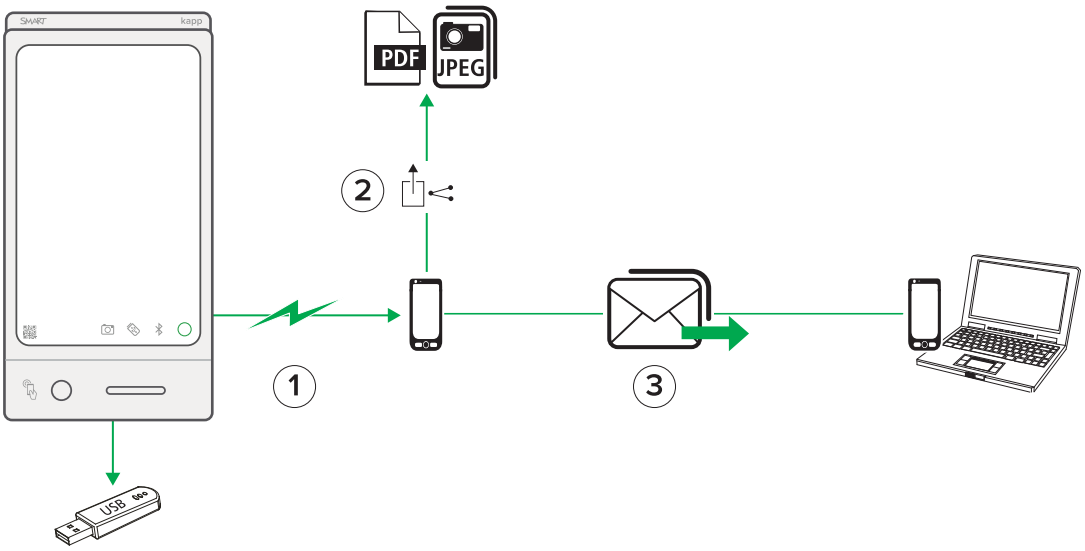
Säkerhetsinformation

SMART kapp

SMART kapp® inkluderar säkerhetsfunktioner som är framtagna för att hålla skrivtavlans innehåll kontrollerat på ett förutsebart sätt. Detta dokument förklarar säkerhetsfunktionerna som SMART kapp använder för att hålla dina data mer säkra.

End-to-end datasäkring

SMART kapp säkerhetsarkitektur använd välkända branschstandard säkerhetsmetoder för att skydda dina data som delas mellan SMART kapp-tavlan, en mobil enhet, e-post eller tredje parters tjänster och delningssessioner. Detta gör att dina data hålls mer säkra från början till slut.



1 Hur SMART kapp säkrar data från tavlan till en mobil enhet

För att säkerställa säkerhet för informationen som du skriver på skrivtavlan så är skrivtavlan utrustad med följande säkerhetsfunktioner:

Internminne	Tavlan har inbyggt internt minne som temporärt lagrar din information. När du suddar bort innehåll från skrivtavlan så raderas det digitala bläcket permanent från tavlans minne. **ANTECKNINGAR** • När du tar skärmdumpar genom att klicka på **Capture** på skrivtavlan, sparas datan inte till skrivtavlans interna minne. • Det enda sättet att spara skärmdumpar på utan att ansluta till en mobil enhet är att ansluta en USB-enhet direkt till skrivtavlans USB-port.
Bluetooth®-parning	Tavlan använder Bluetooth för att kommunicera med din mobila enhet. Den ansluts inte direkt till ett nätverk. Detta betyder att du kan oroa dig mindre om svagheter i nätverkssäkerhet som påverkar kommunikationen mellan din mobila enheter och skrivtavlan. **OBS!** Det krävs inget nätverk för att ansluta din mobila enheter till skrivtavlan via Bluetooth, men din mobila enhet behöver ändå ett nätverk för att starta delningssessionen eller dela skärmdumpar. Varje skrivtavla kan bara anslutas till en mobil enhet åt gången och har en unik QR-kod, NFC-bricka och Board ID. Dessa unika beteckningar gör så att kommunikationen mellan din parade enhet och tavlan när du ansluter genom att skanna QR-koden, knacka NFC-brickan eller mata in Board ID blir mer säker. Anslutningen mellan din mobila enhet och tavlan använder en krypterad Bluetooth-koppling för att förhindra intrång. SMART kapp skyddar denna Bluetooth-anslutning med branschstandardmetoden Secure Simple Pairing. För vidare säkerhet tillför SMART kapp ett lager 128 eller 256 bitar Advanced Encryption Standard (AES-kryptering), elliptic curve assymetric cryoptography och keywrapping på Bluetooth-anslutning, vilket effektivt minskar risken för trådlös datauppsnappning.

