SignArch

An architectural case study of Signal

Duan

Mathieu

Maximilian

Maksim

Dong

Signal: A messaging app known for security

Fast, simple, secure.

Privacy that fits in your pocket.

Android

iPhone

Desktop

Requirements

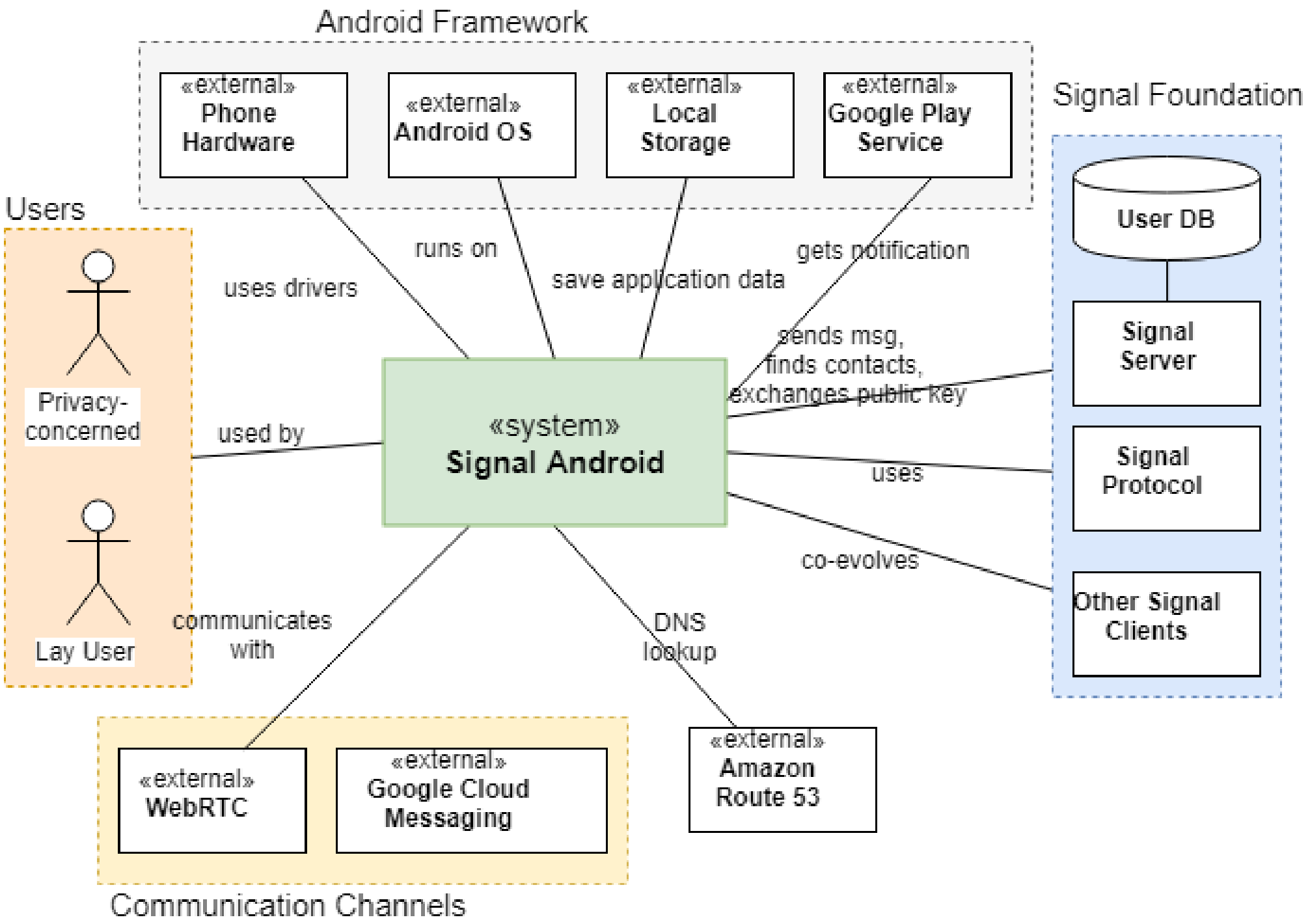
Functional Requirements:

