SURETEK INFOSOFT ***CASE STUDY***

DATA SECURITY- END-TO-END ENCYPRTION

CLIENT PROFILE

Our client is a global equity financial company based in Sweden. Information related to the current stocks on the loose is provided to its customers to help get the better of most of the deals.

BUSINESS CHALLENGE

A growing share of people now use smartphones as their primary means of online access at home. Hence the client decided to catch on to the times of smartphone and launch a business app (Android/iOS) based on the already existing website. Since the dilemma of the sensitivity of the data on both the mobile app and the website they felt suspicious of the hackers and required a comprehensive solution to manage and secure the data transactions by servers to the mobile app.

The client was looking to provide the consumers with absolute data (statistics) that can be highly relied upon.

SURETEK SOLUTION

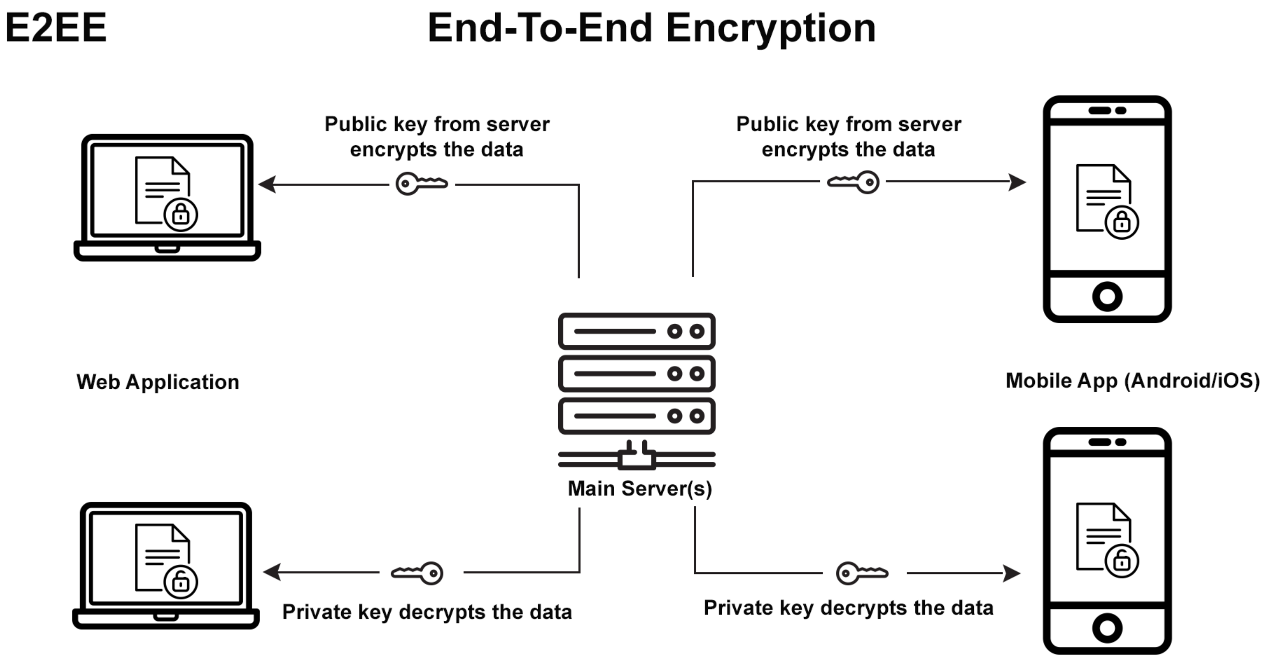
Suretek alongside its client calculated the business requirements and developed a technical solution to realize the business vision. Suretek proposed the use of End-to-End encryption over the network to secure the data revolving around investment in stocks per se.

Tailored to the client’s specific needs we built encryption into their proposed platforms with cost saving methodologies. The solution included intrusion detection along with the fact that end-to-end encryption was implemented to the client’s solution.

SURETEK’S CONTRIBUTION AND WORK PROFILE:

- Employed an algorithm that encrypts data with a key(s) that is associated with the end user.
- The algorithm deployed serves the encryption of transactions from one the server-end to multiple consumers.
- The number of crypto key(s) generated are well coordinated by instrumenting an automated key management system (KMS).
- Encryption only protects information from unauthorized access. But when an authorized user abuses the data, encryption cannot solve this. Hence provided the client with a Data Security Audit to understand how sensitive information moves into and out of the client’s business and who has access to it is essential to assessing security risks.
- Interceptor at the DB layer is implemented to encrypt the values of important data of the application.

- Employed IDS (Intrusion Detection System) to monitor the network for malicious activities and report it to the system admin or at the same time they are also stored at the event management system (EMS).
- An ability to use Data at rest using full disc encryption.
- QSA Report on Compliance on-site audits.
- To top it all off, end-to-end encryption on the business equity app is attained with the best of efforts.


E2EE
End-To-End Encryption
Public key from server encrypts the data
Public key from server encrypts the data
Web Application
Mobile App (Android/iOS)
Main Server(s)
Private key decrypts the data
Private key decrypts the data

TECHNOLOGIES USED

Signal Protocol, CryptoSwitch, Py(NaCL)