iOS Security Essentials

Rachid El Khayari

Fraunhofer
SIT

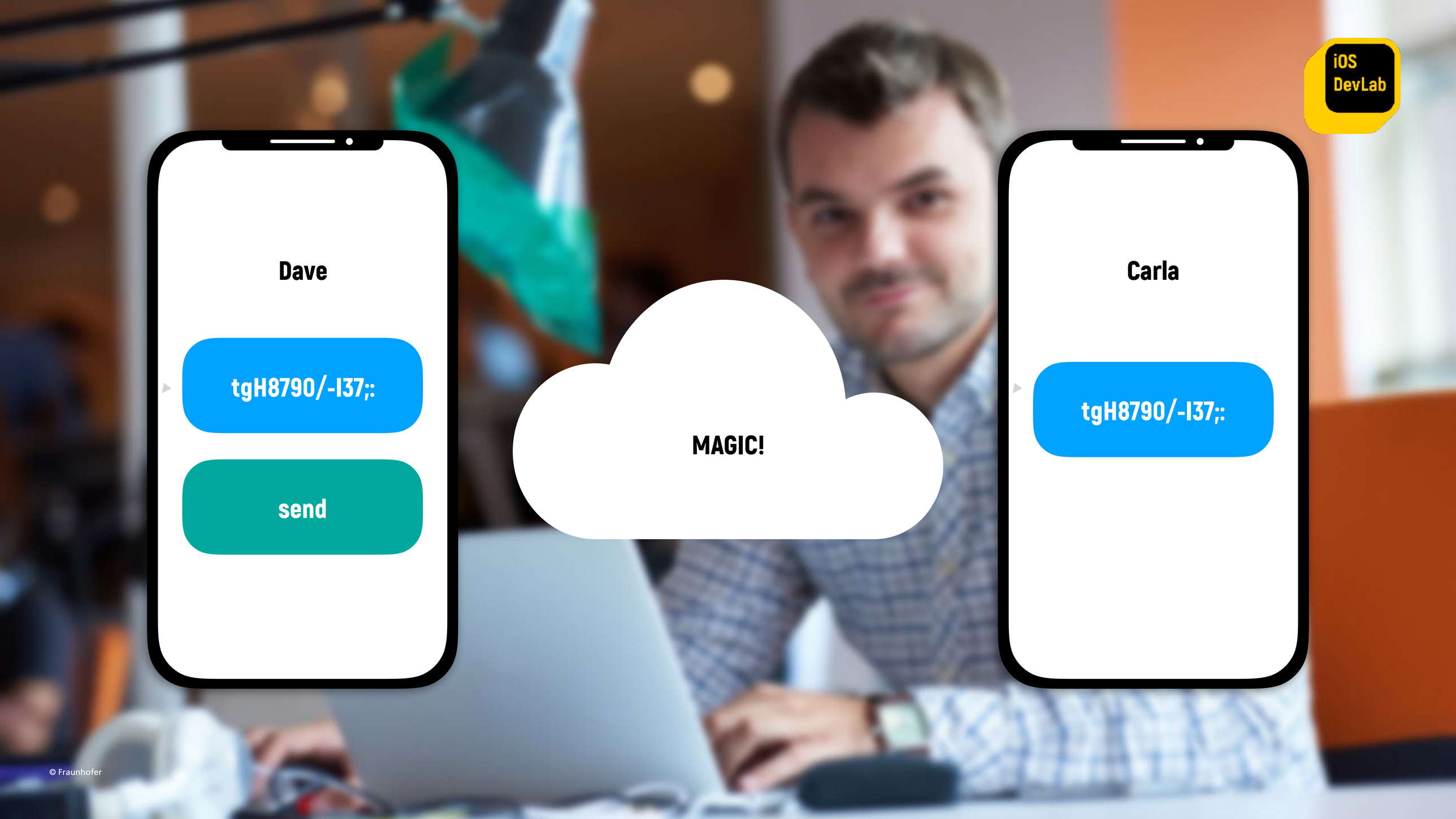
iOS
DevLab

RACHID
#iOSSecGuy

Fraunhofer
SIT

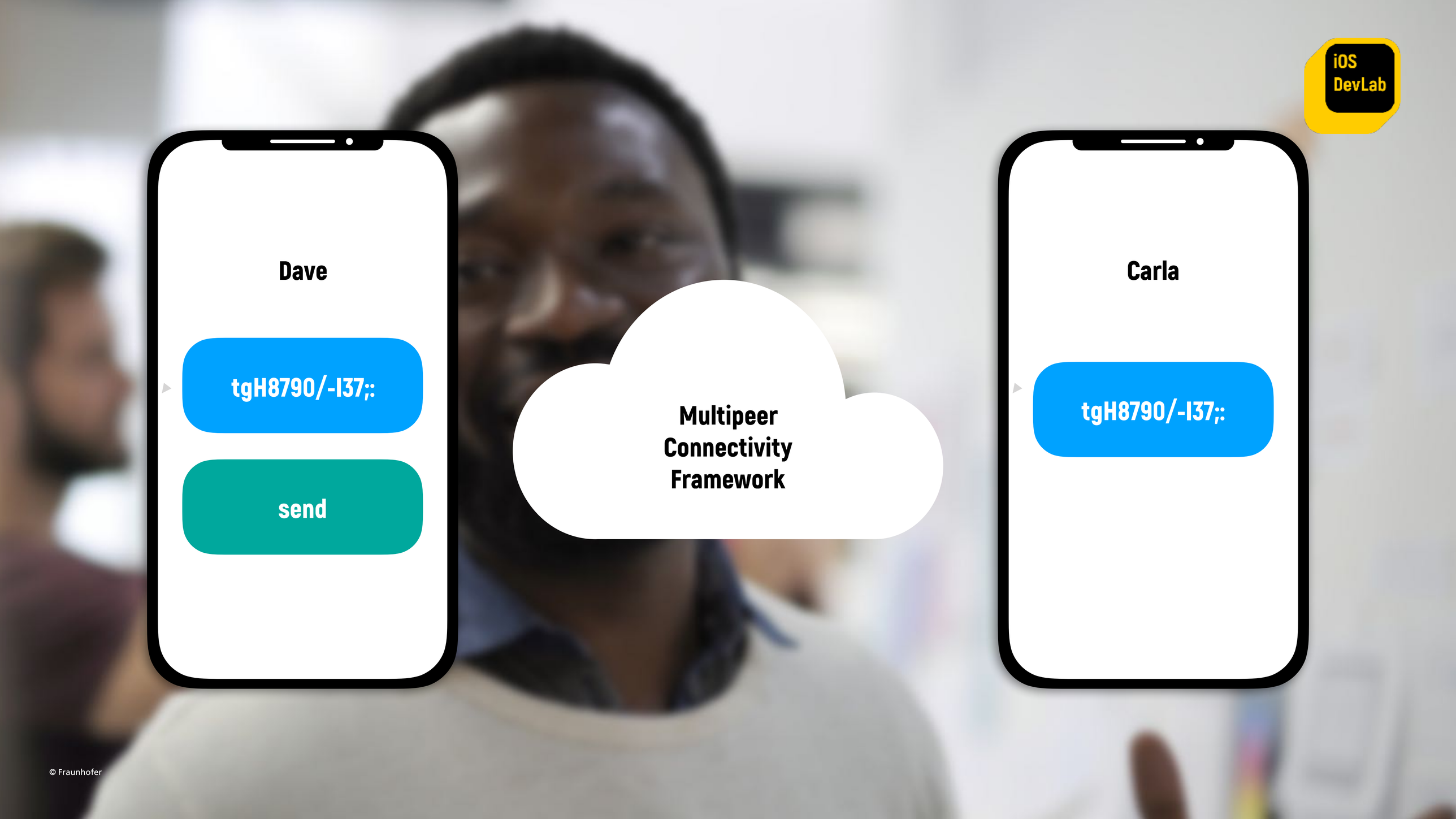

Sandbox
Exploits
Code Signing
Control
iOS DevLab
Pinning
Certifi
ailbreak
File System
Network Security
iOS Security
Boot Chain
Kernel Integrity Protection
Keychain
Crypto Engine
RNG
Secure Enclave
Privacy
Secure Element
Device Keys
© Fraunhofer


iOS
DevLab
DAVE
#CEO
A password generator
that sends passwords
from device to device.
#KeyExchangeProblem
#iPassDrop

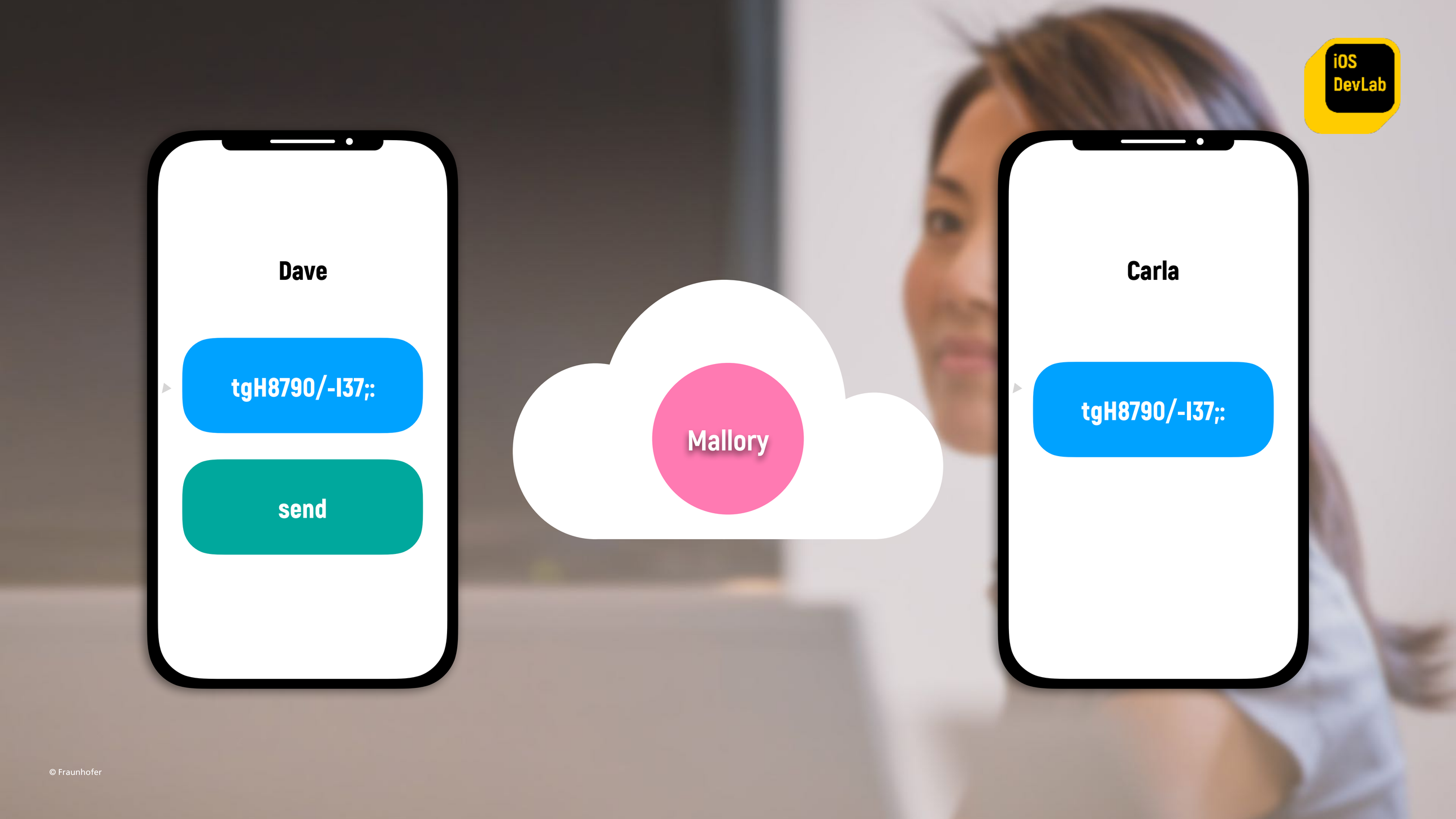



iOS
DevLab
Carla
#CTO
Sounds awesome!
That should be possible.
Let's make the world
more secure!


iOS
DevLab
Eric
#DEV
That's really easy.
I'll use the MPC
Framework.


iOS
DevLab
Dave
tgH8790/-I37;:
send
Multipeer
Connectivity
Framework
Carla
tgH8790/-I37;:


iOS
DevLab
Lili
#CSO
How does that work?
Is that really secure?
The passwords need
to be secured!




iOS
DevLab
Eric
#DEV
Well I don’t know.
It just works.
#3linesofcode


iOS
DevLab
Carla
#CTO
I sniffed the data
via network interface.
It just sends
plain text!
$ rvictl -s b0e8fe73db17d4993bd549418bfbdba70a4af2b1
$ sudo tcpdump -i rvi0 -w trace.pcap
https://developer.apple.com/documentation/network/recording_a_packet_trace


iOS
DevLab
DAVE
#CEO
It won't fly
if it's insecure!
#Sad
#iPassDrop


iOS
DevLab
Eric
#DEV
I'm a bit confused!
It looked correct to me
and all unit tests
are green.