- Text messaging
- Voice chat
- Video chat

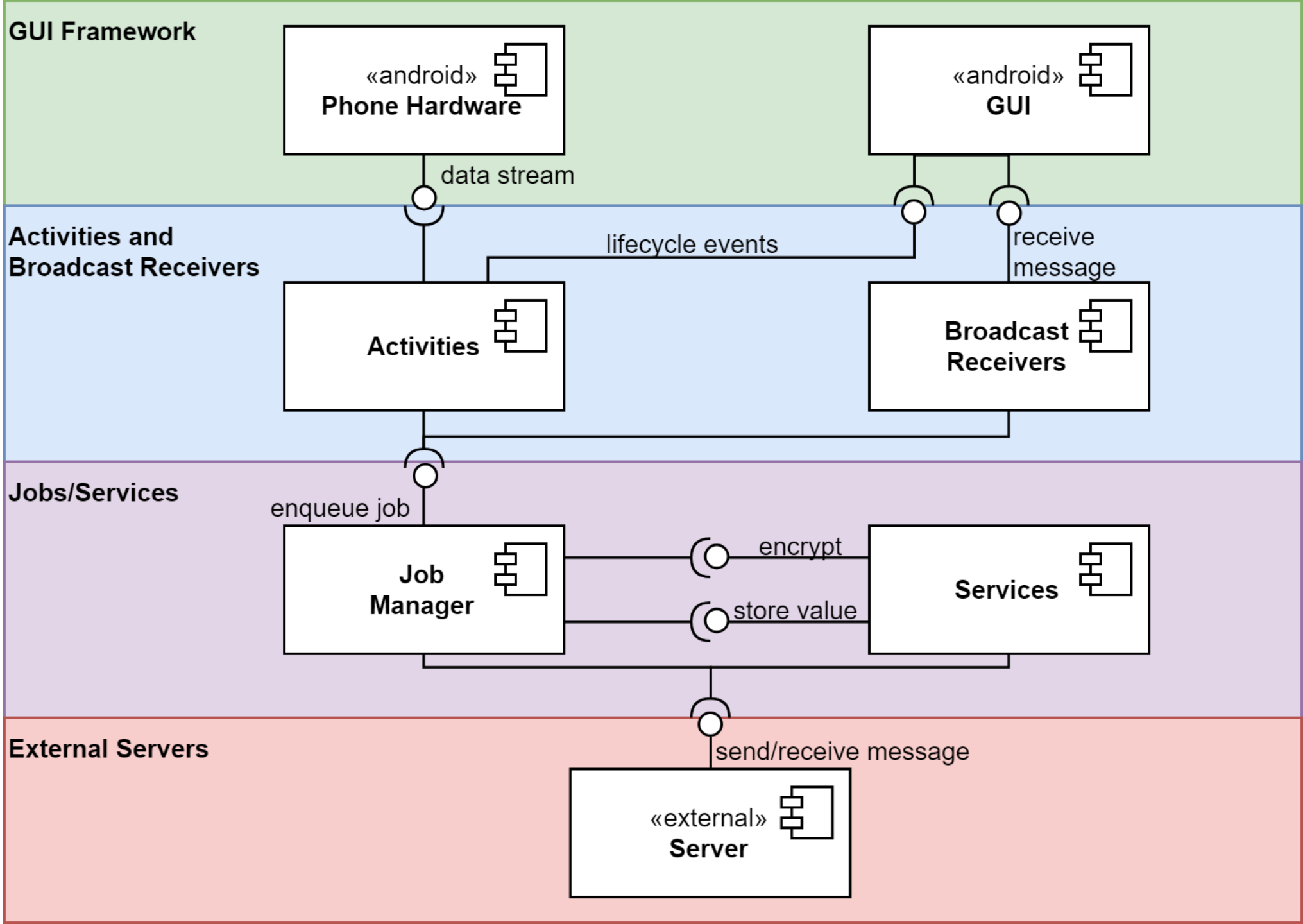
System qualities:

- Private, secure conversation
- High availability
- High-quality, low-latency voice/ video call

