BabelApp

Your Secure Enterprise Communication

www.babelapp.com

I. About BabelApp

BabelApp is a **secure multi-device communication platform** designed for mobile and desktop use in the corporate world and on the internet.

- **Sends and stores encrypted messages and documents**
- **Provides encrypted phone calls**
- **Secures communication with your colleagues, clients and partners**
- **Protects trade secrets, personal data and other confidential information**

BabelApp is a secure alternative to e-mail and instant messaging.
BabelApp is not operated as a shared central service, nor does it download (receive) any information about user contacts from their devices. BabelAppt puts full control and security directly in the hands of users and administrators. Each business runs and manages its own server, controls its communication with other servers and protects the identity of BabelApp users.

II. Key Features

1. Overall security

- **Encrypted phone calls**
  Encrypted phone calls between mobile devices within the network using VoIP. It includes notification of connection and public keys, codecs and protocols exchange for direct communication between devices, while ensuring full confidentiality and integrity.
- **Secure recordings**
  Photos, videos, and sound recordings are stored directly in the app and are not accessible anywhere else. The camera and microphone features are controlled directly by the application code, not by the device.
- **Secure storage**
  All messages, recordings, and documents are stored and encrypted in the application on both the sender´s and the recipient´s devices.
- **Encrypted communication**
  Using strong cryptography BabelApp instantly provides cross-platform encrypted communication between computers with Windows or macOS and mobile devices with iOS and Android – independent of location and connection type.
- **Delivery to recipient's device**
  BabelApp delivers messages and documents to the users, and does not store them for a long time on the server (depending on time specified by the user). The server only provides services for sending and delivering messages, sending delivery alerts, and deleting documents in the case of undelivered messages. It does not – under any circumstances – have any keys that would allow administrators to intercept or read encrypted communication.
- **Totally secured**
  Common types of documents (photos, PDF, MS Office doc, etc.) are directly opened in the application using the application code. Documents are stored in a safe environment of BabelApp and are secured against third-party threats.

2. On-premise BabelApp server installation

On-premise

The server operates in your own network and under your own administration. You have full control over the service and security of your communication.

Server replication

High availability solution – in the event of a server disaster, BabelApp is ready to restore the data to its pre-disaster state within only a few minutes.

3. BabelApp is protected by copyright laws

BabelApp is constantly being driven by the needs of our customers:

BabelApp is flexible – we offer the option of tailoring to customer´s requests, such as adding or changing functions, on-site product support, easier integration compared to global applications, and customizable client´s appearance, such as company logo or corporate colours by using our flexible licensing policy.

4. Easy integration

BabelApp supports easy integration with third party applications such as document management system, customer or mobile device management systems (printers, MS OUtlook, etc.). Moreover, BabelApp ensures automated and secure transfer of data, information, documents and files between business applications and users. With BabelApp, you can also set automatic or assisted synchronization with Active Directory/LDAP directory to simplify user account management.

Method of encryption and defense against attacks:

Every message is encrypted using a standard AES symmetric-key algorithm with a unique Message Key that is randomly generated by the BabelApp application on the sender's device. The recipient has to obtain the Message key to decrypt the message, therefore the Message Key has to be kept encrypted while not used – that is done by using another encryption key – the Contact Key which the sender shares with the recipient. Contact keys are attached to the messages. Contact Keys are not saved anywhere; they are calculated during the transmission using a standard Diffie-Hellman algorithm. For this calculation to happen, each party needs to possess a verified value of the other party's public key. Public keys are securely distributed to all registered mobile devices via BabelApp Messaging Server.
Secure communication is based not only on the encryption of transmitted messages, but also on their authentication and integrity checks so that the recipient can be assured that the data of the legitimate sender was not altered by the attacker. For this purpose, the message is first encrypted and then the resulting ciphertext is "signed" using an HMAC algorithm (Encrypt-then-Authenticate).

III. Cornerstones of BabelApp

BabelApp is aimed at protecting all forms of communication.

Cryptography

From a security point of view BabelApp is completely encrypted and safe.
The cryptographic design of BabelApp was created in cooperation with the leading Czech cryptologist RNDr. Vlastimil Klima.

BabelApp uses combinations of the best cryptography algorithms and protocols to protect your information against both passive and active attacks:

- End-to-end encryption using the symethric AES algorithm for securing instant messaging
- Secure distribution of the public keys from the company server; no need to pay any digital certificates
- Other algorithms used: PBKDF2, SHA-2, Diffie-Hellman, RSA, HMAC-SHA256

Blockchain

Our application uses a unique mechanism for key authentication, which works with modern secure storage, where it is excluded that anyone would be able to modify once entered data in any aspect. This storage is called Blockchain database.

Public Blockchain DB are currently used exclusively for cryptocurrency. The largest and the safest one is used by Bitcoin. Except of using this DB for recording of particular Bitcoin transactions, it is also possible to record other data.

In our case, endpoint device with BabelApp application records to this database information needed for public key verification, which can be read anytime by other participants in this communication. If BabelApp server has active Bitcoin network, protection, anyone can communicate with you without having fear of being attacked by MITM, with no necessity of calling and verifying public keys before commencement of the communication.

