



KONICA MINOLTA

PROTÉGEZ VOTRE COMMUNICATION

▣ Avec les normes de sécurité de Konica Minolta

A l'ère du numérique, les communications mondiales ont connu une croissance sans précédent et, parallèlement, les risques de violations de la sécurité ont grimpé en flèche. Dans tout environnement d'entreprise, les activités quotidiennes d'impression, de copie, de numérisation, d'envoi d'e-mails et de télécopie – en tant qu'applications de communication élémentaires dans les processus métiers et les flux de production – rendent les périphériques multifonctions indispensables à tous les niveaux. Par conséquent, il est primordial que ces appareils bénéficient de la protection nécessaire pour faire face aux menaces qui pèsent actuellement sur la sécurité.



* La passion de l'innovation

Giving Shape to Ideas*

SÉCURITÉ

DÉTECTION FIABLE & PRÉVENTION DES VIOLATIONS DE LA SÉCURITÉ

Vous recherchez des solutions pour détecter et prévenir les violations de la sécurité et vous voulez éviter de subir de graves préjudices financiers et/ou atteintes à votre réputation professionnelle et personnelle ? Faites confiance à la gamme complète de fonctions et d'options de sécurité standard du leader du marché, Konica Minolta.

Les périphériques multifonctions offrent généralement à leurs utilisateurs une large gamme de fonctions et d'options combinées et individuelles. Par conséquent, ils représentent une gamme tout aussi large de failles potentielles de sécurité. On distingue trois grandes catégories d'options de sécurité des périphériques multifonctions :

- Contrôle d'accès/Sécurité des accès
- Sécurité des données/Sécurité des documents
- Sécurité du réseau

Vue d'ensemble des fonctions de sécurité

Contrôle des accès	Comptabilisation des copies/impressions Restriction pour certaines fonctions Impression sécurisée (verrouillage des tâches) Protection des boîtes utilisateur par mot de passe Authentification des utilisateurs (identifiant + mot de passe) Scanner de veines digitales Lecteur de carte sans contact Journal d'événements
Sécurité des données	Chiffrement des données (disque dur) Écrasement des données du disque dur Protection du disque dur par mot de passe Suppression automatique des données
Sécurité du réseau	Filtrage des adresses IP Contrôle d'accès aux niveaux des ports et des protocoles Chiffrement SSL/TLS (HTTPS) Prise en charge IPsec 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 autorisés Filigrane de protection anticopie PDF chiffré Signature des PDF Chiffrement de PDF par identifiant numérique Protection contre la copie (Copy Guard/Password Copy)

ÉVALUATION DE LA SÉCURITÉ ÉPROUVÉE ET FIABLE

Vous voulez pouvoir vous fier totalement à vos multifonctions et bénéficier de la sécurité dont vous avez besoin ? Les imprimantes et les périphériques multi-fonctions Konica Minolta vous offrent une parfaite sérénité, car ils sont presque sans exception certifiés conformes aux normes Critères Communs/ISO 15408 EAL3 et IEEE 2600.1

La certification de conformité aux Critères Communs/ISO 15408 EAL3 est la seule norme reconnue au niveau international pour les tests de sécurité informatique des produits numériques. Les imprimantes, multifonctions et logiciels certifiés ISO 15408 EAL3 ont tous été soumis avec succès à une évaluation de sécurité stricte et sont capables de respecter et d'offrir les niveaux de sécurité qu'une entreprise prudente devrait rechercher et qu'elle est en droit d'attendre.

La certification de conformité aux Critères Communs/IEEE 2600.1 reconnaît la norme de sécurité des périphériques Konica Minolta. Cette certification est une norme de sécurité informatique internationale qui confirme que les fonctions de sécurité des périphériques multifonctions certifiés sont conformes aux normes les plus strictes de l'IEEE (Institute of Electrical and Electronic Engineers). Des tâches de bureau quotidiennes à la gestion des informations et documents hautement confidentiels, toutes les données enregistrées au niveau de l'entreprise ont besoin d'une protection fiable, ce que cette certification vous garantit.

Véritable référence pour les fonctions de sécurité standard, Konica Minolta est le leader du marché dans ce domaine.