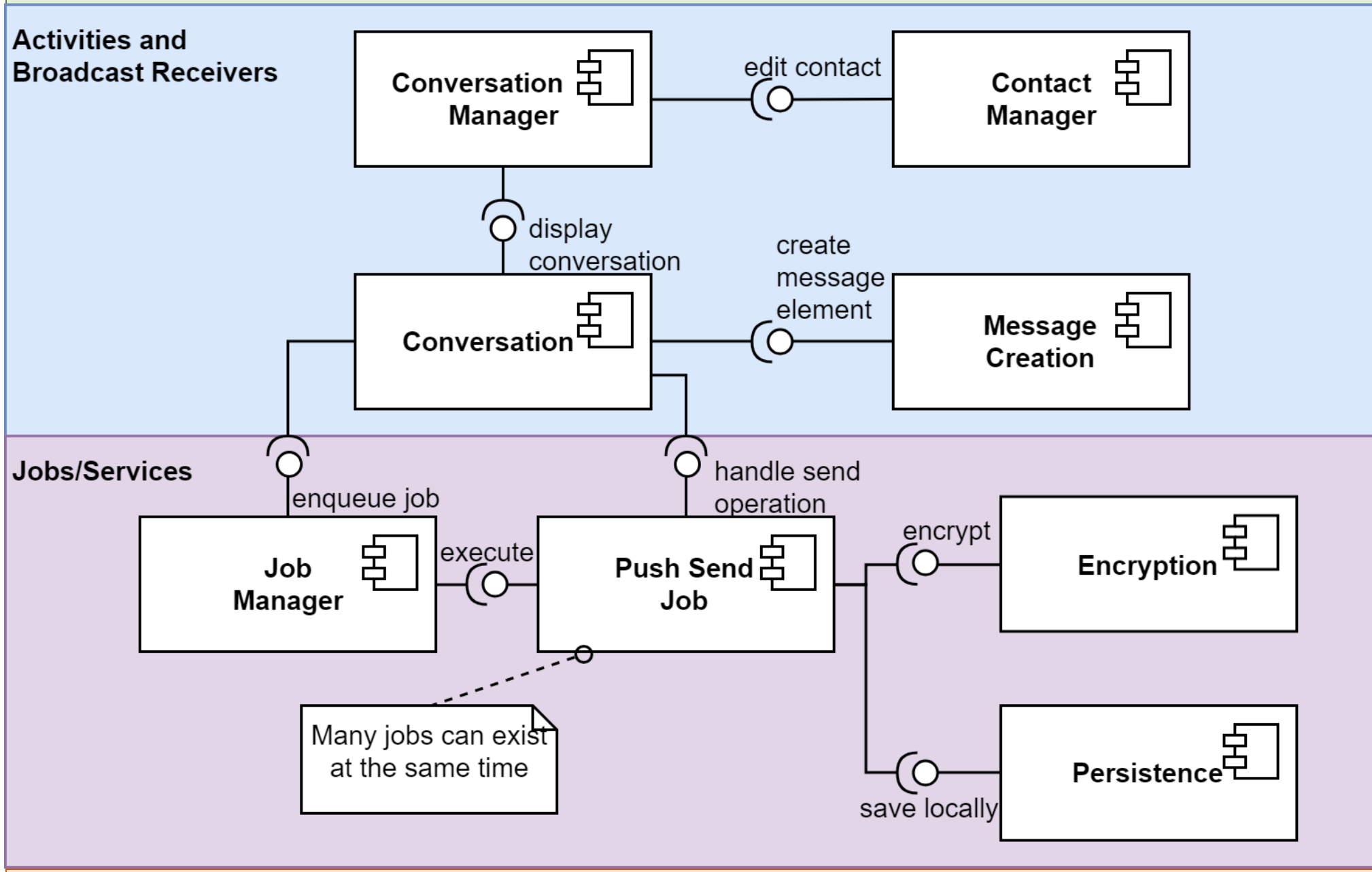
Context


Android Framework
«external»
Phone
Hardware
«external»
Android OS
«external»
Local
Storage
«external»
Google Play
Service
Signal Foundation
User DB
Signal
Server
Signal
Protocol
Other Signal
Clients
Users
Privacy-
concerned
Lay User
uses drivers
runs on
save application data
gets notification
sends msg,
finds contacts,
exchanges public key
used by
«system»
Signal Android
uses
co-evolves
communicates
with
DNS
lookup
«external»
WebRTC
«external»
Google Cloud
Messaging
«external»
Amazon
Route 53
Communication Channels

