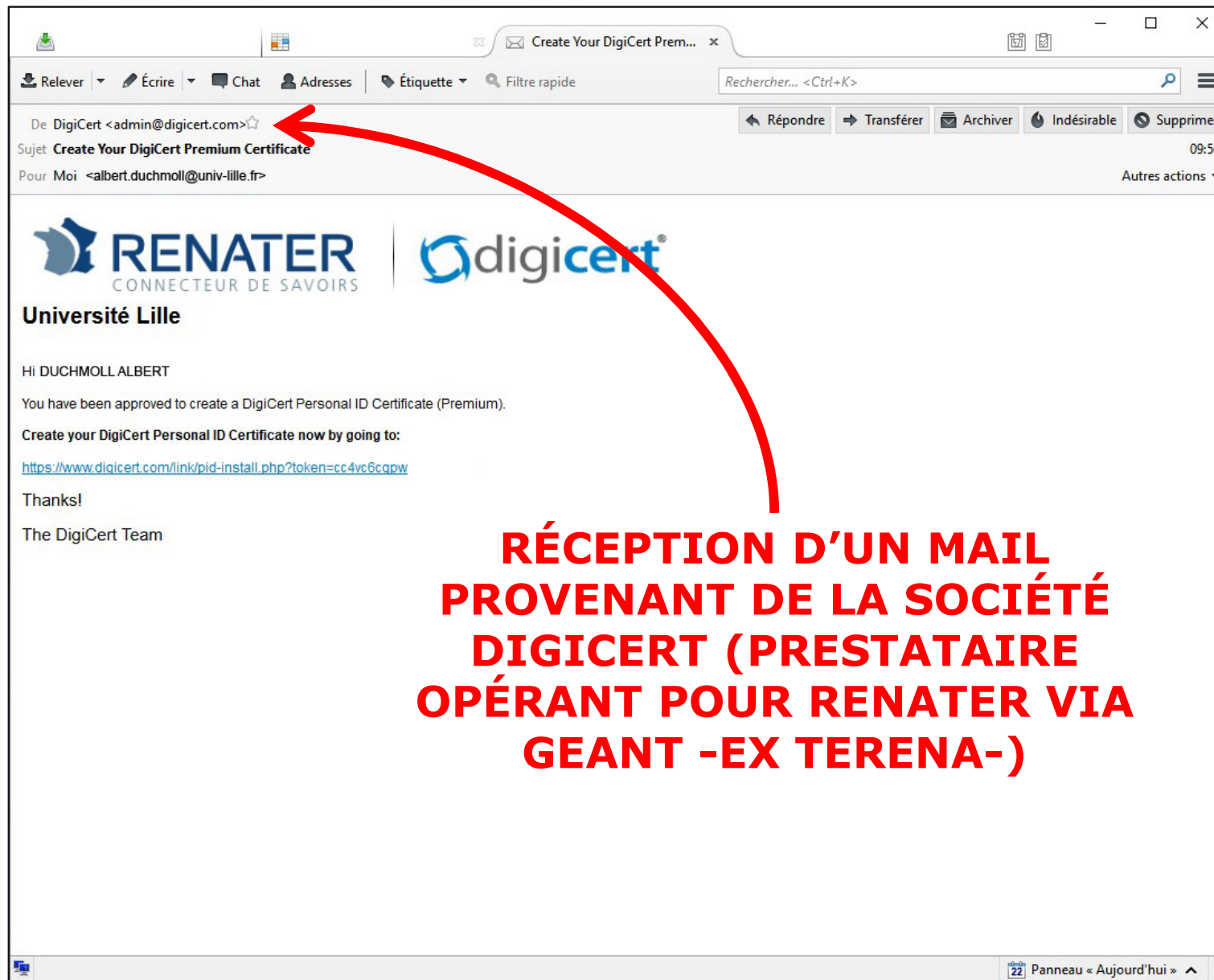
## Demande de certificat

- Envoyer un mail à `ssi@univ-lille.fr`

# Installation et utilisation

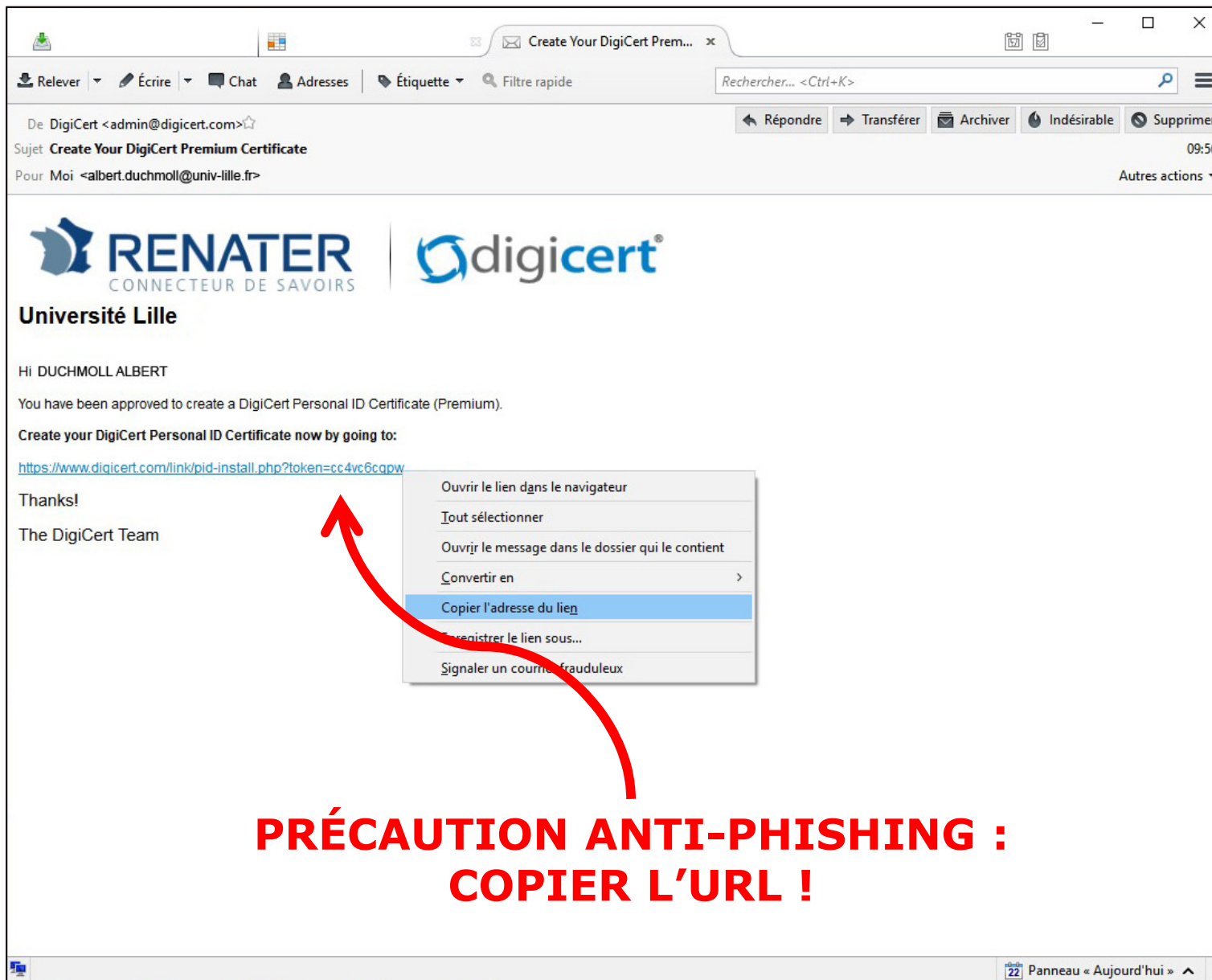
- Attendre le mail d'invite (de « DigiCert [admin@digicert.fr](mailto:admin@digicert.fr) »)
- Suivre le mode d'emploi détaillé dans les pages suivantes
- Exemples basés sur le couple Firefox/Thunderbird ;  
attention : légèrement différent pour IE/Outlook car leur « magasin » de certificats est commun)
- Cf. Annexe 1 pour le « webmail » ZIMBRA

# Mail d'invite – 1/3



**R CEPTION D'UN MAIL  
PROVENANT DE LA SOCI T   
DIGICERT (PRESTATAIRE  
OP RANT POUR RENATER VIA  
GEANT -EX TERENA-)**

# Mail d'invite – 2/3



De: DigiCert <admin@digicert.com> ☆

Sujet: Create Your DigiCert Premium Certificate

Pour: Moi <albert.duchmoll@univ-lille.fr>

09:56

Autres actions ▾

**RENATER**  
CONNECTEUR DE SAVOIRS

**digicert**

**Université Lille**

Hi DUCHMOLL ALBERT

You have been approved to create a DigiCert Personal ID Certificate (Premium).

Create your DigiCert Personal ID Certificate now by going to:

<https://www.digicert.com/link/pid-install.php?token=cc4vc6cqpw>

Thanks!

The DigiCert Team

Ouvrir le lien dans le navigateur

Tout sélectionner

Ouvrir le message dans le dossier qui le contient

Convertir en >

**Copier l'adresse du lien**

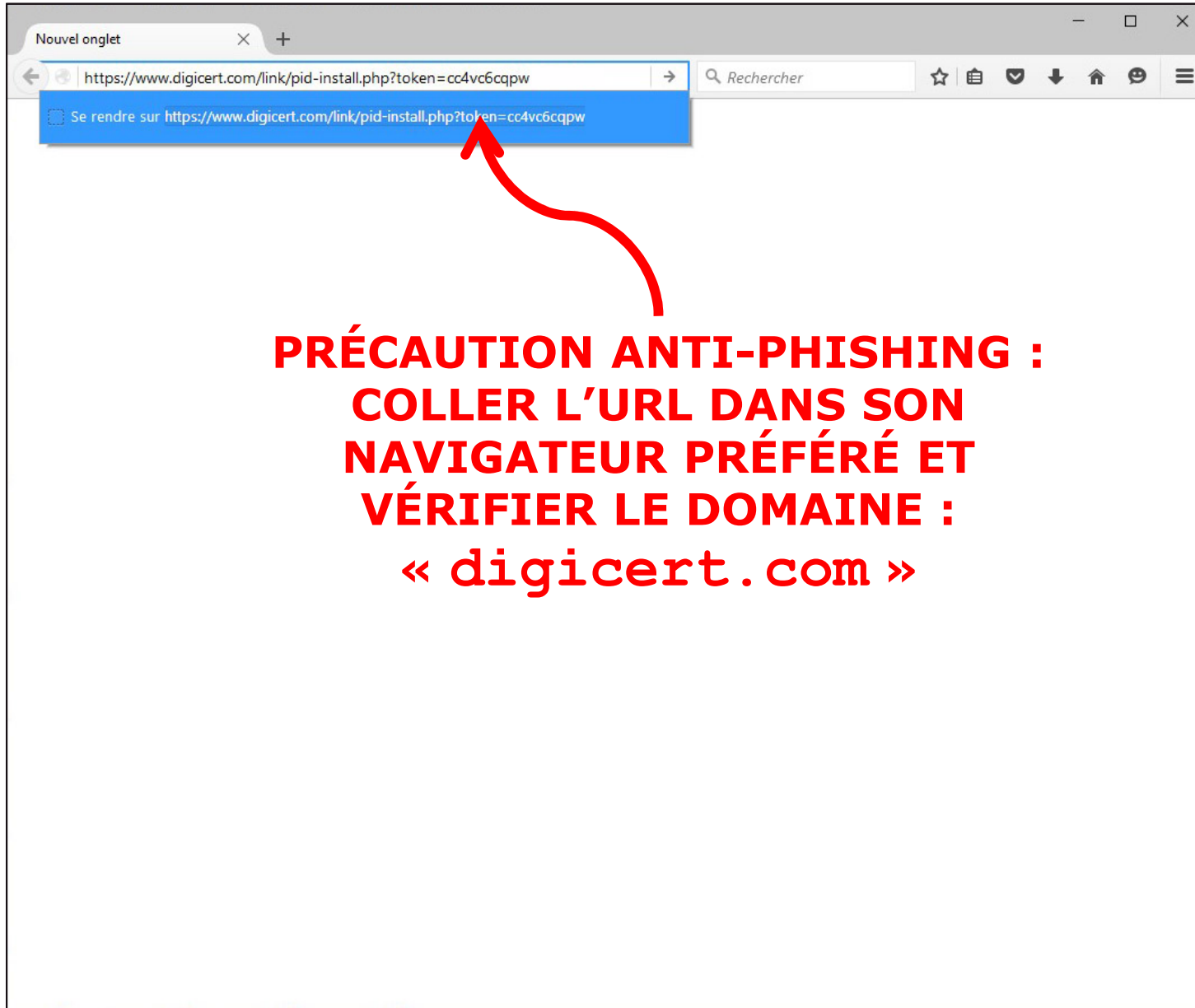
Enregistrer le lien sous...

