KONICA MINOLTA

SÉCURISEZ VOTRE COMMUNICATION

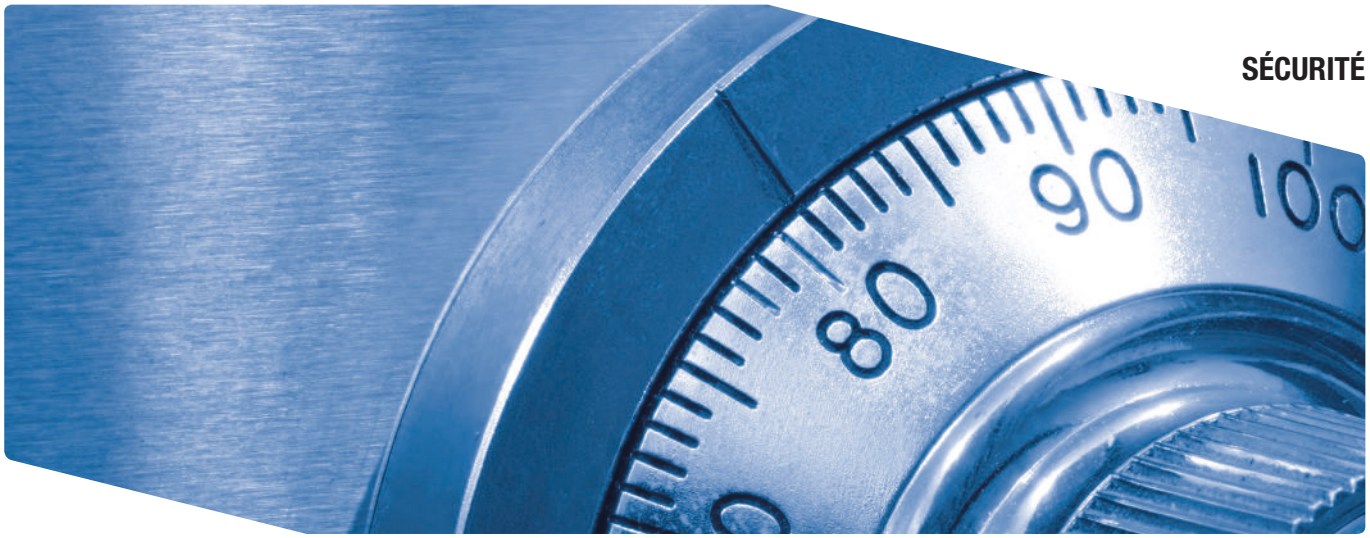
Avec les normes de sécurité de Konica Minolta

Dans l'ère du numérique, nous avons assisté à une croissance des communications sans précèdent, et les failles dans la sécurité ont augmenté en parallèle. Dans n'importe quel environnement d'entreprise, les tâches quotidiennes d'impression, scan, e-mailing et d'envoi des fax sont des activités de communication indispensables à de nombreux niveaux. Par conséquent, il est primordial de sécuriser un maximum vos systèmes d'impression afin de les préserver de possibles failles de sécurité.

* La passion de l'innovation

Giving Shape to Ideas*

SÉCURITÉ



DÉTECTION FIABLE & PRÉVENTION DES **FAILLES DE SÉCURITÉ**

Si vous souhaitez des solutions afin de prévenir et de détecter les failles de sécurité et éviter ainsi un possible préjudice financier et / ou des impacts négatifs envers la réputation de l'entreprise, faites confiance au leader du secteur, Konica Minolta. Nous vous proposons une gamme complète de logiciels de sécurité et d'options afin d'assurer la fiabilité de vos communications.

Les multifonctions offrent généralement à leurs utilisateurs un vaste choix de fonctionnalités combinées. Par conséquent, ils représentent autant de failles de sécurité potentielles. La sécurité du multifonction peut être groupée en trois catégories principales :

- **Contrôle des accès/ de la sécurité**
- **Sécurisation des données et des documents**
- **Sécurité du réseau**