2 Hur SMART kapp säkrar delade skärmdumpar

När du tar skärmdumpar genom att klicka på **Capture** på skrivtavlan eller SMART kapp-appen, sparas datan inte till appens bibliotek. SMART kapp delar inte sparade skärmdumpar med andra program utan ditt tillstånd. Dina skärmdumpar delas endast om du exporterar dem från SMART kapp-appen via e-post eller en tredje parters tjänst, som t.ex. eventuella

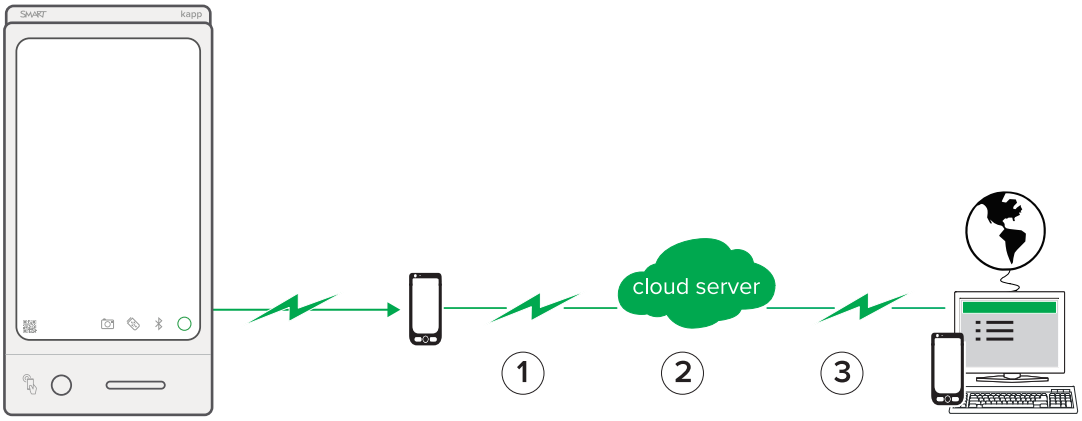
molnprogram som du har på din mobila enhet. När du delar skärmdumpar via e-post eller en tredje parters tjänst, bidrar din e-postleverantörs eller trdje parts standard dataskydd till att hålla din information säker. Mottagare kan sedan spara skärmdumparna till sina lokala enheter. När de sparar dessa skärmdumpar, skyddar deras lokala enhets kryptering eller operativsystemsspecifik sandbox-skydd* mot dataintrång.

3 Hur SMART kapp säkrar inbjudningar för delningssessioner

När du inleder en delningssession från SMART kapp-appen så kan du skicka session URL till andra deltagare via e-post eller en tredje parts tjänst. När andra tar emot inbjudan för att granska din session, får de klicka på URL:en för att se din tavla och skärmdumpar direkt i deras webbläsare. SMART kapp säkrar denna URL med krypterade kommunikationsprotokoll (HTTPS).När du skickar en inbjudan till en session via e-post eller tredje parts tjänst, tillför din e-postleverantörs eller tredje parts tjänsts dataskydd ytterligare ett lager skydd för din information.

Säkra data under delningssessioner

Under delningssessioner överförs dina data från tavlan till din mobila enhet via bluetooth, och sedan från den mobila enheten till kappboard.com:s molnserver, och slutligen till varje deltagares webbläsare.



Hur SMART kapp säkrar data under delningssessioner

För att öka säkerheten för dina känsliga uppgifter vid alla skeden i överföringen från din mobila enhet till en deltagares webbläsare så skyddar SMART kapp dina data på följande sätt:

1 **På vägen till molnservern**	SMART kapp använder endast krypterade kommunikationsprotokoll (HTTPS) för att överföra information till kappboard.coms molnserver.