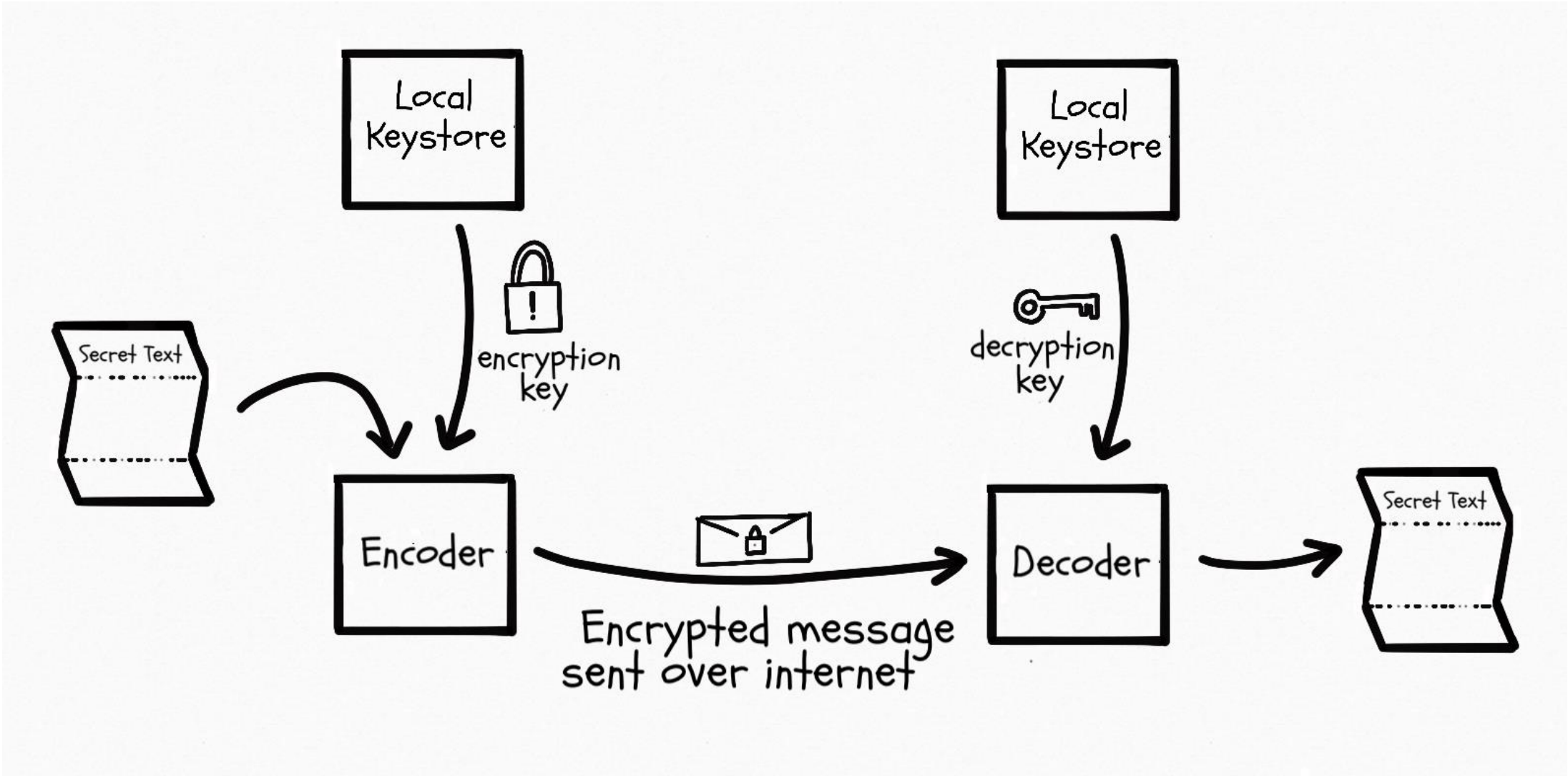
Functional Overview

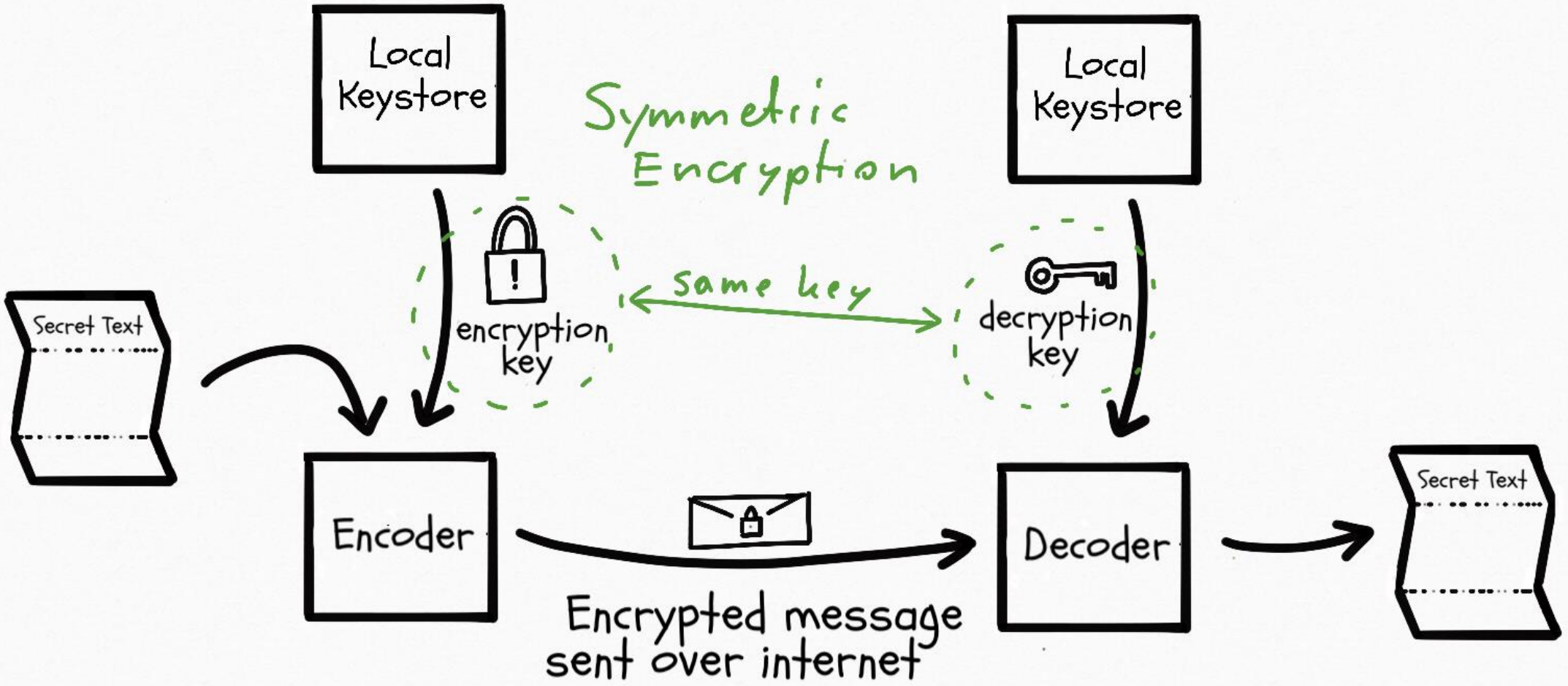


