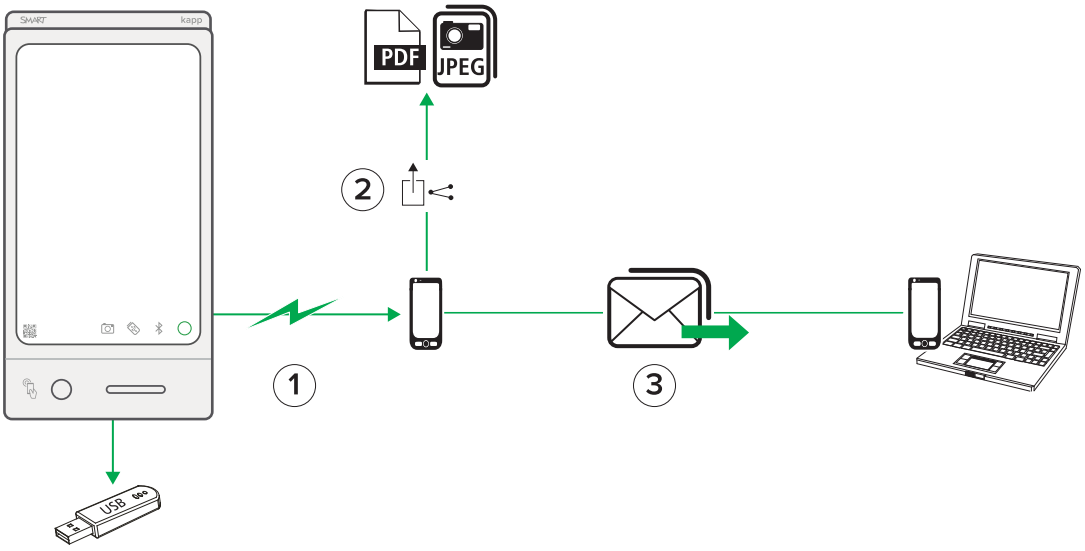
Sicherheitsinformationen

SMART kapp

SMART kapp® ist mit Datenschutzfunktionen ausgestattet, die speziell darauf ausgelegt sind, Ihre Inhalte auf vorhersehbare Weise unter Kontrolle gehalten werden. In diesem Dokument werden die Sicherheitsfunktionen erläutert, die SMART kapp zum Schutz Ihrer Daten verwendet.

Datenschutz während des gesamten Prozesses

Die Sicherheitsarchitektur von SMART kapp nutzt bewährte branchenübliche Sicherheitsverfahren, um Ihre Daten während der Übertragung zwischen dem SMART kapp Board, einem Mobilgerät, E-Mail-Programmen oder Drittanbieter-Diensten und freigegebenen Sitzungen zu schützen. So sind Ihre Daten während des gesamten Prozesses besser geschützt.



1 Wie SMART kapp Daten vom Board auf einem Mobilgerät sichert

Zum Schutz Ihrer auf dem Board geschriebenen Informationen verfügt das Board über die folgenden Sicherheitsfunktionen:

Interner Speicher

Das Board hat einen eigenen internen Speicher, in dem es Ihre Informationen temporär speichert. Wenn Sie die Tinte auf Ihrem Board löschen, wird die digitale Tinte permanent aus dem Speicher des Boards entfernt.

NOTIZEN

- Wenn Sie Snapshots aufnehmen, indem Sie am Board auf **Aufnahme** drücken, werden Ihre Daten nicht im internen Speicher des Boards gespeichert.
- Die einzige Möglichkeit zum Speichern von Snapshots, ohne ein Mobilgerät anzuschließen, ist, ein USB-Laufwerk direkt an den USB-Anschluss des Boards anzuschließen.

Bluetooth® - Kopplung

Das Board nutzt das Bluetooth-Kopplungsverfahren zur Kommunikation mit Ihrem Mobilgerät. Es wird nicht direkt mit einem Netzwerk verbunden. So müssen Sie sich weniger Gedanken in Bezug auf eine Unterbrechung der Netzwerksicherheit machen, die die Kommunikation zwischen Ihrem Mobilgerät und dem Board beeinträchtigt.

HINWEIS

Obwohl die Bluetooth-Verbindung zwischen Ihrem Mobilgerät und dem Board keine Netzwerkverbindung erfordert, benötigt Ihr Mobilgerät eine, um eine freigegebene Sitzung zu initiieren oder Sitzungs-Snapshots weiterzuleiten.

Jedes Board lässt sich nur jeweils mit einem Mobilgerät verbinden und hat einen eindeutigen QR-Code, NFC-Tag und eine eindeutige Board-ID. Diese eindeutigen Kennungen gewährleisten, dass beim Koppeln Ihres Mobilgeräts durch Scannen des QR-Codes, Berühren des NFT-Tags oder manuelles Eingeben der eindeutigen Board-ID die Kommunikation zwischen dem gekoppelten Gerät und dem Board besser geschützt ist.

