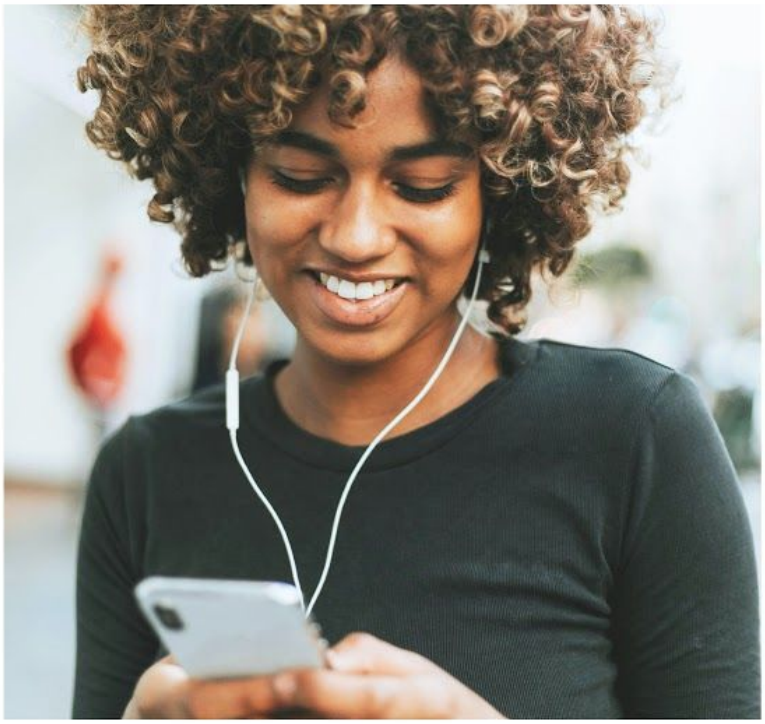
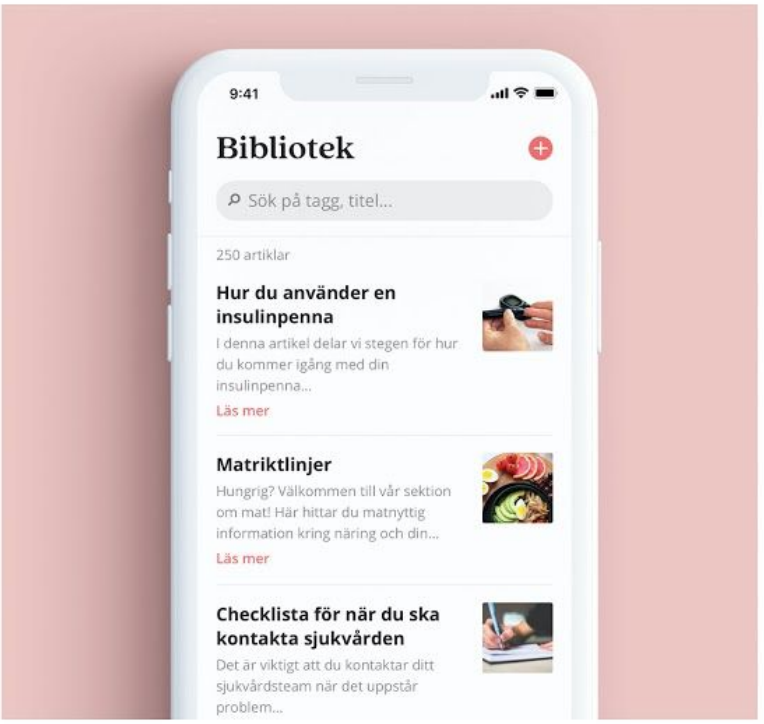
