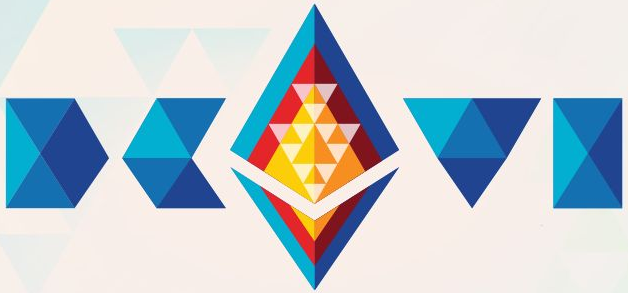


dm3

Decentralized, Secure and Open Messaging Protocol

Heiko Burkhardt

Lead developer, corpus.ventures

What is dm3?

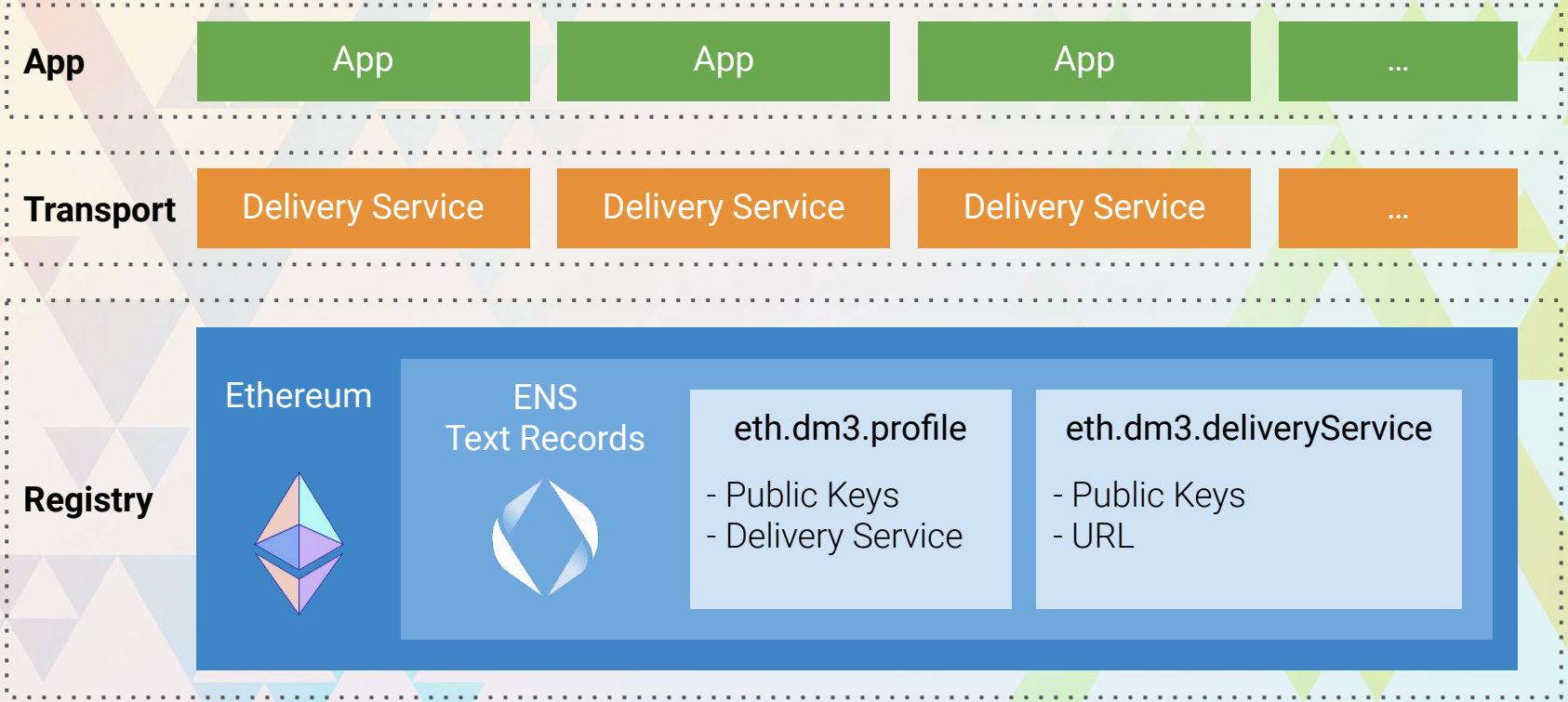
dm3 is a **simple** protocol enabling

decentralized, **open**, and **secure**

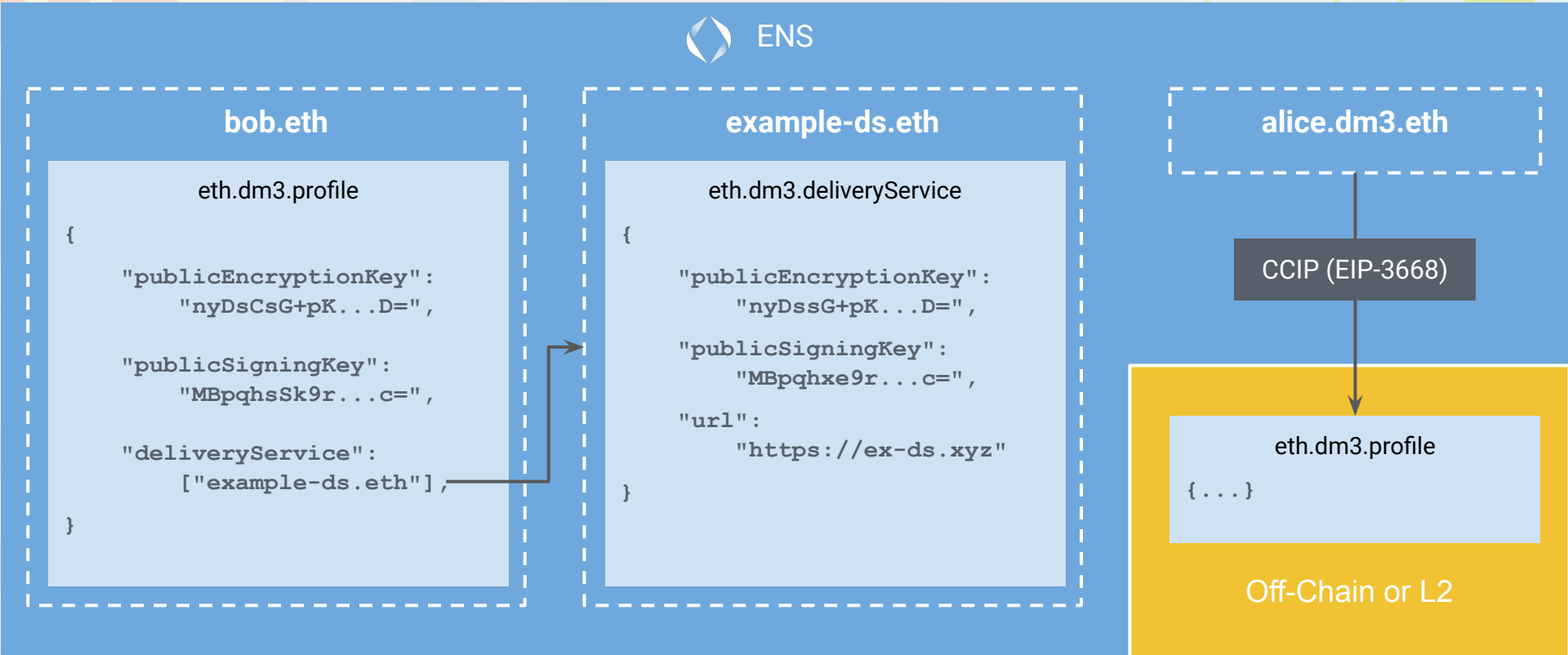
messaging
using established web3 services.

- Censorship Resistance
- No single point of failure
- Users are in control of their data
- Everyone can write an own implementation