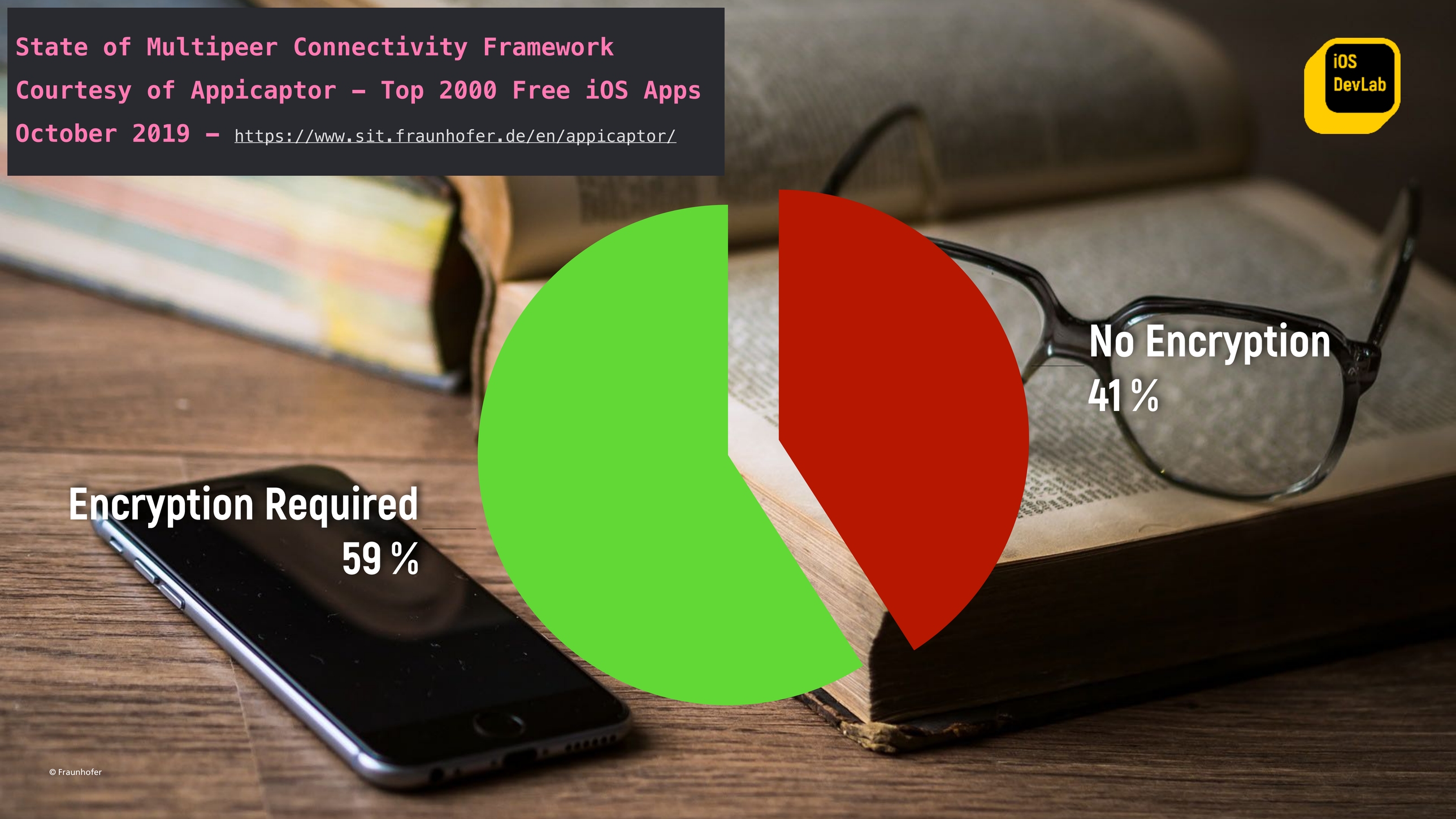
#DEVELOPERSPERSPECTIVE

```
import MultipeerConnectivity
let mpcSession = MCSession(peer: myPeerID, securityIdentity: nil, encryptionPreference: .none)
mpcSession.send(password.data(using: .utf8)!, toPeers: [otherPeerID], with: .reliable)
```