Signaler un courriel frauduleux

**PRÉCAUTION ANTI-PHISHING :  
COPIER L'URL !**

22 Panneau « Aujourd'hui »

# Mail d'invite – 3/3



The screenshot shows a web browser window with the address bar containing the URL `https://www.digicert.com/link/pid-install.php?token=cc4vc6cqpw`. A blue tooltip is visible over the URL, containing the text "Se rendre sur https://www.digicert.com/link/pid-install.php?token=cc4vc6cqpw". A red arrow points from the warning text below to the URL in the address bar.

**PRÉCAUTION ANTI-PHISHING :**  
**COLLER L'URL DANS SON**  
**NAVIGATEUR PRÉFÉRÉ ET**  
**VÉRIFIER LE DOMAINE :**  
**« digicert.com »**



# Génération du certificat – 1/5

Generate your DigiCert Premium Certificate

For technical assistance or to make corrections, contact your administrator.

**DigiCert Personal ID Details**

**Name:** DUCHMOLL ALBERT

**Email Address:** albert.duchmoll@univ-lille.fr

**Organization:** UNIVERSITE LILLE

**Subscriber Agreement:**

CERTIFICATE SUBSCRIBER AGREEMENT  
PLEASE READ THIS AGREEMENT CAREFULLY BEFORE PROCEEDING. YOU MUST CHECK "I AGREE" BELOW TO ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO IT. IF YOU DO NOT ACCEPT THIS AGREEMENT, DO NOT ORDER OR APPROVE THE ISSUANCE OF A DIGITAL CERTIFICATE. IF YOU HAVE ANY QUESTIONS REGARDING THIS AGREEMENT, PLEASE E-MAIL DIGICERT AT LEGAL@DIGICERT.COM OR CALL 1-800-896-7973. THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE

These certificate terms of use are between DigiCert, Inc., a Utah corporation ("DigiCert") and the entity applying for a Certificate, as identified in the account or issued certificates. "Certificate" means a digitally signed electronic data file issued by DigiCert to a person, group, or role in order to confirm your authorization for use of the Private Key corresponding to the Public Key contained in the certificate. You and DigiCert agree as follows:

I agree to the terms of the subscriber agreement

Your Personal ID will be valid for 3 years from the time it is issued. You have until January 19, 2016 to generate this certificate or you will need to contact your organization administrator to request a new email.

If your web server is configured to require "Client Authentication", you may need to configure it to allow client certs issued by DigiCert SHA2 Assured ID CA, as well as DigiCert Assured ID CA-1.

Due to new security standards, any SSL certificate expiring on or after January 1, 2017, will be issued using SHA-2 regardless of whether SHA-2 is chosen.

Generate Certificate

**ACCEPTER LE « CONTRAT »**

# Génération du certificat – 2/5

**VALIDER LA GÉNÉRATION DU CERTIFICAT DANS LE NAVIGATEUR**

**Generate your DigiCert Premium Certificate**

For technical assistance or to make corrections, contact your administrator.

**DigiCert Personal ID Details**

**Name:** DUCHMOLLALBERT

**Email Address:** albert.duchmoll@univ-lille.fr

**Organization:** UNIVERSITE LILLE

**Subscriber Agreement:** CERTIFICATE SUBSCRIBER AGREEMENT  
PLEASE READ THIS AGREEMENT CAREFULLY BEFORE PROCEEDING. YOU MUST CHECK "I AGREE" BELOW TO ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO IT. IF YOU DO NOT ACCEPT THIS AGREEMENT, DO NOT ORDER OR APPROVE THE ISSUANCE OF A DIGITAL CERTIFICATE. IF YOU HAVE ANY QUESTIONS REGARDING THIS AGREEMENT, PLEASE E-MAIL DIGICERT AT LEGAL@DIGICERT.COM OR CALL 1-800-896-7973. THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE  
These certificate terms of use are between DigiCert, Inc., a Utah corporation ("DigiCert") and the entity applying for a Certificate, as identified in the account or issued certificates. "Certificate" means a digitally signed electronic data file issued by DigiCert to a person, group, or role in order to confirm your authorization for use of the Private Key corresponding to the Public Key contained in the Certificate. You and DigiCert agree as follows:

I agree to the terms of the subscriber agreement

Your Personal ID will be valid for 3 years from the time it is issued. You have until January 19, 2016 to generate this certificate or you will need to contact your organization administrator to request a new email.

If your web server is configured to require "Client Authentication", you may need to configure it to allow client certs issued by DigiCert SHA2 Assured ID CA, as well as DigiCert Assured ID CA-1.

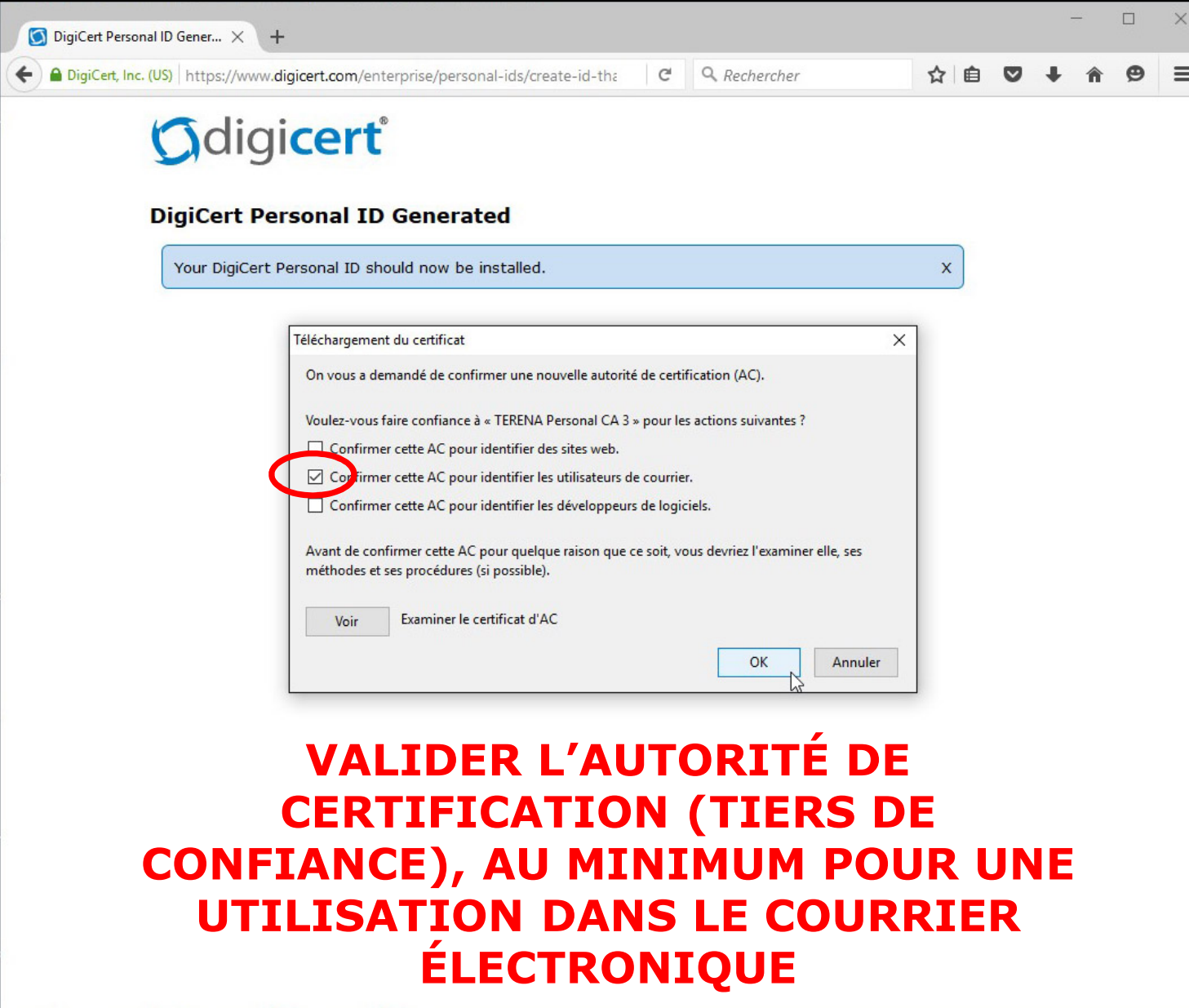
Due to new security standards, any SSL certificate expiring on or after January 1, 2017, will be issued using SHA-2 regardless of whether SHA-2 is chosen.

**Generate Certificate**

# Génération du certificat – 3/5

**LE CERTIFICAT EST STOCKÉ DANS LE « MAGASIN » DE CERTIFICATS DU NAVIGATEUR (OU DE L'UTILISATEUR SI LE NAVIGATEUR EST INTERNET EXPLORER)**

# Génération du certificat – 4/5



**DigiCert Personal ID Generated**

Your DigiCert Personal ID should now be installed.

**Téléchargement du certificat**

On vous a demandé de confirmer une nouvelle autorité de certification (AC).

Voulez-vous faire confiance à « TERENA Personal CA 3 » pour les actions suivantes ?

- Confirmer cette AC pour identifier des sites web.
- Confirmer cette AC pour identifier les utilisateurs de courrier.
- Confirmer cette AC pour identifier les développeurs de logiciels.