Common Criteria Validated

« La sécurité est au cœur de la stratégie globale de Konica Minolta... »

Konica Minolta propose une gamme complète de fonctions de sécurité pour l'impression et les documents, dont la plupart sont intégrées en standard sur ses systèmes business hub. Plutôt que de certifier des kits de sécurité en option, Konica Minolta propose la plus large gamme de systèmes multifonctions entièrement certifiés ISO 15408 du marché. »

Source : Quocirca (2011), étude de marché « Closing the print security gap. The market landscape for print security », page 11. Ce rapport indépendant a été rédigé par Quocirca Ltd., un grand cabinet de recherche et d'analyse spécialisé dans l'étude de l'impact des technologies de l'information et de la communication sur l'économie. Ltd., une entreprise de recherche et d'analyse spécialisée dans l'impact commercial des technologies de l'information et des communications (TIC).



CONTRÔLE D'ACCÈS INDIVIDUEL POUR UNE SÉCURITÉ TOTALE

Aujourd'hui, bien que la sécurité soit généralement l'une des priorités des secteurs publics et privés, les menaces que les périphériques multifonctions font peser sur la sécurité sont souvent complètement ignorées. De nombreuses entreprises sont certes conscientes des risques, mais dans la plupart des cas, ceux-ci sont tout simplement négligés, tout particulièrement lorsqu'ils concernent des documents et des informations sensibles. Cette négligence est très risquée pour les périphériques multifonctions ou les imprimantes installés dans les lieux publics, car le personnel, les sous-traitants et même les visiteurs peuvent y accéder.

Les fonctions avancées actuellement disponibles sur les périphériques multifonctions permettent de copier et distribuer facilement les informations au sein et au-delà des frontières physiques et virtuelles de l'entreprise. La première étape logique est d'interdire formellement l'utilisation d'un périphérique multifonction par des personnes non autorisées. Des mesures préventives sont requises, premièrement pour contrôler l'accès aux périphériques multifonctions, et deuxièmement pour établir une certaine politique de sécurité reflétant l'utilisation réelle des appareils. Konica Minolta réalise tout cela en affectant en aucune manière la convivialité des systèmes.

Authentification complète des utilisateurs

Le chemin d'authentification commence par l'établissement d'une politique pour définir et configurer les utilisateurs et les groupes d'utilisateurs autorisés à se servir d'un périphérique multifonction. Cette politique peut imposer des limitations aux droits d'accès, par exemple en autorisant certains utilisateurs et pas d'autres à utiliser des fonctions telles que l'impression couleur.

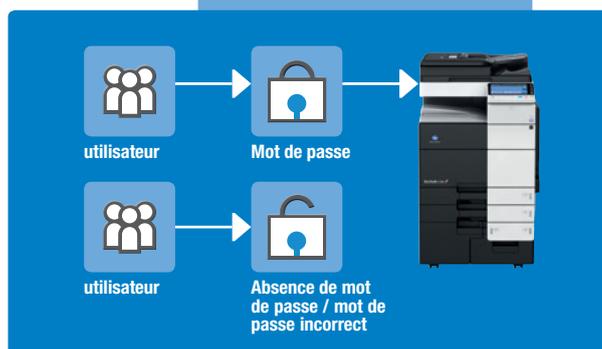
Konica Minolta propose trois technologies de base pour l'authentification de l'utilisateur :

1. Mot de passe personnel

Ce mot de passe est un code alphanumérique de 8 caractères maximum saisi sur le panneau de commande du périphérique multifonction. Ces codes peuvent être créés pour les administrateurs et les utilisateurs. Un aspect important est que leur gestion peut être centralisée.

2. Authentification par carte d'identification

La plupart des appareils Konica Minolta peuvent être équipés d'un lecteur de cartes d'identification. Les cartes d'identification offrent commodité et rapidité, car il suffit de les placer sur ou à proximité de l'interface du lecteur pour accéder au système et s'en déconnecter.



Authentification de l'utilisateur



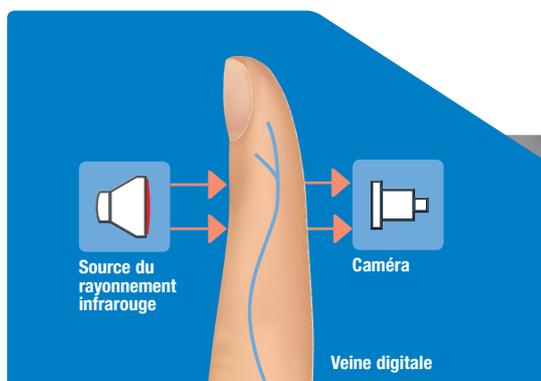
3. Scanner de veines digitales biométrique.

