Secure Socket Layer (SSL)

Appareils concernés :

HL-4040CN	✓
HL-4050CDN	✓
HL-4070CDW	✓
DCP-9040CN	✓
DCP-9045CDN	✓
MFC-9440CN	✓
MFC-9840CDW	✓

Sommaire

1: Généralités

Le SSL (Secure Socket Layer) est une méthode efficace qui protège les données envoyées sur un réseau local ou longue distance ; il est désormais disponible sur les appareils réseau laser couleur de Brother. Il crypte les données envoyées sur un réseau, par ex. un travail d'impression, de manière à ce que toute personne essayant de capturer ces données ne puisse les lire.

Il peut être configuré sur les réseaux câblés et sans fil et il fonctionne avec d'autres outils de sécurité, tels que les pare-feu et les clés WPA.

2: Bref historique de SSL

Le SSL a été créé à l'origine pour sécuriser les informations circulant sur Internet, notamment les données envoyées entre les navigateurs Web et les serveurs. Par exemple, lorsque vous utilisez un service bancaire sur Internet, si vous voyez https:// et un petit cadenas en bas à droite du navigateur Web, cela signifie que vous utilisez le SSL. Il a ensuite été développé pour fonctionner avec d'autres applications, telles que Telnet, les imprimantes et les logiciels FTP, et est devenu une solution universelle de sécurité en ligne. Ses fonctions premières sont toujours utilisées actuellement par de nombreux revendeurs en ligne et par la plupart des banques pour sécuriser leurs données sensibles, telles que les numéros de carte de crédit, les fichiers clients, etc.

Le SSL utilise des niveaux ce cryptage extrêmement élevés et est agréé par les banques du monde entier, car la violation d'un tel système est peu probable. Selon VeriSign™, l'une des meilleures autorités de certification (AC)[1] SSL, il faudrait plus d'une vie entière à un pirate pour déchiffrer un document standard crypté SSL.

3: Avantage de l'utilisation de SSL

L'unique avantage à utiliser le SSL sur les appareils réseau laser couleur de Brother est d'assurer une impression sécurisée sur un réseau IP en empêchant les utilisateurs non autorisés de lire les données envoyées à l'imprimante. Son principal argument est qu'il peut être utilisé pour imprimer des données confidentielles en toute sécurité. Par exemple, le service des ressources humaines d'une grande entreprise est amené à imprimer des bulletins de paye régulièrement. Sans cryptage, les données figurant sur ces bulletins de paye pourraient être lues par d'autres utilisateurs du réseau. Avec le SSL, toute personne essayant de capturer ces données ne verra qu'une page codée illisible et non le bulletin de paye réel.

4: Utilisation (installation standard)

L'impression sur un réseau sécurisé requiert l'installation d'un certificat numérique sur l'imprimante et sur le périphérique qui envoie les données à l'imprimante, par exemple un ordinateur. Pour configurer le certificat, l'utilisateur doit se connecter à l'imprimante à distance par le biais d'un navigateur Web utilisant son adresse IP, puis cliquer sur Configuration réseau et sur Configurer un certificat. A partir de là, l'utilisateur a deux possibilités :

1. Pour créer et installer un certificat auto signé

2. Pour utiliser un certificat émis par une autorité de certification[1] (AC)

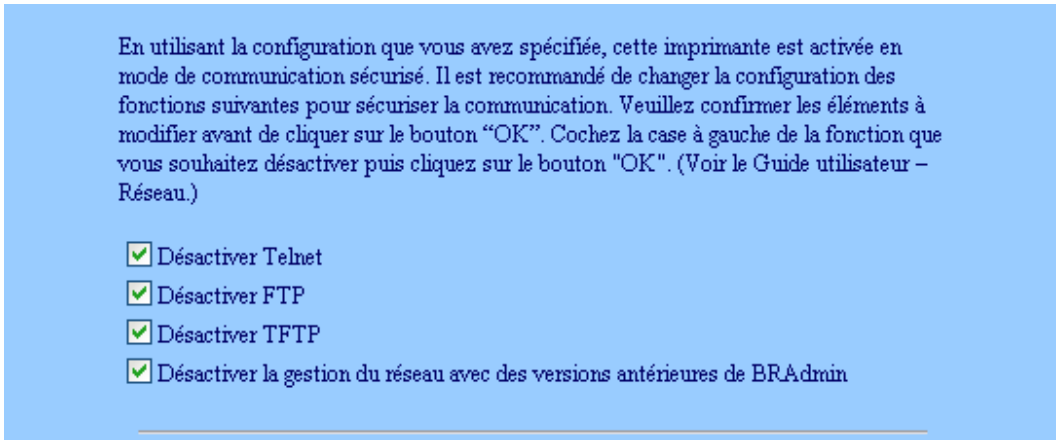
[1] *L'AC est une organisation externe qui atteste de l'authenticité des informations d'identification figurant sur un certificat numérique.*