Server

BabelApp server is the foundation of the platform. This server maintains a database of registered user accounts, their devices and associated public keys. The server is equipped with SSL certificates and provides the end users with client application licenses.

The server does not store any private or secret keys and cannot decrypt any messages. It mediates data communication among BabelApp users and allows notifications but is not involved in the encryption process. If the sender or recipient is not online, the server provides notifications and asynchronous delivery of encrypted messages.

All devices must be registered with the server using a One Time Password (OTP) that users typically receive along with initial instructions from their administrators. During the registration process, the server obtains and verifies the user's public key and synchronizes it.

Unlimited communication is provided by servers that communicate securely with clients and with each other via internet. Administrators have the ability to allow or deny multi-server communication.

Server Communication Services:

- Centralized contacts
- Distribution and synchronization of users' public keys
- Communication among multiple BabelApp servers for public key synchronization and cross-server communication
- Asynchronous delivery of messages and attachments to recipients' devices
- Synchronization of sent messages in all the sender's devices
- Temporary storage of encrypted attachments – until downloaded by the recipient
- Gateway for sending push notifications
- Delivery reports (sent, delivered, read)
- Communication gateway with REST API for easy integration with applications and programmable devices for encrypted message distribution and business processes automation

Administrative Server Function:

- Full control over the application infrastructure
- Web console for system administration
- Import of User information from LDAP/AD
- Synchronization of changes in user accounts from LDAP/AD
- Managing user accounts and groups for both internal and external users
- One-time generated password or LDAP authentication
- Minimum password length required to ensure security
- Ability to remove registered devices
- Key revocation
- Ability to block specific users
- Possibility to reset server accounts on remote servers
- Option to delete a remote server from the local server database
- System logging of server and user events
- Traffic & usage statistics
- The ability to send scheduled automatic messages informing users of new available updates, etc.

BabelApp Application

BabelApp can securely make phone calls, encrypt, decrypt, send and receive messages, and attach documents via their server and take photos, videos, voice recording directly in the application. Additionally, you can save messages and documents in encrypted form, with multi-party conversations, or search for contacts in the app and in the centralized contacts.

BabelApp is available for all major mobile and desktop platforms free of charge through App Store and Google Play or in the form of an installation package.

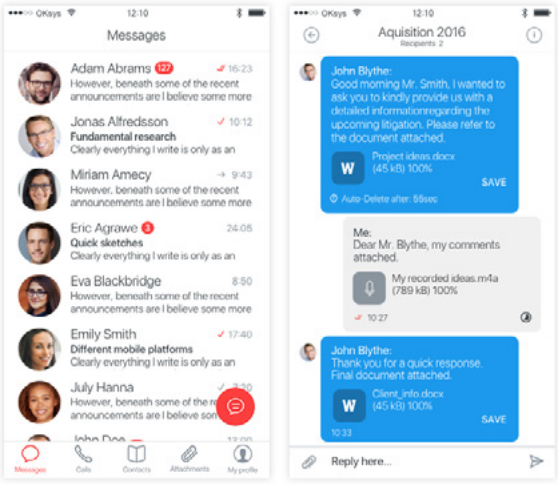
BabelApp on mobiles:

a) iOS b) Android c) BlackBerry

BabelApp on desktops:

a) Windows b) macOS (OS X)

You can have multiple devices with multiple operational systems connected to the same account. Each device can be connected to multiple servers.



iOS version

macOS version

BabelApp Features

The main features of BabelApp are available on all platforms.
Phone calls are available only on mobile phones.

Phone Calls:

- encrypted phone calls within the data network using VoIP technologies
- high-quality sound
- minimal data consumption (0.5 MB per minute)

Basic Communication Features:

- encrypted text messages using internet or data
- asynchronous communication (sender or recipient does not need to be on-line)
- encrypted attachments (photos, videos, voice messages, etc.)
- encrypted text messages via SMS (if there is no roaming, no data or no server)
- ability to connect devices to multiple servers
- communication with multiple recipients at the same time
- communication in group or individual chats
- forwarding messages to other recipients
- delivery reports (sent, delivered/undelivered, read)
- notifications of messages waiting to be delivered

Message Set up and Deletion:

- set up message expiration
- message auto-delete
- remote delete (from recipient´s device)
- deletion of whole conversations
- drafts

Documents and Attachments:

- preating basic attachments directly in the application - photo, video, audio recording
- securely store encrypted received and sent messages and documents directly in the application
- preview attachments without downloading them
- a list of all documents sent and received, sorted by different criteria

Contacts:

- ability to edit contacts
- business cards – the ability to view and send a virtual business card in order to add a contact to BabelApp
- my profile – editing your own information (name, photos, generation of authorization codes to pair with another device)
- displaying key codes for authentication with the counterparty in an alternative way

Other features:

- password protected application
- ability to use PIN code, Touch ID or Face ID to open the app
- customization (English, Czech, Russian)