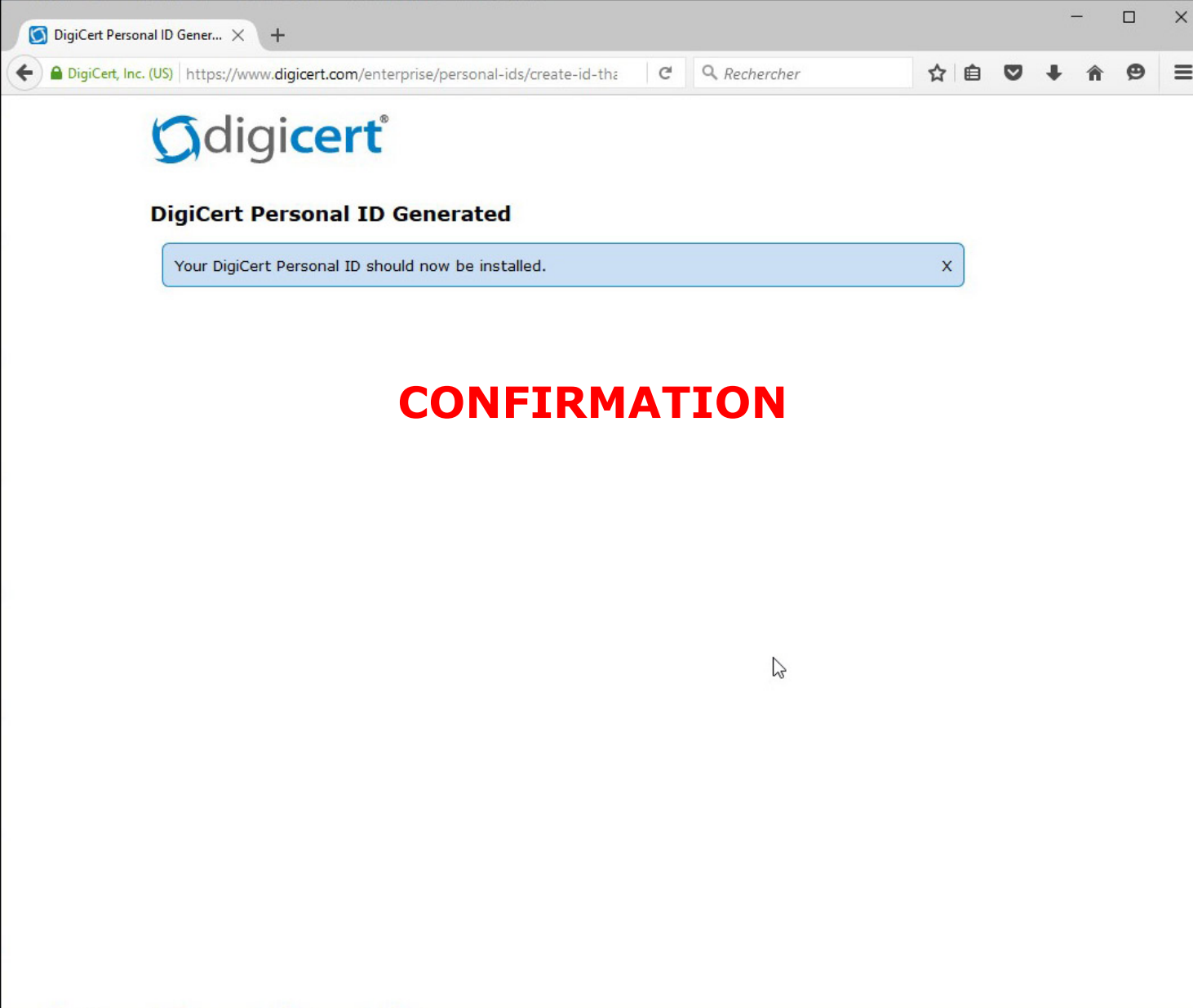
Avant de confirmer cette AC pour quelque raison que ce soit, vous devriez l'examiner elle, ses méthodes et ses procédures (si possible).

Voir Examen le certificat d'AC

OK Annuler

**VALIDER L'AUTORITÉ DE CERTIFICATION (TIERS DE CONFIANCE), AU MINIMUM POUR UNE UTILISATION DANS LE COURRIER ÉLECTRONIQUE**

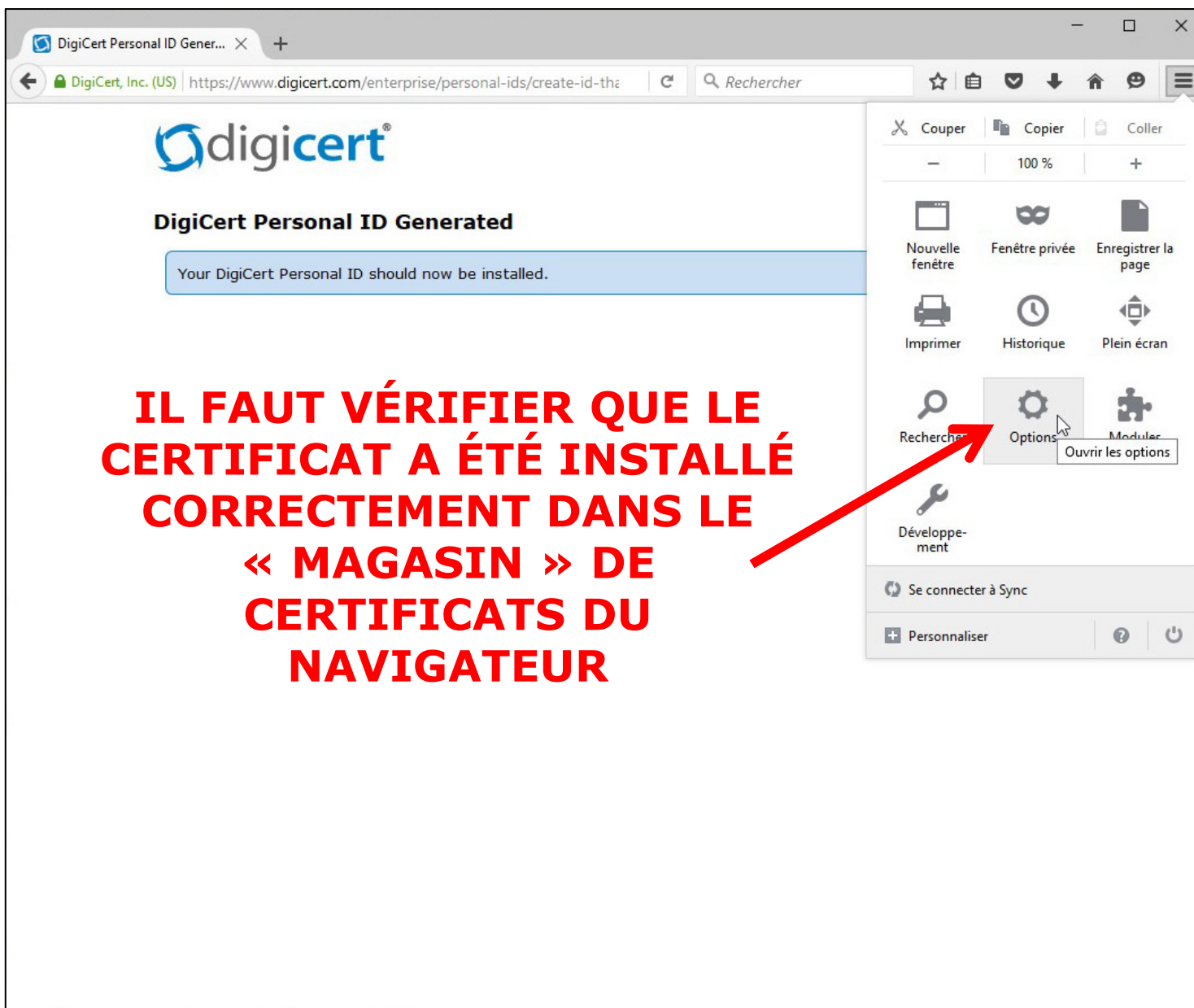
# Génération du certificat – 5/5



The screenshot shows a web browser window with the following elements:

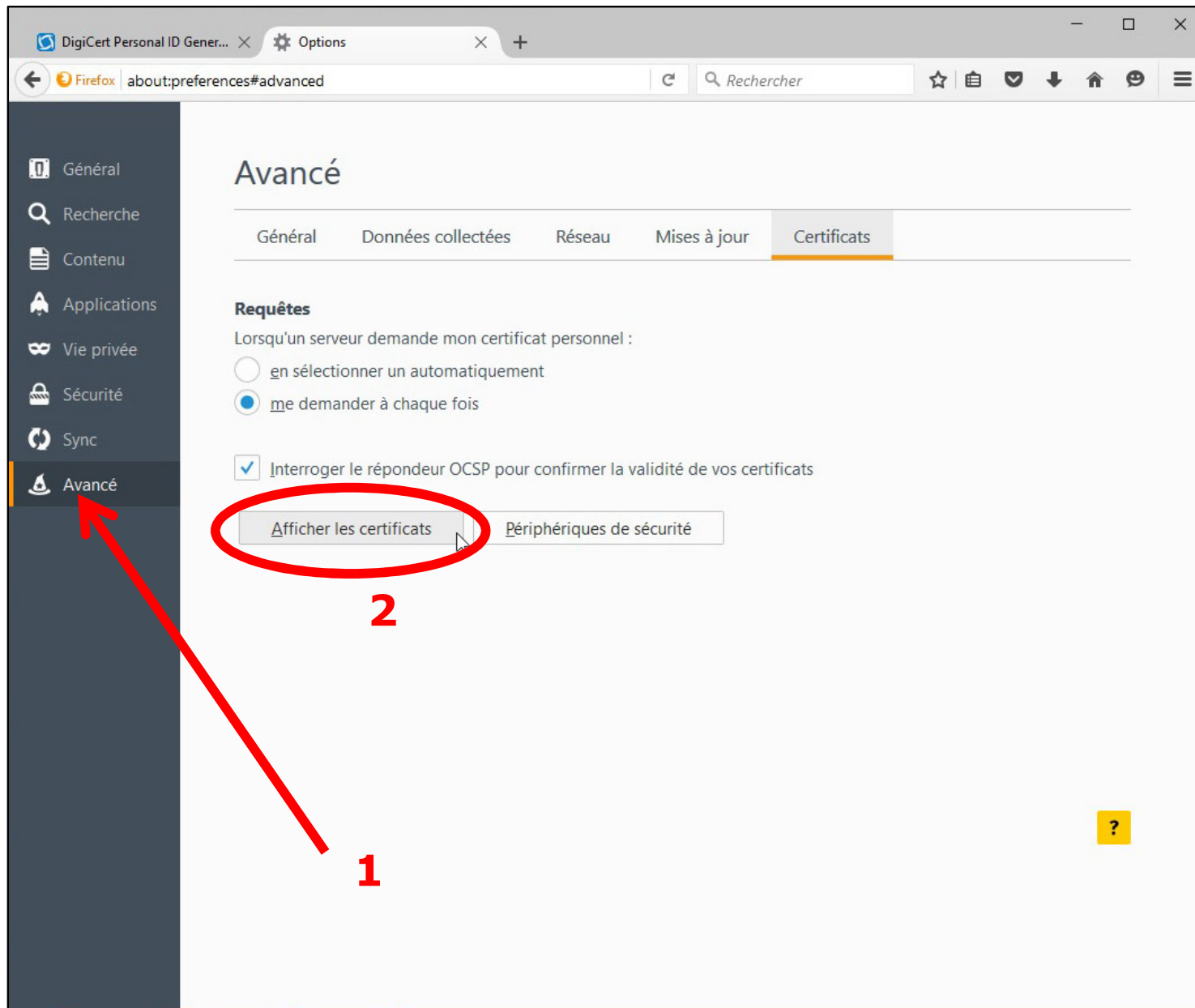
- Browser tab: DigiCert Personal ID Gener... X +
- Address bar: DigiCert, Inc. (US) | https://www.digicert.com/enterprise/personal-ids/create-id-thz | Rechercher
- Logo: digicert®
- Section Header: DigiCert Personal ID Generated
- Message box: Your DigiCert Personal ID should now be installed. X
- Large red text: **CONFIRMATION**