4.1. Création d’un certificat auto signé

Après avoir cliqué sur Créer un certificat auto signé, vous devrez entrer un nom d’hôte ou une adresse IP, ainsi qu'une date de validité (généralement renseignée), puis cliquer sur Envoyer. L’appareil inscrira alors ces informations sur un certificat.

Au bout de quelques instants, un message vous demandera quel niveau de sécurité vous souhaitez pour la connexion SSL (ce qui correspond à la désactivation de certaines fonctions).

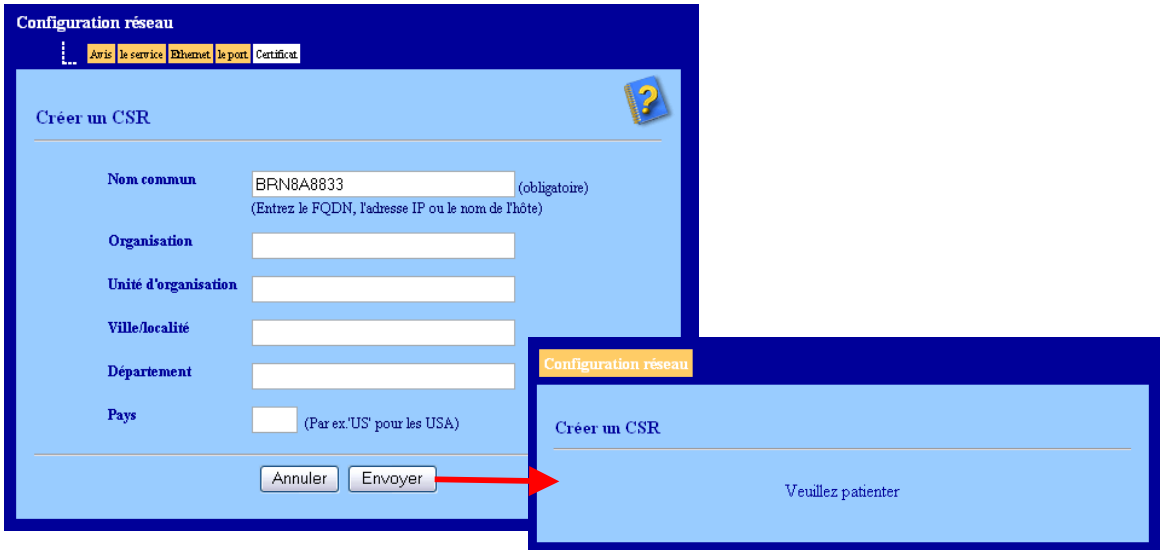
Pour une communication sécurisée, Brother recommande de désactiver les protocoles Telnet, FTP, TFTP et la gestion réseau avec des versions antérieures de BRAdmin (2.8 ou moins). Si vous les autorisez, l'authentification des utilisateurs ne sera pas sécurisée.



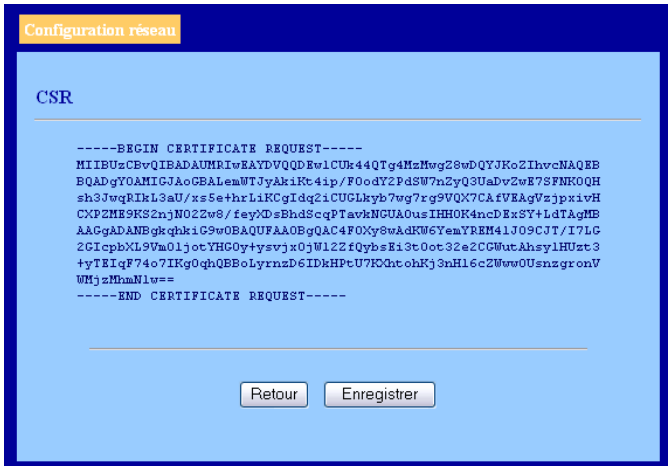
4.2. Création d’une requête de signature de certificat (CSR)

Un CSR est une requête qui est envoyée à une autorité de certification afin d’authentifier les informations d’identification figurant sur le certificat.

