Polygant

Secure corporate messenger

About client

A Russian company with offices in Moscow and London, specializing in blockchain project development and deployment. Polygant experts have been creating cryptocurrencies, tokens and smart contracts, offering consultation to customers and helping them to hold ICOs (initial coin offerings for investors) for over two years.

Duration
12 months

Industry
Information security

Team
Project manager — 1
QA engineer — 2
Analyst— 1
Back-end developer— 1
Front-end developer— 1
Mobile developer— 1

Technologies
🤖 Android
🟨 JavaScript
⚛️ React
⬡ Node.JS

Challenge

The customer's clients are large companies, which prioritise corporate security and the protection of confidential data. They could use popular commercial solutions like WhatsApp or Telegram for message and file exchange, but that would not guarantee the safety of their data. All the information would then be stored on remote servers, accessible to third parties or security services. The customers needed to guarantee that the messenger would have no "backdoors" and would not be compromised, and nobody would be able to intercept the data in transfer. A decision was made to develop a customised application based on the security requirements. The customer came to us with this request.

Solution

The requirement was to remove the slightest risk of messages being intercepted, application compromised, devices impersonated or someone's account accessed without authorisation. Apart from end-to-end 256 bit encryption to ensure maximum security for user communications, the developers applied few creative solutions:

- Remote servers are completely removed from the data transmission sequence.
- Encrypted information is only stored on users' devices.
- Messages can be automatically deleted after some time.
- The messenger only functions within the internal company network.

Seven developers had been working at the Android mobile client and the web interface desktop version for 12 months.

Result

Our corporate messenger complies with all the security standards of today. Two-factor authentication is used to authorise access to accounts, with the application associated with a phone number. With remote servers removed from the data transmission sequence, third parties cannot access corporate data. The application is now actively used by large companies with over 15,000 employees. Customers can use it to make major deals and collaborate on important projects without any worries about data security.