State of Multipeer Connectivity Framework

Courtesy of Appicaptor – Top 2000 Free iOS Apps

October 2019 – https://www.sit.fraunhofer.de/en/appicaptor/



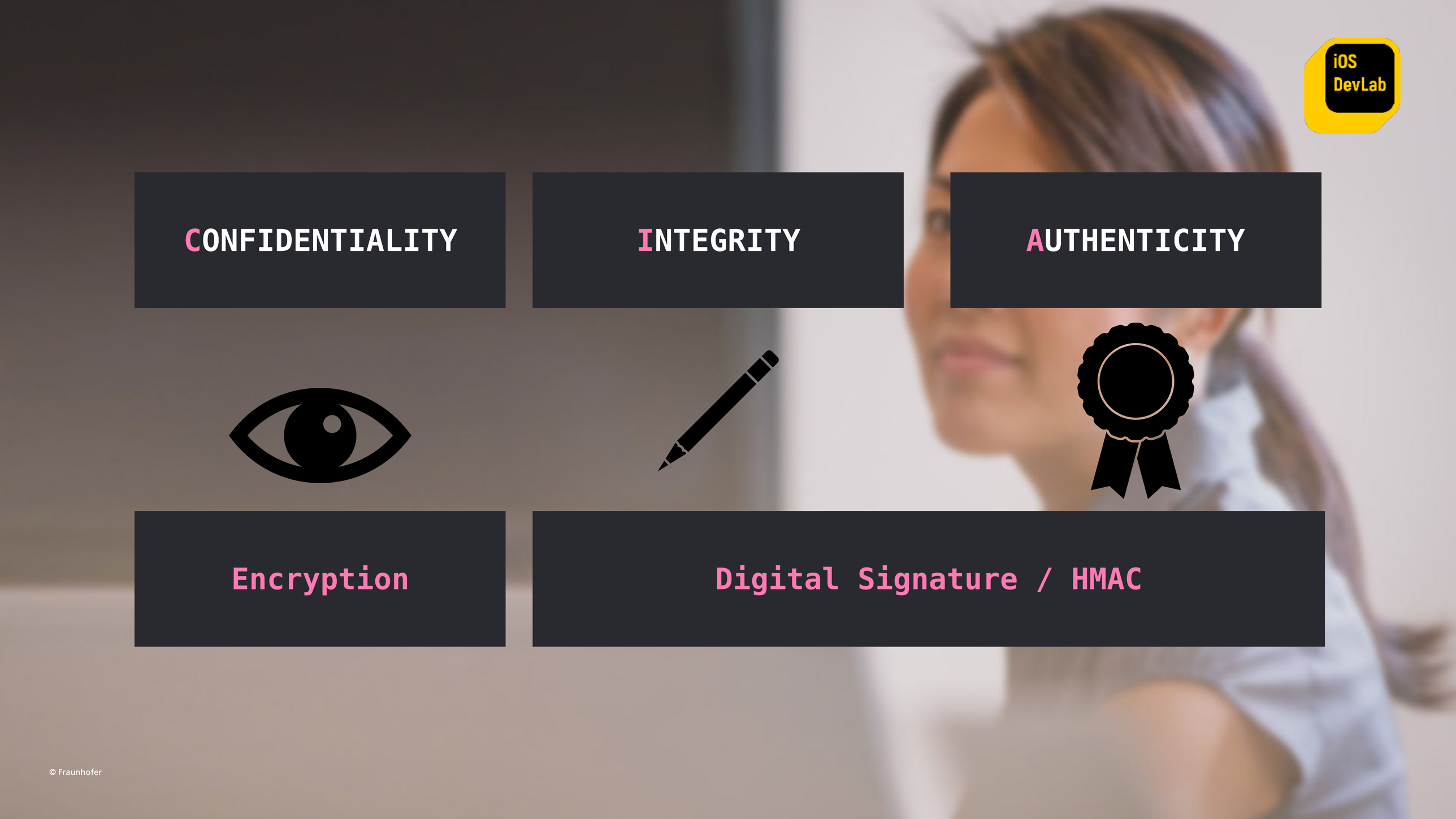
iOS DevLab

#BUGFIXING

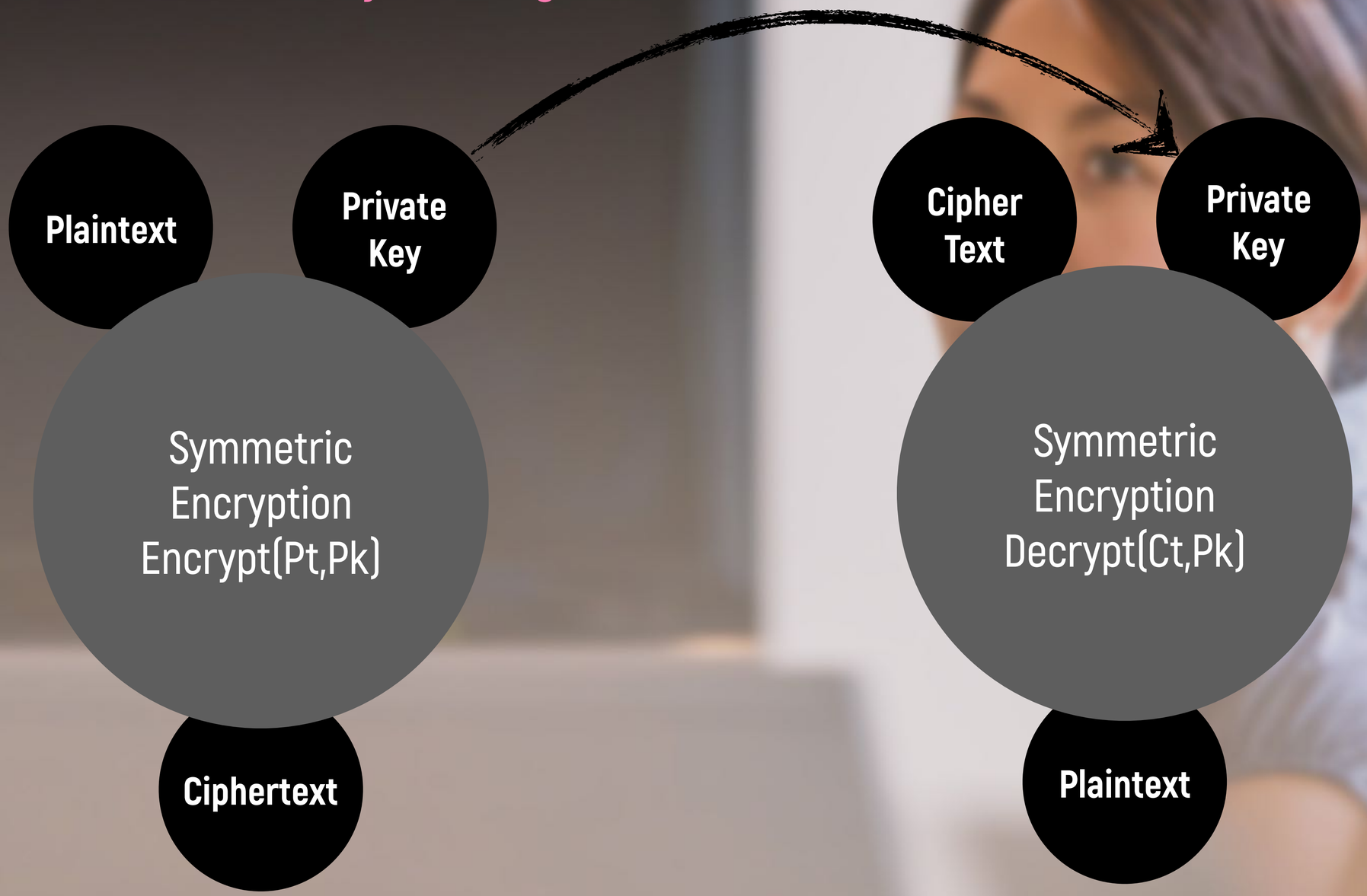
```
import MultipeerConnectivity
let mpcSession = MCSession(peer: myPeerID, securityIdentity: nil, encryptionPreference: .required)
mpcSession.send(password.data(using: .utf8)!, toPeers: [otherPeerID], with: .reliable)
```


iOS
DevLab
Carla
#CTO
I re-ran the sniffing and now everything is encrypted!