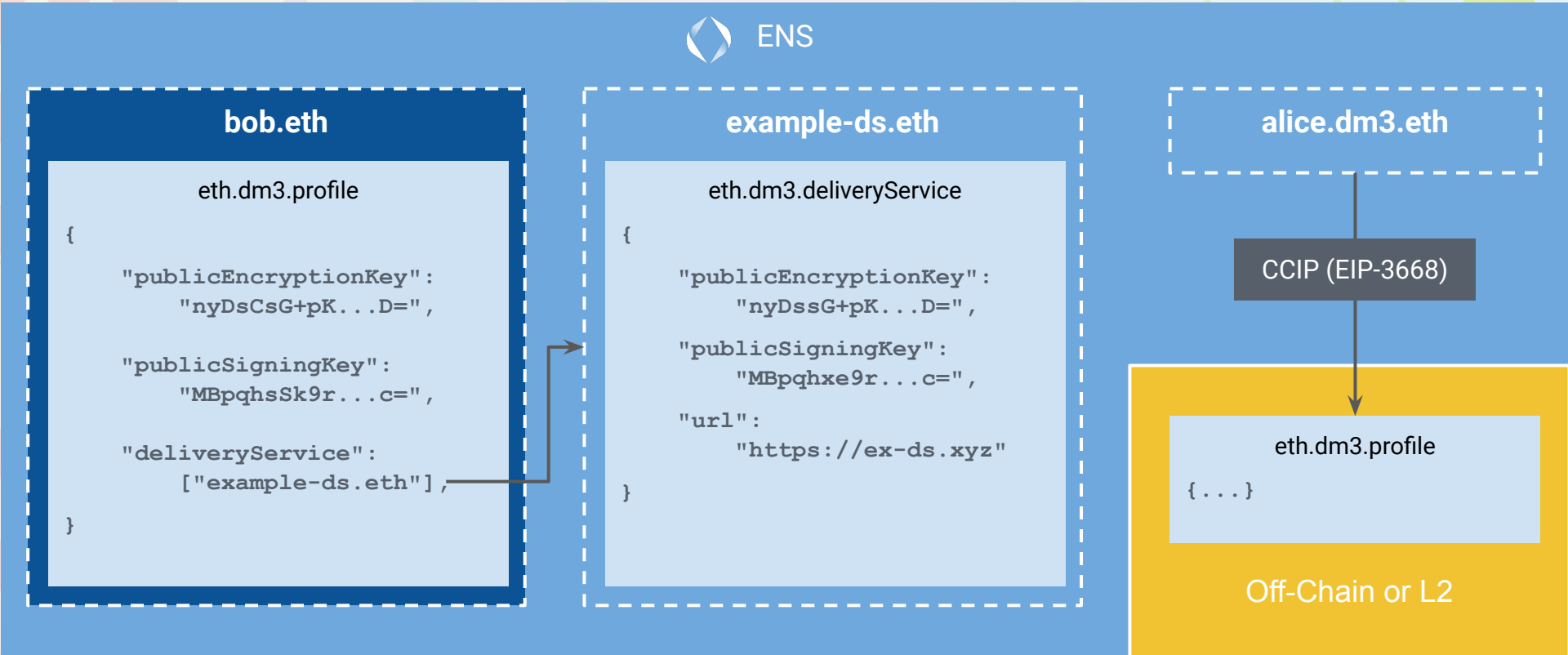
Architecture



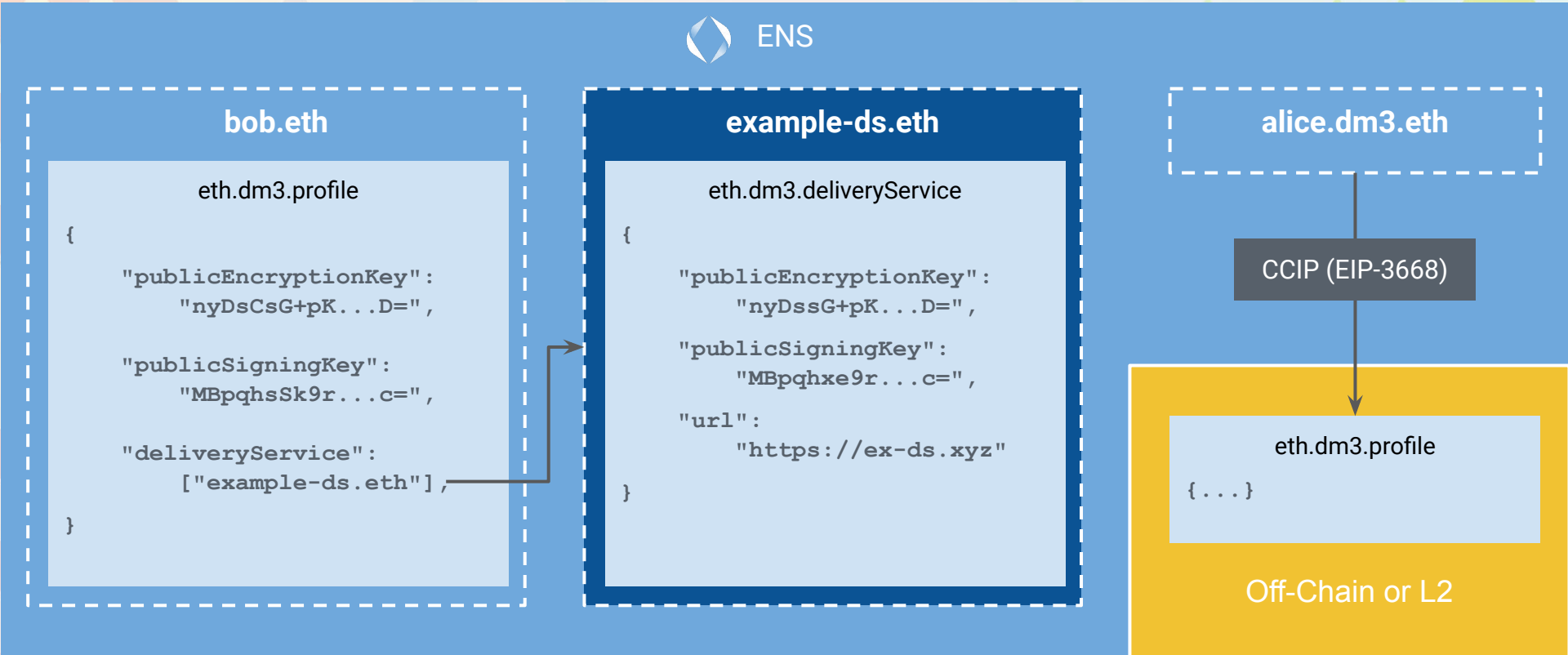
Registry


ENS
bob.eth
eth.dm3.profile
{
"publicEncryptionKey":
"nyDsCsG+pK...D=",
"publicSigningKey":
"MBpqhsSk9r...c=",
"deliveryService":
["example-ds.eth"],
}
example-ds.eth
eth.dm3.deliveryService
{
"publicEncryptionKey":
"nyDssG+pK...D=",
"publicSigningKey":
"MBpqhxe9r...c=",
"url":
"https://ex-ds.xyz"
}
alice.dm3.eth
CCIP (EIP-3668)
eth.dm3.profile
{...}
Off-Chain or L2