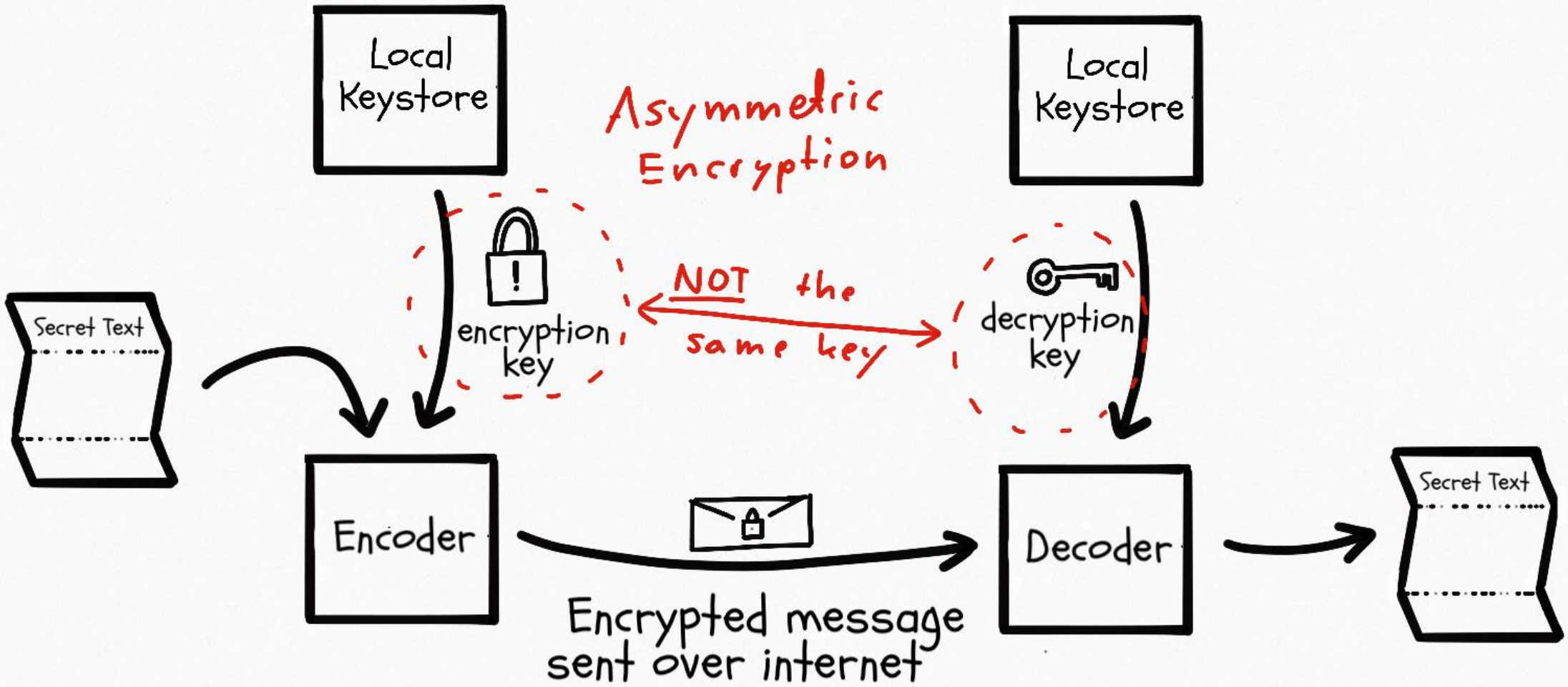
Functional Overview