Après avoir cliqué sur Créer un CSR, vous devrez saisir les informations relatives à votre société, puis cliquer sur Suivant. Ces informations sont obligatoires pour que l’autorité de certification puisse confirmer votre identité et la prouver aux personnes extérieures.

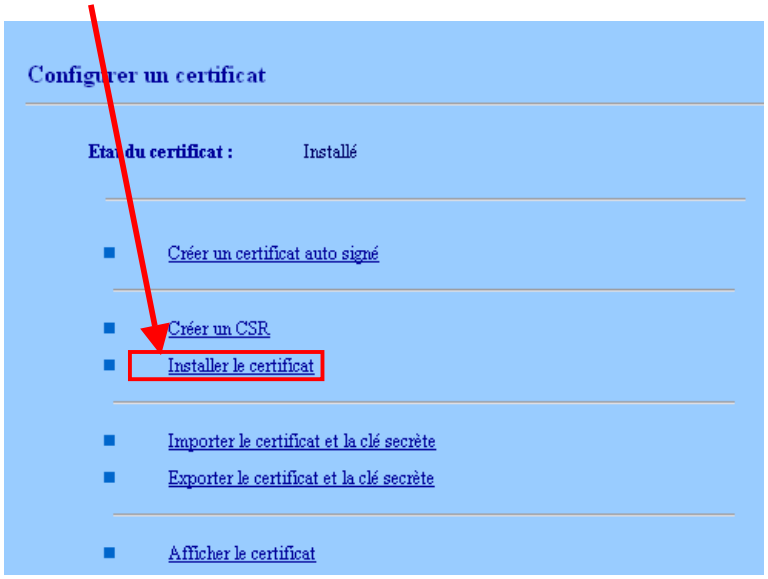


Au bout de quelques instants, le certificat s’affichera ; vous pourrez l’enregistrer dans un petit fichier ou le copier et le coller directement dans un formulaire CSR en ligne fourni par une autorité de certification. Parmi les autorités de certification, on peut citer VeriSign™ et Thawte™. Brother vous recommande de suivre les directives de votre AC pour savoir comment lui envoyer un CSR.



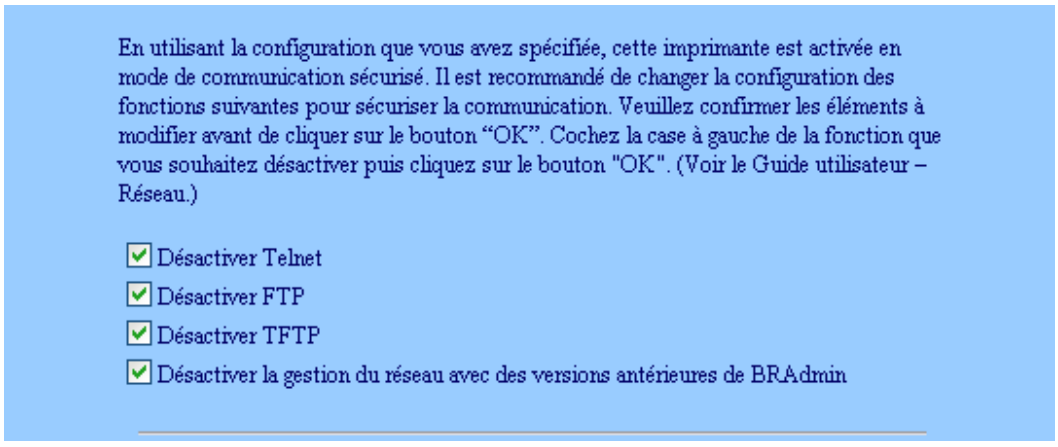
Lorsque vous avez reçu le certificat d'une AC, suivez les étapes ci-dessous pour l'installer sur le serveur d'impression (seul un certificat émis avec le CSR de cette imprimante peut être installé).