# Vérifier la présence du certificat – 1/4



**IL FAUT VÉRIFIER QUE LE CERTIFICAT A ÉTÉ INSTALLÉ CORRECTEMENT DANS LE « MAGASIN » DE CERTIFICATS DU NAVIGATEUR**

# Vérifier la présence du certificat – 2/4



# Vérifier la présence du certificat – 3/4

**1**

**UN CERTIFICAT PERSONNEL DOIT ÊTRE PRÉSENT**

Nom du certificat	Périphérique de sécurité	Numéro de série	Expire le
TERENA			
DUCHMOLL ALBERT	Sécurité personnelle	08:4F:16:19:E3:BD:9A:BA:6...	samedi 22 décembre...

**2**

**AFFICHER SES PROPRIÉTÉS**



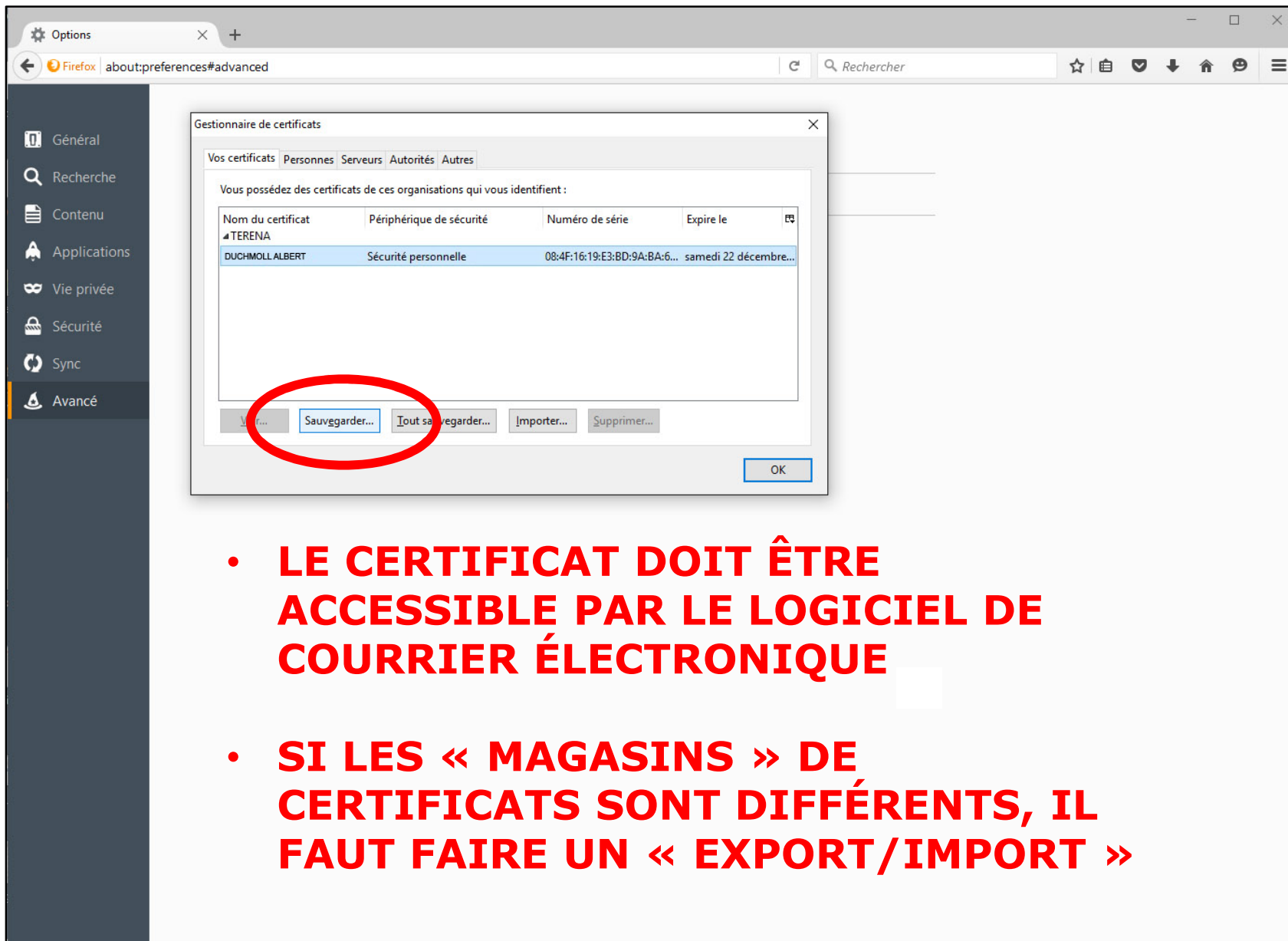
# Vérifier la présence du certificat – 4/4

The screenshot shows the Firefox 'Options' window, specifically the 'Avancé' (Advanced) section. A dialog box titled 'Détails du certificat : "ID TERENA de DUCHMOLL ALBERT"' is open, displaying the following information:

- Ce certificat a été vérifié pour les utilisations suivantes :**
  - Certificat client SSL
  - Certificat de signature de courrier
  - Certificat de réception de courrier
- Émis pour**
  - Nom commun (CN): DUCHMOLL ALBERT
  - Organisation (O): UNIVERSITE LILLE
  - Unité d'organisation (OU): <Ne fait pas partie du certificat>
  - Numéro de série: 08:4F:16:19:E3:BD:9A:BA:6C:9B:35:8B:81:F2:EA:CD
- Émis par**
  - Nom commun (CN): TERENA Personal CA 3
  - Organisation (O): TERENA
  - Unité d'organisation (OU): <Ne fait pas partie du certificat>
- Période de validité**
  - Début le: mardi 22 décembre 2015
  - Expire le: samedi 22 décembre 2018
- Empreintes numériques**
  - Empreinte numérique SHA-256: FD:FF:2B:6F:C7:DA:2A:5F:32:C9:E0:64:B0:D7:59:C6:66:00:13:DC:C1:BF:60:F8:C7:20:EC:A5:3C:93:7D:00
  - Empreinte numérique SHA1: 8F:67:02:E0:5F:4D:91:75:51:B7:F3:A2:E9:96:AE:8A:BB:C6:4D:79

Red arrows point from the text 'VÉRIFIER' to the 'USAGES', 'NOM', and 'VALIDITÉ (3 ANS)' sections. The word 'VÉRIFIER' is written in large red letters on a grey background box.

# Sauvegarder le certificat dans un fichier – 1/4



The screenshot shows the Firefox 'Gestionnaire de certificats' (Certificate Manager) window. The 'Vos certificats' tab is active, displaying a table of certificates. The first certificate is highlighted in blue:

Nom du certificat	Périphérique de sécurité	Numéro de série	Expire le
TERENA			
DUCHMOLL ALBERT	Sécurité personnelle	08:4F:16:19:E3:BD:9A:BA:6...	samedi 22 décembre...

The 'Sauvegarder...' button is circled in red. Other buttons visible are 'Tout sauvegarder...', 'Importer...', 'Supprimer...', and 'OK'.

- **LE CERTIFICAT DOIT ÊTRE ACCESSIBLE PAR LE LOGICIEL DE COURRIER ÉLECTRONIQUE**
- **SI LES « MAGASINS » DE CERTIFICATS SONT DIFFÉRENTS, IL FAUT FAIRE UN « EXPORT/IMPORT »**

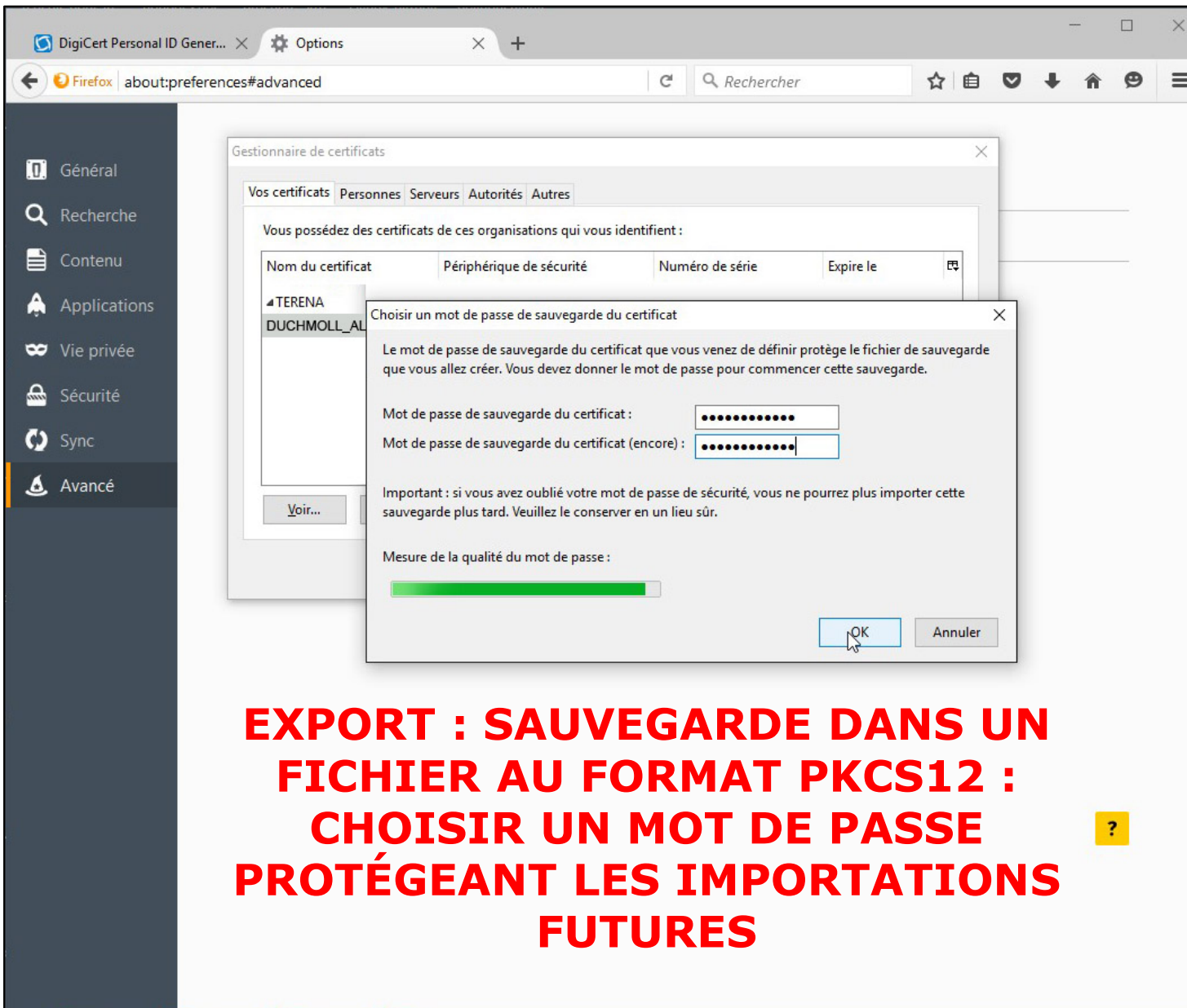
# Sauvegarder le certificat dans un fichier – 2/4

