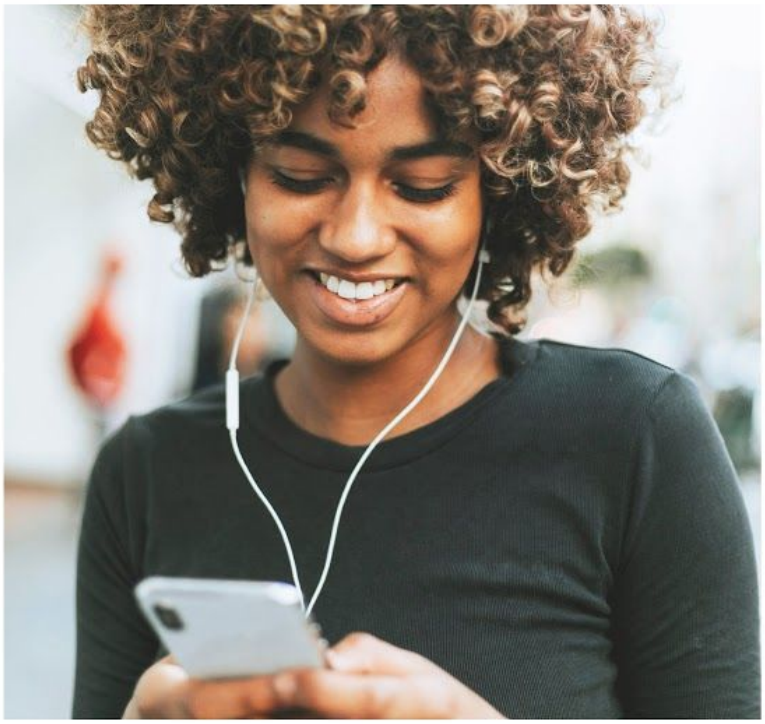
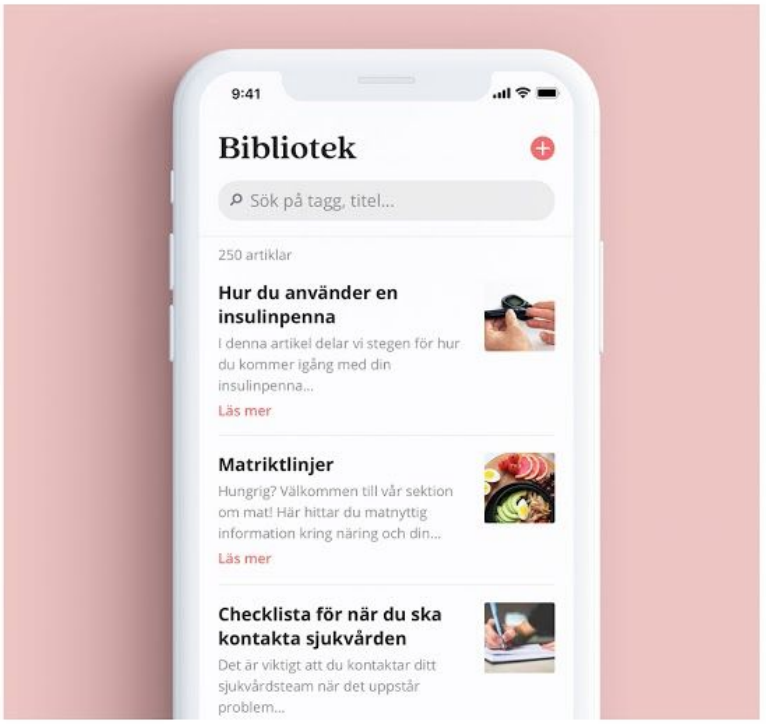
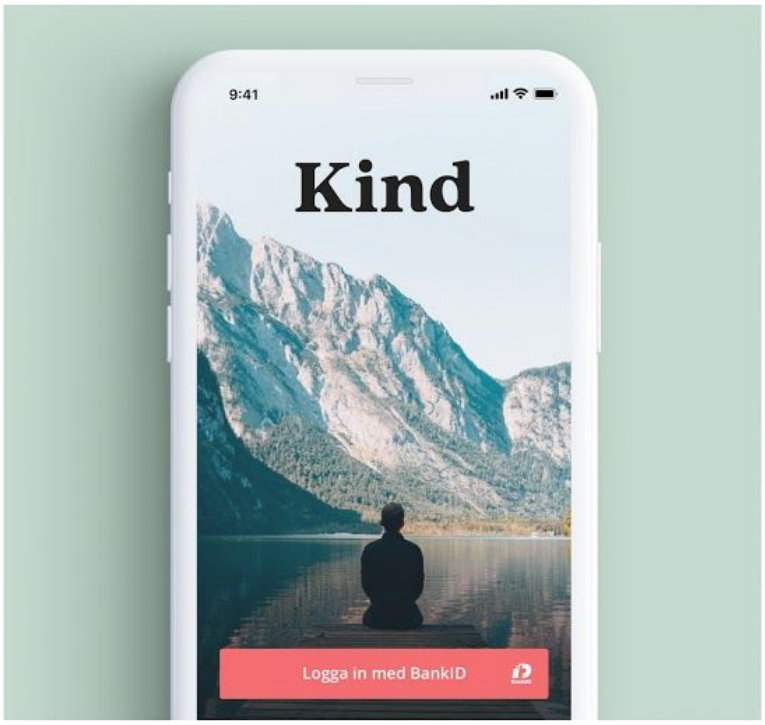
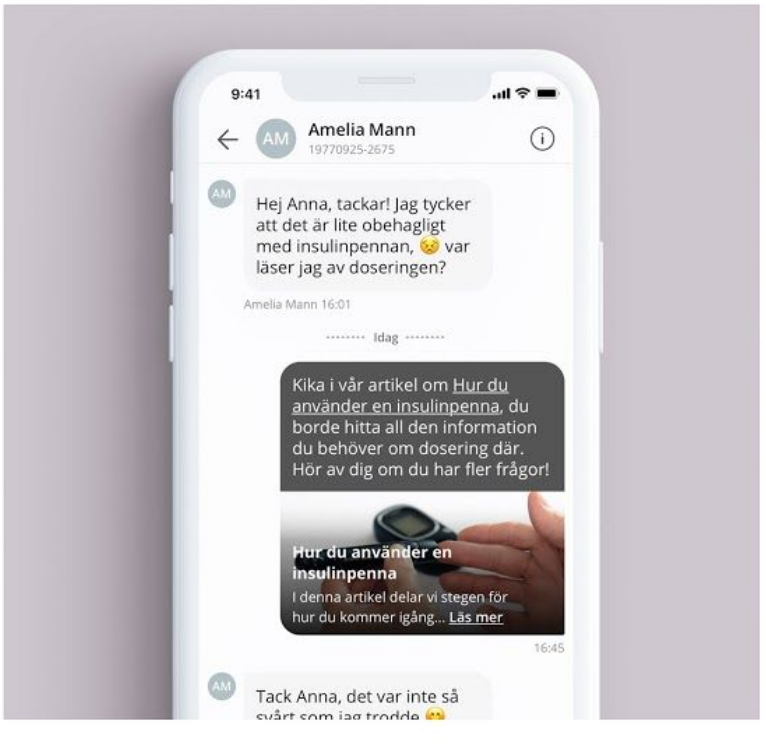






