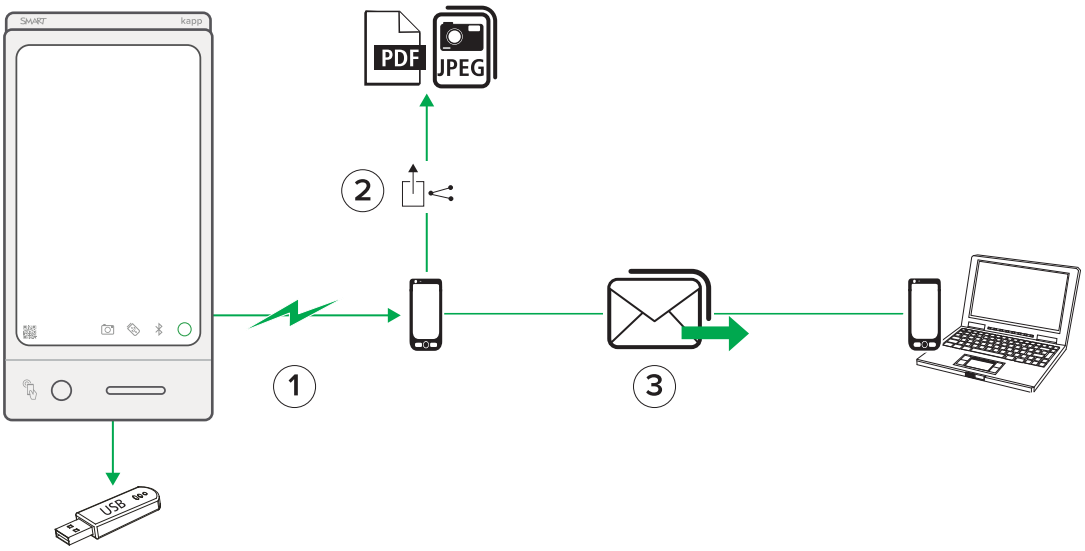
Informations sur la sécurité

SMART kapp

SMART kapp® inclut des fonctionnalités de sécurisation des données conçues pour contrôler de manière prévisible votre contenu. Ce document explique quelles fonctionnalités de sécurisation utilise SMART kapp pour protéger vos données.

Sécuriser les données de bout en bout

L'architecture de sécurité de SMART kapp a recours à des pratiques de sécurisation standard afin de protéger vos données lors de leur partage entre le tableau SMART kapp, un appareil mobile, des services de messagerie ou tiers et des sessions de partage. Vos données sont ainsi davantage protégées de bout en bout.



1 Comment SMART kapp sécurise les données entre le tableau et un appareil mobile

Pour protéger les informations que vous écrivez sur le tableau, celui-ci dispose des fonctionnalités de sécurisation suivantes :

Mémoire interne

Le tableau est équipé de sa propre mémoire interne, dans laquelle il stocke temporairement vos informations. Lorsque vous effacez le tableau, l'encre numérique est définitivement supprimée de la mémoire du tableau.

REMARQUES

- Lorsque vous effectuez des copies d'écran en appuyant sur **Capturer** sur le tableau, vos données ne sont pas enregistrées dans la mémoire interne du tableau.
- La seule manière d'enregistrer des copies d'écran sans connecter un appareil mobile consiste à brancher une clé USB directement au port USB du tableau.

Association Bluetooth®

Le tableau utilise l'association Bluetooth pour communiquer avec votre appareil mobile. Il ne se connecte pas directement à un réseau. Cela signifie que vous n'avez pas à vous inquiéter que des interruptions dans la sécurité réseau affectent la communication entre votre appareil mobile et le tableau.

REMARQUE

Même si la connexion Bluetooth entre votre appareil mobile et le tableau ne nécessite pas de connexion réseau, votre appareil mobile aura besoin d'une connexion réseau pour initier une session de partage ou pour partager les copies d'écran d'une session.

Chaque tableau se connecte à un seul appareil mobile à la fois et dispose d'un code QR, d'une balise CCP et d'un ID de tableau uniques. Ces identifiants uniques vous garantissent, lorsque vous associez votre appareil mobile en scannant le code QR, touchant la balise CCP ou saisissant manuellement l'ID du tableau, une communication plus sûre entre l'appareil que vous avez associé et le tableau.