The screenshot shows the Firefox 'Gestionnaire de certificats' (Certificate Manager) window. The 'Vos certificats' tab is active, displaying a table of certificates. One certificate is selected: 'DUCHMOLL ALBERT' issued by 'Sécurité personnelle' with a serial number '08:4F:16:19:E3:BD:9A:BA:6...' and an expiration date of 'samedi 22 décembre...'. Below this, a 'Nom de fichier à sauvegarder' (Save File Name) dialog box is open. The file name is 'DUCHMOLL\_ALBERT - Terena\_Personnal\_CA3-20151222-20181222.p12' and the type is 'Fichiers PKCS12 (\*.p12)'. The file is being saved to the path 'Ce PC > DONNEES (E:) > certificats > Certificats\_personnels-RENATER'. A large red text overlay is centered over the dialog box.

Nom du certificat	Périphérique de sécurité	Numéro de série	Expire le
TERENA			
DUCHMOLL ALBERT	Sécurité personnelle	08:4F:16:19:E3:BD:9A:BA:6...	samedi 22 décembre...

**EXPORT : SAUVEGARDE  
DANS UN FICHIER AU  
FORMAT PKCS12 :  
CHOISIR  
L'EMPLACEMENT, ET  
UN NOM SIGNIFICATIF**

# Sauvegarder le certificat dans un fichier – 3/4



The screenshot shows the Firefox 'Gestionnaire de certificats' (Certificate Manager) dialog box. The 'Vos certificats' tab is active, displaying a table of certificates. A sub-dialog box titled 'Choisir un mot de passe de sauvegarde du certificat' is overlaid on top. This sub-dialog contains two password input fields, a warning message, and a password strength meter. The warning message reads: 'Important : si vous avez oublié votre mot de passe de sécurité, vous ne pourrez plus importer cette sauvegarde plus tard. Veuillez le conserver en un lieu sûr.' The password strength meter shows a green bar, indicating a strong password. The 'OK' button is highlighted with a mouse cursor.

**EXPORT : SAUVEGARDE DANS UN FICHER AU FORMAT PKCS12 : CHOISIR UN MOT DE PASSE PROTÉGEANT LES IMPORTATIONS FUTURES**

# Sauvegarder le certificat dans un fichier – 4/4

**EXPORT TERMINÉ : COPIER LE FICHER AU FORMAT PKCS12 EN LIEU SÛR (EX : CLEF USB STOCKÉE DANS UN « COFFRE »)**

# Importer le certificat dans la messagerie – 1/7

**LOGICIEL DE COURRIER ÉLECTRONIQUE**

1

2

3

4

**AFFICHAGE DU « MAGASIN » DE CERTIFICATS DU LOGICIEL DE COURRIER ÉLECTRONIQUE**

Options

Général Affichage Rédaction Messagerie instantanée Vie privée Sécurité Pièces jointes Avancé Agenda SOGo

Général Lecture et affichage Réseau et espace disque Mise à jour Certificats

Lorsqu'un serveur demande mon certificat personnel :

en sélectionnant un automatiquement  me demander chaque fois

Voir les certificats Validation Périphériques de sécurité

OK Annuler

# Importer le certificat dans la messagerie – 2/7

Courrier entrant - albert.duchm... Agenda x Create Your DigiCert Prem... x

Relever Écrire Chat Adresses Étiquette Filtre rapide Rechercher... <Ctrl+K>

De DigiCert <admin@digicert.com> ☆ Répondre Transférer Archiver Indésirable Supprimer

Sujet **Create Your DigiCert Premium Certificate** 09:56

Pour Moi <albert.duchmoll@univ-lille.fr> Autres actions ▾

**RENATER** | **digicert**  
CONNECTEUR DE SAVOIRS

**Université Lille**

HI DUCH... Options

You have b... Général Affichage Rédaction Messagerie instantanée Vie privée Sécurité Pièces jointes Avancé Agenda SOGo

https://www... Général Lecture et affichage Réseau et espace disque Mise à jour Certificats

Thanks! Lorsqu'un serveur demande mon certificat personnel :

The Digi... en sélectionner... Voir les certificats

**Gestionnaire de certificats**

Vos certificats Personnes Serveurs Autorités Autres

Vous possédez des certificats de ces organisations qui vous identifient :

Nom du certificat	Périphérique de sécurité	Numéro de série	Expire le
<b>IMPORT NÉCESSAIRE</b>			

Voir... Sauvegarder... Tout sauvegarder... Importer... Supprimer... OK

# Importer le certificat dans la messagerie – 3/7

The screenshot shows an email client interface with an email from DigiCert. The email content includes logos for RENATER and digicert, and the text "Université Lille". A file explorer window is open over the email content, showing a file named "DUCHMOLL\_ALBERT-Terena\_Personnal\_CA3-20151222-20181222.p12" selected. A red text overlay reads "IMPORTANT : DÉSIGNER LE FICHIER AU FORMAT PKCS12".

**IMPORTANT : DÉSIGNER LE FICHIER AU FORMAT PKCS12**



# Importer le certificat dans la messagerie – 4/7

The screenshot shows an email client window with the following details:

- Subject: Create Your DigiCert Premium Certificate
- Sender: DigiCert <admin@digicert.com>
- Recipient: Moi <albert.duchmoll@univ-lille.fr>

The email content includes logos for RENATER (CONNECTEUR DE SAVOIRS) and digicert, and the text "Université Lille".

Overlaid on the screenshot is a red text box with the following message:

**ATTENTION ! CE MOT DE PASSE EST LE MOT DE PASSE « PASSE « MAÎTRE » (THUNDERBIRD), PAS CELUI PERMETTANT D'OUVRIR LE FICHIER AU FORMAT PKCS12**

A red arrow points from this text box to a "Mot de passe requis" (Password required) dialog box. The dialog box contains the text: "Veillez saisir le mot de passe principal de Sécurité personnelle." (Please enter the main Personal Security password.) and a password input field with masked characters. The dialog has "OK" and "Annuler" (Cancel) buttons.

# Importer le certificat dans la messagerie – 5/7

The screenshot shows an email client interface with a message from DigiCert. The message content includes logos for RENATER and digicert, and the text "Université Lille". A "Gestionnaire de certificats" window is open, displaying a list of certificates. A "Fenêtre de saisie du mot de passe" (Password prompt) dialog box is overlaid on the certificate manager, asking for a portable security password. A red arrow points from the text box to the password prompt.

**CE MOT DE PASSE EST CELUI PERMETTANT D'OUVRIR LE FICHER AU FORMAT PKCS12**

# Importer le certificat dans la messagerie – 6/7

Courrier entrant - albert.duchm... Agenda x Create Your DigiCert Prem... x

Relever Écrire Chat Adresses Étiquette Filtre rapide Rechercher... <Ctrl+K>

De DigiCert <admin@digicert.com> ☆ Répondre Transférer Archiver Indésirable Supprimer

Sujet **Create Your DigiCert Premium Certificate** 09:56

Pour Moi <albert.duchmoll@univ-lille.fr> Autres actions ▾

**RENATER** | **digicert**  
CONNECTEUR DE SAVOIRS

**Université Lille**

Hi DUCH Options

You have b

Create yo

https://www

Thanks!

The Digi

Général Lecture et affichage Réseau et espace disque Mise à jour Certificats

Lorsqu'un serveur demande mon certificat personnel :

en sélectionner t

Voir les certificats

Gestionnaire de certificats

Vos certificats Personnes Serveurs Autorités Autres

Vous possédez des certificats de ces organisations qui vous identifient :

Nom du certificat	Périphérique de sécurité	Numéro de série	Expire le

Alerte

⚠ Récupération des certificats et clés privées réussie.

OK

Voir... Sauvegarder... Tout sauvegarder... Importer... Supprimer...

OK

Eric.Ca

tal : 52 22 Panneau « Aujourd'hui »

# Importer le certificat dans la messagerie – 7/7

Courrier entrant - albert.duchm... | Agenda | Create Your DigiCert Prem... x

Relever | Écrire | Chat | Adresses | Étiquette | Filtre rapide | Rechercher... <Ctrl+K>

De DigiCert <admin@digicert.com> ☆ | Répondre | Transférer | Archiver | Indésirable | Supprimer | 09:56

Sujet **Create Your DigiCert Premium Certificate**

Pour Moi <albert.duchmoll@univ-lille.fr> | Autres actions ▾

**RENATER** | **digicert**  
CONNECTEUR DE SAVOIRS

**Université Lille**

Hi DUCH...  
You have b...  
Create you...  
<https://www...>  
Thanks!  
The Digi...

Options  
Général | Affichage | Rédaction | Messagerie instantanée | Vie privée | Sécurité | Pièces jointes | Avancé | Agenda | SOGo

Général | Lecture et affichage | Réseau et espace disque | Mise à jour | Certificats

Lorsqu'un serveur demande mon certificat personnel...  
 en sélectionner...  
Voir les certificats

Gestionnaire de certificats  
Vos certificats | Personnes | Serveurs | Autorités | Autres

Vous possédez des certificats de ces organisations qui vous identifient :

Nom du certificat	Périphérique de sécurité	Numéro de série	Expire le
TERENA			
DUCHMOLL ALBERT	Sécurité personnelle	08:4F:16:19:E3:BD:9A:BA:6...	22/12/2018

**IMPORT TERMINÉ = CERTIFICAT PRÉSENT**

Voir... | Sauvegarder... | Tout sauvegarder... | Importer... | Supprimer... | OK

# Définir le certificat pour la « signature » – 1/4

**1**

**2**

**3**

**CONFIGURER LE LOGICIEL DE COURRIER ELECTRONIQUE POUR UTILISER LE CERTIFICAT QUI VIENT D'ÊTRE IMPORTÉ**

# Définir le certificat pour la « signature » – 2/4

Paramètres des comptes Courrier et Groupes

**Sélectionner un certificat**

Certificat : ID TERENA de DUCHMOLL ALBERT [08:4F:16:19:E3:BD:9A:BA:6C:9B:35:8B:B1:F2:EA:CD]

Détails du certificat sélectionné :

Émis pour : CN=DUCHMOLL ALBERT O=UNIVERSITE LILLE, L=Villeneuve d'Ascq, ST=NORD, C=FR  
Numéro de série: 08:4F:16:19:E3:BD:9A:BA:6C:9B:35:8B:B1:F2:EA:CD  
Valide de 22/12/2015 01:00:00 pour 22/12/2018 13:00:00  
Usage de la clé de certificat: Signature, Chiffrement de la clé  
Adresse électronique: albert.duchmoll@univ-lille.fr  
Émis par : CN=TERENA Personal CA 3, O=TERENA, L=Amsterdam, ST=Amsterdam-Holland, C=NL  
Stocké dans : Sécurité personnelle

OK Annuler

**SÉLECTIONNER LE BON CERTIFICAT**

# Définir le certificat pour la « signature » – 3/4

Thunderbird

Vous devriez aussi spécifier un certificat que d'autres personnes peuvent utiliser pour vous envoyer du courrier chiffré. Voulez-vous utiliser le même certificat pour chiffrer et déchiffrer les messages qui vous sont envoyés ?