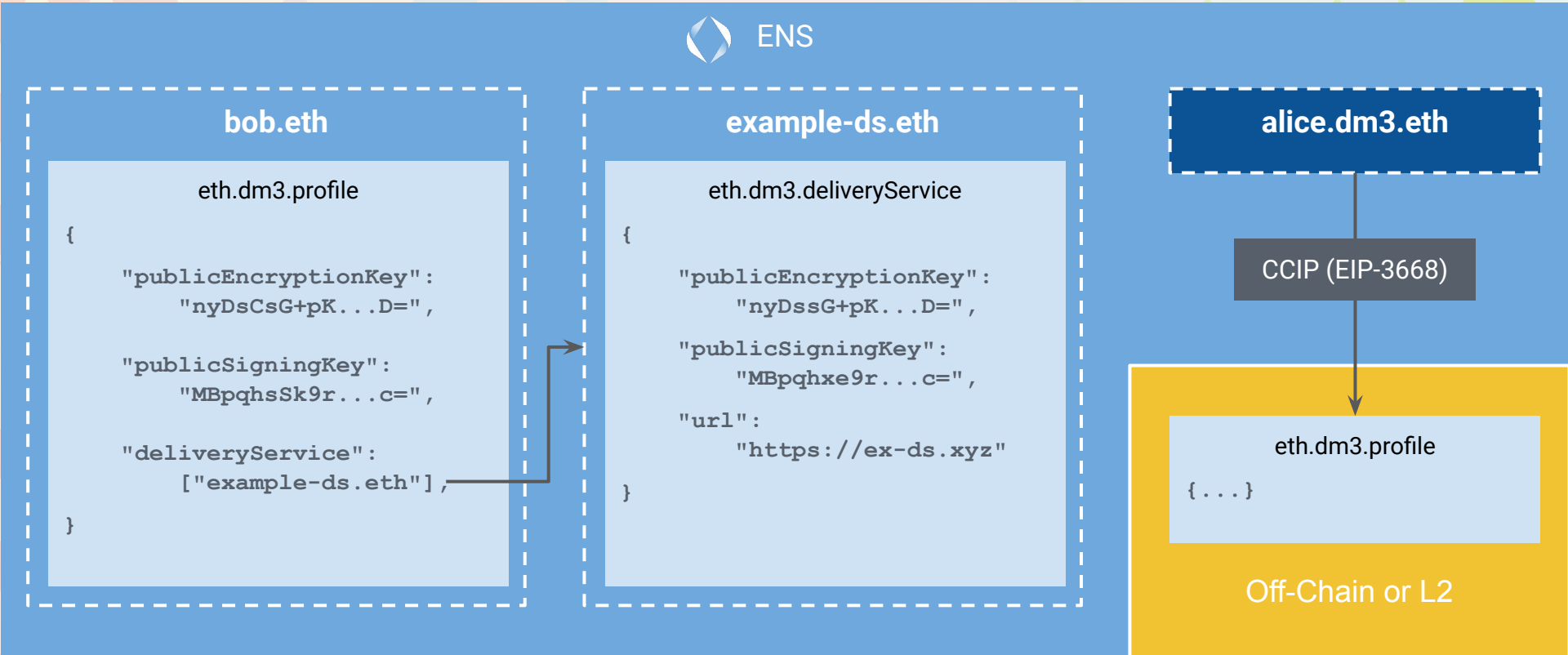
Registry


ENS
bob.eth
eth.dm3.profile
{
"publicEncryptionKey":
"nyDsCsG+pK...D=",
"publicSigningKey":
"MBpqhsSk9r...c=",
"deliveryService":
["example-ds.eth"],
}
example-ds.eth
eth.dm3.deliveryService
{
"publicEncryptionKey":
"nyDssG+pK...D=",
"publicSigningKey":
"MBpqhxe9r...c=",
"url":
"https://ex-ds.xyz"
}
alice.dm3.eth
CCIP (EIP-3668)
eth.dm3.profile
{...}
Off-Chain or L2

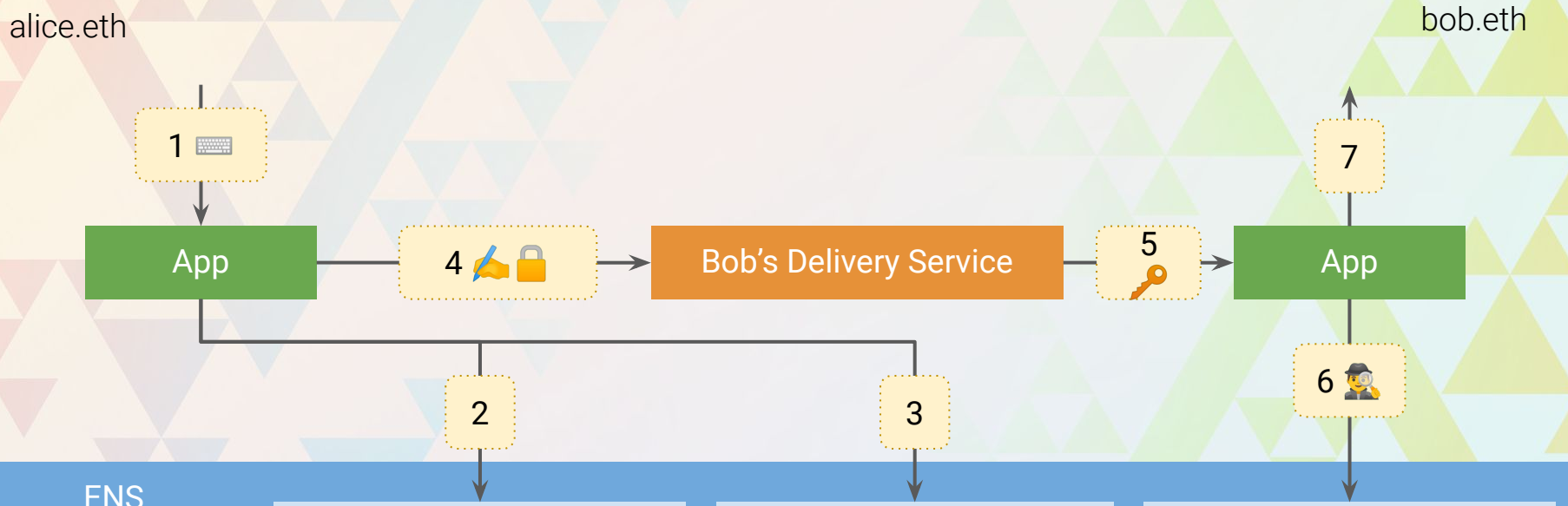
Registry


ENS
bob.eth
eth.dm3.profile
{
"publicEncryptionKey":
"nyDsCsG+pK...D=",
"publicSigningKey":
"MBpqhsSk9r...c=",
"deliveryService":
["example-ds.eth"],
}
example-ds.eth
eth.dm3.deliveryService
{
"publicEncryptionKey":
"nyDssG+pK...D=",
"publicSigningKey":
"MBpqhxe9r...c=",
"url":
"https://ex-ds.xyz"
}
alice.dm3.eth
CCIP (EIP-3668)
eth.dm3.profile
{...}
Off-Chain or L2

