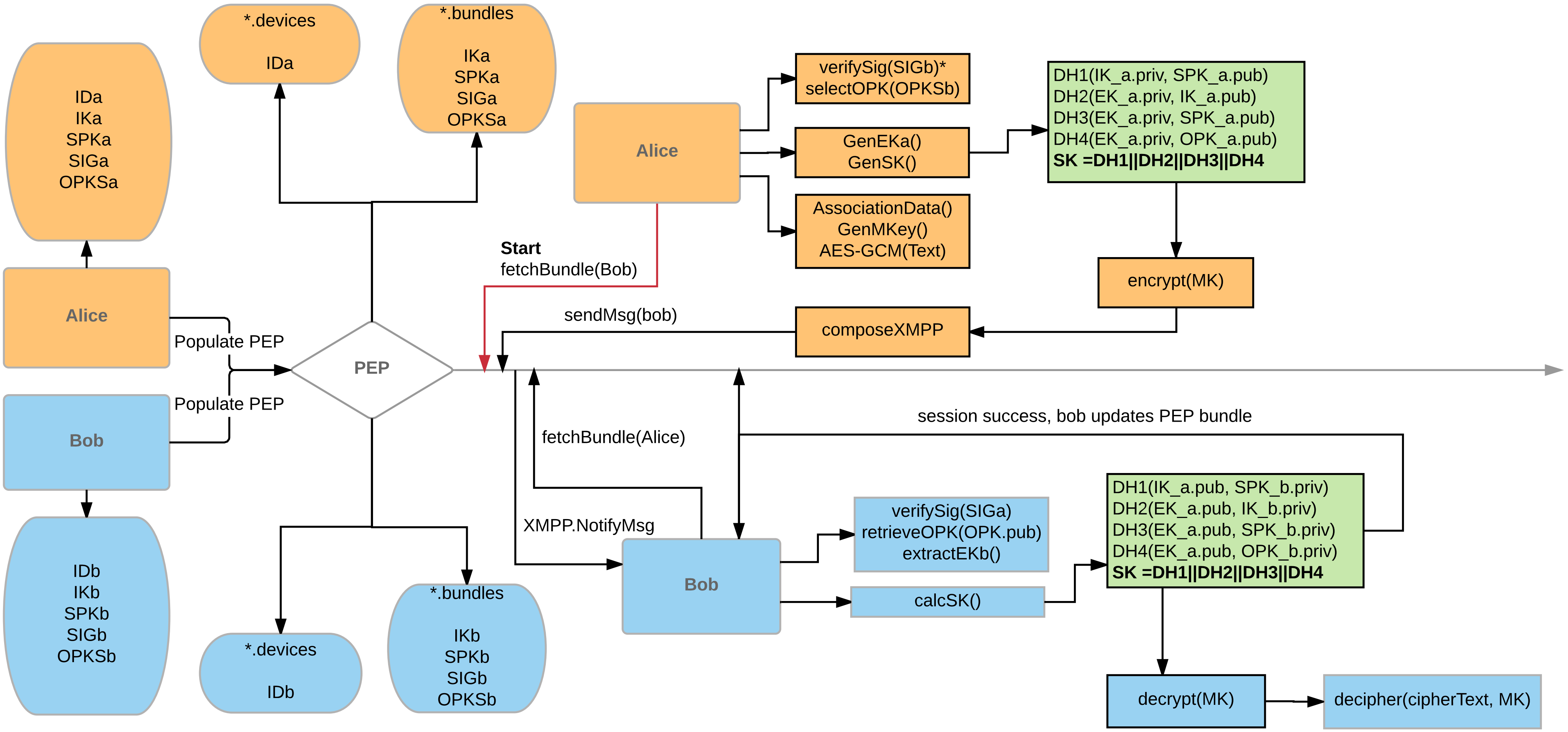
LIBSIG-OMEMO PROTOCOL FLOW - SINGLE MESSAGE

Bassel Khatib | September 23, 2017



IDa
IKa
SPKa
SIGa
OPKSa

*.devices

IDa

*.bundles

IKa
SPKa
SIGa
OPKSa

Alice

Populate PEP

PEP

Populate PEP

Bob

IDb
IKb
SPKb
SIGb
OPKSb

*.devices

IDb

*.bundles

IKb
SPKb
SIGb
OPKSb

Alice

verifySig(SIGb)*
selectOPK(OPKSb)

GenEKa()
GenSK()

AssociationData()
GenMKey()
AES-GCM(Text)

DH1(IK_a.priv, SPK_a.pub)
DH2(EK_a.priv, IK_a.pub)
DH3(EK_a.priv, SPK_a.pub)
DH4(EK_a.priv, OPK_a.pub)
SK =DH1||DH2||DH3||DH4

encrypt(MK)

Start
fetchBundle(Bob)

sendMsg(bob)

composeXMPP

fetchBundle(Alice)

session success, bob updates PEP bundle

XMPP.NotifyMsg

Bob

verifySig(SIGa)
retrieveOPK(OPK.pub)
extractEKb()

calcSK()

DH1(IK_a.pub, SPK_b.priv)
DH2(EK_a.pub, IK_b.priv)
DH3(EK_a.pub, SPK_b.priv)
DH4(EK_a.pub, OPK_b.priv)
SK =DH1||DH2||DH3||DH4

decrypt(MK)

decipher(cipherText, MK)

GCM:
AD = Encode(IKA) || Encode(IKB)
nonce = IV
cipher:
decipher:
next keys:
Message structure:
https://www.npmjs.com/package/node-aes-256-gcm
https://tools.ietf.org/html/rfc5288

PreKeySignalMessage: Session establishment
SignalMessage: message sent after session
KeyTransportElement: file transfer
implementation note: preKey.pub used as key for preKey.priv in the stored bundle. XEP does not specify "key ids", unlike CC's impl.
Implementation question: do we send the message to all devices? our example deals with one device.