Die Kopplung zwischen Ihrem Mobilgerät und einem Board erfolgt über eine verschlüsselte Bluetooth-Verbindung, was hilft, einen unbefugten Zugriff zu verhindern. SMART kapp schützt diesen Bluetooth-Kopplungsvorgang mithilfe des branchenüblichen Standardverfahrens "Secure Simple Pairing". Um noch mehr Sicherheit zu bieten, schützt SMART kapp die Bluetooth-Verbindungen mit Funktionen wie die AES (Advanced Encryption Standard)-Verschlüsselung mit 128 oder 256 Bit, die Elliptische-Kurven-Kryptography (asymetrisch) und der Key-Wrapping-Algorithmus, um das Risiko eines unbefugten Zugriffs auf drahtlose Daten zu verringern.

2 So sichert SMART kapp Snapshots:

Wenn Sie Snapshots durch Drücken von **Aufnahme** am Board oder in der SMART kapp App aufnehmen, werden Ihre Daten in der Sitzungsbibliothek der App gespeichert. SMART kapp leitet ohne Ihre Genehmigung keine gespeicherten Snapshots an andere Anwendungen weiter. Ihre Snapshots werden nur weitergeleitet, wenn Sie sie mithilfe eines E-Mail-Programms oder einem Drittanbieter-Dienst wie etwaige Cloud-Anwendungen auf Ihrem Mobilgerät aus der SMART kapp App exportieren. Wenn Sie Ihre Snapshots über ein E-Mail-Programm oder einen Drittanbieter-Dienst weiterleiten, werden die Informationen unter Verwendung des von Ihrem E-Mail-Anbieter oder Drittanbieter-Dienst angebotenen Standard-Datenschutzes geschützt. Empfänger können dann die Snapshots auf ihrem lokalen Gerät anzeigen. Falls sie diese Snapshots speichern, werden die Daten unter Verwendung der Verschlüsselung ihres lokalen Geräts oder der betriebssystemspezifischen Sandbox-Schutzfunktion geschützt.* (z. B. auf die Datei-Deskriptoren oder den Speicher des Geräts).

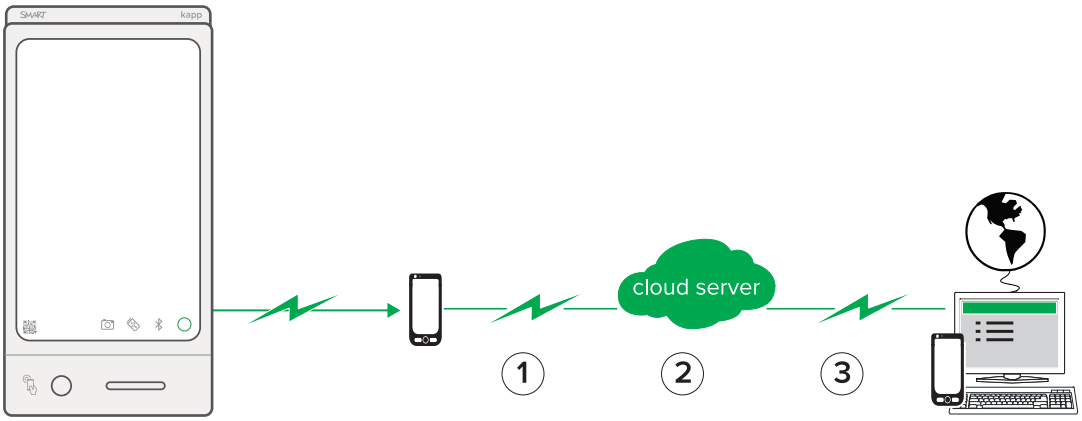
3 So sichert SMART kapp das Teilen von Session-Einladungen:

Wenn Sie eine freigegebene Sitzung über die SMART kapp App initiieren, können Sie die Sitzungs-URL per E-Mail oder einen Drittanbieter-Dienst an andere Teilnehmer senden. Wenn andere die Einladung zur Ansicht Ihrer Sitzung empfangen, drücken oder klicken sie auf die URL, um Ihre Board- und Sitzungs-Snapshots in ihren Webbrowsern anzuzeigen. SMART kapp schützt diese URL mit verschlüsselten Kommunikationsprotokollen (HTTPS). Wenn Sie eine Einladung zu einer Session über ein E-Mail-Programm oder einen Drittanbieter-Dienst weiterleiten, werden die Informationen unter Verwendung des von Ihrem E-Mail-Anbieter oder Drittanbieter-Dienst angebotenen Standard-Datenschutzes geschützt.

Schützen von Daten während einer freigegebenen Sitzung

Während einer freigegebenen Sitzung werden Ihre Daten über eine sichere Bluetooth-Verbindung vom Board an Ihr Mobilgerät und dann von Ihrem Mobilgerät an den Cloud-Server kappboard.com und schließlich an den Browser der an der freigegebenen Sitzung teilnehmenden Person übertragen.