Cette technologie de pointe représente une avancée par rapport aux lecteurs d'empreinte digitale standard. Le système compare l'image des motifs veineux numérisés du doigt avec ceux stockés en mémoire. La veine digitale est une caractéristique biométrique quasiment impossible à falsifier, ce qui la rend extrêmement fiable pour identifier une personne à partir d'une caractéristique physique personnelle. Contrairement aux lecteurs d'empreintes digitales, la veine digitale ne peut pas être numérisée si la personne n'est pas physiquement présente et vivante.

Le scanner de veines digitales biométrique signifie que la personne n'a pas besoin de mémoriser des mots de passe ni d'avoir sur elle des cartes.

Les informations d'authentification peuvent être stockées (chiffrées) sur le périphérique multifonction ou extraites des données Windows Active Directory existantes.

Grâce à la journalisation continue des informations d'accès et d'utilisation pour chaque appareil, toutes les violations de la sécurité sont immédiatement détectées et signalées.



▀ Suivi des comptes utilisateurs pour plus de transparence

Comme le contrôle des utilisateurs à des fins de sécurité exige que chaque utilisateur se connecte à l'appareil de sortie, les données générées représentent un moyen de surveillance efficace à plusieurs niveaux (utilisateur, groupe et/ou service). Les différentes fonctions d'un appareil peuvent être suivies individuellement au niveau de la machine ou à distance, que ce soit la copie, la numérisation ou la télécopie monochrome ou couleur, ou encore l'impression noir et blanc ou couleur. En analysant ces données et en dégagant des tendances, il est possible d'obtenir des informations précises sur l'utilisation qui est faite de l'appareil, en se plaçant de différents points de vue. Ces données peuvent ensuite servir à assurer la conformité des périphériques multifonctions et à suivre les accès non autorisés. Et surtout, elles permettent de suivre l'utilisation de l'ensemble du parc d'imprimantes et de multifonctions dans un environnement d'entreprise.

▀ Accès individualisé avec restriction des fonctions

Il est possible de limiter différentes fonctions des périphériques multifonctions pour chaque utilisateur. Toutes les fonctions de contrôle d'accès et de sécurité Konica Minolta offrent une sécurité accrue contre les menaces pouvant faire perdre de l'argent aux entreprises et entacher leur réputation. Elles peuvent également servir de base pour améliorer la gouvernance et responsabiliser les utilisateurs.



SÉCURITÉ TOTALE POUR LES DONNÉES ET LES DOCUMENTS

Les périphériques multifonctions et les imprimantes étant souvent installés dans des lieux publics, c'est-à-dire aisément accessibles par le personnel, les sous-traitants et les visiteurs, la mise en œuvre de politiques de sécurité des données appropriées est essentielle. Les données sensibles stockées sur le disque dur des périphériques multifonctions, ainsi que les documents confidentiels qui attendent d'être récupérés dans les bacs de sortie, sont initialement non protégés et peuvent facilement tomber entre de mauvaises mains. Pour éviter que cela se produise et garantir la sécurité totale des documents et données, Konica Minolta propose une gamme de mesures de sécurité adaptées.

▀ Sécurité des disques durs sans faille

La plupart des imprimantes et des périphériques multifonctions sont équipés de disques durs et de modules de mémoire capables de stocker plusieurs giga-octets de données éventuellement confidentielles collectées sur de longues périodes.

Des protections fiables doivent donc être mises en place pour garantir une conservation sécurisée des informations sensibles de l'entreprise. Sur les systèmes Konica Minolta, plusieurs fonctions complémentaires et interdépendantes fournissent cette garantie :

– Fonction de suppression automatique

La fonction de suppression automatique efface les données stockées sur le disque dur au bout d'un certain temps.

– Protection par mot de passe du disque dur interne

Après le retrait du disque dur, la lecture des données qu'il contient, parmi lesquelles se trouvent bien évidemment des données confidentielles, ne peut se faire qu'en saisissant un mot de passe. Ce mot de passe est lié à l'appareil. Les données sont donc inaccessibles après le retrait du disque dur de l'appareil.

– Écrasement du disque dur

La méthode la plus sûre pour formater un disque dur est celle qui consiste à écraser les données qu'il contient. Cette opération est réalisée en conformité avec plusieurs normes.