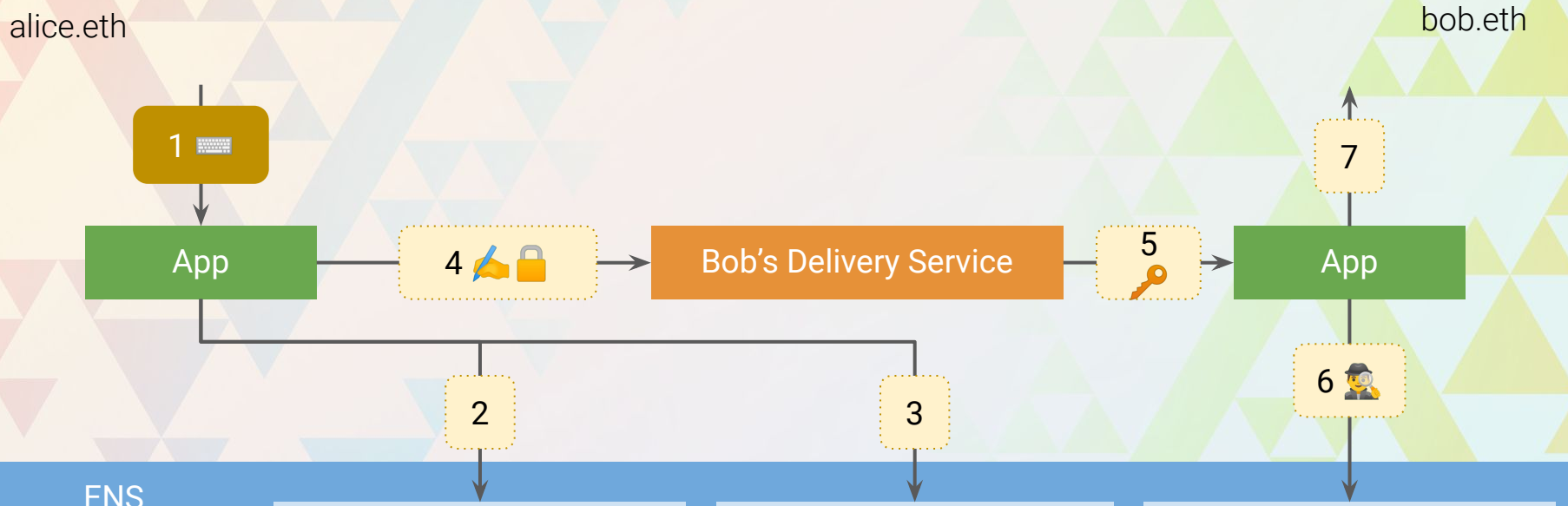
Registry


ENS
bob.eth
eth.dm3.profile
{
"publicEncryptionKey":
"nyDsCsG+pK...D=",
"publicSigningKey":
"MBpqhsSk9r...c=",
"deliveryService":
["example-ds.eth"],
}
example-ds.eth
eth.dm3.deliveryService
{
"publicEncryptionKey":
"nyDssG+pK...D=",
"publicSigningKey":
"MBpqhxe9r...c=",
"url":
"https://ex-ds.xyz"
}
alice.dm3.eth
CCIP (EIP-3668)
eth.dm3.profile
{...}
Off-Chain or L2