Cliquez sur Installer le certificat dans la page Configurer un certificat.



Spécifiez le fichier de certificat qui a été délivré par une AC, puis cliquez sur Envoyer.
Une fois le certificat créé, cochez la case figurant à gauche de chaque fonction que vous souhaitez désactiver, puis cliquez sur OK.

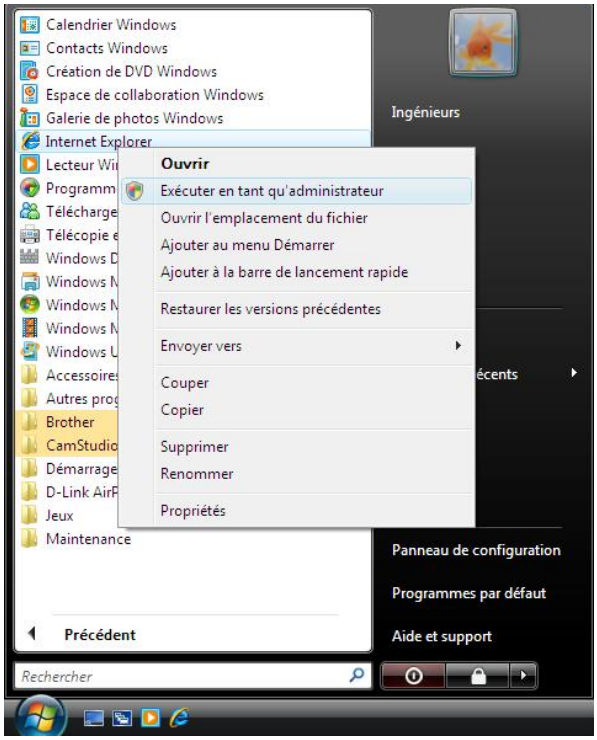
Pour une communication sécurisée, Brother recommande de désactiver les protocoles Telnet, FTP, TFTP et la gestion réseau avec des versions antérieures de BRAdmin (2.8 ou moins). Si vous les autorisez, l'authentification des utilisateurs ne sera pas sécurisée.



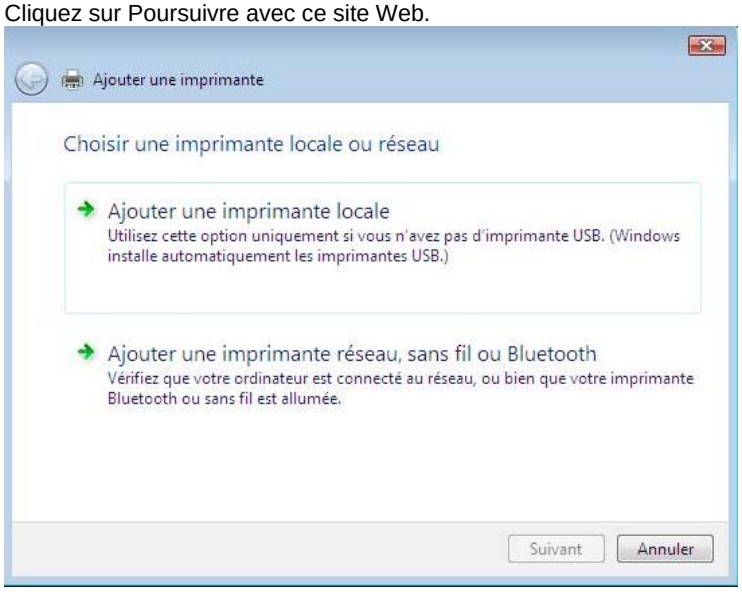
Redémarrez l'imprimante pour activer la configuration.

4.3 Installation du certificat sur Windows Vista™

Commencez par vous connecter à votre ordinateur avec les droits d'administrateur. Cliquez sur Démarrer, puis sur Tous les programmes. Ensuite, cliquez sur Internet Explorer avec le bouton droit de la souris, puis sélectionnez Exécuter en tant qu'administrateur.



Cliquez sur Poursuivre avec ce site Web.

