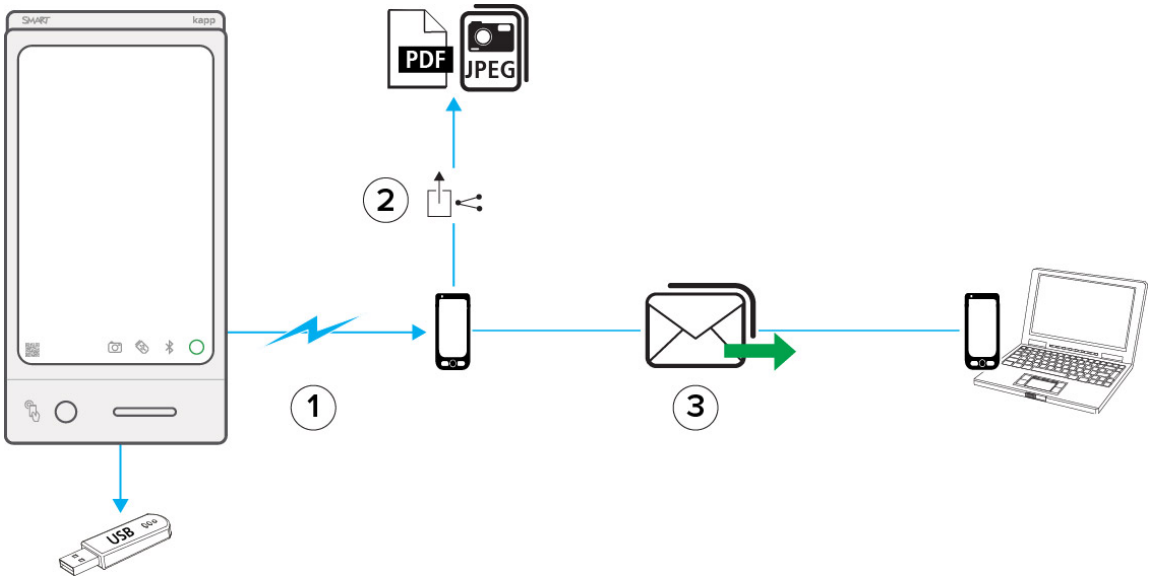
Security information

SMART kapp

SMART kapp™ includes data security features designed to keep your content controlled in a predictable way. This document explains the security features SMART kapp uses to make your data more secure.

Securing data from end to end

SMART kapp's security architecture uses well known, industry-standard security practices to help protect your data as it is shared between the SMART kapp capture board, a mobile device, email or third-party services and sharing sessions. This makes your data more secure from end to end.



① Securing data from the capture board to a mobile device

To help secure the information you write on the board, the capture board has the following security features:

Internal memory

The capture board has its own internal memory where it temporarily stores your information. When you erase the board, the digital ink is permanently removed from the capture board's memory.

> **NOTE**
>
> When you take snapshots by pressing **Capture** on the capture board, your data is not saved to the capture board's internal memory. The only way to save snapshots without connecting a mobile device is to connect a USB drive directly to the board's USB port. For more information about USB drive security, see *Security FAQ* on page 5.

Bluetooth® pairing

The capture board uses Bluetooth pairing to communicate with your mobile device. It does not connect directly to a network. This means you can worry less about interruptions to network security affecting the communication between your mobile device and the capture board.

> **NOTE**
>
> Although the Bluetooth connection between your mobile device and capture board does not require a network connection, your mobile device will need a network connection to initiate a sharing session or share any session snapshots.

Each capture board connects with only one mobile device at a time and has a unique QR code, NFC tag and board ID. These unique identifiers ensure that when you pair your mobile device by scanning the QR code, tapping the NFC tag or entering the unique board ID manually, the communication between your paired device and the capture board is more secure.

The pairing between your mobile device and a capture board uses an encrypted Bluetooth connection to help prevent any interception. SMART kapp protects this Bluetooth pairing using the industry-standard "Secure Simple Pairing" method. To provide even greater protection, SMART kapp adds a layer of 128 or 256-bit Advanced Encryption Standard (AES) encryption, elliptic curve asymmetric cryptography and key wrapping to the Bluetooth connection, effectively reducing the risk of wireless data interception.

② Securing shared snapshots

When you take snapshots by pressing **Capture** on the capture board or in the SMART kapp app, your data is saved to the app's library. SMART kapp doesn't share saved snapshots with other applications without your permission. Your snapshots are shared only if you export them from the SMART kapp app via email or a third-party service, such as cloud applications you have on your mobile device. When you share snapshots through email or a third-party service, the standard data protection offered by your email provider or third-party service helps to secure your information. Recipients can then save the snapshots to their local device. When they save these snapshots, their local device's encryption or operating system-specific sandbox protection[1] helps keep the data secure.