– Chiffrement du disque dur

Les données stockées sur les disques durs des appareils Konica Minolta peuvent être chiffrées au moyen d'un système algorithmique 128 bits. Cette fonction est conforme aux politiques de sécurité des données d'entreprise. Une fois qu'un disque dur est chiffré, les données qu'il contient ne peuvent plus être lues ou extraites, même s'il est physiquement retiré du périphérique multifonction.

▀ Protégez vos documents avec l'impression sécurisée

Les périphériques d'impression présentent un risque pour la sécurité qui ne doit pas être négligé. Au niveau le plus simple, les documents qui attendent d'être récupérés dans le bac de sortie peuvent être vus et lus par n'importe qui. Il n'y a pas de moyen plus facile pour des personnes non autorisées d'accéder à des informations confidentielles. L'impression sécurisée est une fonction qui permet de préserver la confidentialité d'un document en demandant à l'utilisateur qui lance un travail d'impression de définir un mot de passe de sécurité avant l'impression proprement dite. Après cela, l'impression ne peut être lancée qu'en saisissant ce mot de passe directement sur le périphérique d'impression. Il s'agit d'un moyen simple et efficace d'éviter que des documents confidentiels ne tombent entre de mauvaises mains.



Impression avec authentification individuelle

La fonction « **Touch & Print** » est basée sur l'authentification via un scanner de veines digitales ou un lecteur de carte d'identification. La fonction ID & Print requiert quant à elle l'authentification de l'utilisateur via un identifiant et un mot de passe. Pour lancer le travail d'impression, l'utilisateur doit s'authentifier sur le périphérique multifonction en plaçant sa carte d'identification sur le lecteur de cartes ou en confirmant son identité à l'aide du scanner de veines digitales. L'avantage de cette fonction particulière est sa rapidité. Elle ne nécessite aucun identifiant ni mot de passe d'impression sécurisée supplémentaire.

Réduction des copies non autorisée

La **fonction de protection** contre la copie appose un filigrane sur les impressions et les copies durant le processus d'impression. Ce filigrane est à peine visible sur l'original, mais en cas de copie du document, il passe de l'arrière-plan au premier plan pour indiquer qu'il s'agit d'une copie.

Fonction Copy Guard pour garder le contrôle

La fonction « **Copy Guard / Password Copy** » appose un filigrane de sécurité caché sur l'original durant l'impression pour rendre sa copie impossible. Bien qu'à peine visible sur l'original protégé, il empêche la copie du document en bloquant l'appareil. La fonction Password Copy peut annuler la fonction Copy Guard et autoriser la production de copies en saisissant le mot de passe correct sur le panneau de commande du périphérique multifonction.

Chiffrement intelligent des PDF

Les **PDF cryptés** sont protégés par un mot de passe utilisateur. L'autorisation d'imprimer ou de copier le PDF et l'autorisation d'ajouter du contenu au PDF peuvent être configurées durant le processus de numérisation sur le périphérique multifonction.

Signature numérique utile des PDF

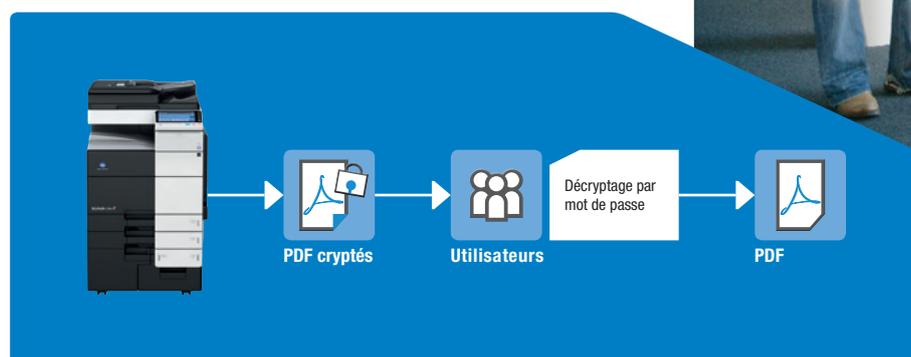
Cette fonction permet d'ajouter une signature numérique au PDF durant la numérisation. Cela permet de surveiller les modifications apportées au PDF après sa création.

Réception sécurisée

Lorsque cette fonction est activée, les télécopies reçues sont placées dans une boîte utilisateur protégée pour préserver leur confidentialité.

