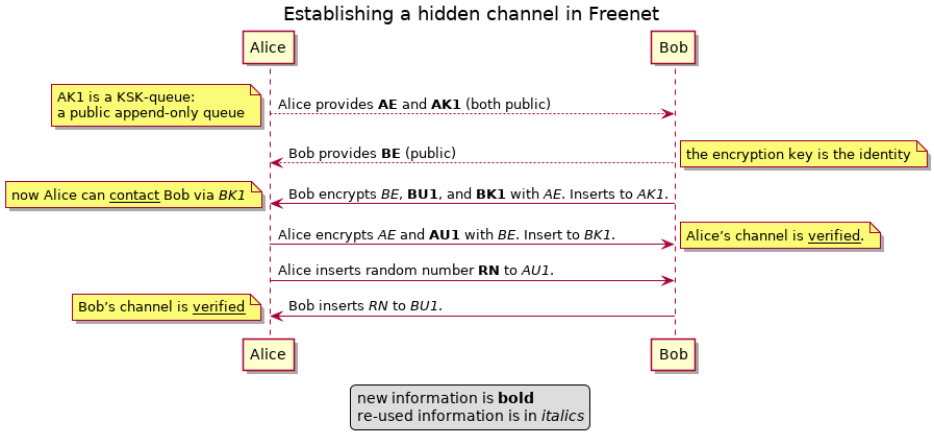
Establishing a hidden, encrypted communication channel over Freenet

Dr. Arne Babenhauserheide

<2021-01-05 Di>

Freenet provides the primitives needed to establish confidential communication, but it isn't always widely known how to do that.

This article provides the concepts to use. For practical implementation see the Freenet Communication Primitives Part 1: Files and Sites and Part 2: Discovery.



Step 0: use-case

- Alice provides a public point-of-contact.
- Bob wants to establish a hidden channel with Alice which they can afterwards use for confidential communication.

Step 1: Public Knowledge

- Alice and Bob each advertise an encryption key: **AE** and **BE**. These double as identity markers.
- Alice advertises a KSK Queue: **AK1**. This is the point-of-contact.

Step 2: Bob's keys

- Bob uses **AE** to encrypt a message with his encryption-key **BE**, a USK **BU1**, and a KSK **BK1**.
- Bob inserts the encrypted message as one entry to the KSK **AK1**.
- Alice decrypts what she gets on the KSK Queue **AK1**.
- Alice now knows the USK **BU1**, the KSK **BK1**, and the claim that these belong to Bob (**BE**).

Step 3: Alice's keys

- Alice uses **BE** to encrypt a message with her encryption-key **AE** and a USK link **AU1**.
- Alice inserts the encrypted message to Bobs KSK **BK1**.
- Bob decrypts what he gets from **BK1**.
- Bob now knows the USK **AU1** *and* Bob knows that the USK **AU1** is from Alice *(because Alice controls **AE**, otherwise Alice would not have known the KSK **BK1**).*

Step 4: Verify Bob's side of the channel

- Alice writes a long random number **RN** to **AU1**.
- Bob repeats the random number **RN** on **BU1**.
- Alice now knows that Bob knows **AU1** *(because Bob controls **BE**, otherwise Bob could not have read the random number from **AU1**).*

Done

Now Bob and Alice are the only ones who know **AU1** and **BU1**.

IFF the keys **AE** and **BE** were correct, then **Bob and Alice are connected** and an outside observer can only see that someone tried to establish a channel to Alice, but can see neither whether the channel was used, nor how the channel was used, nor who used it.

Alice and Bob now have a confidential channel: Alice writes her messages for Bob to **AU1** and Bob writes his messages for Alice to **BU1**.