Les fonctions de sécurité de Konica Minolta en un coup d'œil

Contrôle des accès	Copie / Impression Restriction de fonctionnalités Impression sécurisée (verrouillage des tâches) Boite utilisateur protégée par mot de passe Authentification de l'utilisateur (ID + mot de passe) Authentification biométrique Lecteur de carte sans contact Journal d'évènements
Sécurité	Cryptage et écrasement des données du disque dur Protection du disque dur par mot de passe Suppression automatique des données
Sécurité du réseau	Filtrage IP Contrôle d'accès aux ports et aux protocoles Cryptage du SSL/TL (HTTPS) IP sec S/MIME Prise en charge de 802.1x
Sécurité de numérisation	Authentification des utilisateurs POP avant SMTP Authentification SMTP (SASL) Blocage manuel de destination
Autres	Protection du mode service Protection du mode administrateur Acquisition de données Verrouillage des accès non autorisées Protection contre la copie grâce au filigrane PDF crypté Signature des PDF Cryptage de PDF par ID numérique Copie protégée (avec mot de passe)

UNE TECHNOLOGIE CERTIFIÉE SUR LAQUELLE VOUS POUVEZ COMPTER

Voulez-vous vraiment être en mesure de compter sur vos périphériques d'impression, tout en garantissant la sécurité dont vous avez besoin ? Les imprimantes et les multifonctions Konica Minolta sont certifiés conformes aux normes ISO 15408 EAL3 et IEEE 2600.1.

La certification ISO 15408 EAL3 est la seule norme reconnue internationalement pour les tests de sécurité des produits informatiques. Les imprimantes, multifonctions et logiciels compatibles avec la norme ISO 15408 EAL3 ont tous passé une évaluation de sécurité très stricte et sont en mesure de satisfaire et garantir un niveau de sécurité propre à une transaction commerciale prudente et légitime.

La certification IEEE 2600.1 prouve le haut niveau de sécurité de Konica Minolta. Cette certification est une norme internationale de sécurité informatique qui garantit que les tâches quotidiennes mais aussi les documents hautement confidentiels sont protégés au sein de l'entreprise.

Konica Minolta se positionne comme le leader du secteur dans le domaine de la sécurité des données.

Common Criteria Validated

« La sécurité est l'élément clé de la stratégie globale de Konica Minolta…

Konica Minolta propose un vaste éventail de fonctions d'impression et de sécurité qui se trouvent dans les produits de la gamme business hub. Plutôt que de certifier uniquement les kits de sécurité en option, Konica Minolta aspire à obtenir la gamme la plus vaste certifiée ISO 15408 sur le marché des multifonctions.»

Source: Quocirca (2011), Étude de marché « Closing the print security gap.The market landscape for print security », p. 11. Ce rapport indépendant a été écrit par Quocirca Ltd., une entreprise de recherche et d'analyse spécialisée dans l'impact commercial des technologies de l'information et des communications (TIC).

CONTRÔLE INDIVIDUEL DES ACCÈS POUR UNE SÉCURITÉ TOTALE

Bien que de nos jours, l'augmentation de la sécurité est une priorité dans le domaine public et privé, les menaces rendant incertaines la sécurité des multifonctions sont souvent ignorées. Les risques dans les entreprises sont souvent négligés, surtout lorsque des documents et des informations sensibles sont concernés. Cela est particulièrement risqué pour tout multifonction ou imprimante situé dans un endroit public, accessible au personnel ou même à des visiteurs.

En raison des caractéristiques avancées des multifonctions, il est facile de copier et de partager de l'information en interne et au-delà des frontières des entreprises. Le premier pas logique est d'en éviter l'accès aux personnes non autorisées. D'une part, des mesures préventives sont nécessaires pour contrôler l'accès aux multifonctions, d'autre part, il est important d'établir une politique de sécurité reflétant l'utilisation des systèmes d'impression dans la vie réelle. Konica Minolta relève ce défi sans restreindre la convivialité des systèmes.

Authentification de l'utilisateur

La mise en place de l'authentification commence par la définition et la configuration des profils utilisateurs ou des groupes autorisés à utiliser le multifonction. Cela peut inclure des limitations de droit. Certains utilisateurs seront donc autorisés, par exemple à se servir de l'impression couleur et d'autres non.

Konica Minolta propose trois technologies de base pour l'authentification de l'utilisateur:

1. **Mot de passe personnel**
   Le mot de passe, un code alphanumérique jusqu'à 8 caractères, est saisi sur l'écran du multifonction. Ces codes peuvent être créés pour les administrateurs et les utilisateurs. Ils peuvent être gérés de manière centralisée.