*Die Sandbox-Schutzfunktion ist ein Sicherheitsmechanismus, der vor potenziell schadhaften Programmen, die möglicherweise einen Virus oder schadhaften Code enthalten, schützen, indem er den Zugriff des Programms auf die Ressourcen eines lokalen Geräts beschränkt



So sichert SMART kapp Daten während der Freigabe (dem Teilen) von Sessions:

Um die Sicherheit Ihrer sensitiven Daten zu jeder Zeit während der Übertragung von Ihrem Mobilgerät auf den Browser des Teilnehmers sicher sind, schützt SMART kapp Ihre Daten wie folgt:

1 **Während der Übertragung zum Cloud-Server**	SMART kapp nutzt nur verschlüsselte Kommunikationprotokolle (HTTPS) zum Senden von Informationen zum Cloud-Server kappboard.com.
2 **Im Cloud-Server**	Der Cloud-Server von SMART kapp wird von den Amazon Web Services (AWS) gehostet und nutzt die branchenübliche Standardverschlüsselung von AWS zum Schutz Ihrer Daten in der Cloud. Ihre Sitzungsdaten sind nur während der freigegebenen Sitzung in der Cloud verfügbar. Nach Ende der freigegebenen Session können nur die Sitzungsteilnehmer eine Kopie der Sitzung vom Browser-Fenster aus herunterladen, das sie zur Anzeige der Session verwendet haben. Nachdem Sie die Session beendet und alle Teilnehmer ihre Browser geschlossen haben, sind Ihre Daten nicht mehr vom Cloud-Server aus zugänglich.
3 **Während der Übertragung zum Teilnehmer-Webbrowser**	Die URL, die die Teilnehmer zur Teilnahme an Ihrer freigegebenen Sitzung verwenden, wird mittels HTTPS geschützt. Diese URL enthält eine eindeutige alphanumerische Kennung, die speziell für jede Ihrer Sitzungen erstellt wird. Wenn Sie ein Premium-Abonnement für die App haben, können Sie eine statische URL (d. h. dieselbe URL wird für all Ihre freigegebenen Sitzungen verwendet) oder eine dynamische URL (d. h. jede neue URL ist eindeutig und nicht aufeinander folgend) herstellen. Premium-Abonnenten der App können ihre Sitzungen auch mit einer PIN schützen. **HINWEIS** Weitere Informationen zu den Unterschieden zwischen der Premium- und der Basis-App finden Sie unter: smartkapp.com/app.

FAQ zur Sicherheit

Was passiert, wenn ich mein Mobilgerät mit gespeicherten Snapshots in Form von JPEG-Bildern oder PDF-Dateien verliere?

Die vom Betriebssystem Ihres Mobilgeräts bereitgestellte Sicherheit schützt die in der internen Bibliothek Ihres Mobilgeräts gespeicherten Sitzungsdaten. Android-Geräte nutzen eine Verschlüsselung, und iOS-Geräte nutzen das Sandbox-Schutzverfahren. Die auf Ihrem Mobilgerät gespeicherten Daten werden mithilfe der automatisch von Ihrem Mobilgerät bereitgestellten Sicherheitsfunktionen oder durch die Sicherheitsfunktionen geschützt, die Sie auf Ihrem Gerät einrichten (wie z. B. eine PIN). Falls Sie Ihr Gerät verlieren, befolgen Sie die Datensicherheitsverfahren Ihres Unternehmens bezüglich verlorener Geräte, die vertrauliche Informationen enthalten.

Benötige ich für das Board eine Antivirensoftware?

Nein, das Board ist nicht anfällig für Viren, da es kein herkömmliches Betriebssystem verwendet. Die einzige Software, die auf einem Board ausgeführt wird, ist die SMART kapp Firmware.

Warum sollte ich den USB-Anschluss des Boards verwenden? Sind die auf einem USB-Laufwerk gespeicherten Dateien sicher?

Wenn Sie kein Mobilgerät an das Board anschließen wollen, können Sie ein USB-Laufwerk über den vorhandenen USB-Anschluss am das Board anschließen, um die während der Sitzung aufgenommenen Snapshots zu speichern. Diese Snapshots werden als ungeschützte PDF-Dateien auf Ihrem USB-Laufwerk gespeichert. Einige USB-Laufwerke sind mit eigenen Sicherheitsfunktionen ausgestattet (wie z. B. einer Verschlüsselung oder einer Passwortschutzfunktion), die für den Fall, dass das USB-Laufwerk verloren geht, Ihre Daten schützt. Sie können Ihr USB-Laufwerk auch verschlüsseln oder jede Datei manuell mit einem Passwort versehen.

Müssen während der Verwendung des Boards bestimmte Ports offen sein?

Nein, SMART kapp verwendet nur das Netzwerk des gekoppelten Mobilgeräts zur Kommunikation und benötigt kein herkömmliches Netzwerk.

Speichert SMART kapp irgendwelche persönlichen Informationen wie die Benutzer-ID, die IP-Adresse oder die Telefonnummer?

Nein, SMART kapp speichert keine persönlichen Daten.

Erstellt SMART kapp Berichte oder Auditprotokolle über die Nutzung des Boards?

SMART kapp bietet derzeit keine öffentliche Berichterstattungsfunktionen.