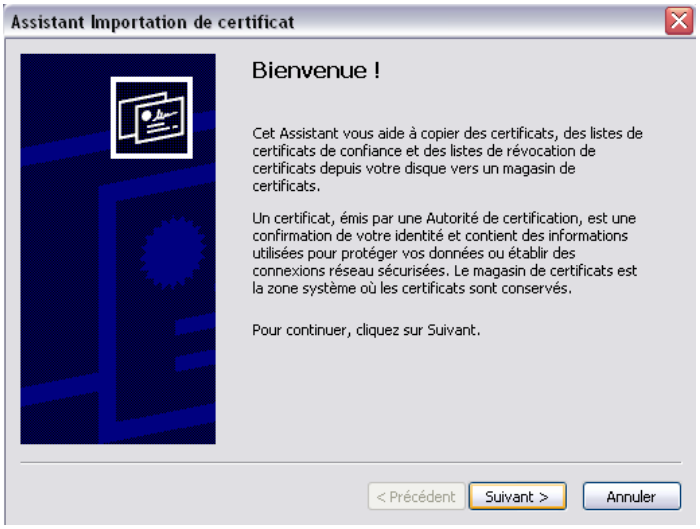


Cliquez sur Erreur de certificat, puis sur Afficher les certificats. Pour poursuivre l'installation, passez au paragraphe 4.4.

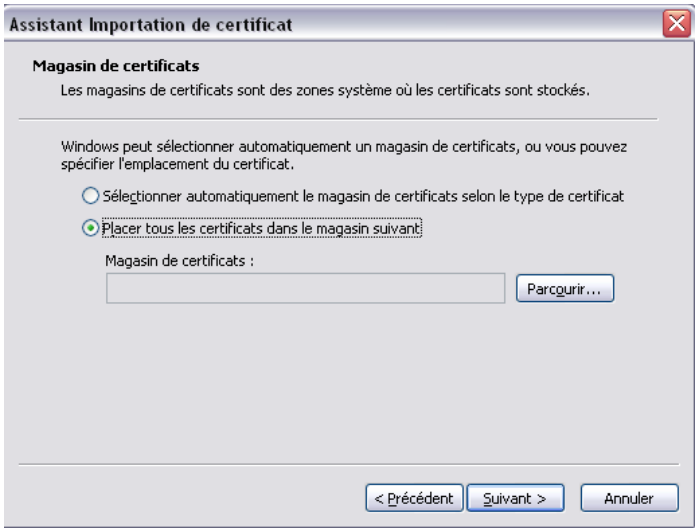
4.4 Installation du certificat sur Windows® XP

Lancez Internet Explorer, puis tapez https://adresse IP de l'imprimante/ dans votre navigateur pour accéder à votre imprimante. Ensuite, cliquez sur Afficher le certificat, puis sur Installer le certificat.

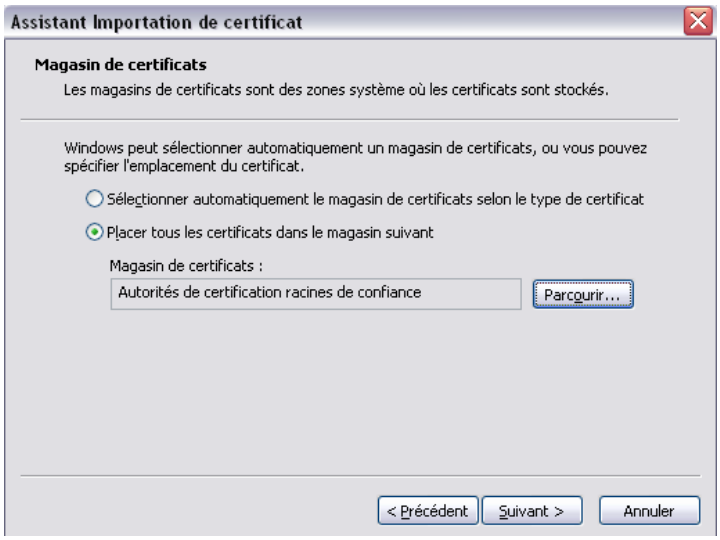
Un écran Assistant Importation de certificat s'affichera alors. Appuyez sur Suivant pour poursuivre.



Vous devrez indiquer l'emplacement d'installation du certificat. Brother recommande de sélectionner Placer tous les certificats dans le magasin suivant. Cliquez ensuite sur Parcourir.



Choisissez ensuite Autorités de certification racines de confiance, cliquez sur OK, puis sur Suivant.