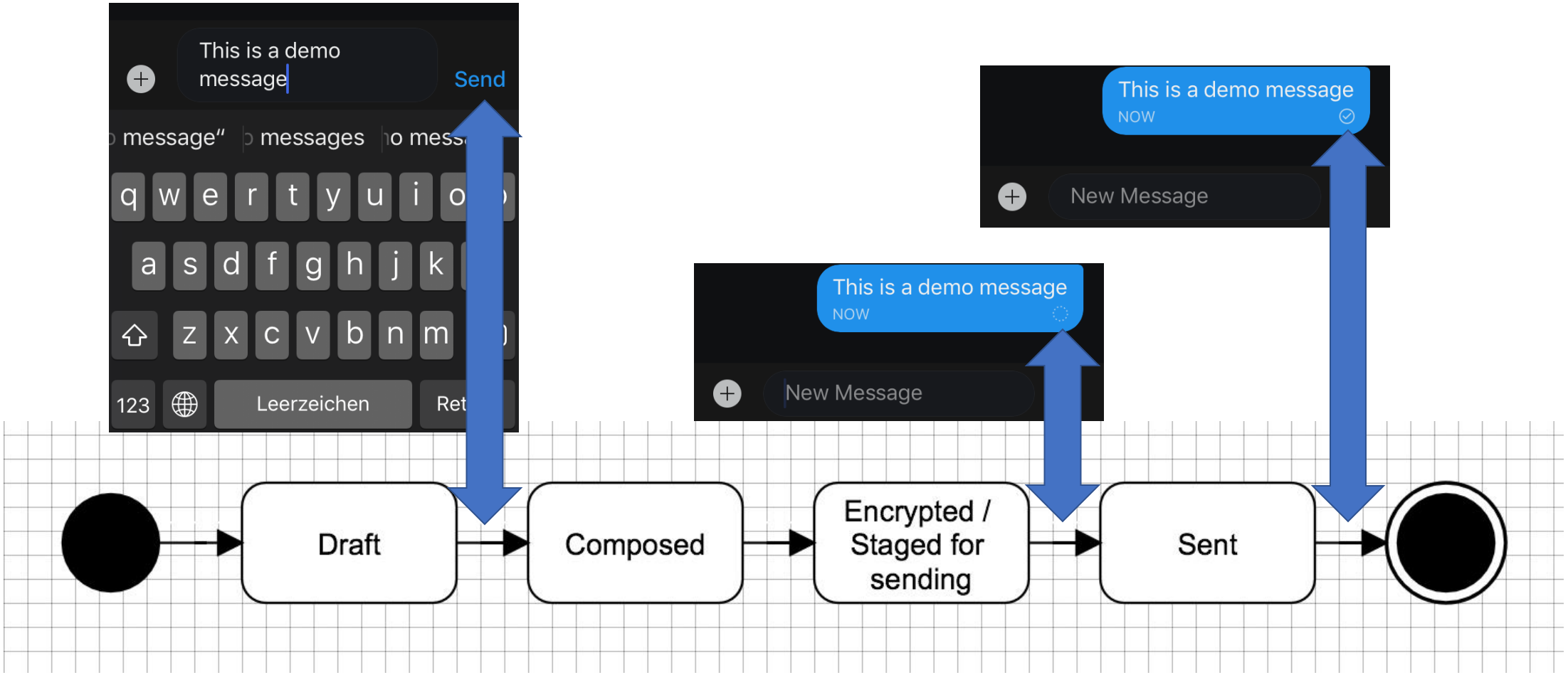
Key management in the context of *End-to-end encrypted* messaging