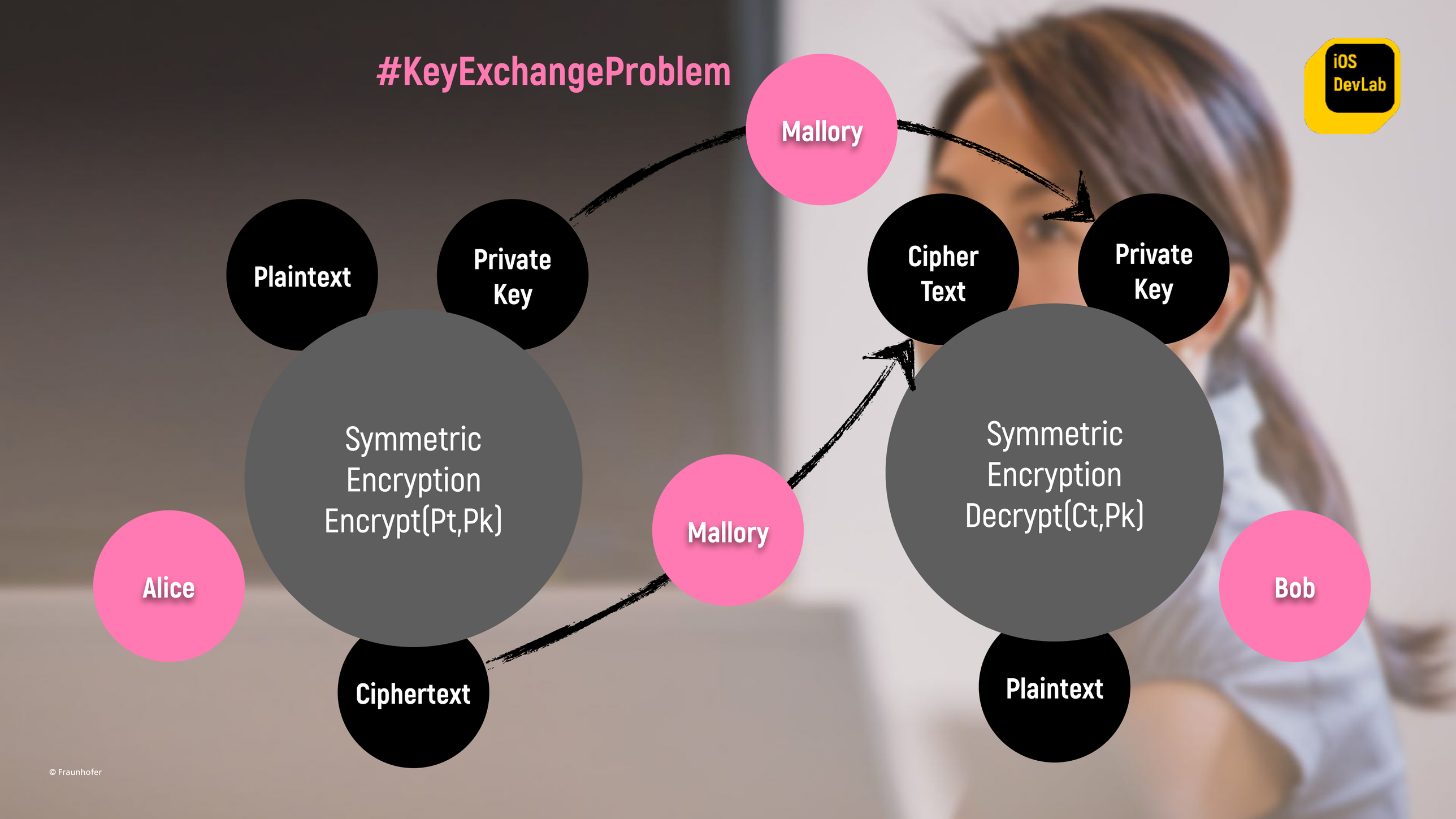

iOS
DevLab
Lili
#CSO
That's not enough.
You just covered the C
of CIA
And you didn't solve
the Key Exchange.


iOS
DevLab
CONFIDENTIALITY
INTEGRITY
AUTHENTICITY
Encryption
Digital Signature / HMAC

