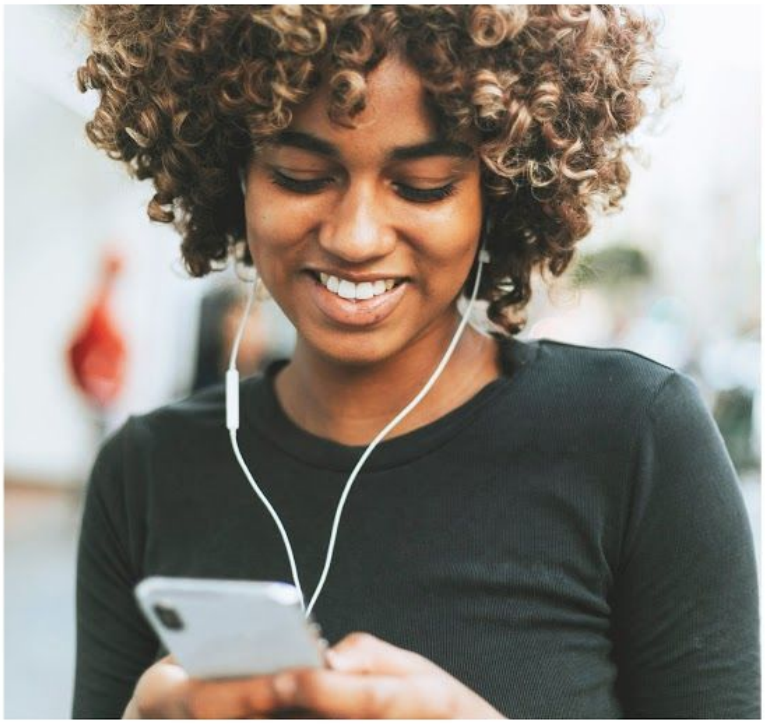
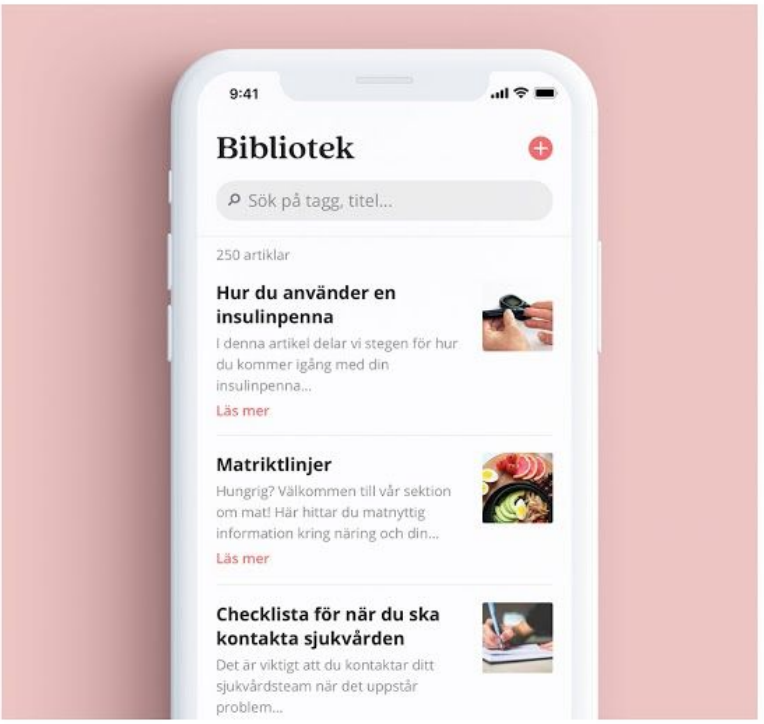
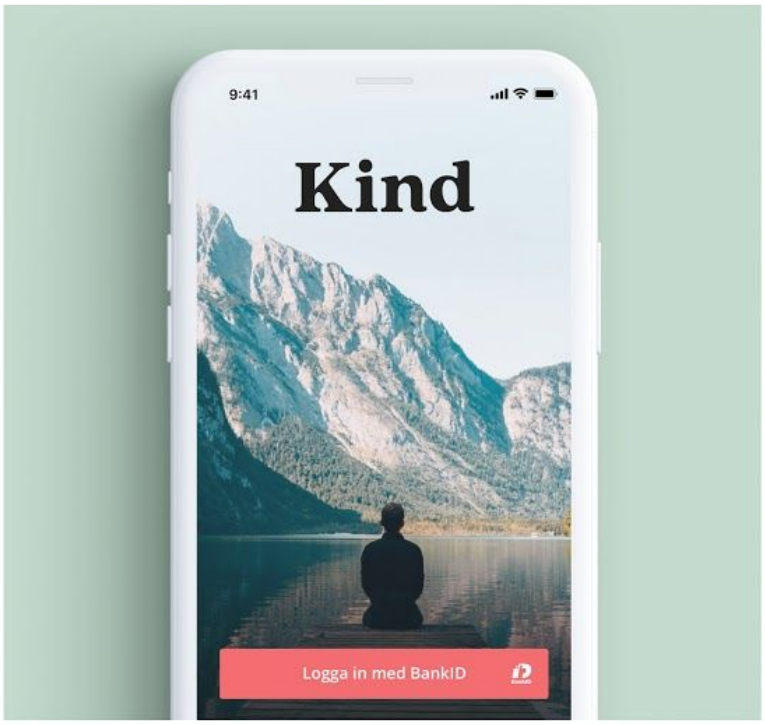
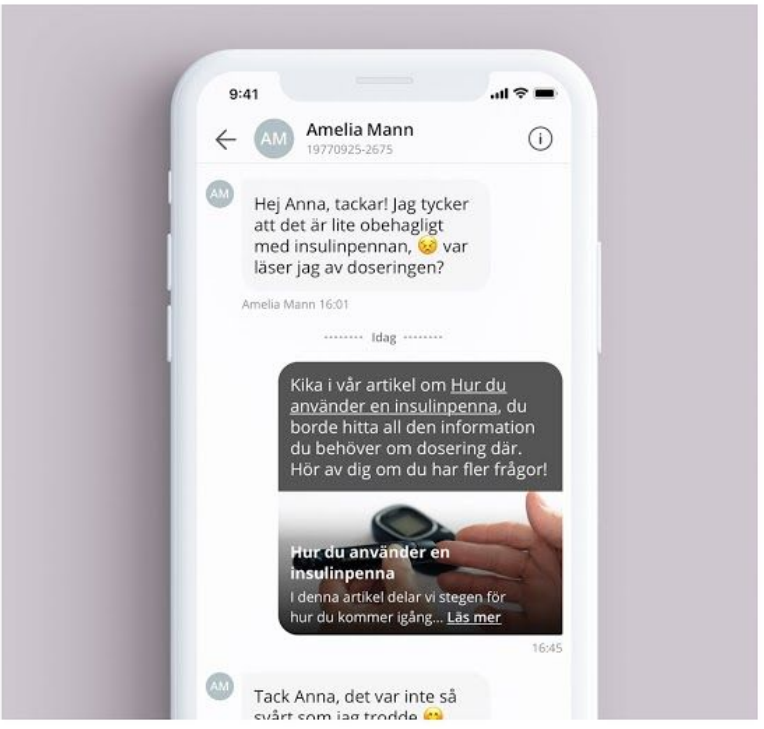