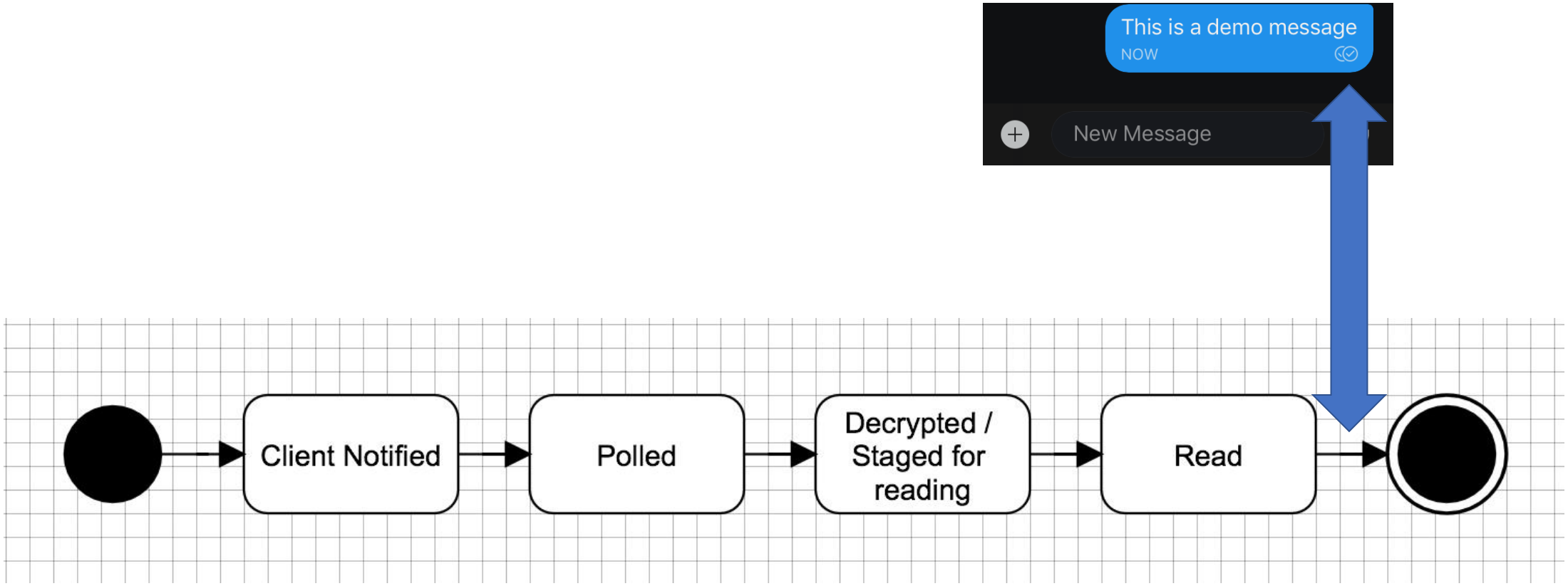

Local Keystore
Symmetric Encryption
Local Keystore
Secret Text
encryption key
same key
decryption key
Encoder
Decoder
Secret Text
Encrypted message sent over internet


Local Keystore
Asymmetric Encryption
Local Keystore
Secret Text
encryption key
NOT the same key
decryption key
Encoder
Decoder
Secret Text
Encrypted message sent over internet

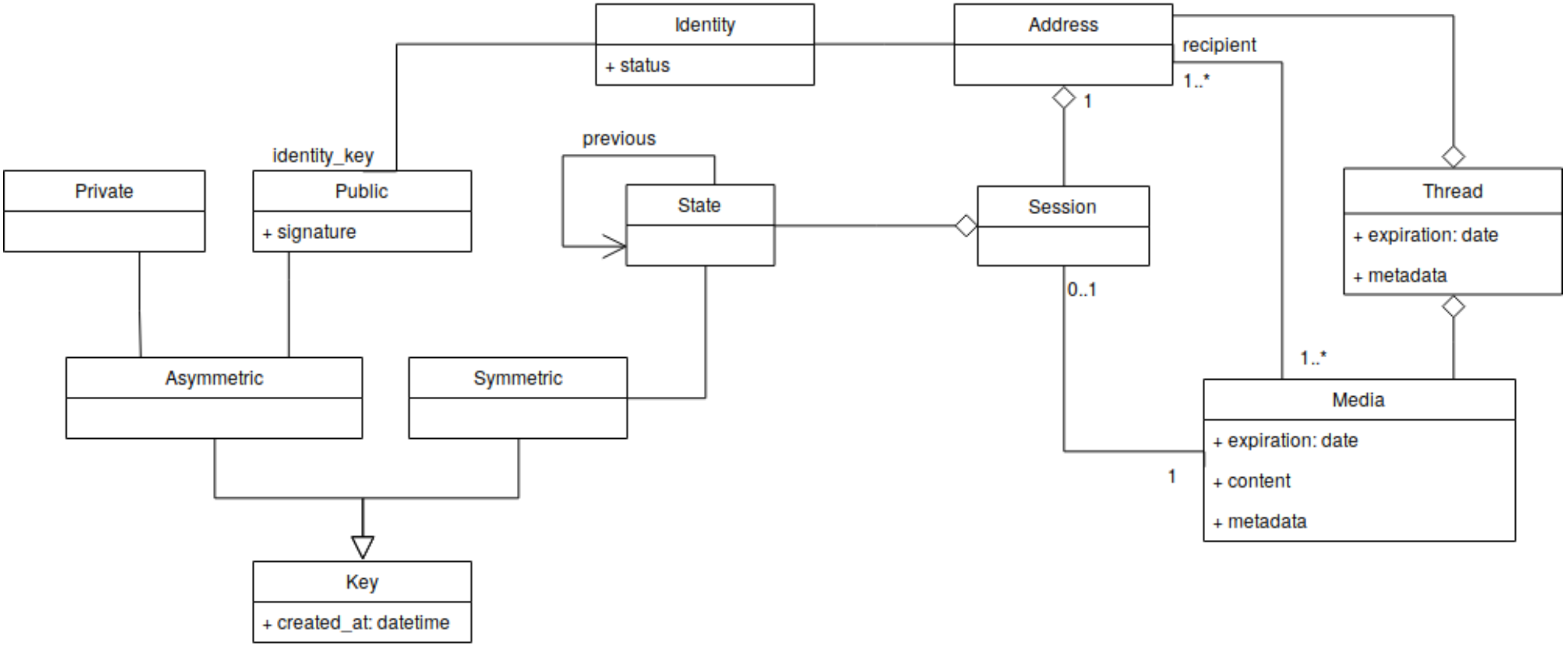
Signal's message pipeline (Sending)