Sécurité des boîtes utilisateur

Des boîtes utilisateur sont disponibles pour des personnes seules et des groupes. Elles permettent de stocker en toute sécurité des documents sur le disque dur du périphérique multifonction avant son impression ou sa copie. Les boîtes utilisateur peuvent être protégées par un mot de passe alphanumérique à huit chiffres. En saisissant le mot de passe correct, il est possible d'accéder aux documents placés dans la boîte et de les visualiser. Avec ce système, seules les personnes autorisées peuvent accéder aux documents et données confidentiels.



PDF cryptés

SÉCURISEZ VOTRE RÉSEAU

Aujourd'hui, la communication et la connectivité sont indispensables dans le monde de l'entreprise. Les périphériques d'impression Konica Minolta tiennent compte de cela et offrent une intégration aisée dans les environnements réseau. Comme vous le savez certainement, les imprimantes et les périphériques multifonctions réseau ont évolué au point de fonctionner comme des hubs de traitement de documents sophistiqués faisant partie intégrante du réseau. Ils sont capables d'imprimer, de copier et de numériser des documents et des données vers différentes destinations réseau, ainsi que d'envoyer des e-mails.

Pour votre bureau, ce type de scénario signifie que ces technologies, lorsqu'elles ne sont pas protégées, posent un risque pour la sécurité. Elles sont donc exposées aux mêmes menaces et nécessitent la mise en œuvre des mêmes politiques de sécurité que n'importe quel autre appareil réseau. Pour éviter les vulnérabilités face aux attaques réseau internes et externes, Konica Minolta vous aide à vous assurer que votre équipement est entièrement conforme aux normes de sécurité les plus strictes. Sur les appareils Konica Minolta, cette conformité est rendue possible par les mesures suivantes :

▀ Blocage d'adresses IP

Contrôlez les accès aux ports et protocoles avec ce pare-feu interne intégrant une capacité de filtrage d'adresses IP.

▀ Gestion des ports

Votre administrateur peut ouvrir, fermer, activer et désactiver des ports et des protocoles, directement sur la machine ou depuis un site distant.

▀ Communications par e-mail sécurisées

La plupart des périphériques multifonctions Konica Minolta prennent en charge le chiffrement S/MIME (Secure/Multi-purpose Internet Mail Extensions) afin de sécuriser les communications par e-mail vers les destinataires désignés. Le chiffrement S/MIME sécurise votre trafic d'e-mails en chiffrant les messages électroniques et leur contenu au moyen d'un certificat de sécurité.

▀ Authentification réseau

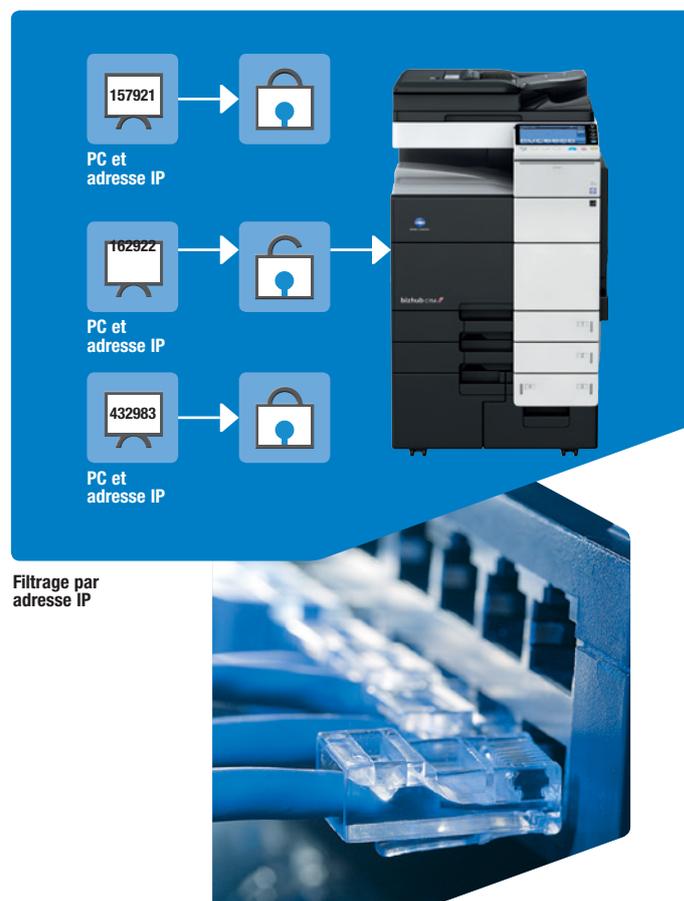
Les normes d'authentification basée sur le port IEEE 802.1x sont reconnues pour le contrôle d'accès aux réseaux WAN et LAN. Ces normes sécurisent efficacement votre réseau en fermant les communications réseau (ex., DHCP ou HTTP) vers les appareils non autorisés, à l'exception des demandes d'authentification.