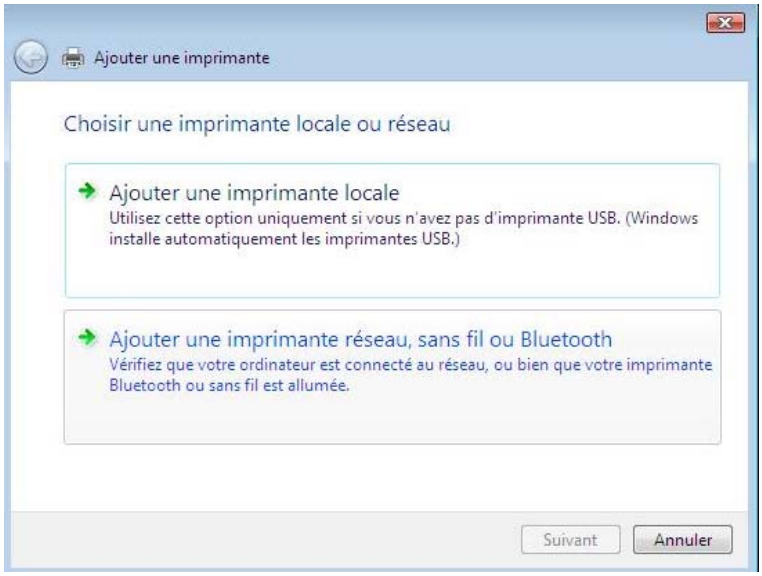
Dans l'écran suivant, cliquez sur Terminer. Vous serez alors invité à installer le certificat ; pour ce faire, cliquez sur Oui.

Cette procédure doit être réalisée sur chaque ordinateur visant à assurer une impression sécurisée. Toutefois, une fois ce certificat installé, il ne sera plus nécessaire de répéter ces étapes, sauf si le certificat est modifié.

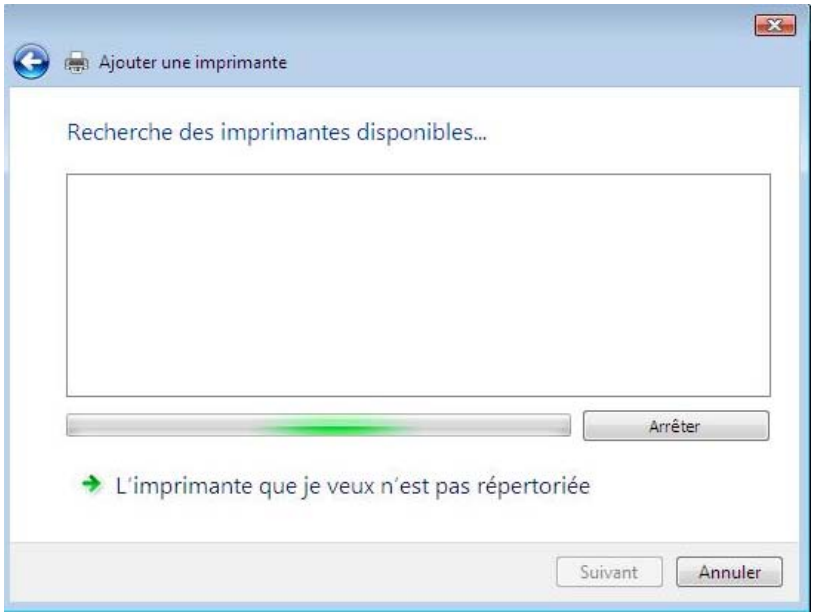
L'impression sécurisée aura lieu uniquement dans le cadre d'une configuration avec l'IPP (Internet Printing Protocol[2]) et non par le biais d'une installation réseau standard. Pour configurer l'IPP, reportez-vous au guide de l'utilisateur en réseau.

4.5 Configuration de IPP sur Windows Vista™

Allez dans l'Assistant Ajout d'imprimante, puis cliquez sur Ajouter une imprimante réseau, sans fil ou Bluetooth.