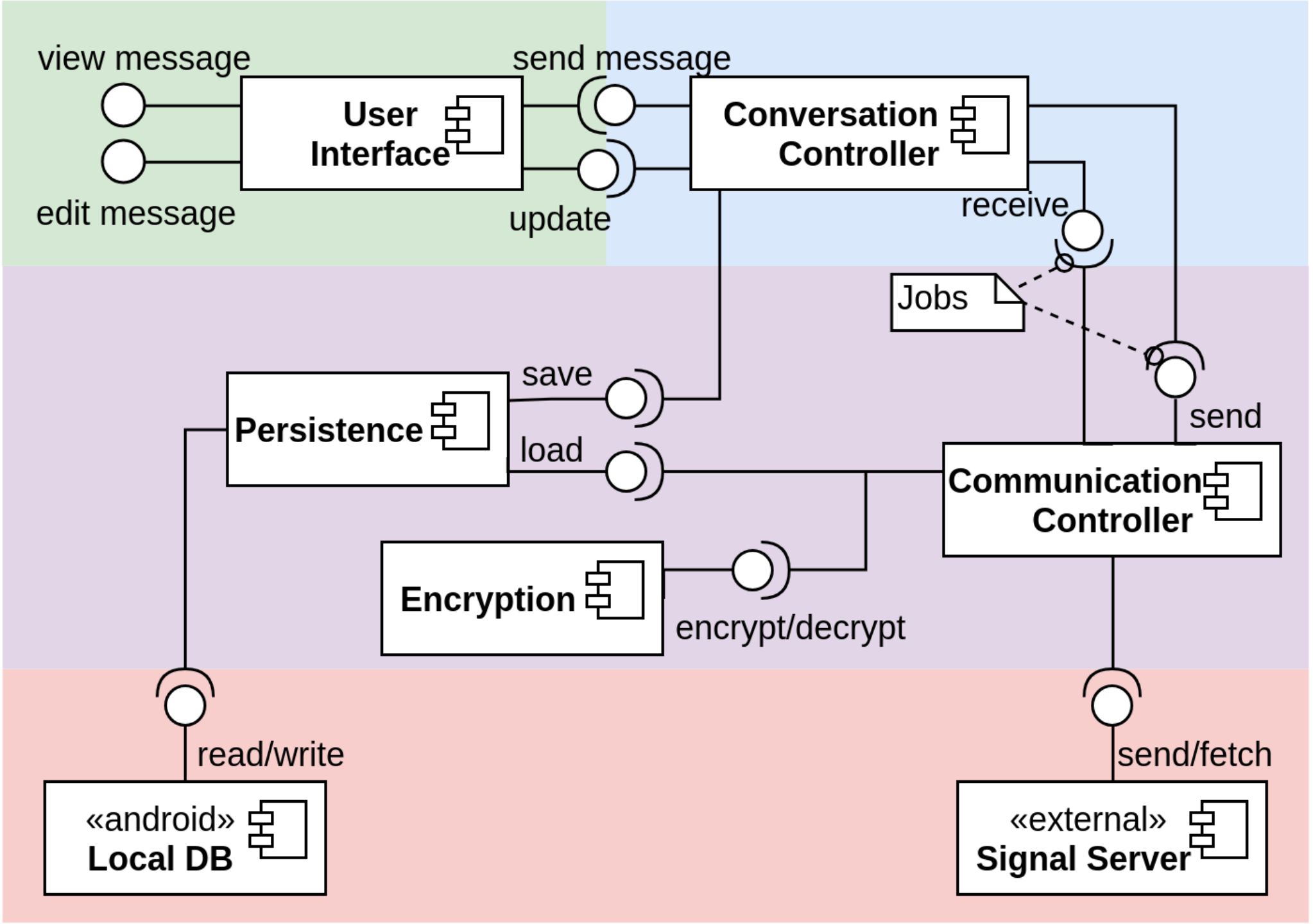
Signal's message pipeline (Receiving)



Key management and media



Sending Messages



TELUS
14:17
30 %
Awesome group
Tap here for settings
Group created.
Hey Mathieu, gg !
NOW
Mathieu Nassif
Yeah! Good job team!
NOW
MN
New Message