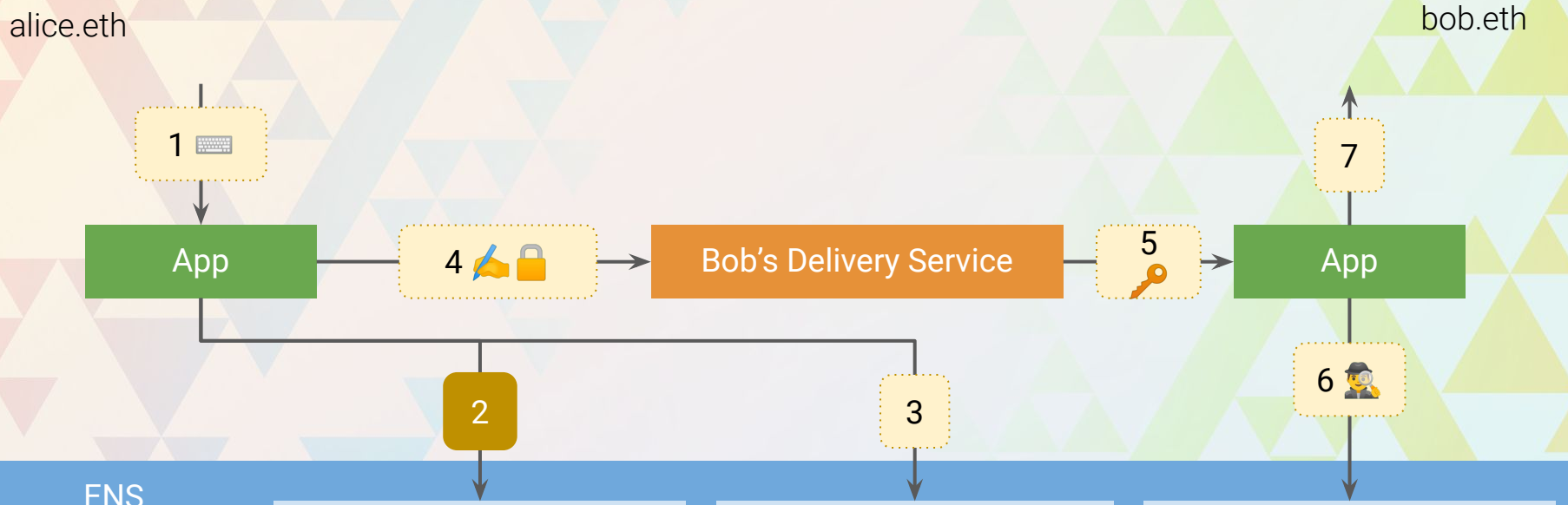
Message Delivery



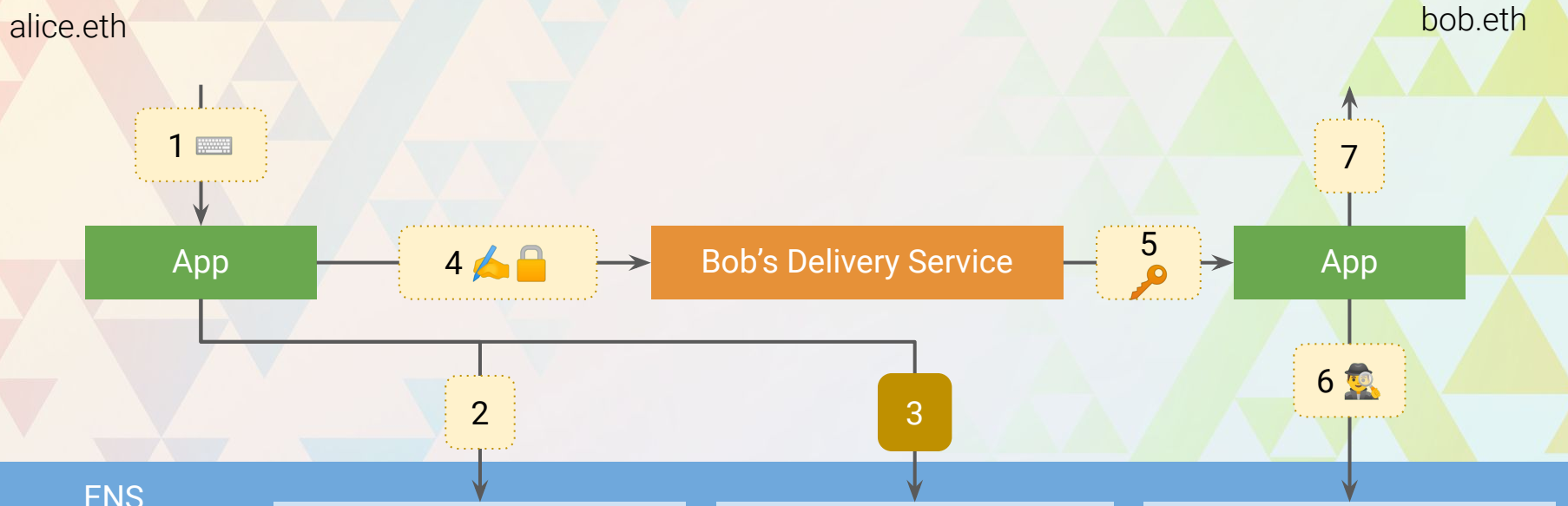
Message Delivery



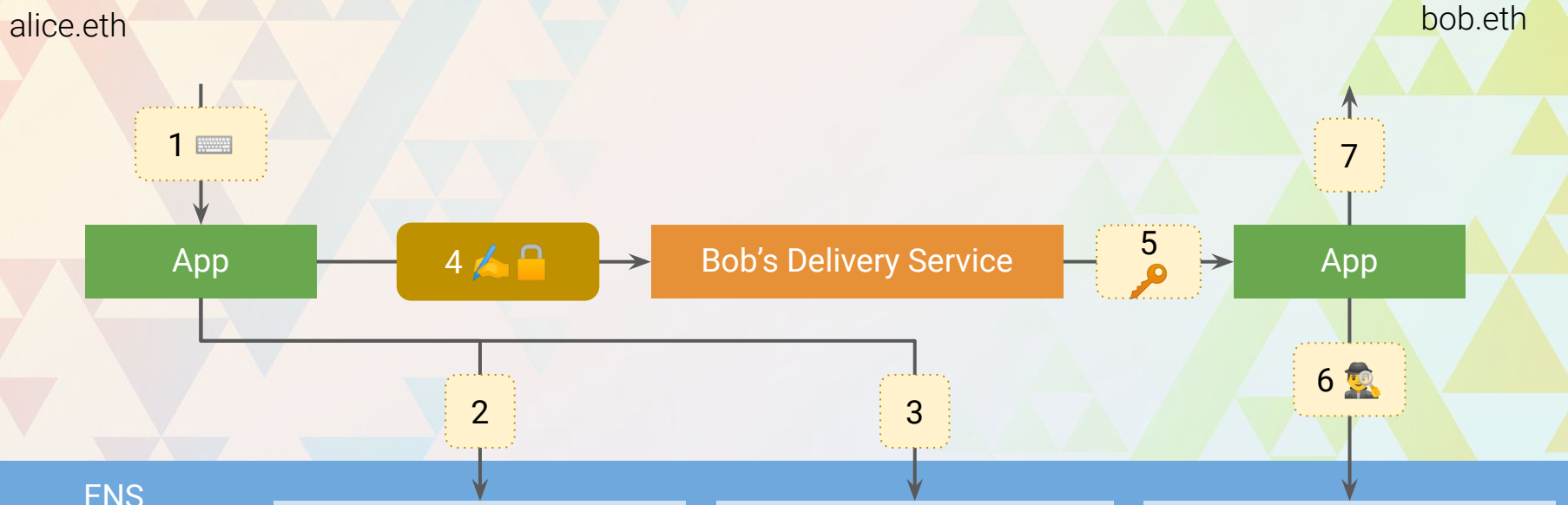
Message Delivery



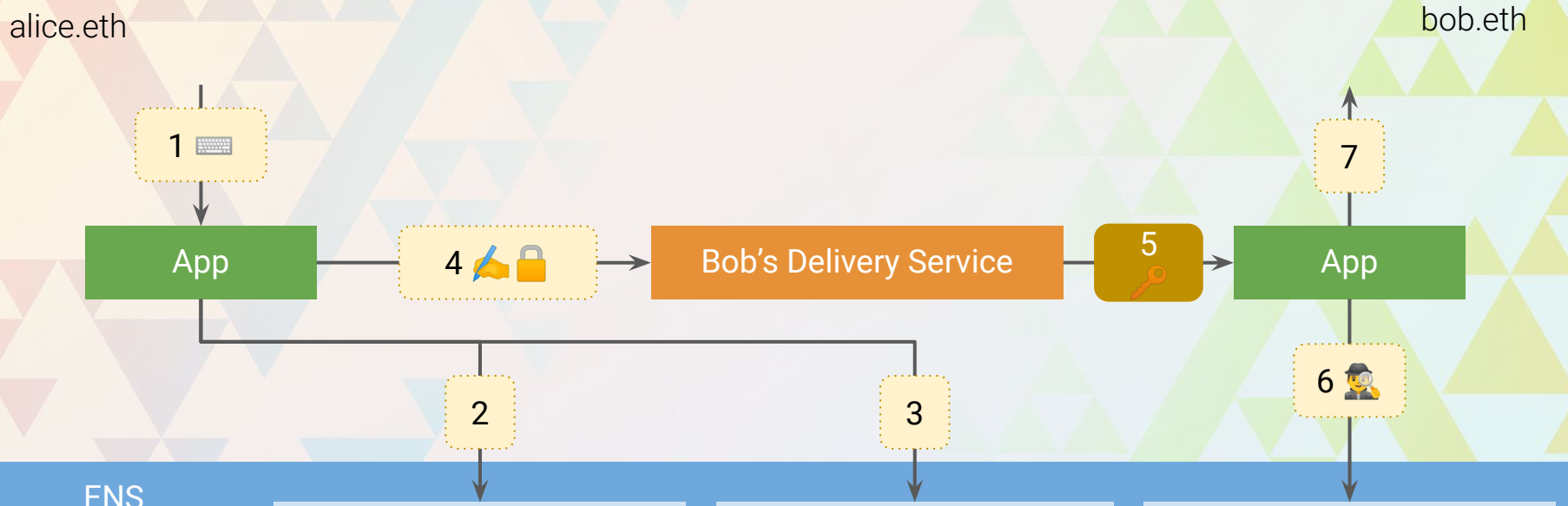
Message Delivery



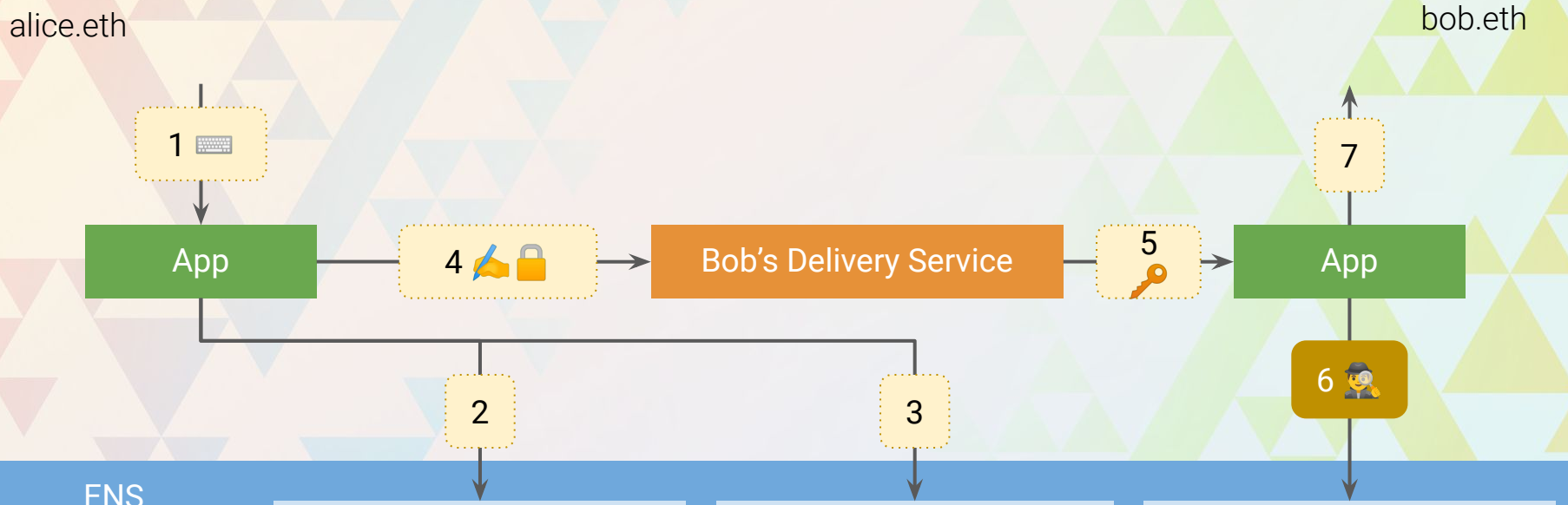
Message Delivery



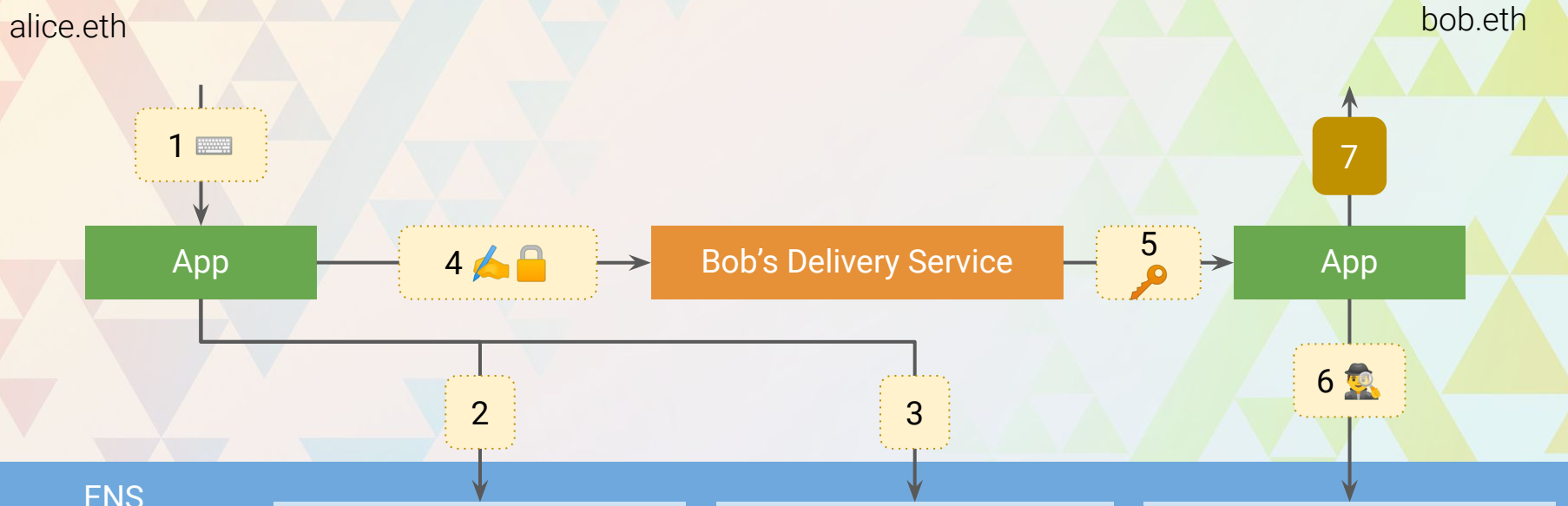
Message Delivery

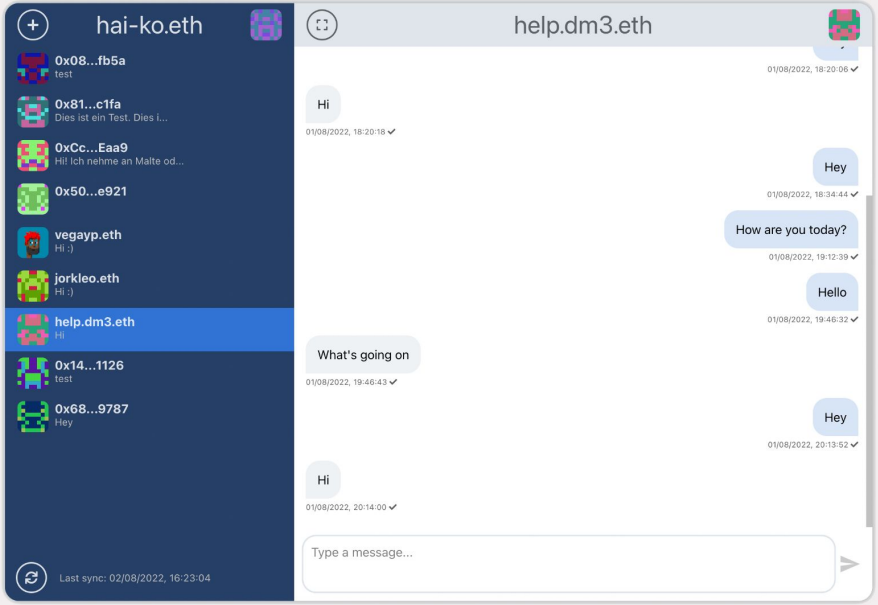


Message Delivery



Message Delivery





Live at: https://app.dm3.chat/

Reference Implementation Packages