2. **Authentification par badge**
   La plupart des produits Konica Minolta peuvent être équipés d'un lecteur de badge. Il offre vitesse et confort car il suffit de l'approcher du lecteur du multifonction pour y avoir accès ou pour se déconnecter.

Authentification de l'utilisateur

3. **Authentification biométrique par scanner de veines**
   Le système d'impression fonctionne en comparant l'image des veines du doigt avec celles qui sont dans la mémoire du système. La veine du doigt est une caractéristique biométrique presque impossible à falsifier, ce qui permet d'identifier une personne sur la base d'une caractéristique individuelle. Contrairement aux systèmes d'empreintes, la veine du doigt ne peut être scannée sans que la personne soit présente et vivante.

   Le scanner biométrique des veines améliore la sécurité car il n'y a plus besoin de se souvenir des mots de passe ou porter des badges.

L'information de l'authentification peut être stockée soit sur le multifonction (cryptage) soit dans les données existantes de Windows Active Directory.

Les informations concernant les accès et usages de chaque matériel sont accessibles en permanence, ce qui signifie que les failles de sécurité sont détectées immédiatement et signalées.

Suivi des comptes utilisateurs pour plus de transparence

Le contrôle de la sécurité exige que chaque utilisateur se connecte à l'appareil, ainsi les données générées représentent un moyen efficace de surveillance à plusieurs niveaux : utilisateur, groupe et / ou département. Quel que soit la fonction utilisée : impression, copie, scan ou fax, en couleur ou en noir et blanc, elles peuvent être toutes contrôlées soit depuis le matériel soit à distance. L'analyse de ces données fournit des informations importantes sur l'usage du multifonction. Les données peuvent être étudiées pour assurer la sécurité et traquer l'accès non autorisé. Enfin, ce contrôle permet surtout d'assurer la surveillance de l'ensemble du parc d'imprimantes ou de multifonctions dans l'entreprise.

Restrictions de fonctionnalités

Il est possible de limiter les diverses fonctionnalités du multifonction d'une manière individuelle. Ces restrictions au-delà de réduire totalement le danger lié à l'extraction des données du multifonction, peuvent aussi permettre de mesurer et d'analyser l'utilisation qui en est faite. Ces fonctions peuvent être aussi utilisées pour une meilleure gouvernance et une prise de conscience des utilisateurs.

SÉCURITÉ GLOBALE
DES DONNÉES ET DES DOCUMENTS

Implémenter une protection appropriée est essentiel car les imprimantes et les multifonctions sont souvent situés dans des lieux publics, où ils peuvent facilement être accessibles par le personnel et les visiteurs. Des données sensibles peuvent se trouver stockées dans le disque dur du multifonction et des impressions oubliées à proximité. Ces données peuvent tomber entre de mauvaises mains. Afin d'éviter ce type d'incidents et d'assurer une sécurité des données et des documents, Konica Minolta vous offre une gamme adaptée de mesures de sécurité.

Pas de failles de sécurité du disque dur

La plupart des imprimantes et multifonctions sont équipés de disques durs qui conservent plusieurs giga-octets d'informations confidentielles stockées sur de longues périodes.

Des garanties fiables doivent donc être mises en place pour assurer la protection des informations sensibles de l'entreprise. Dans les systèmes Konica Minolta, un certain nombre de caractéristiques sont disponibles afin d'assurer vos données :

- **Fonction de suppression automatique des données**
  La fonction de suppression automatique efface les données stockées sur le disque dur après une période déterminée.

- **Protection du disque dur par mot de passe**
  L'extraction des données du disque dur nécessite un mot de passe après le retrait manuel du disque dur. Ce mot de passe est lié au système d'impression donc, dès que le disque dur est détaché du système, les données s'y trouvant ne sont plus accessibles.

- **Écrasement des données du disque dur**
  L'écrasement des données du disque dur est la méthode la plus efficace pour le formater.

- **Cryptage du disque dur**
  Sur les disques durs inclus dans les systèmes d'impression Konica Minolta, les données peuvent être stockées sous forme chiffrée basée sur un système d'algorithme à 128-bits. Une fois qu'un disque dur est crypté, les données ne peuvent ni être lues ni récupérées, même si le disque dur a été physiquement enlevé.