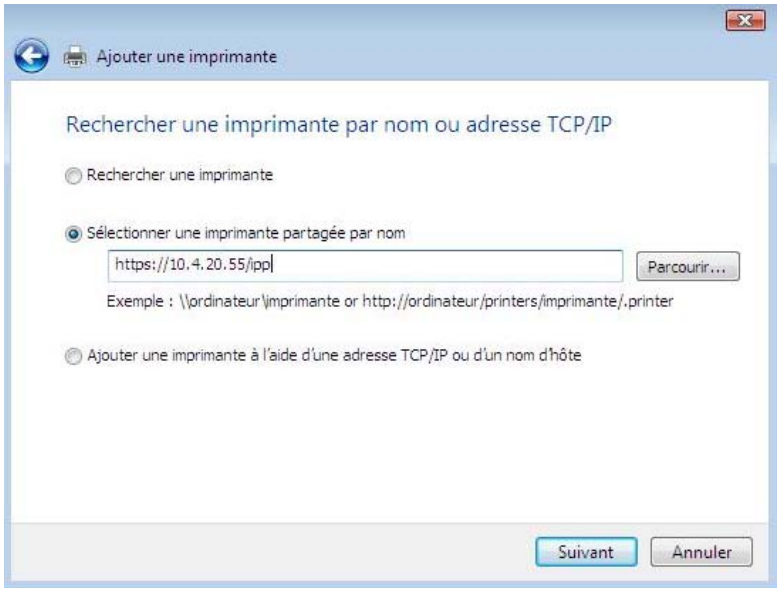


Cliquez sur L'imprimante que je veux n'est pas répertoriée.



Sélectionnez Sélectionner une imprimante partagée par nom, puis entrez l'adresse suivante dans le champ URL : https://adresse IP de l'imprimante/ipp (où adresse IP de l'imprimante correspond à l'adresse IP ou au nom de noeud de l'imprimante).

Veuillez noter :
Il est important d'utiliser https:// et non http:// ; autrement, l'impression sur IPP ne sera pas sécurisée.

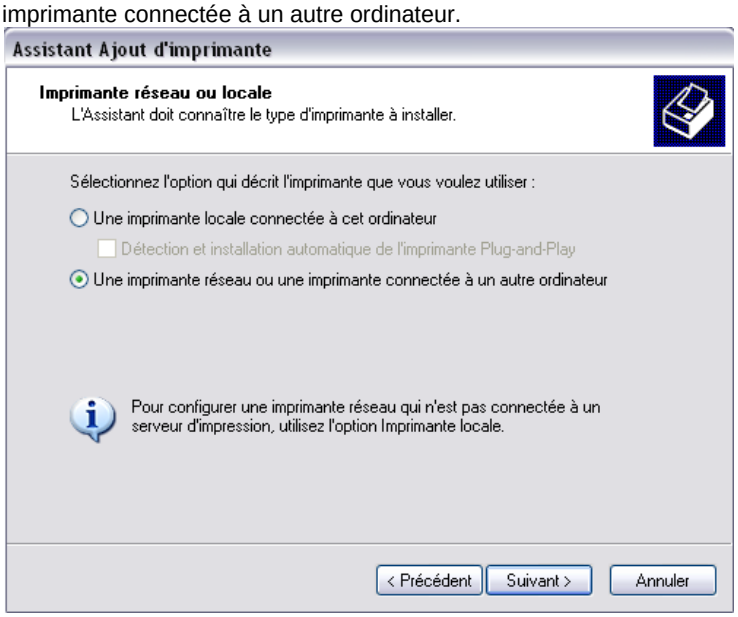


L'assistant recherchera l'imprimante sur le réseau ; s'il ne trouve pas les pilotes, il vous demandera de sélectionner un fabricant sur une liste ou sur un disque. Si le pilote est sur un disque, cliquez sur Parcourir, puis sélectionnez son emplacement.

Le pilote de l'imprimante s'installera et un message vous demandera si vous souhaitez faire de cet appareil l'imprimante par défaut et imprimer une page test. L'imprimante est alors installée et prête à assurer une impression sécurisée.