Säkerhetsåtgärder



# Kind

Kind är tillgänglig för både vårdpersonal och patienter runt om i världen. Säkerhet är högsta prioritet för oss eftersom vi anser dina personuppgifter vara högst konfidentiella.
I det här dokumentet sammanfattas alla våra säkerhetsåtgärder som säkerställer en hög säkerhetsnivå för våra applikationer.

## Kryptering

Kind använder kryptering både ”In transit” och “At rest”. Det betyder att dina data krypteras från din enhet (telefon, webbläsare) till vår infrastruktur, och att våra skivor också är krypterade.

### In transit

För att kryptera “In transit”-trafik använder vi HTTPS med en kombination av Secure Sockets
Layer (SSL) / Transport Layer Security (TLS).
Data som skickas från en klient, antingen webbaserad eller mobil, skickas över en säker
HTTPS-anslutning säkras av ett 2048-bitars SSL-certifikat.

### At rest

När någon information har skickats från kunden till vår infrastruktur lagras data (personuppgifter, meddelanden, bilagor) säkert i AWS med hjälp av krypteringsstandarder.
Den data som lagras på volymerna, disken I / O och ögonblicksbilder skapade från volymerna är alla krypterade. Krypteringsnycklarna EBS (Elastic Block Storage) och S3 (Simple Storage Service) använder

AES-256-algoritmen och hanteras och skyddas helt av AWS-nyckelhanteringsinfrastrukturen genom AWS Key Management Service (AWS KMS).

## Access

Vi använder principen om “less privileges” över hela Kind organisation. Det innebär att vi ger varje anställd den minsta tillgång som krävs för att utföra sina uppgifter. I AWS innebär detta att man har “fined-grained” behörighetsnivåer med hjälp av AWS IAM (Identity and Access Management). Varje ny användare måste konfigurera MFA (Multi Factor Authentication) mekanism innan man kan utföra några åtgärder på plattformen. Detta lägger till en annan säkerhetsnivå: även med användarnamnet och lösenordet kommer en hacker inte att kunna komma åt vår infrastruktur.

En bastion har också blivit utplacerad för att isolera vår plattform från internet. Det betyder att ingen databas eller fil kan hämtas från internet utan att ha tillgång till bastionen. Vår bastion är säkrad av både en krypterad 2048 bit RSA keypair och en IP-begränsning. På så sätt kan någon utanför vår organisation inte nå vår infrastruktur, även om den personen får giltiga uppgifter.

Varje tillgång till vår infrastruktur loggas med både CloudTrail och VPC FlowLogs. CloudTrail tillhandahåller API-aktivitetsdata, inklusive API-sändarens identitet, tiden för ett API-samtal, källan till API-sändarens IP-adress, “request parameters” och “response elements” som returneras av AWS-tjänsten. Vid eventuell misstänkt

aktivitet uppkommer ett larm och skickas till våra administratörer för granskning.

## Data separation

För att skydda dina personuppgifter, separerade vi dem helt från andra applikationsdata (till exempel meddelanden och bilagor). Vi använder generiska ids för att korrelera data mellan våra olika tjänster, inte användarnamn eller e-postadresser. I händelse av att en av våra databaser utsätts skulle det inte vara möjligt att korrelera den läckta informationen med en viss individ.

## Backup / High availability

Vi säkerhetskopierar vår app dagligen i händelse av fel. Dessa säkerhetskopior är krypterade med AES-256-algoritmen och hanteras och skyddas helt av AWS-nyckelhanteringsinfrastrukturen, genom AWS Key Management Service (AWS KMS).

Vår infrastruktur är också “highly available” eftersom den sträcker sig över flera AWS-tillgänglighetszoner. Tillgänglighetszoner består av ett eller flera diskreta datacentraler, vardera med redundant strömförsörjning, nätverk och anslutning, inrymda i separata lokaler. I händelse av ett avbrott i en tillgänglighetszon omdirigeras all trafik till de återstående tillgänglighetszoner. Således kommer påverkan på kunden att vara minimal.