L'association entre votre appareil mobile et un tableau passe par une connexion Bluetooth cryptée afin d'empêcher toute interception. SMART kapp protège son association Bluetooth par la méthode "Secure Simple Pairing" standard. Pour assurer une protection encore plus grande, SMART kapp ajoute à la connexion Bluetooth une couche de cryptage Advanced Encryption Standard (AES) 128 ou 256 bits, une cryptographie asymétrique à courbe elliptique et l'enveloppement de clé, ce qui réduit efficacement le risque d'interception des données sans fil.

2 Comment SMART kapp sécurise les copies d'écran partagées

Lorsque vous effectuez des copies d'écran en appuyant sur **Capturer** sur le tableau ou dans l'application SMART kapp, vos données sont enregistrées dans la bibliothèque de sessions de l'application. SMART kapp ne partage pas les copies d'écran enregistrées avec d'autres applications sans votre autorisation. Vos copies d'écran ne sont partagées que si vous les exportez de l'application SMART kapp par e-mail ou vers un service tiers, comme des applications de type cloud installées sur votre appareil mobile. Lorsque vous partagez des copies d'écran par e-mail ou par le biais d'un service tiers, c'est la protection des données standard proposée par votre fournisseur de messagerie ou votre service tiers qui sécurise vos informations. Les destinataires peuvent ensuite enregistrer les copies d'écran sur leur appareil local. Lorsqu'ils enregistrent ces copies d'écran, c'est le cryptage ou la protection bac à sable* spécifique au système d'exploitation de leur appareil local qui sécurise les données.

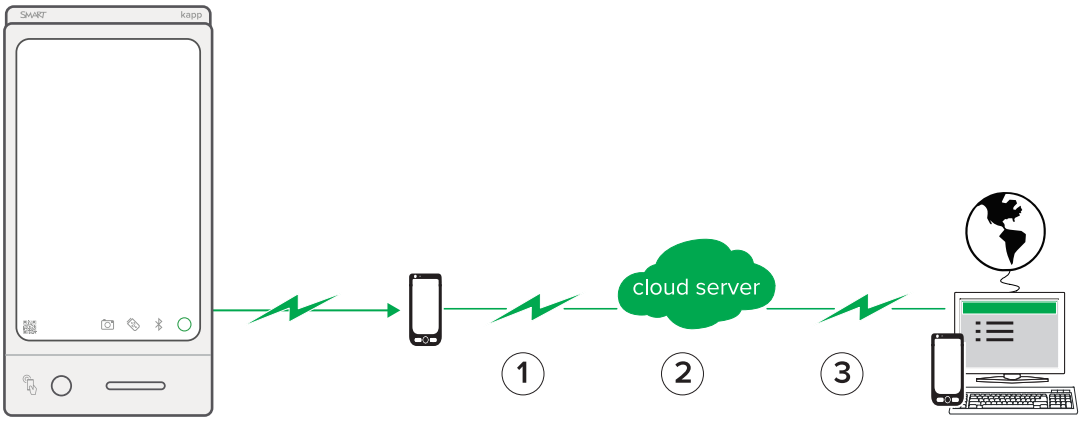
3 Comment SMART kapp sécurise les invitations aux sessions de partage

Lorsque vous initiez une session de partage à partir de l'application SMART kapp, vous pouvez envoyer l'URL de la session à d'autres participants par e-mail ou par le biais d'un service tiers. Lorsque ces autres personnes reçoivent l'invitation à consulter votre session, elles appuient sur l'URL ou cliquent dessus pour voir votre tableau et les copies d'écran de la session dans leur navigateur Internet. SMART kapp sécurise cette URL à l'aide de protocoles de communication cryptés (HTTPS). Lorsque vous envoyez une invitation à une session par e-mail ou par le biais d'un service tiers, c'est la protection des données standard proposée par votre fournisseur de messagerie ou votre service tiers qui sécurise vos informations.

Sécuriser les données lors des sessions de partage

Lors d'une session de partage, vos données sont transférées du tableau à votre appareil mobile par le biais d'une connexion Bluetooth sécurisée, puis de votre appareil mobile au serveur cloud kappboard.com, et enfin au navigateur du participant à la session de partage.

*La protection bac à sable est un mécanisme de sécurité qui protège contre les programmes potentiellement dangereux pouvant contenir un virus ou du code nocif en limitant l'accès du programme aux ressources d'un appareil local (par exemple, les descripteurs de fichier ou la mémoire d'un appareil).