**UTILISER LE MÊME CERTIFICAT POUR LE CHIFFREMENT (FACULTATIF)**

# Définir le certificat pour la « signature » – 4/4

The screenshot shows the Outlook 'Paramètres des comptes Courrier et Groupes' dialog box, specifically the 'Sécurité' (Security) tab. The 'Signature' section is active, showing a checked checkbox for 'Signer les messages numériquement' (Digitally sign messages). A red arrow points to this checkbox. The background shows an email from DigiCert with the subject 'Create Your DigiCert Premium Certificate'.

**INDIQUER QU'ON VEUT « SIGNER » TOUS LES MAILS**

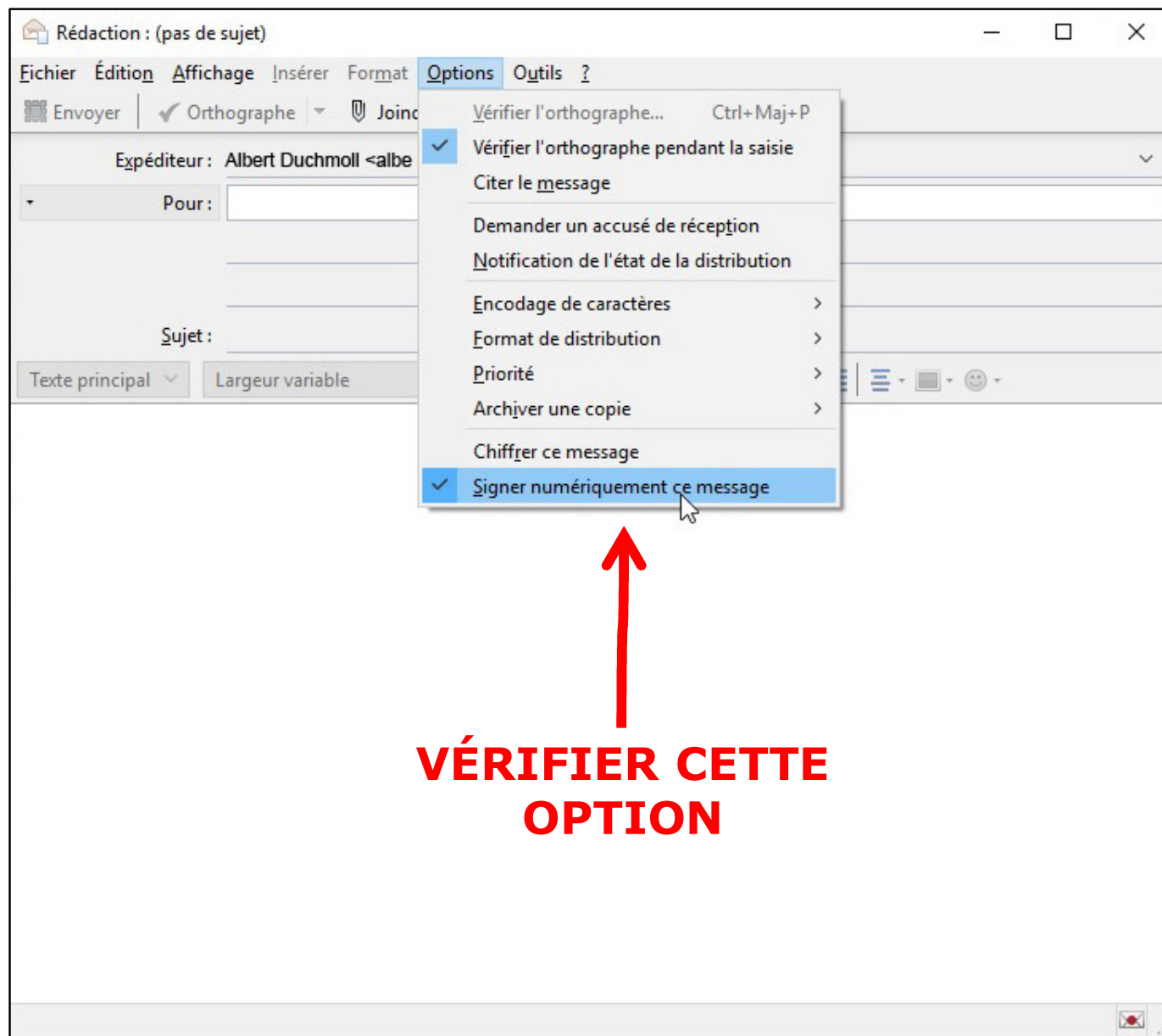


# Vérifier l'égalité entre son adresse d'émetteur et l'adresse électronique contenue dans le certificat (« Nom alternatif du sujet du certificat »)

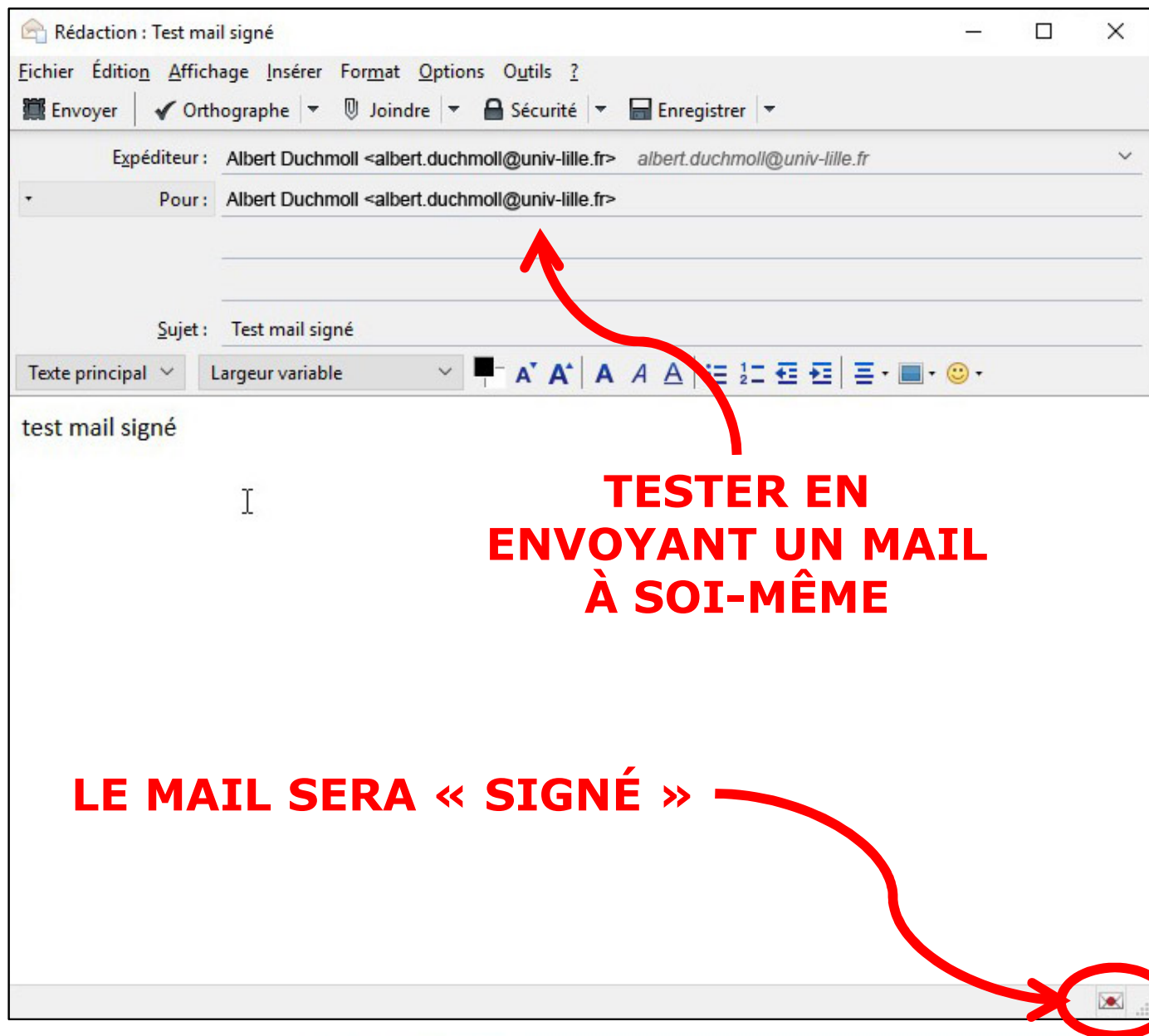
The image shows two overlapping windows from a Windows operating system. The left window is titled "Paramètres des comptes Courrier et Groupes" and displays the configuration for the account "albert.duchmoll@univ-lille.fr". The "Paramètres du compte" section is active, showing the account name, email address, and other settings. The email address "albert.duchmoll@univ-lille.fr" is circled in red. The right window is titled "Détails du certificat : 'ID TERENA de DUCHMOLL ALBERT'" and shows the details of a certificate. The "Nom alternatif du sujet du certificat" field is highlighted in blue, and its value "albert.duchmoll@univ-lille.fr" is circled in red. A red callout box at the bottom of the image contains the text: "!!! Configurer le logiciel de messagerie pour émettre avec EXACTEMENT la même adresse que celle qui est stockée dans le certificat (respecter majuscules/minuscules) !!!".

!!! Configurer le logiciel de messagerie pour émettre avec **EXACTEMENT** la même adresse que celle qui est stockée dans le certificat (respecter majuscules/minuscules) !!!

