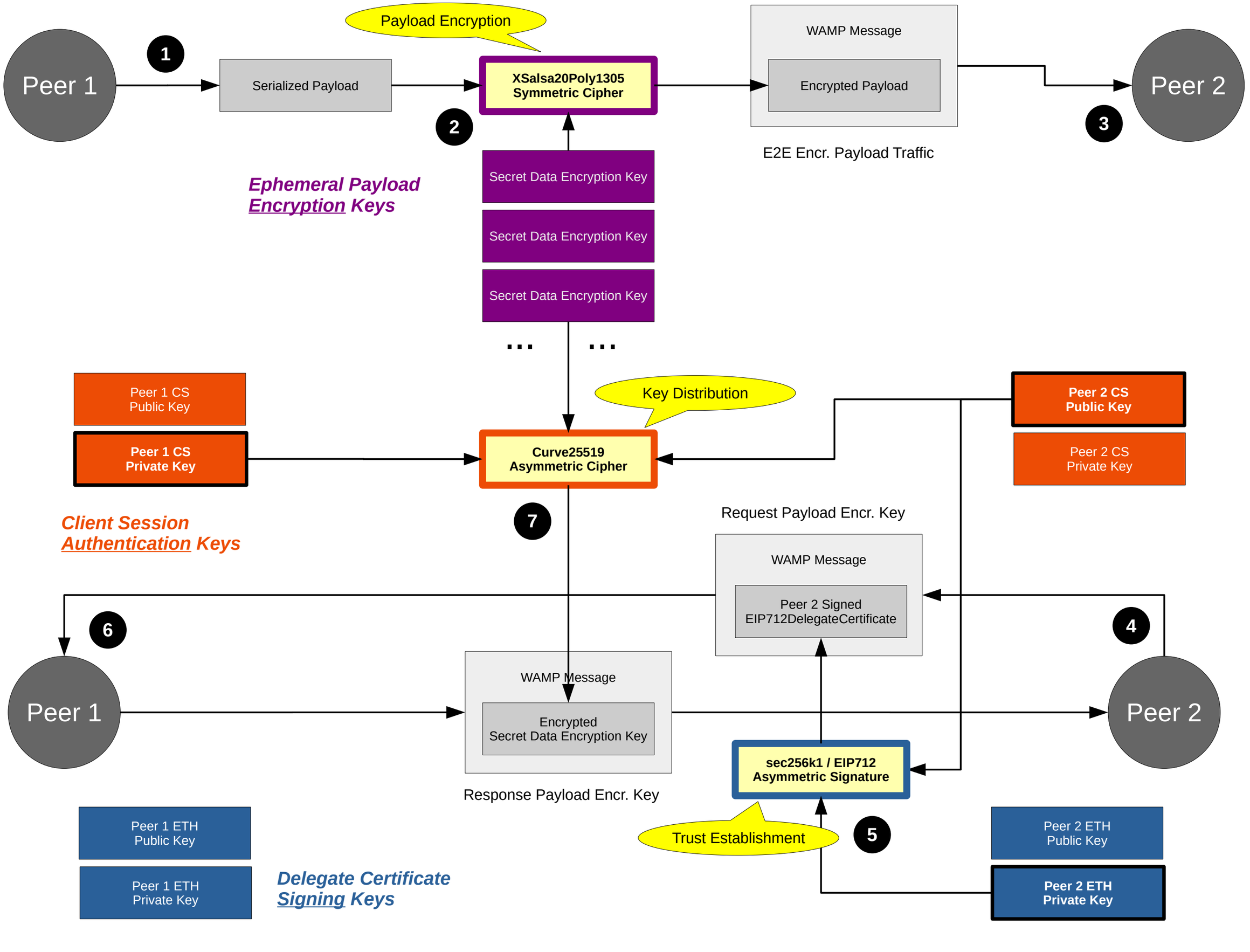
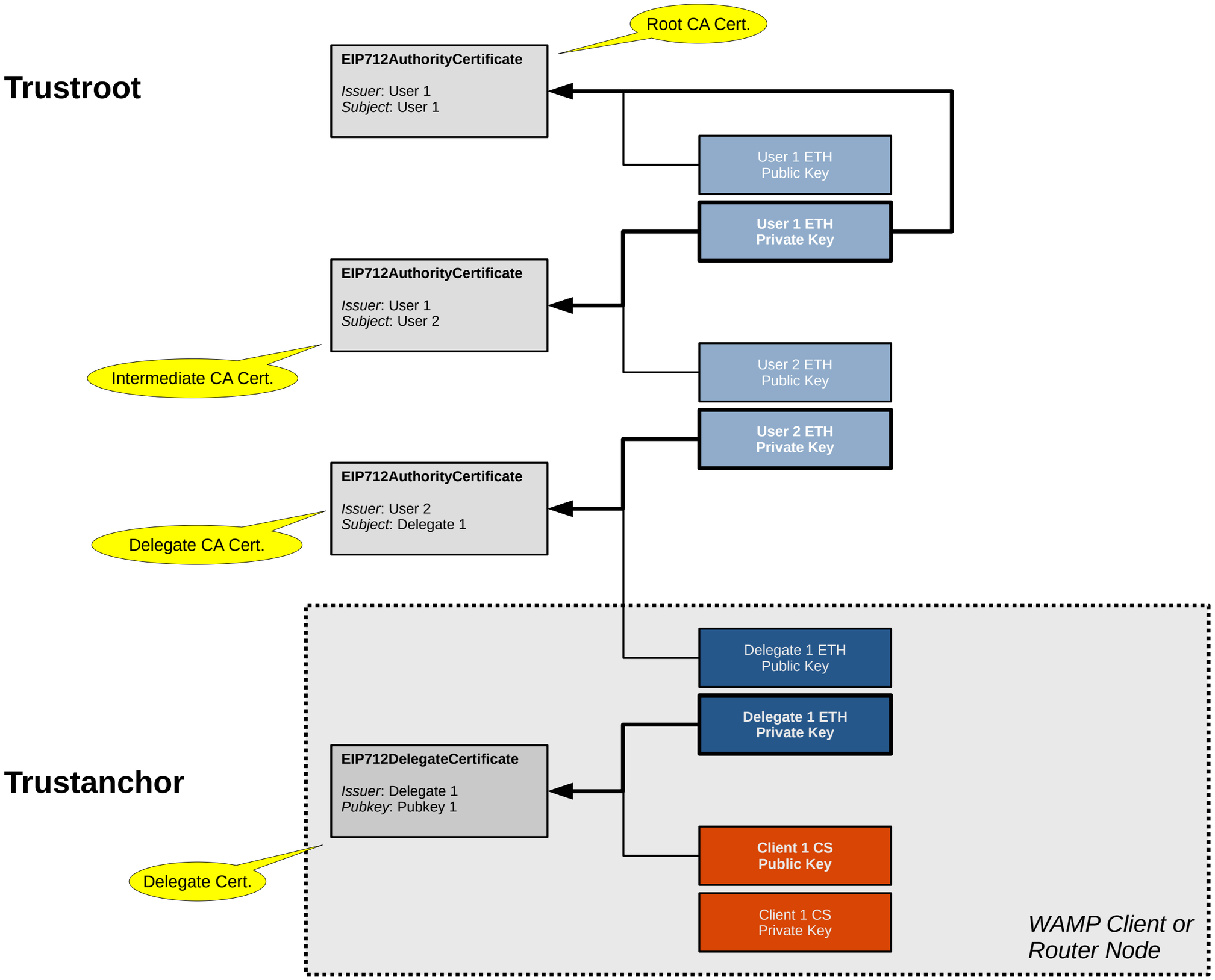