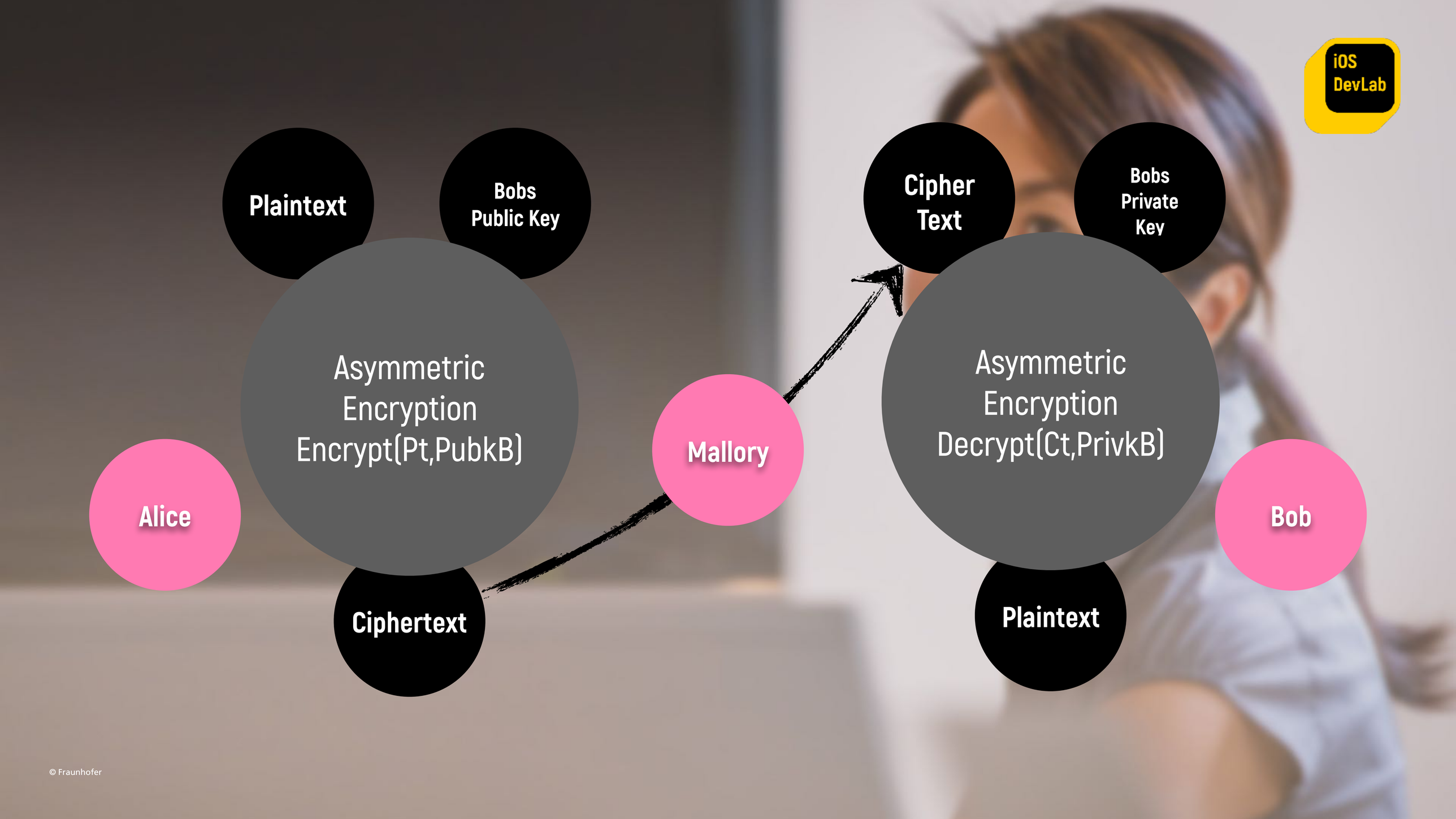
#KeyExchangeProblem

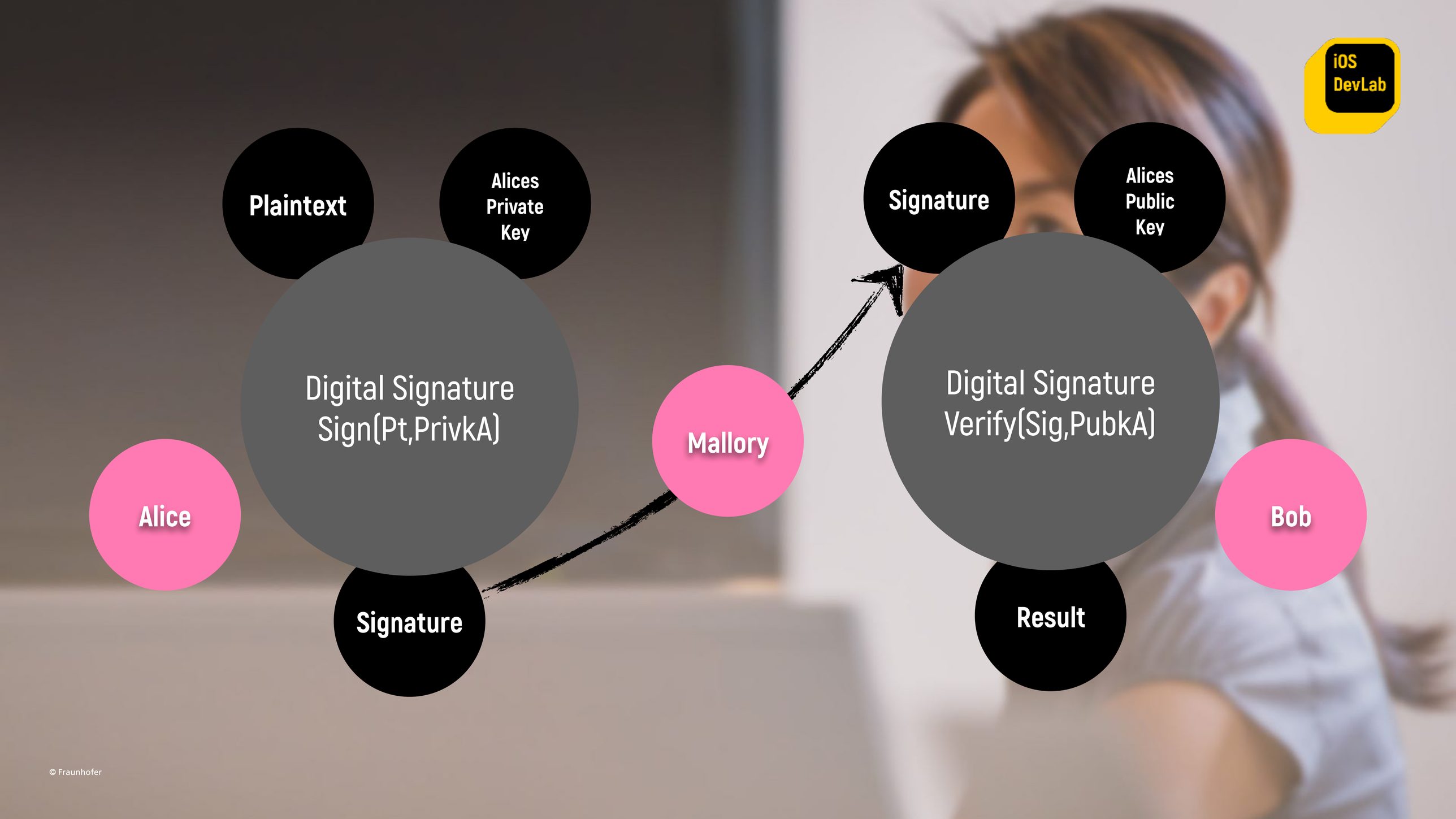


iOS DevLab

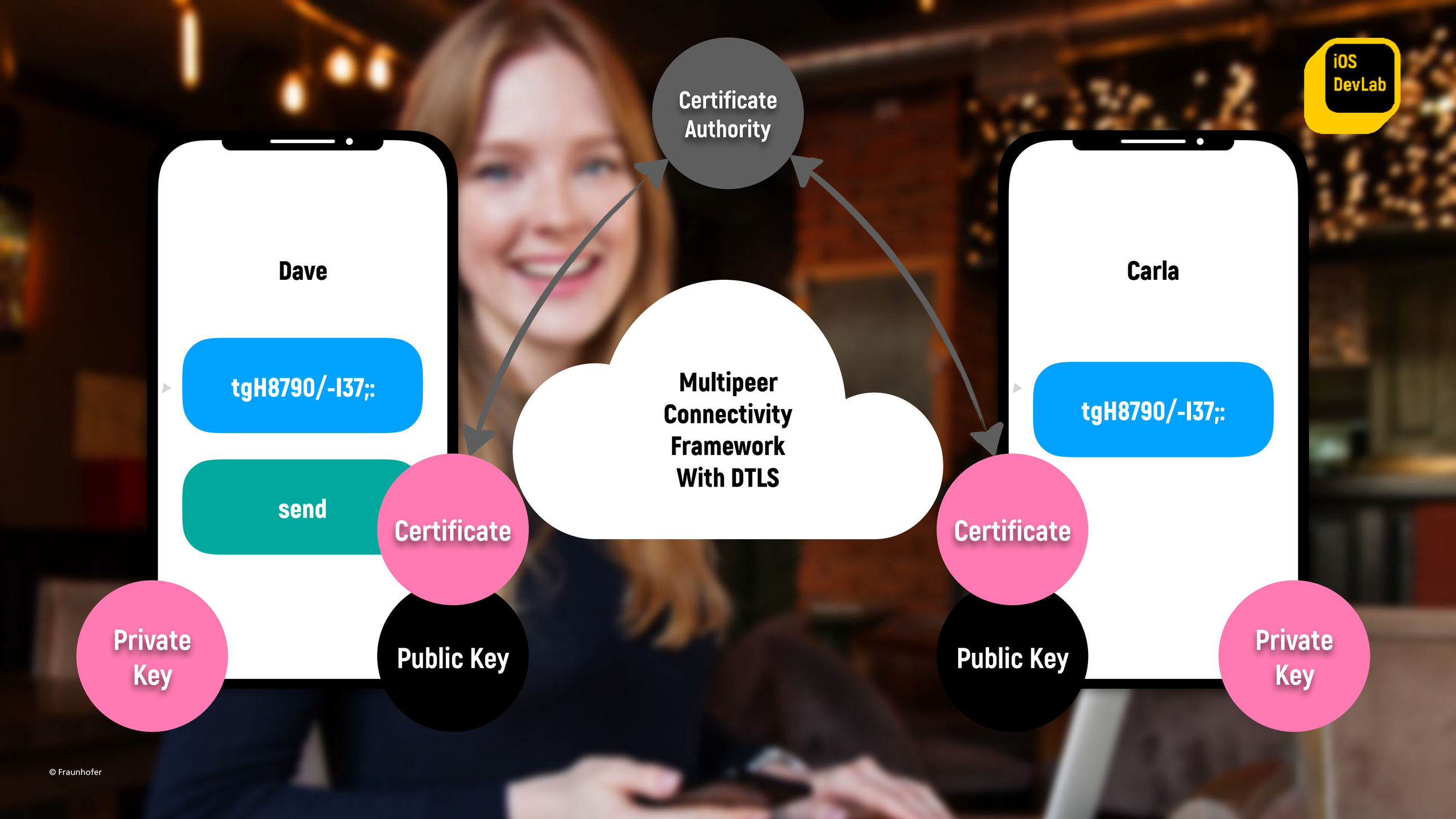

#KeyExchangeProblem
iOS DevLab
Mallory
Plaintext
Private Key
Cipher Text
Private Key
Symmetric Encryption Encrypt(Pt,Pk)
Symmetric Encryption Decrypt(Ct,Pk)
Alice
Mallory
Bob
Ciphertext
Plaintext
© Fraunhofer

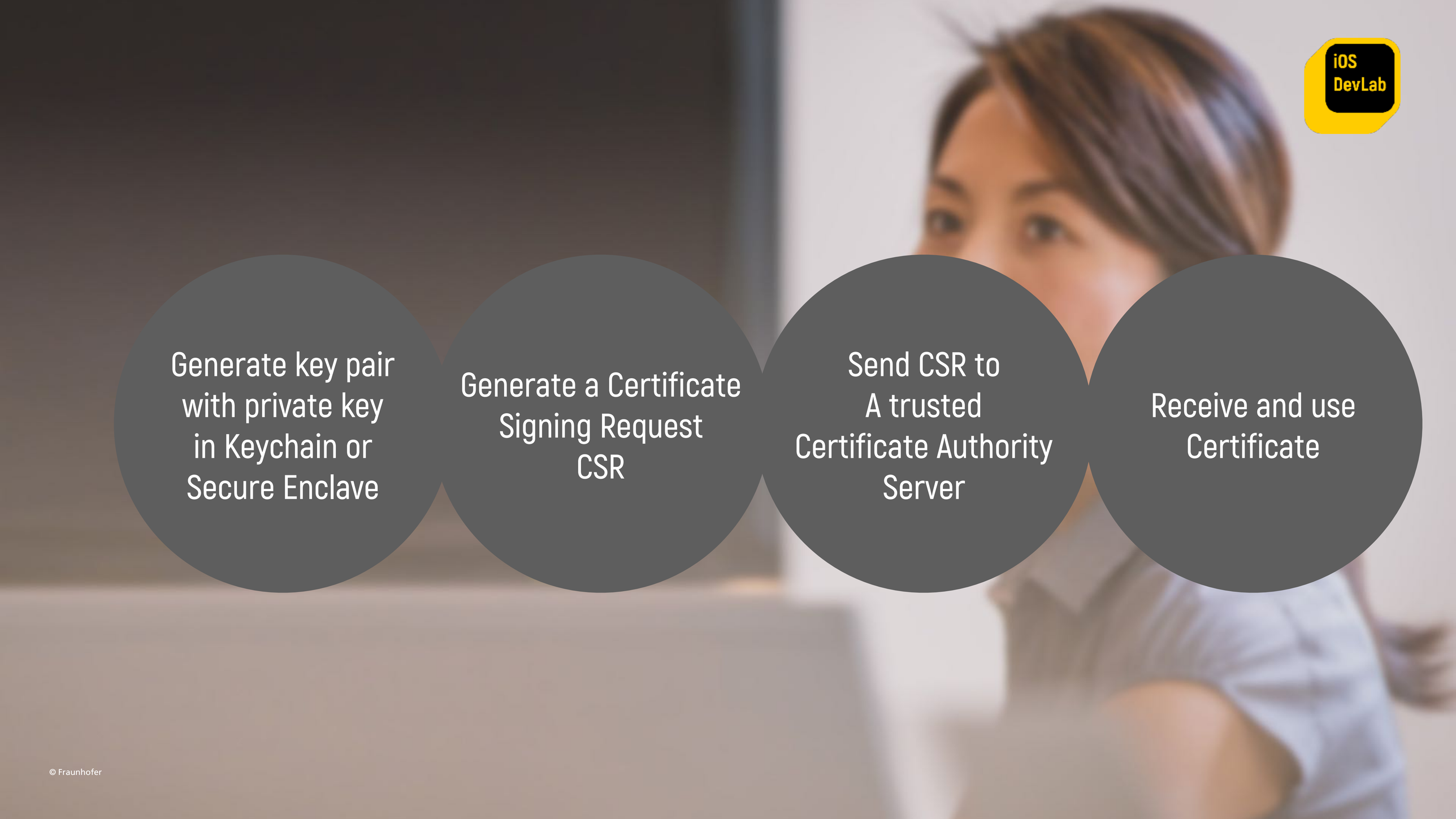

iOS
DevLab
Lili
#CSO
You have to use
asymmetric encryption
with client certificates


iOS DevLab
Plaintext
Bobs Public Key
Asymmetric Encryption Encrypt(Pt,PubkB)
Alice
Ciphertext
Mallory
Cipher Text
Bobs Private Key
Asymmetric Encryption Decrypt(Ct,PrivkB)
Bob
Plaintext


iOS DevLab
Plaintext
Alices Private Key
Digital Signature Sign(Pt,PrivkA)
Alice
Signature
Mallory
Signature
Alices Public Key
Digital Signature Verify(Sig,PubkA)
Bob
Result


iOS
DevLab
Carla
#CTO
So we need unique client certificates generated by a Certificate server for our devices?