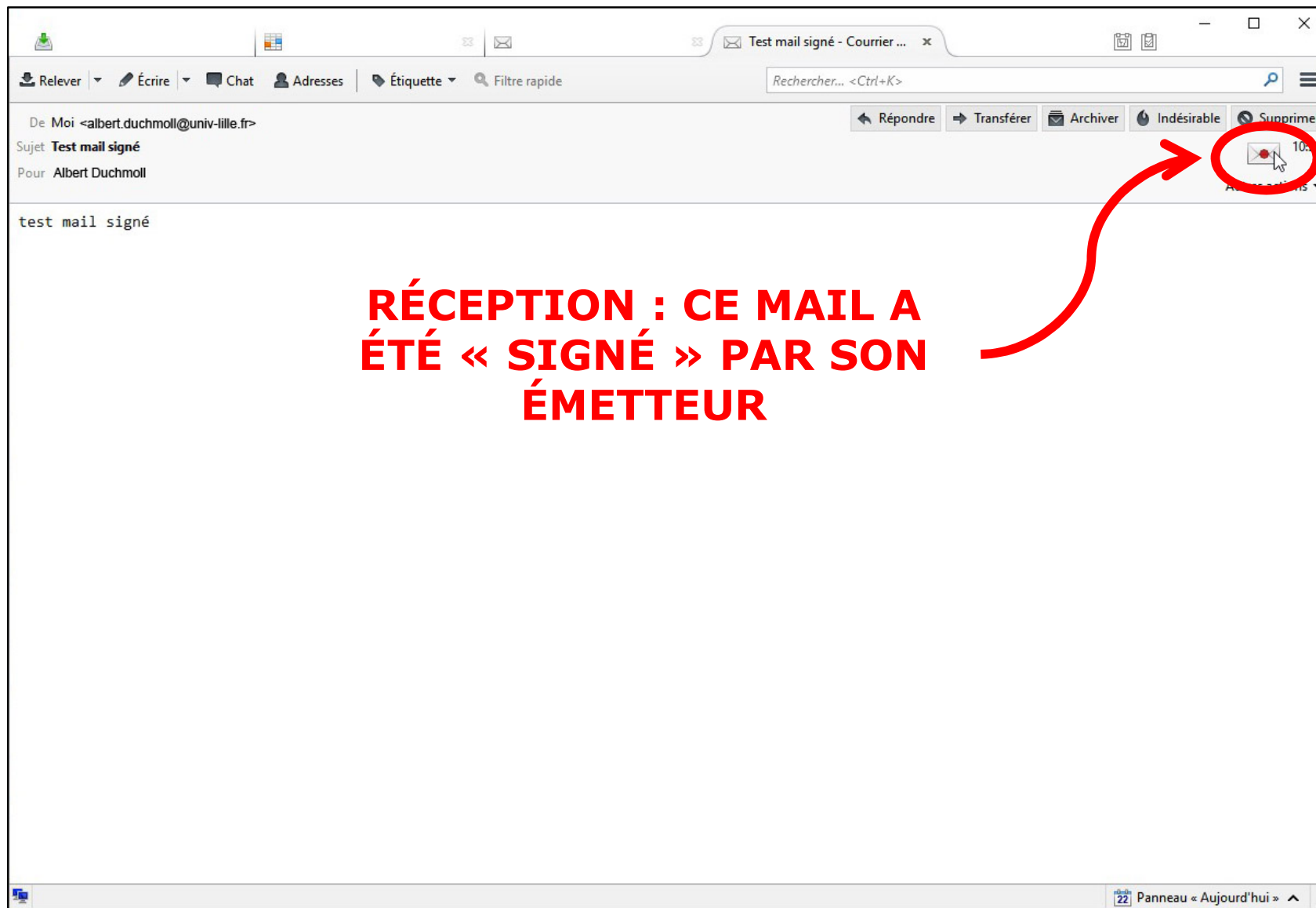
# Tester en « signant » un mail – 1/2



# Tester en « signant » un mail – 2/2



# Vérifier la « signature » d'un mail – 1/2



# Vérifier la « signature » d'un mail – 2/2

The screenshot shows an email client interface with a message titled "Test mail signé" from "Moi <albert.duchmol@univ-lille.fr>". The message content is "test mail signé". A security warning dialog box titled "Sécurité des messages" is open, displaying the following information:

- Ce message est signé**  
Ce message inclut une signature numérique valide. **Ce message n'a pas été modifié** depuis qu'il a été envoyé.
- Signé par : **DUCHMOLL ALBERT**
- Adresse électronique : **albert.duchmol@univ-lille.fr**
- Certificat fourni par : TERENA Personal CA 3
- [Voir la signature du certificat](#)
- Message non chiffré**  
Ce message n'a pas été chiffré avant d'être envoyé. Les informations envoyées sur Internet sans être chiffrées peuvent être vues par d'autres personnes pendant leur parcours.

Red arrows point from the text "L'ÉMETTEUR EST AUTHENTIFIÉ" to the sender's name "DUCHMOLL ALBERT" and from "LE CONTENU N'A PAS ÉTÉ ALTÉRÉ" to the text "Ce message n'a pas été modifié".

- GARANTIES :**
- **L'ÉMETTEUR EST AUTHENTIFIÉ**
  - **LE CONTENU N'A PAS ÉTÉ ALTÉRÉ**

# **ANNEXE 1**

# **CONFIGURATION DU WEBMAIL ZIMBRA**

# Importer le certificat – 1/4

The screenshot shows the Zimbra web interface for 'Préférences' (Preferences) under 'Secure Email'. The 'Default Setting for New Emails' section has 'Do not sign or encrypt' selected. The 'Certificate' section prompts the user to upload a certificate, with a red circle highlighting the 'Browse to certificate...' button. A calendar for May 2018 is visible at the bottom left.

**IMPORT NÉCESSAIRE**

# Importer le certificat – 2/4

The screenshot shows the Zimbra webmail interface for the University of Lille. The 'Préférences' (Preferences) page is open, specifically the 'Secure Email' section. The 'Default Setting for New Emails' is set to 'Do not sign or encrypt'. The 'Certificate' section prompts the user to upload a certificate, with a 'Browse to certificate...' button. A file explorer window is open, showing the file 'DUCHMOLL\_ALBERT-20180502.p12' selected in the 'certificats' folder. A red text overlay reads 'IMPORTANT : DÉSIGNER LE FICHER AU FORMAT PKCS12'.

**IMPORTANT : DÉSIGNER LE FICHER AU FORMAT PKCS12**



# Importer le certificat – 3/4

Zimbra: Préférences: Secure Em X +

https://zimbra.univ-lille.fr/mail#2

Rechercher

Rechercher Albert Duchmoll

Mail Contacts Calendrier Tâches Préférences

Enregistrer Annuler Annuler les modifications

Préférences

- Général
- Comptes
- Mail
- Secure Email**
- Filtres
- Signatures
- Hors du bureau
- Adresses acceptées
- Contacts
- Calendrier
- Partage
- Notifications
- Périphériques et applis connectés
- Importer/Exporter
- Raccourcis

**Secure Email**

**Default Setting for New Emails**

You can change this when sending an email.

- Remember setting from last email
- Do not sign or encrypt
- Sign only
- Sign and encrypt

**Certificate**

Uploading and verifying... Valid file types are .p12 and .pfx

Drag and Drop a certificate here or [Browse to certificate...](#)

**Password Required**

Please enter password for this certificate:

.....

Submit Cancel

**MOT DE PASSE PERMETTANT D'OUVRIR LE FICHER AU FORMAT PKCS12**

« « Mai 2018 » »

Lun	Mar	Mer	Jeu	Ven	Sam	Dim
30	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

# Importer le certificat – 4/4

Zimbra: Préférences: Secure Em X

https://zimbra.univ-lille.fr/mail#2

Rechercher

Rechercher Albert Duchmoll

Mail Contacts Calendrier Tâches Préférences

Enregistrer Annuler Annuler les modifications

Préférences

- Général
- Comptes
- Mail
- Secure Email**
- Filtres
- Signatures
- Hors du bureau
- Adresses acceptées
- Contacts
- Calendrier
- Partage
- Notifications
- Périphériques et applis connectés
- Importer/Exporter
- Raccourcis

**Secure Email**

**Default Setting for New Emails**  
You can change this when sending an email.

- Remember setting from last email
- Do not sign or encrypt
- Sign only
- Sign and encrypt

**Certificate**

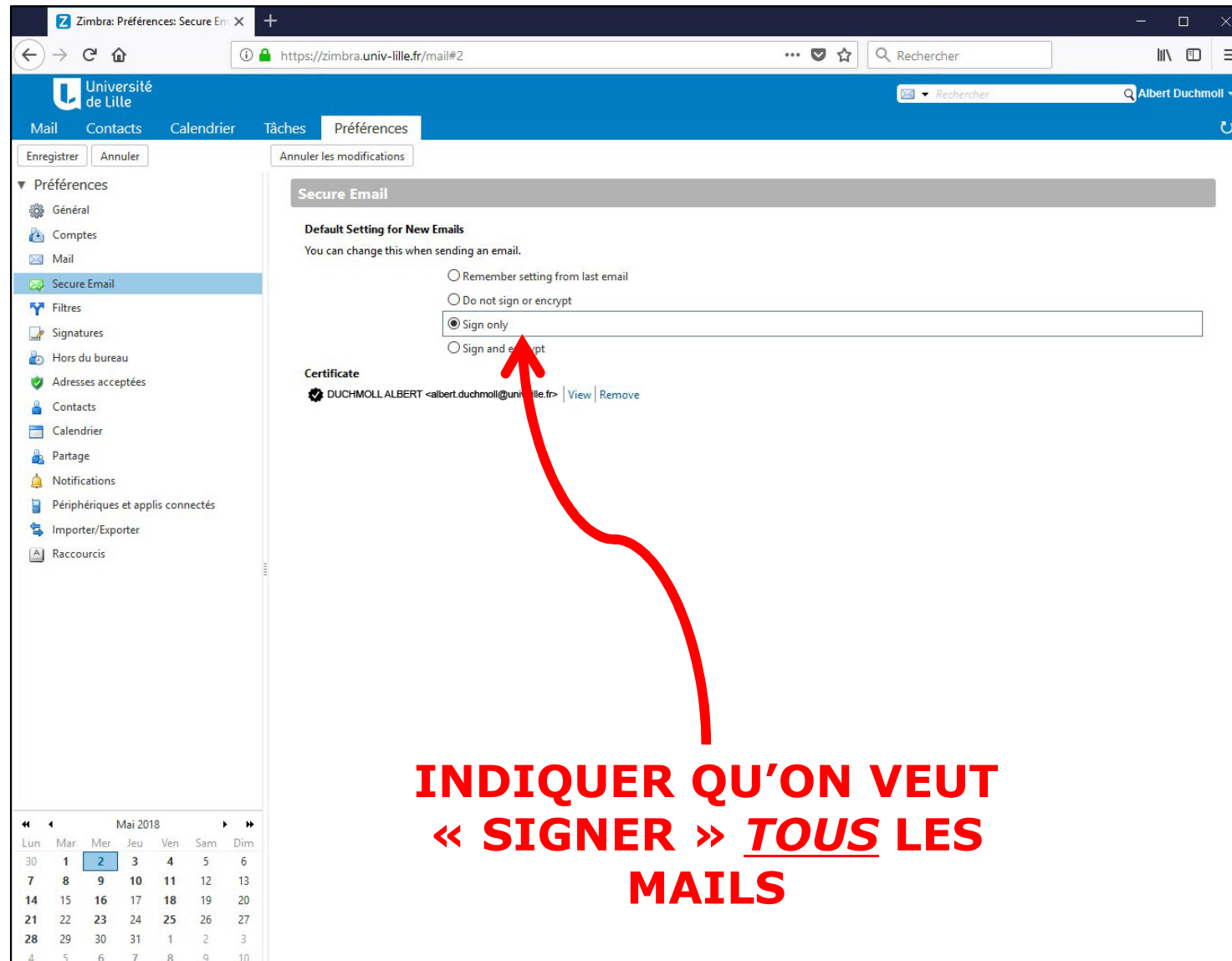
- DUCHMOLL ALBERT <albert.duchmoll@univ-lille.fr> | [View](#) | [Remove](#)