Security whitepaper



Kind

Kind is available for both healthcare professionals and patients around the world. Security is a never-ending concern for us as we consider your personal data as strictly confidential.
This document resumes all our security measures to insure a high level of security across our applications.

Encryption

Kind uses both encryption in transit and at rest. It means that your data is encrypted from your device (phone, browser) to our infrastructure, and that our disks are also encrypted.

In transit

In order to encrypt in-transit traffic, we use HTTPS with a combination of Secure Sockets
Layer (SSL)/Transport Layer Security (TLS).
Data being sent from a client, whether web-based or a mobile application, is sent over a secure
HTTPS connection secured by a 2048-bit SSL certificate.

At rest

Once any information has been sent from the client to our infrastructure, the data (personal information, messages, attachments) is securely stored in AWS using encryption standards. The data stored on the volumes, the disk I/O and the snapshots created from the volumes are all encrypted. The EBS (Elastic Block Storage) and S3 (Simple Storage Service) encryption keys use AES-256

algorithm and are entirely managed and protected by the AWS key management infrastructure, through AWS Key Management Service (AWS KMS).

Access

We use the principle of less privileges across the whole Kind organization. It means that we give every employee the minimal amount of access required to perform its tasks. In AWS, this translates into having fined-grained levels of permissions using AWS IAM (Identity and Access Management). Every new user has to set up MFA (Multi Factor Authentication) mechanism before being able to perform any action on the platform. This adds another level of security : even with the username and password, a hacker won't be able to access our infrastructure.

A bastion has also been deployed in order to isolate our platform from the internet. It means that no database or file can be retrieved from the internet without having an access to the bastion. Our bastion is secured by both an encrypted 2048 bit RSA keypair and an IP restriction. This way, someone outside our organization will not be able to reach our infrastructure, even if that person gets valid credentials.

Every access to our infrastructure is logged using both CloudTrail and VPC FlowLogs. CloudTrail provides API activity data including the identity of the API caller, the time of an API call, the source of the IP address of the API caller, the request parameters and the response

elements returned by the AWS service. In case of any suspicious activity, an alarm is raised and sent to our administrators for reviewing.

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 / High availability

We backup our application on a daily basis in case of any failure. Those backups are encrypted using AES-256 algorithm and are entirely managed and protected by the AWS key management infrastructure, through AWS Key Management Service (AWS KMS).

Our infrastructure is also highly available since it spans across multiple AWS Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities. In case of an outage of an availability zone, all the traffic will be redirected to the remaining availability zones. Thus the impact on the customer will be minimal.