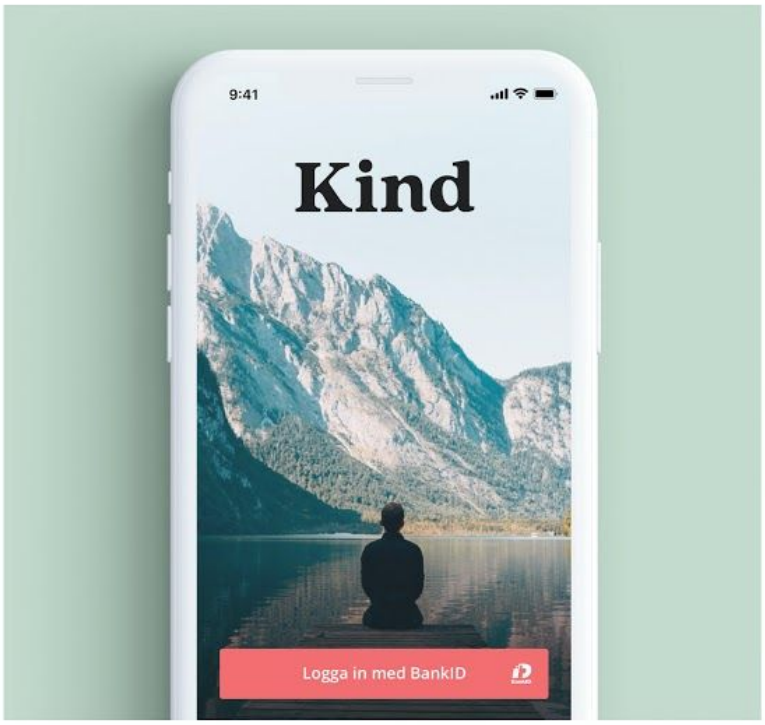
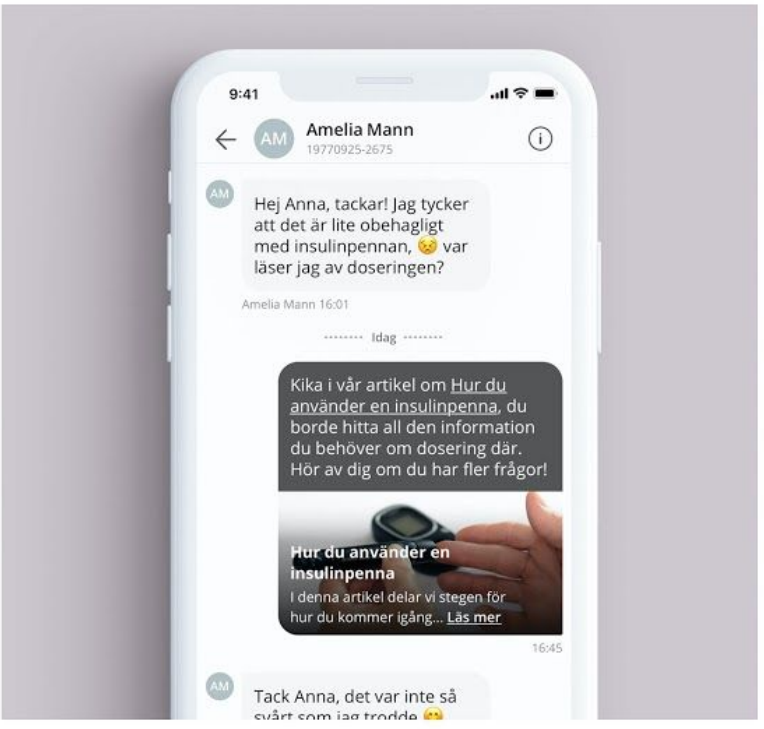






