SMART kapp

security information

SMART kapp includes data security features designed to keep dry-erase content controlled in a predictable way, making it easy to deploy in any space with minimal IT management

No access to company networks required

SMART kapp does not connect directly to a network, and relies on users' connected iOS and Android mobile devices or USB thumb drives to save board snapshots.

- SMART kapp uses Bluetooth® to communicate with users' iOS and Android mobile devices
- Snapshots saved to a USB thumb drive can be transferred to a PC connected to a network

Secure dry-erase user data

Users of SMART kapp control the saving and sharing of contents written on the board to their mobile devices.

- When the board's surface is erased, content data created is erased from the board's memory
- Snapshots are saved to a connected mobile device and remain there until the user chooses to remove or share
- The snapshot data saved to a mobile device is only accessible by the SMART kapp mobile app and are in a proprietary format.

Connecting Bluetooth® devices

When a mobile device is connected to a board, it uses a secured Bluetooth® connection that is encrypted to prevent interception.

- Bluetooth® discovery and pairing are protected using the industry-standard "Secure Simple Pairing" method
- An additional layer of AES 128-bit encryption is used over the Bluetooth® connection, over and above the encryption already provided by Bluetooth®
- Bluetooth® connections are initiated by scanning a QR code, tapping a NFC tag, or manually typing in the unique board ID using the mobile app
- Each SMART kapp digital capture board has its own unique QR code, NFC tag and board ID
- A "Bluetooth® connected" indicator light will notify a user when a device is connected to the board
- Only one mobile device may connect via Bluetooth® to the board at a time
- Moving a connected mobile device out of Bluetooth® wireless communication range (typical 10-30M or approximately 30-100 feet depending on the environment) will disconnect the device from the board and will stop live sharing.
- SMART kapp digital capture boards use industry-leading RSA and Elliptic Curve cryptography to ensure that only connections from the official SMART kapp™ apps for iOS and Android are accepted

Live Sharing and cloud services

SMART kapp and a connected mobile device do not share board data to cloud services unless initiated by the user.

- The user initiates the Live Sharing feature allowing other users to view content from the session on any web browser.
- The Live Sharing URL expires after the session is ended by the connected mobile device
- The Live Sharing URL contains a universally unique identifier created specifically for each session, and is not sequential from previous Live Sharing URLs.
- The Live Sharing URL is shared with others using the user's choice of sharing service installed on the mobile device (e.g. email and SMS)
- Live Sharing from the mobile device sends data to cloud server using encrypted communication protocols (HTTPS). The sharing URL is also secured by HTTPS.
- The mobile device requires an active internet connection to live share data
- The user ends Live Sharing by disconnecting the mobile device from the board. The URL expires and the cloud server data is no longer accessible in any way after a few minutes.
- The user can export saved snapshots as PDF and jpg files from the mobile device to installed cloud services apps, etc.
- Evernote users may choose to link the SMART kapp app to an Evernote account, allowing automatic upload of all saved snapshot