iOS DevLab
Certificate Authority
Dave
tgH8790/-I37;:
send
Certificate
Private Key
Public Key
Multipeer Connectivity Framework With DTLS
Carla
tgH8790/-I37;:
Certificate
Public Key
Private Key


iOS
DevLab
Generate key pair with private key in Keychain or Secure Enclave
Generate a Certificate Signing Request CSR
Send CSR to A trusted Certificate Authority Server
Receive and use Certificate


iOS
DevLab
Eric
#DEV
So I just need to create a trust object containing the certificate.

iOS DevLab

#SOLVED?!

```
import MultipeerConnectivity
let mpcSession = MCSession(peer: myPeerID, securityIdentity: trustObject, encryptionPreference: .required)
mpcSession.send(password.data(using: .utf8)!, toPeers: [otherPeerID], with: .reliable)
```

State of Multipeer Connectivity Framework

Courtesy of Appicaptor – Top 2000 Free iOS Apps

October 2019 – https://www.sit.fraunhofer.de/en/appicaptor/

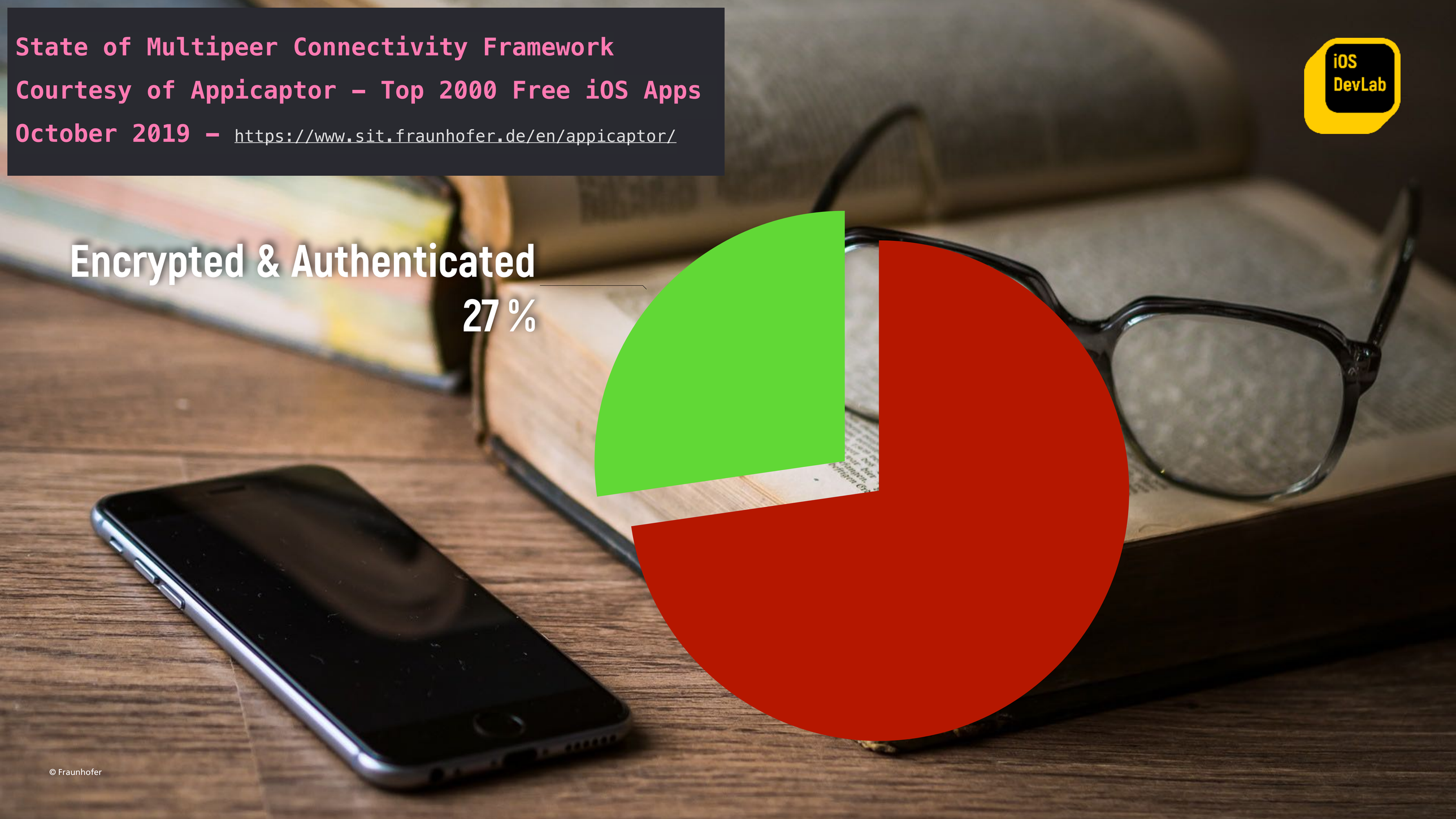
iOS DevLab

State of Multipeer Connectivity Framework

Courtesy of Appicaptor – Top 2000 Free iOS Apps

October 2019 – https://www.sit.fraunhofer.de/en/appicaptor/

iOS DevLab




iOS
DevLab
DAVE
#CEO
Awesome!
We can go live now!
#Success
#iPassDrop


Sandbox
Exploits
Code Signing
Control
iOS DevLab
Pinning
Certifi
ailbreak
File System
Network Security
iOS Security
Boot Chain
Kernel
Keychain
Crypto Engine
RNG
Secure Enclave
Privacy
Secure Element
Device

Image Licenses

Image from Juraj Varga on Pixabay

Dariusz Sankowski on Pixabay

Alyibel Colmenares on Pixabay

Анастасия Гепп on Pixabay

Free-Photos on Pixabay

rawpixel auf Pixabay

SCAN ME

RACHID EL KHAYARI

khayari@sit.fraunhofer.de

Questions?