▀ Communication protégée

Ce protocole protège toutes les communications destinées aux appareils ou initiées par ceux-ci. Il couvre les outils d'administration en ligne et les transmissions Windows Active Directory, par exemple.

▀ Communication réseau chiffrée

La plupart des appareils business hub prennent également en charge le protocole IPsec pour assurer un cryptage complet de toutes les données du réseau transmises vers et depuis votre périphérique multifonction. Le protocole de sécurité IP chiffre toutes les communications réseau entre l'intranet local (serveur, PC client) et vos appareils.



▀ Fonctionnalités de sécurité et disponibilité

Fonctionnalités	Systèmes multifonctions Couleur				Systèmes multifonctions Monochrome						Imprimantes		
	business hub C25	business hub C3350 C3850	business hub C224e C284e C364e C454e C554e	business hub C654e C754e	business hub 25e	business hub 215	business hub 3320 4020	business hub 4050 4750	business hub 224e 284e 364e 454e 554e	business hub 654e 754e	business hub C3100P	business hub 3300P	business hub 4000P 4700P
Contrôle des accès													
Comptabilisation (copies et impressions)	-	+	+	+	+	+	-	+	+	+	-	-	-
Restrictions de fonctions (copie/impression/scan/fax/boîtes/couleur)	+***	-	+	+	+	-	-	+	+	+	0	-	-
Impression sécurisée (verrouillage tâches)	+	+	+	+	+	+	+	+	+	+	0	-	+
Protection boîtes utilisateurs (mot de passe)	-	-	+	+	-	-	-	+	+	+	-	-	-
Authentification utilisateurs (ID, mot de passe)	0	+	+	+	+	+	-	+	+	+	-	-	-
Scanner de veines digitales	-	-	0	0	-	-	-	0	0	0	-	-	-
Lecteur de carte à puce	-	+	0	0	-	-	-	0	0	0	0	-	-
Journal d'évènement	-	+	+	+	-	-	+	+	+	+	-	+	-
Sécurité des données													
Chiffrements des données (disque dur)	-	+	+	+	-	-	+	+	+	+	0	-	-
Ecrasement des données du disque dur	-	+	+	+	-	-	+	+	+	+	0	-	-
Protection disque dur par mot de passe	-	-	+	+	-	-	-	-	+	+	0	-	-
Suppression automatique des données	-	-	+	+	-	-	-	-	+	+	0	-	-
Puce TPM (Trusted Platform Module)	-	-	0	0	-	-	-	-	0	0	-	-	-
Sécurité du réseau													
Filtrage d'adresses IP	+	+	+	+	+	-	+	+	+	+	+	+	+
Contrôle d'accès des ports et des protocoles	+	+	+	+	+	+***	+	+	+	+	+	+	+
Chiffrement SSL/TLS (HTTPS)	+	+	+	+	+	+	+	+	+	+	+	+	+
Prise en charge IPsec	+	+	+	+	-	-	+	+	+	+	+	+	+
S/NIME	-	+	+	+	-	-	-	+	+	+	-	-	-
Prise en charge IEEE 802.1x NIME	+	+	+	+	-	-	+	+	+	+	+	+	+
Sécurité de la 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 autorisés	-	-	+	+	-	-	-	-	+	+	+	-	-
Filigrane de protection anticopie	-	+	+	+	+	-	-	+	+	+	-	-	-
PDF chiffré	-	+	+	+	+	-	-	+	+	+	-	-	-
Signature de PDF	-	-	0	0	-	-	-	-	0	0	-	-	-
Chiffrement PDF par identification numérique	-	-	0	0	-	-	-	-A18	0	0	-	-	-
Protection contre la copie (Copy Guard / Password Copy)	-	-	0	0	-	-	-	-	0	0	-	-	-
Certification de sécurité													
Certifié ISO 15408 EAL 3	-	+**	+	+	-	-	+**	+**	+	+	+***	-	-
IEEE std 2600.1 (-2009)	-	+**	+**	+**	-	-	-	+**	+**	+	-	-	-

+ : en standard, 0 : en option, - : non disponible, * Pour l'impression uniquement, ** En-cours d'évaluation, *** sous certaines réserves