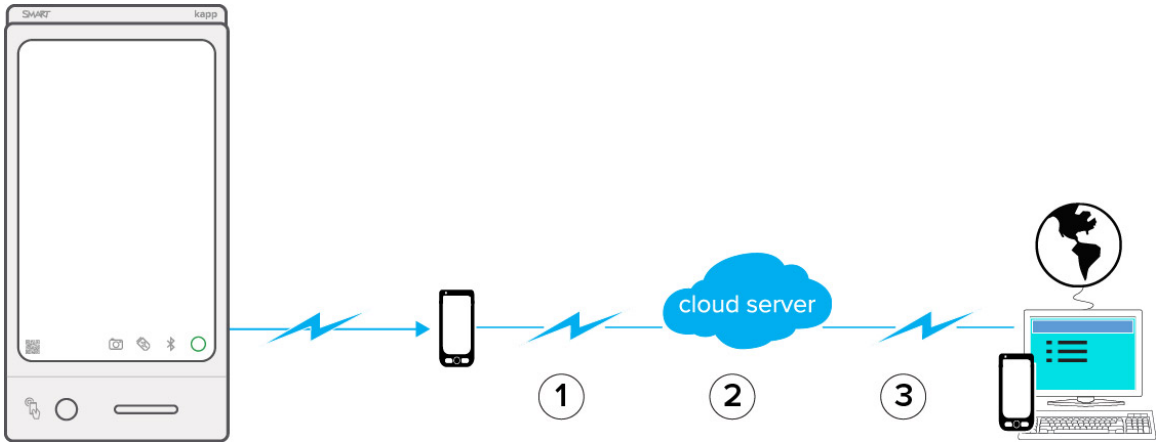
③ Securing sharing session invites

When you initiate a sharing session from the SMART kapp app, you can send the session URL to other participants through email or a third-party service. When others receive the invitation to view your session, they press or click the URL to view your capture board and session snapshots in their web browser. SMART kapp secures this URL using encrypted communication protocols (HTTPS). When you send a session invite through email or a third-party service, the standard data protection offered by your email provider or third-party service helps to secure your information.

[1]Sandbox protection refers to a security mechanism that protects against potentially harmful programs that may contain a virus or harmful code by restricting the program's access to a local device's resources (for example, a device's file descriptors or memory).

Securing data during sharing sessions

During a sharing session, your data is transferred from the capture board to your mobile device using a secure Bluetooth connection, then from your mobile device to the kappboard.com cloud server, and finally to a sharing session participant's browser.



To increase the security of your sensitive information at all points during the transmission from your mobile device to a participant's browser, SMART kapp protects your data in the following ways:

1 In transit to the cloud server	SMART kapp uses only encrypted communication protocols (HTTPS) to send information to the kappboard.com cloud server.
2 In the cloud server	SMART kapp's cloud server is hosted by Amazon Web Services (AWS) and uses the industry-standard security provided with AWS to help protect your data in the cloud. Your session data is available from the cloud only during the sharing session. After you end a sharing session, only the session's participants can download a copy of the session from the browser window they used to view the session. After you end a session and all the participants have closed their browsers, your data is no longer accessible from the cloud server.
3 In transit to participant's web browser	The URL that participants use to join your sharing session is protected with HTTPS. This URL contains a unique alphanumeric identifier created specifically for each of your sessions. If you have a premium app subscription, you can make this URL static (the same URL is used for all of your sharing sessions) or dynamic (each new URL is unique and non-sequential). Premium app subscribers can also protect sessions with a PIN.

NOTE

For more information about the differences between the premium and basic app, visit smartkapp.com/get-app.

Security FAQ

What happens if I lose my mobile device with saved snapshot JPEG images or PDF files?
The security provided by your mobile device's operating system protects session data saved to your mobile device's internal library. Android devices use encryption, and iOS devices use a sandbox protection. The data you've saved to your mobile device is protected with the security that your device provides automatically or by the security features you set up on your device (such as a PIN). If your device is lost, follow your company's data security procedures for lost devices that contain sensitive information.

Does the capture board require antivirus software?
No, the capture board is not vulnerable to viruses because it does not have a traditional operating system. The only software that runs on a capture board is the SMART kapp firmware.

Why would I use the capture board's USB port? Are the files saved to a USB drive secure?
If you do not want to connect a mobile device to the capture board, you can insert a USB drive into the provided USB port on the capture board to save the snapshots you take during your session. These snapshots are saved to your USB drive as unsecured PDF files. Some USB drives come with their own security features (such as encryption or password protection) which can help protect your data if the USB drive is lost. You can also encrypt your USB drive or add a password to each file manually.

Does the capture board require specific ports to be open in order to work?
No, SMART kapp uses only the paired mobile device's network to communicate and does not require a traditional network.

Does SMART kapp retain any personal information, such as a user ID, IP address or phone number?
No, SMART kapp does not keep any personally identifiable information.

Does SMART kapp provide reports or audits on the usage of the capture board?
SMART kapp does not currently offer public reporting capabilities.

---

smartkapp.com