🌐 **dm3-web:** dm3 web app

🧩 **dm3-react:** ui component library

⚙️ **dm3-backend:** delivery and storage service

📚 **dm3-lib:** basic protocol functions

All of it is open source.

corpus-ventures/dm3

Possible Protocol Extensions

- **Message Access Specification**
  Specifies how received messages on a delivery service can be accessed.
- **Message Storage Specification**
  Specifies how messages are persisted after they are delivered.
- **Public Message Feed Specification**
  Specifies how a public message feed is created and accessed.
- **Group Messaging Specification**
  Specifies a protocol extension to enable group messaging.
- **Privacy Onion Routing Specification**
  Specifies a protocol extension to enable privacy preserving onion routing.
- **Spam Protection Specification**
  Specifies additional methods, based on web3 technology, the prevent spam on the receiver's side.

Here's the roadmap.

Protocol Draft and Reference Implementation

Q3 2022

- Specification version 0.2 published
- Reference implementation

Finalize Protocol

Q4 2022

- Discussion with other protocols/apps and revision
- Finalization (version 1.0) and proposal for ENS-RFP
- Update reference implementation

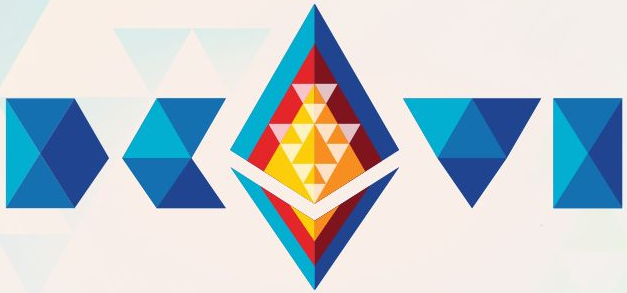
Join the specification discussion

Adoption

Q1 2023

- Interoperability
- Integration in other apps

Let us know if you want to integrate dm3



Thank you!

Heiko Burkhardt

Lead developer, corpus.ventures

heiko@corpus.ventures

@Hei_Koo