**IMPORT TERMINÉ = CERTIFICAT PRÉSENT**

Mai 2018

Lun	Mar	Mer	Jeu	Ven	Sam	Dim
30	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

# Définir le certificat pour la « signature » - 1/1



Zimbra: Préférences: Secure Em... X

https://zimbra.univ-lille.fr/mail#2

Rechercher

Rechercher Albert Duchmoll

Mail Contacts Calendrier Tâches Préférences

Enregistrer Annuler Annuler les modifications

Préférences

- Général
- Comptes
- Mail
- Secure Email**
- Filtres
- Signatures
- Hors du bureau
- Adresses acceptées
- Contacts
- Calendrier
- Partage
- Notifications
- Périphériques et applis connectés
- Importer/Exporter
- Raccourcis

**Secure Email**

**Default Setting for New Emails**  
You can change this when sending an email.

- Remember setting from last email
- Do not sign or encrypt
- Sign only
- Sign and encrypt

**Certificate**  
DUCHMOLL.ALBERT <albert.duchmoll@univ-lille.fr> | View | Remove

INDIQUER QU'ON VEUT « SIGNER » TOUS LES MAILS

Mai 2018

Lun	Mar	Mer	Jeu	Ven	Sam	Dim
30	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

# Tester en « signant » un mail – 1/1

Expéditeur: Compte principal (Albert Duchmoll <albert.duchmoll@univ-lille.fr>)

À: Albert Duchmoll\*

Cc:

Sujet: Test mail signé

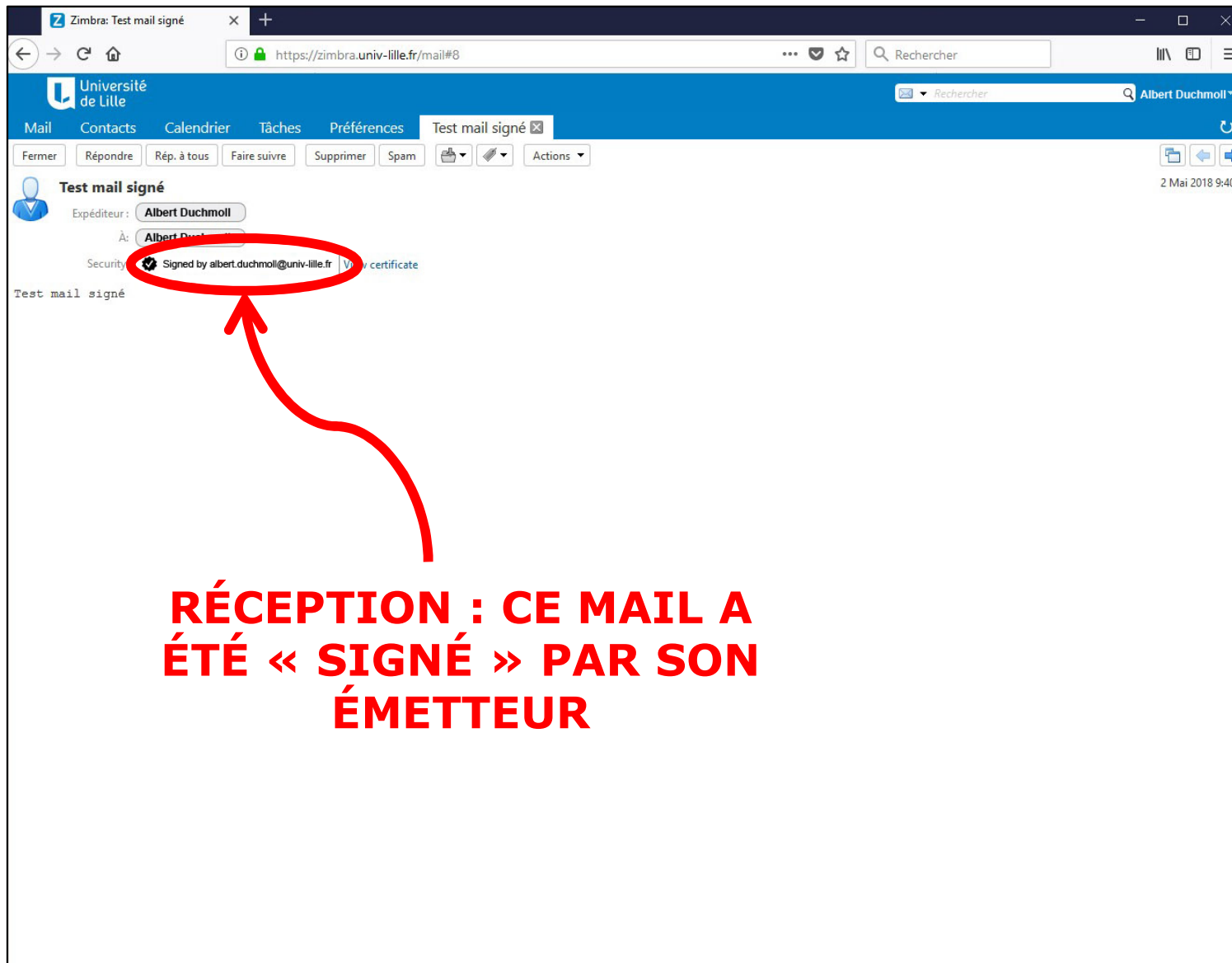
Joindre: Remarque : Pour joindre un ou plusieurs fichiers à ce mail, il vous suffit de les faire glisser depuis leur emplacement de stockage.

Test mail signé

**TESTER EN ENVOYANT UN MAIL À SOI-MÊME**

**LE MAIL SERA « SIGNÉ »**

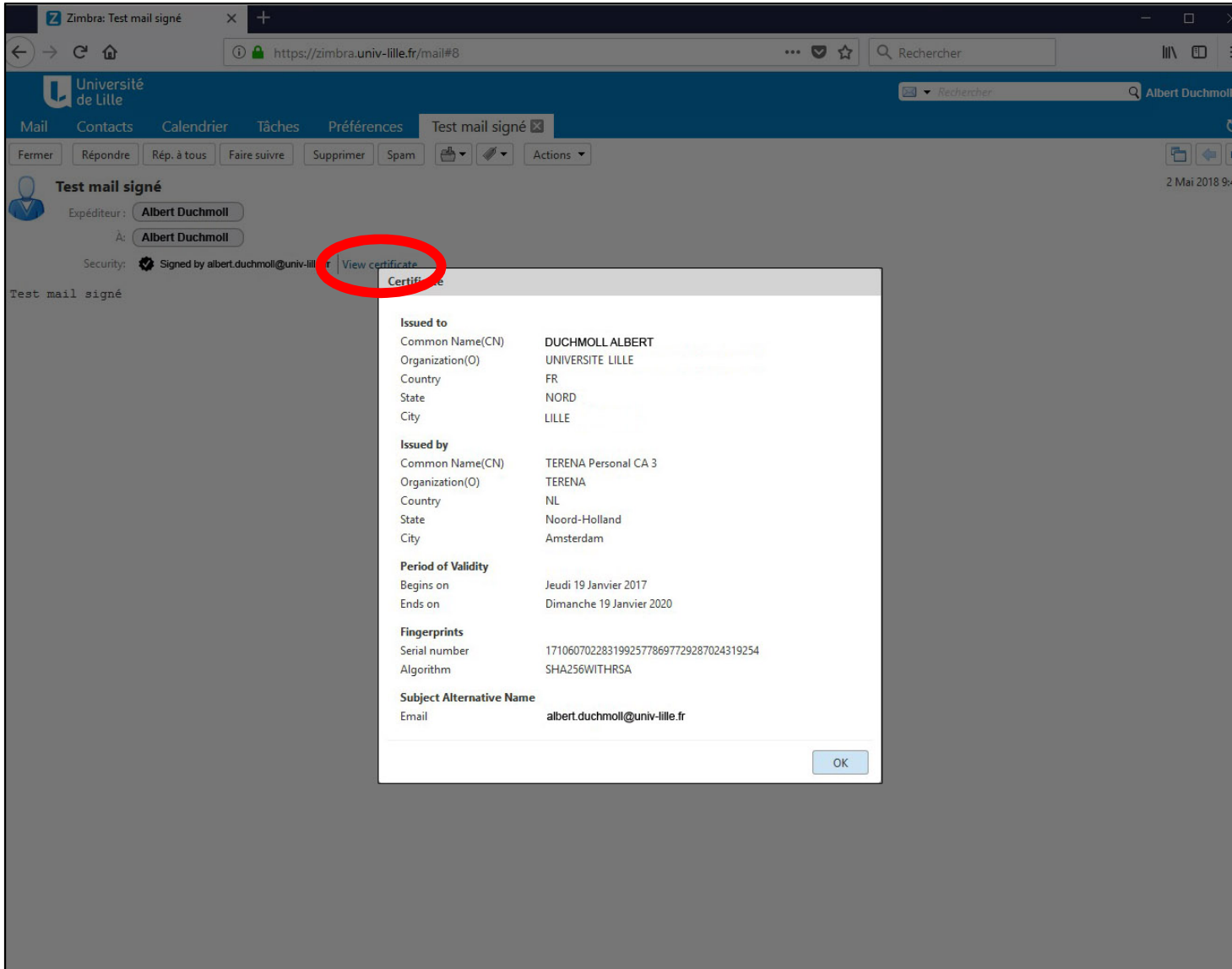
# Vérifier la « signature » d'un mail – 1/2



The screenshot shows a Zimbra web interface for a user named Albert Duchmoll. The email subject is "Test mail signé". The sender is listed as "Expéditeur: Albert Duchmoll". The recipient is "À: Albert Duchmoll". In the "Security" section, there is a checkmark icon and the text "Signed by albert.duchmoll@univ-lille.fr | View certificate". This text is circled in red. A red arrow points from this text to a large red text block below the screenshot.

**RÉCEPTION : CE MAIL A ÉTÉ « SIGNÉ » PAR SON ÉMETTEUR**

# Vérifier la « signature » d'un mail – 2/2



The screenshot shows a Zimbra web interface for an email titled "Test mail signé". The email is from Albert Duchmoll. A red circle highlights the "View certificate" link in the security information. A modal window titled "Certificat" is open, displaying the following details:

Issued to	
Common Name(CN)	DUCHMOLL ALBERT
Organization(O)	UNIVERSITE LILLE
Country	FR
State	NORD
City	LILLE

Issued by	
Common Name(CN)	TERENA Personal CA 3
Organization(O)	TERENA
Country	NL
State	Noord-Holland
City	Amsterdam

Period of Validity	
Begins on	Jeudi 19 Janvier 2017
Ends on	Dimanche 19 Janvier 2020

Fingerprints	
Serial number	17106070228319925778697729287024319254
Algorithm	SHA256WITHRSA

Subject Alternative Name	
Email	albert.duchmoll@univ-lille.fr