Whitepaper over onze beveiliging



Kind

Kind is beschikbaar voor zowel zorgverleners als patiënten over de hele wereld. Beveiliging is een eindeloze zorg voor ons omdat we uw persoonlijke gegevens als strikt vertrouwelijk beschouwen.
Dit document bevat al onze beveiligingsmaatregelen om een hoog beveiligingsniveau voor al onze applicaties te garanderen.

Versleuteling

Kind gebruikt beide versleutelingen tijdens het transport en in rust. Het betekent dat uw gegevens worden gecodeerd van uw apparaat (telefoon, browser) naar onze infrastructuur en dat onze schijven ook worden gecodeerd.

In transit

Om in-transit verkeer te coderen, gebruiken we HTTPS met een combinatie van Secure Sockets
Laag (SSL) / Transportlaagbeveiliging (TLS).
Gegevens die vanaf een client worden verzonden, ongeacht of dit via het web of een mobiele applicatie is, worden via een beveiligde manier verzonden
HTTPS-verbinding beveiligd door een 2048-bit SSL-certificaat.

In rust

Nadat alle informatie van de klant naar onze infrastructuur is verzonden, worden de gegevens (persoonlijke informatie, berichten, bijlagen) veilig opgeslagen in AWS met behulp van coderingsstandaarden.

De gegevens die zijn opgeslagen op de volumes, de schijf-I / O en de snapshots die van de volumes zijn gemaakt, zijn allemaal gecodeerd. De EBS (Elastic Block Storage) en S3 (Simple Storage Service) coderingssleutels gebruiken AES-256-algoritme en worden volledig beheerd en beschermd door de AWS key management-infrastructuur, via AWS Key Management Service (AWS KMS).

Toegang

We gebruiken het principe van minder rechten in de hele Kind-organisatie. Het betekent dat we elke medewerker zo min mogelijk toegang geven om zijn taken uit te voeren. In AWS vertaalt dit zich in het hebben van fijnmazige machtigingsniveaus met behulp van AWS IAM (Identity and Access Management). Elke nieuwe gebruiker moet een MFA-mechanisme (Multi Factor Authentication) instellen voordat hij actie op het platform kan uitvoeren. Dit voegt nog een beveiligingsniveau toe: zelfs met de gebruikersnaam en het wachtwoord heeft een hacker geen toegang tot onze infrastructuur.

Er is ook een bastion ingezet om ons platform te isoleren van internet. Het betekent dat geen database of bestand van internet kan worden opgehaald zonder toegang tot het bastion. Ons bastion wordt beveiligd door zowel een gecodeerde 2048 bit RSA keypair als een IP-beperking. Op deze manier kan iemand buiten onze organisatie onze infrastructuur niet bereiken, zelfs niet als die persoon geldige inloggegevens krijgt.

Elke toegang tot onze infrastructuur wordt vastgelegd met behulp van zowel CloudTrail als VPC FlowLogs. CloudTrail biedt API-activiteitsgegevens, waaronder de identiteit van de API-beller, het tijdstip van een API-aanroep, de bron van het IP-adres van de API-beller, de aanvraagparameters en de reactie-elementen die door de AWS-service worden geretourneerd. In geval van verdachte activiteiten wordt een alarmsignaal gegeven en ter beoordeling naar onze beheerders gestuurd.

Data separation

In order to keep your personal data secure, we separated it completely from any application data (such as messages and attachments). We use generic ids to correlate data between our different services, not usernames nor email addresses. In the eventuality of one of our databases being compromised, there would be no way to correlate the leaked information with a specific individual.

Backup / Hoge beschikbaarheid

We maken dagelijks een back-up van onze applicatie in geval van een storing. Die back-ups worden gecodeerd met behulp van het AES-256-algoritme en worden volledig beheerd en beschermd door de AWS-sleutelbeheerinfrastructuur, via AWS Key Management Service (AWS KMS).

Kind

Onze infrastructuur is ook in hoge mate beschikbaar omdat deze zich uitstrekt over meerdere AWS-beschikbaarheidszones. Beschikbaarheidszones bestaan uit een of meer discrete datacenters, elk met redundante stroomvoorziening, netwerken en connectiviteit, ondergebracht in afzonderlijke faciliteiten. In het geval van een uitval van een beschikbaarheidszone, wordt al het verkeer omgeleid naar de resterende beschikbaarheidszones. De impact op de klant zal dus minimaal zijn.