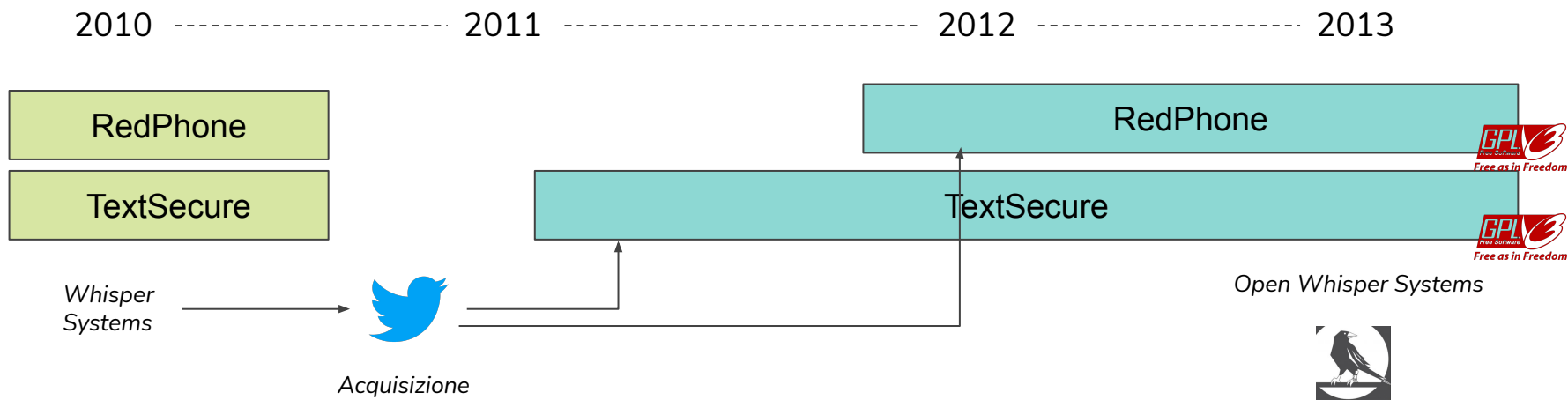


SIGNAL

La crittografia a portata di tua nonna
(storia di un successo)

Signal Timeline




Ref. Wikipedia


Signal Timeline

2014 ----- 2015 ----- 2017 ----- 2018 -----

RedPhone



TextSecure
(2nd version)



Free as in Freedom

Signal



Open Whisper Systems



RedPhone



WebRTC

+

Standalone apps

Signal technology foundation
+
Signal Messenger LLC



Ref. Wikipedia



Dove siamo arrivati

Open sourced non profit organization con una missione: comunicazioni private e sicure per tutti

Modello di sviluppo che non abbia il bisogno di dati personali per progredire

Source code disponibile su GitHub:

- Signal Android
- Signal Desktop
- Signal iOS
- Signal Server (*)

(*) Architettura centralizzata vs. federata

Ref: [reddit](#)



Publicazioni e referenze

- ["A Formal Security Analysis of the Signal Messaging Protocol"](#)
"Practically speaking, [le proprietà di sicurezza di Signal] imply secrecy and authentication of the message keys which Signal derives, even under a variety of adversarial compromise scenarios..."
K. Cohn-Gordon et al - 2017 IEEE European Symposium on Security and Privacy (EuroS&P)
- [European Commission to use open source messaging service Signal](#)
"Signal has been selected as the recommended application for public instant messaging.". The solution will be used for external communication between Commission staff and people outside the organization."