*(Sandbox-skydd är säkerhetsmekanism som skyddar mot potentiellt farliga program som kan innehåll ett virus eller skadlig kod genom att begränsa programmets tillgång till en lokal enhets resurser (t.ex. en enhets deskriptorer eller minne).

2	**I molnservern**	SMART kapps molnserver understöds av Amazon Web Services (AWS) och använder den branschstandard säkerhet som erbjuds av AWS för att skydda dina data i molnet. Din sessionsdata är endast tillgänglig i molnet under sessionens gång. När du avslutat en delningssession kan endast deltagarna i sessionen hämta en kopia på sessionen från webbläsarfönstret som användes för att delta i sessionen. När du avslutat en session och alla deltagare stängt sina webbläsare, är dina data ej längre åtkomliga via molnservern.
3	**På vägen till deltagares webbläsare**	URL:en som deltagarna använde för att gå med i din session skyddas med HTTPS. Denna URL innehåller en unika alfanumerisk beteckning som skapas för varje session. Om du har en prenumeration på premium-appen, kan du välja om du vill att denna URL ska vara statisk (dvs. samma URL för alla dina sessioner) eller dynamisk (varje nya URL blir unik och slumpvis). Prenumeranter på premium kan även skydda sessioner med PIN-kod. **OBS!** För vidare information om skillnaderna mellan den vanliga appen och premiumversionen, besök smartkapp.com/app.

Vanliga frågor om säkerhet

Vad händer om jag förlorar min mobila enhet med sparade skärmdumpar eller PDF-filer?

Säkerheten som tillhandahålls av dina mobila enhets operativsystem skyddar data som finns sparade i din mobila enhets interna bibliotek. Android använder kryptering och iOS-enhet använder sandbox-skydd. Alla data som du sparar till din mobila enhet skyddas av säkerhetsmetoden som din enhet automatiskt tillhandahåller eller säkerhetsfunktionerna som du konfigurerar på din enhet (t.ex. PIN). Om enheter förloras, följer du ditt företags rutiner för datasäkerhet som gäller för förlorade enheter som innehåller känsliga uppgifter.

Kräver tavlan något antivirusprogram?

Nej, tavlan kan inte påverkas av virusar då den inte använder ett traditionellt operativsystem. Den enda mjukvaran på tavlan är SMART kapps firmware.

I vilka sammanhang skulle jag behöva använda tavlans USB-port? Är filer som sparas till en USB-enhet mer säkra?

Om du inte vill ansluta en mobil enhet till tavlan så kan du infoga en USB-enhet till tavlans USB-port och spara skärmdumparna från din session. Dessa skärmdumpar sparas till din USB-enhet som osäkrade PDF-filer. Vissa USB-enhet innehåller egna säkerhetsfunktioner (t.ex. kryptering eller lösenordsskydd) som kan skydda dina data om USB-enheten förloras. Du kan även

kryptera USB-enheten eller manuellt lägga till ett lösenord för varje fil.

Måste specifika portar vara öppna för att tavlan ska fungera?

Nej, SMART kapp använder endast den parade mobila enhetens nätverk för att kommunicera och kräver inte ett traditionellt nätverk.

Lagrar SMART kapp någon personlig information, såsom användarnamn, IP-adress eller telefonnummer?

Nej, SMART kapp lagrar inte någon personligt identifierbar information.

Tillhandahåller SMART kapp några rapporter eller kontroller på tavlans användning?

SMART kapp erbjuder för närvarande inte offentliga rapporteringsfunktioner.

© 2016 SMART Technologies ULC. Alla rättigheter förbehålls. SMART kapp, smarttech, SMART-logotypen och alla SMART-slogans är varumärken eller registrerade varumärken tillhörande SMART Technologies ULC i USA och/eller i andra länder. Alla tredjepartsprodukter och företagsnamn kan vara varumärken som tillhör dess respektive ägare. Innehållet kan ändras utan förvarning. 12-2016.