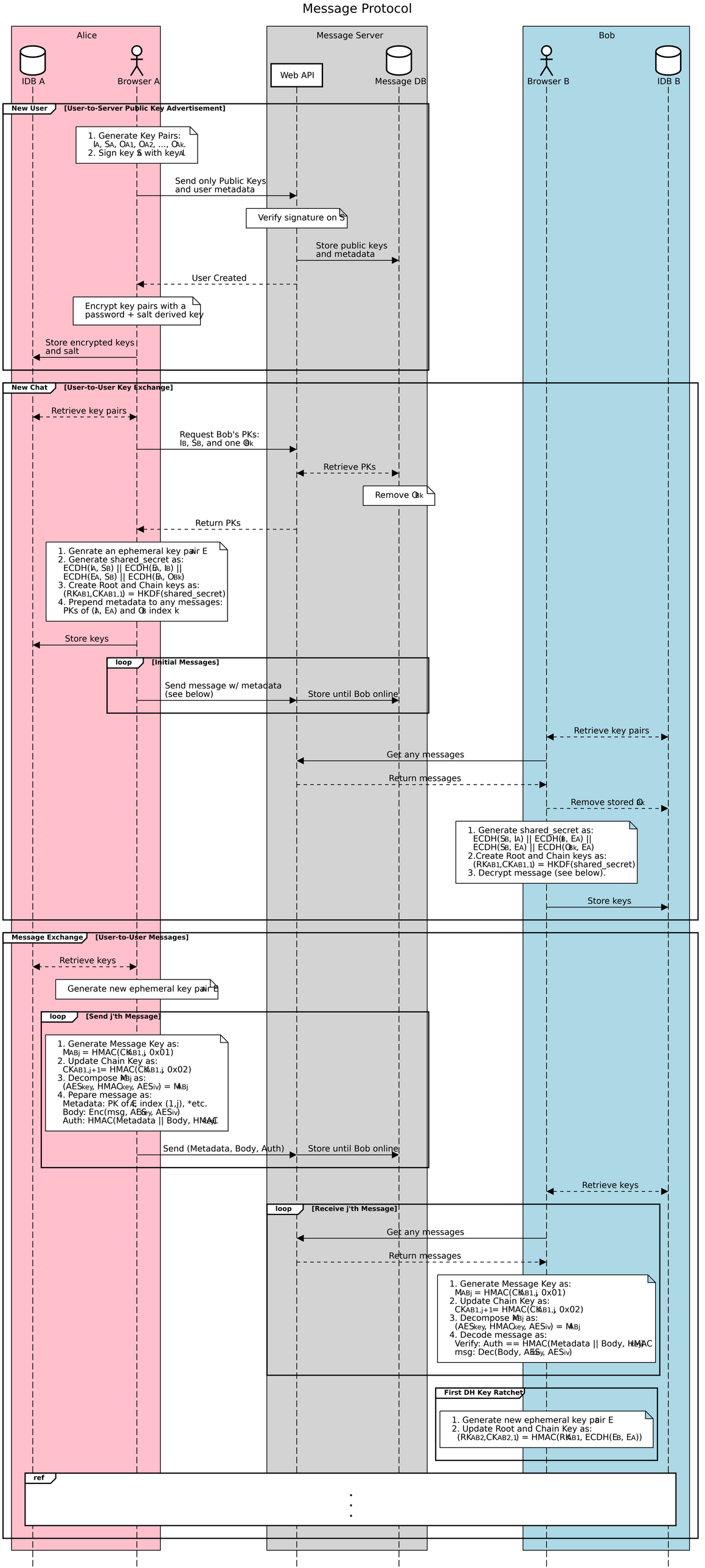
Message Protocol
Alice
Message Server
Bob
IDB A
Browser A
Web API
Message DB
Browser B
IDB B
New User
[User-to-Server Public Key Advertisement]
1. Generate Key Pairs:
IA, SA, OA1, OA2, ..., OAk.
2. Sign key S with key IA.
Send only Public Keys
and user metadata
Verify signature on S
Store public keys
and metadata
User Created
Encrypt key pairs with a
password + salt derived key
Store encrypted keys
and salt
New Chat
[User-to-User Key Exchange]
Retrieve key pairs
Request Bob's PKs:
IB, SB, and one OBk
Retrieve PKs
Remove OBk
Return PKs
1. Genrate an ephemeral key pair E
2. Generate shared_secret as:
ECDH(IA, SB) || ECDH(EA, IB) ||
ECDH(EA, SB) || ECDH(EA, OBk)
3. Create Root and Chain keys as:
(RKAB1,CKAB1,1) = HKDF(shared_secret)
4. Prepend metadata to any messages:
PKs of (IA, EA) and OB index k
Store keys
loop
[Initial Messages]
Send message w/ metadata
(see below)
Store until Bob online
Retrieve key pairs
Get any messages
Return messages
Remove stored OBk
1. Generate shared_secret as:
ECDH(SB, IA) || ECDH(IB, EA) ||
ECDH(SB, EA) || ECDH(OBk, EA)
2.Create Root and Chain keys as:
(RKAB1,CKAB1,1) = HKDF(shared_secret)
3. Decrypt message (see below).
Store keys
Message Exchange
[User-to-User Messages]
Retrieve keys
Generate new ephemeral key pair E
loop
[Send j'th Message]
1. Generate Message Key as:
MABj = HMAC(CKAB1,j, 0x01)
2. Update Chain Key as:
CKAB1,j+1= HMAC(CKAB1,j, 0x02)
3. Decompose MABj as:
(AESkey, HMACkey, AESiv) = MABj
4. Pepare message as:
Metadata: PK of EA, index (1,j), *etc.
Body: Enc(msg, AESkey, AESiv)
Auth: HMAC(Metadata || Body, HMACkey)
Send (Metadata, Body, Auth)
Store until Bob online
Retrieve keys
loop
[Receive j'th Message]
Get any messages
Return messages
1. Generate Message Key as:
MABj = HMAC(CKAB1,j, 0x01)
2. Update Chain Key as:
CKAB1,j+1= HMAC(CKAB1,j, 0x02)
3. Decompose MABj as:
(AESkey, HMACkey, AESiv) = MABj
4. Decode message as:
Verify: Auth == HMAC(Metadata || Body, HMACkey)
msg: Dec(Body, AESkey, AESiv)
First DH Key Ratchet
1. Generate new ephemeral key pair E
2. Update Root and Chain Key as:
(RKAB2,CKAB2,1) = HMAC(RKAB1, ECDH(EB, EA))
ref