Protégez vos documents avec l'impression sécurisée

Les systèmes d'impression sont considérés comme un risque de sécurité qui ne devrait pas être sous-estimé: les documents qui se trouvent dans le bac de sortie peuvent être vus et lus par tout le monde. C'est la forme la plus simple pour les personnes non autorisées d'avoir accès à des informations confidentielles. La fonctionnalité d'impression sécurisée est un moyen de garantir la confidentialité des documents car c'est l'auteur spécifique d'un travail d'impression qui doit définir un mot de passe avant de lancer le processus d'impression. Par la suite, l'impression ne peut démarrer que si l'on tape ce mot de passe directement dans l'imprimante ou le multifonction. C'est donc un moyen simple et efficace de prévention afin d'éviter que les documents confidentiels tombent entre de mauvaises mains.

Impression avec authentification individuelle

« **Touch & Print** » est un système basé sur l'authentification via le scan de la veine du doigt ou système par badge tandis que « **ID & Print** » nécessite une authentification par mot de passe. Le but est d'imprimer immédiatement après que l'utilisateur se soit authentifié, soit par le biais du badge soit en plaçant son doigt dans le scanner.

Protection contre la copie non autorisée

La **fonction de protection** contre la copie ajoute un filigrane aux impressions et aux copies. Il est à peine visible sur la copie originale mais si le document est copié, il se déplace de l'arrière-plan au premier plan pour indiquer que c'est une copie.

Garder le contrôle avec Copy Guard

« **Copy Guard** » et « **Password Copy** » ajoutent un filigrane au document original pendant l'impression afin d'éviter qu'il soit copié. Le filigrane a beau être à peine visible dans le document original, il n'est pas possible de recopier le document car le multifonction se bloque en détectant cette opération. La fonction « Password Copy » peut alors être activée et permet la copie de ce document si le mot de passe est correctement saisi sur l'écran du multifonction.

Cryptage des PDF

Les **PDF cryptés** sont protégés par un mot de passe : c'est lui qui va donner la permission pour imprimer ou copier le PDF ou pour y ajouter du contenu. Tout cela peut être configuré pendant la phase de scan.

Signature numérique des PDF

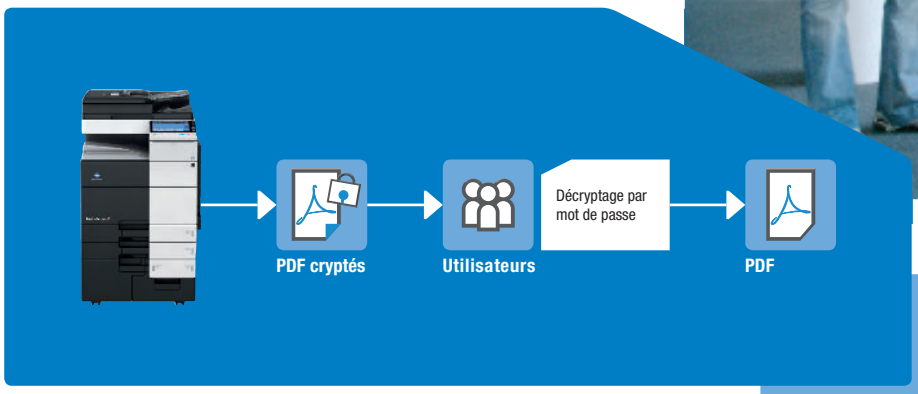
Grâce à cette fonctionnalité, une signature numérique peut être rajoutée au PDF lors de sa numérisation. Après la création d'un PDF, il est donc possible de suivre les modifications.

Réception de fax sécurisé

Quand cette fonctionnalité est active, tous les fax reçus sont confidentiels et stockés dans une boîte protégée.

Sécurité de la boîte utilisateur

Les boites utilisateur sont disponibles à un niveau individuel et collectif et permettent de stocker en toute sécurité vos documents dans le disque dur du multifonction avant d'imprimer ou de copier. Ces boites sont protégées avec un mot de passe alphanumérique à huit chiffres. Lorsque le bon mot de passe est saisi, il est possible d'accéder et de visualiser les documents de la boite. Ce système limite efficacement l'accès aux documents et données confidentiels.