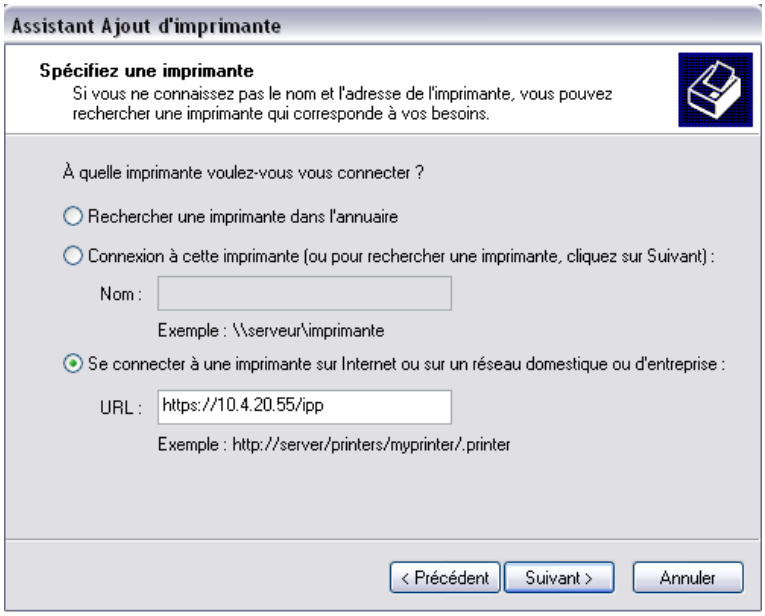
4.6 Configuration de IPP sur Windows® XP

Allez dans l'Assistant Ajout d'imprimante, puis sélectionnez Une imprimante réseau ou une imprimante connectée à un autre ordinateur.



Allez dans l'Assistant Ajout d'imprimante, puis sélectionnez Une imprimante réseau ou une imprimante connectée à un autre ordinateur. Sélectionnez l'option Se connecter à une imprimante sur Internet ou sur un réseau domestique ou d'entreprise, puis tapez le texte suivant dans le champ URL : https://adresse IP de l'imprimante/ipp. Ensuite, cliquez sur Suivant.

Veuillez noter :
Il est important de taper https:// et non http:// ; autrement, l'impression sur IPP ne sera pas sécurisée.



L'assistant recherchera l'imprimante sur le réseau ; s'il ne trouve pas les pilotes, il vous demandera de sélectionner un fabricant sur une liste ou sur un disque. Si le pilote est sur un disque, cliquez sur Parcourir, puis sélectionnez son emplacement.

Le pilote de l'imprimante s'installera et un message vous demandera si vous souhaitez faire de cet appareil l'imprimante par défaut et imprimer une page test. L'imprimante est alors installée et prête à assurer une impression sécurisée.

Pour des instructions plus détaillées sur l'utilisation, reportez-vous au guide de l'utilisateur.

5: Présentation technique

Le SSL (Secure Socket Layer) est une méthode de protection des données figurant sur une couche de transport qui sont envoyées sur un réseau local ou longue distance par IPP (Internet Printing Protocol) afin d'empêcher les utilisateurs non autorisés de les lire.
Pour ce faire, il utilise des protocoles d'authentification sous la forme de clés numériques de 2 types :

1. Une clé publique, connue de tous ceux qui impriment.
2. Une clé privée, connue uniquement de l'imprimante utilisée pour décrypter les paquets et les rendre de nouveau lisibles par l'imprimante.

La clé publique utilise le cryptage 1 024 bits et elle est incluse dans un certificat numérique qui doit être installé sur le PC client. Ces certificats peuvent être auto signés ou agréés par une autorité de certification (AC).

En premier lieu, il existe trois différents types de clé : privée, publique et partagée.

La clé privée, connue uniquement de l'imprimante, est associée à la clé publique, mais elle n'est pas incluse dans le certificat numérique des clients (expéditeurs). Une fois la connexion établie par l'utilisateur, l'imprimante envoie la clé publique avec le certificat. Le PC client assume en toute confiance que cette clé publique provient de l'imprimante munie du certificat. Le client génère la clé partagée et la code avec la clé publique, puis procède à l'envoi sur l'imprimante. L'imprimante code la clé partagée avec la clé privée. L'imprimante et le client partagent alors la clé partagée en toute sécurité et ils établissent une connexion sécurisée pour le transfert des données d'impression.

Les données d'impression sont codées et décodées avec la clé partagée.

Le SSL n'empêche pas les utilisateurs non autorisés d'accéder aux paquets, mais il les rend illisibles sans clé privée (que seule l'imprimante possède).

Il peut être configuré sur les réseaux câblés et sans fil et il fonctionne avec d'autres outils de sécurité, tels que les pare-feu et les clés WPA, selon la configuration appropriée.