Comment SMART kapp sécurise les données au cours des sessions de partage

Pour accroître la sécurité de vos informations sensibles de bout en bout pendant leur transfert entre votre appareil mobile et le navigateur d'un participant, SMART kapp protège vos données de la façon suivante :

1 **Lors du transfert vers le serveur cloud**	SMART kapp a uniquement recours à des protocoles de communication cryptés (HTTPS) afin d'envoyer des informations au serveur cloud kappboard.com.
2 **Dans le serveur cloud**	Le serveur cloud de SMART kapp, hébergé par Amazon Web Services (AWS), utilise la sécurité standard fournie avec AWS afin de protéger vos données dans le cloud. Les données de votre session ne sont disponibles dans le cloud qu'au cours de la session de partage. Lorsque vous mettez fin à une session de partage, seuls les participants à la session peuvent télécharger une copie de la session à partir de la fenêtre de navigateur qu'ils utilisaient pour assister à la session. Après que vous avez mis fin à une session et que tous les participants ont fermé leur navigateur, vos données ne sont plus accessibles à partir du serveur cloud.
3 **Lors du transfert vers le navigateur Internet d'un participant**	L'URL qu'utilisent les participants pour rejoindre votre session de partage est protégée par HTTPS. Cette URL contient un identifiant alphanumérique unique créé spécifiquement pour chacune de vos sessions. Si vous disposez d'un abonnement premium à l'application, vous pouvez rendre cette URL statique (la même URL est utilisée pour toutes vos sessions de partage) ou dynamique (chaque nouvelle URL est unique et non séquentielle). Les abonnés à l'application premium peuvent aussi protéger les sessions à l'aide d'un PIN.

REMARQUE

Pour plus d'informations sur les différences entre l'application de base et premium, rendez-vous à l'adresse smartkapp.com/app.

FAQ sur la sécurité

Que se passe-t-il si je perds mon appareil mobile qui contient des copies d’écran enregistrés sous forme d'images JPEG ou de fichiers PDF ?

La sécurité fournie par le système d'exploitation de votre appareil mobile protège les données de la session enregistrées dans la bibliothèque interne de votre appareil mobile. Les appareils Android ont recours au cryptage, tandis que les appareils iOS utilisent une protection bac à sable. Les données que vous avez enregistrées sur votre appareil mobile sont protégées par la sécurité que fournit automatiquement votre appareil, ou par les fonctionnalités de sécurisation que vous avez paramétrées sur votre appareil (comme un PIN). Si vous perdez votre appareil, suivez les procédures de votre entreprise vis-à-vis de la sécurité des données, qui s'appliquent aux appareils perdus contenant des informations sensibles.

Le tableau nécessite-t-il un logiciel antivirus ?

Non, le tableau n'est pas vulnérable aux virus, car il ne comporte pas de système d'exploitation traditionnel. Le seul logiciel qui s'exécute sur un tableau est le micrologiciel SMART kapp.

Quelle est l'utilité du port USB du tableau ? Les fichiers enregistrés sur une clé USB sont-ils sécurisés ?

Si vous ne voulez pas connecter un appareil mobile au tableau, vous pouvez brancher une clé USB au port USB du tableau afin d'enregistrer les copies d'écran que vous effectuez au cours de votre session. Ces copies d’écran sont enregistrées sur votre clé USB en tant que fichiers PDF non sécurisés. Certaines clés USB disposent de leurs propres fonctionnalités de sécurité (comme la protection par cryptage ou mot de passe) qui peuvent contribuer à protéger vos données si vous perdez la clé USB. Vous pouvez aussi crypter votre clé USB ou ajouter un mot de passe manuellement à chaque fichier.

Le tableau nécessite-t-il d'ouvrir des ports spécifiques pour fonctionner ?

Non, SMART kapp utilise uniquement le réseau de l'appareil mobile associé afin de communiquer, et il ne nécessite pas de réseau traditionnel.

SMART kapp conserve-t-il des informations personnelles, comme l'ID, l'adresse IP ou le numéro de téléphone de l'utilisateur ?

Non, SMART kapp ne garde aucune information nominative.

SMART kapp fournit-il des rapports ou des audits sur l'utilisation du tableau ?

Actuellement, SMART kapp ne propose pas de capacités publiques de rapport.

© 2016 SMART Technologies ULC. Tous droits réservés. SMART kapp, smarttech, le logo SMART et tous les slogans SMART sont des marques de commerce ou des marques déposées de SMART Technologies ULC aux États-Unis et/ou dans d'autres pays. Tous les noms de produits et de sociétés tiers peuvent être des marques de commerce appartenant à leurs détenteurs respectifs. Le contenu peut être modifié sans préavis. 12-2016.