PDF cryptés

SÉCURISEZ **VOTRE RÉSEAU**

Aujourd'hui, la communication et la connectivité sont indispensables dans le monde des affaires. Les multifonctions Konica Minolta prennent cela en compte et permettent une intégration facile dans les environnements en réseau. Vous êtes conscient, sans doute, que les imprimantes et les multifonctions ont évolué jusqu'à devenir des centres de traitement de documents sophistiqués et compatibles avec votre réseau. Ils permettent à la fois d'imprimer, de copier et de scanner des documents au travers du réseau interne d'une entreprise mais aussi de communiquer vers l'extérieur pour l'envoi de mail par exemple.

Pour votre bureau, cela signifie qu'une telle technologie représente un risque si elle n'est pas protégée et elle doit donc faire face aux mêmes menaces et politiques de sécurité que n'importe quel autre périphérique. Afin d'éviter toute vulnérabilité externe et interne, Konica Minolta vous assure que tout votre équipement est conforme aux normes de sécurité les plus strictes.

Blocage de l'adresse IP

Protocole de contrôle et d'accès au port avec un pare-feu basic qui inclut un filtre des adresses IP.

Administration des ports des protocoles

L'administrateur du parc d'impression peut ouvrir, fermer, activer et désactiver les ports et les protocoles, soit directement depuis le système d'impression, soit confortablement depuis un poste à distance.

Communication par e-mail sécurisé (S/MIME)

Plusieurs produits Konica Minolta prennent en charge la norme de sécurité S/MIME (Secure / Multipurpose Internet Mail Extensions) afin de sécuriser la communication e-mail depuis vos multifonctions vers des destinataires spécifiques. S/MIME va sécuriser votre flux d'e-mail en cryptant les messages et leur contenu à l'aide d'un certificat de sécurité.

Authentification du réseau (IEEE802.1x)

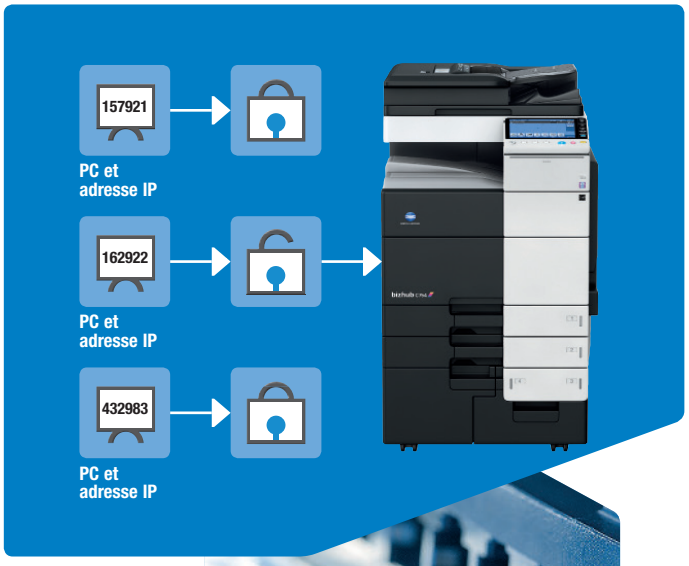
Les normes décrites dans la famille IEEE802.1x sont des normes d'authentification basées sur le contrôle d'accès aux réseaux WAN et WLAN. Ces normes sécurisent efficacement votre réseau en fermant toute communication (par exemple, DHCP ou HTTP) pour les systèmes non autorisés sauf pour les demandes d'authentification.

Communication protégée

Ce protocole offre une protection pour toutes les communications entre les appareils, par exemple, en couvrant les outils d'administration en ligne et les transmissions de Windows Active Directory.

Communication cryptée du réseau (IPsec)

La plupart de nos produits business hub prennent également en charge le protocole IPsec afin d'assurer un cryptage complet de toutes les données du réseau transmises vers et depuis votre multifonction. Le protocole de sécurité IP va crypter toutes les informations entre votre intranet local (serveur, client PC) et vos systèmes d'impression.



Filtrage par adresse IP

Avec Ecofolio tous les papiers se recyclent.

Konica Minolta Business Solutions France 365–367 route de Saint-Germain 78424 Carrières-sur-Seine Cedex
Tél : 01 30 86 60 00 **www.konicaminolta.fr**
S.A.S au capital de 26 490 000 € - RCS Versailles B302 695 614

02/2014