Peer 1
1
Serialized Payload
Payload Encryption
XSalsa20Poly1305
Symmetric Cipher
2
WAMP Message
Encrypted Payload
Peer 2
3
E2E Encr. Payload Traffic
Ephemeral Payload Encryption Keys
Secret Data Encryption Key
Secret Data Encryption Key
Secret Data Encryption Key
Peer 1 CS
Public Key
Peer 1 CS
Private Key
Key Distribution
Curve25519
Asymmetric Cipher
Peer 2 CS
Public Key
Peer 2 CS
Private Key
7
Request Payload Encr. Key
WAMP Message
Peer 2 Signed
EIP712DelegateCertificate
Client Session Authentication Keys
6
4
Peer 1
WAMP Message
Encrypted
Secret Data Encryption Key
Peer 2
sec256k1 / EIP712
Asymmetric Signature
Response Payload Encr. Key
Trust Establishment
5
Peer 1 ETH
Public Key
Peer 1 ETH
Private Key
Delegate Certificate Signing Keys
Peer 2 ETH
Public Key
Peer 2 ETH
Private Key

Certificate Chain



I. Standalone Trustroot

User 1 Authority Domain

EIP712AuthorityCertificate

Issuer: User 1
Subject: User 1

EIP712AuthorityCertificate

Issuer: User 1
Subject: User 2

EIP712AuthorityCertificate

Issuer: User 1
Subject: User 3

EIP712AuthorityCertificate

Issuer: User 1
Subject: Delegate A

EIP712AuthorityCertificate

Issuer: User 1
Subject: Delegate B

EIP712DelegateCertificate

Issuer: Delegate A
Pubkey: Pubkey A

EIP712DelegateCertificate

Issuer: Delegate B
Pubkey: Pubkey B

II. Shared Trustroot

User 1 Authority Domain

Realm

Owner: User 1

EIP712AuthorityCertificate

Issuer: User 1
Subject: User 1

Trust establishment, admission can be:
open, permissioned or private

EIP712AuthorityCertificate

Issuer: User 1
Subject: User 2

EIP712AuthorityCertificate

Issuer: User 1
Subject: User 3

EIP712AuthorityCertificate

Issuer: User 2
Subject: Delegate A

EIP712AuthorityCertificate

Issuer: User 3
Subject: Delegate B

EIP712DelegateCertificate

Issuer: Delegate A
Pubkey: Pubkey A

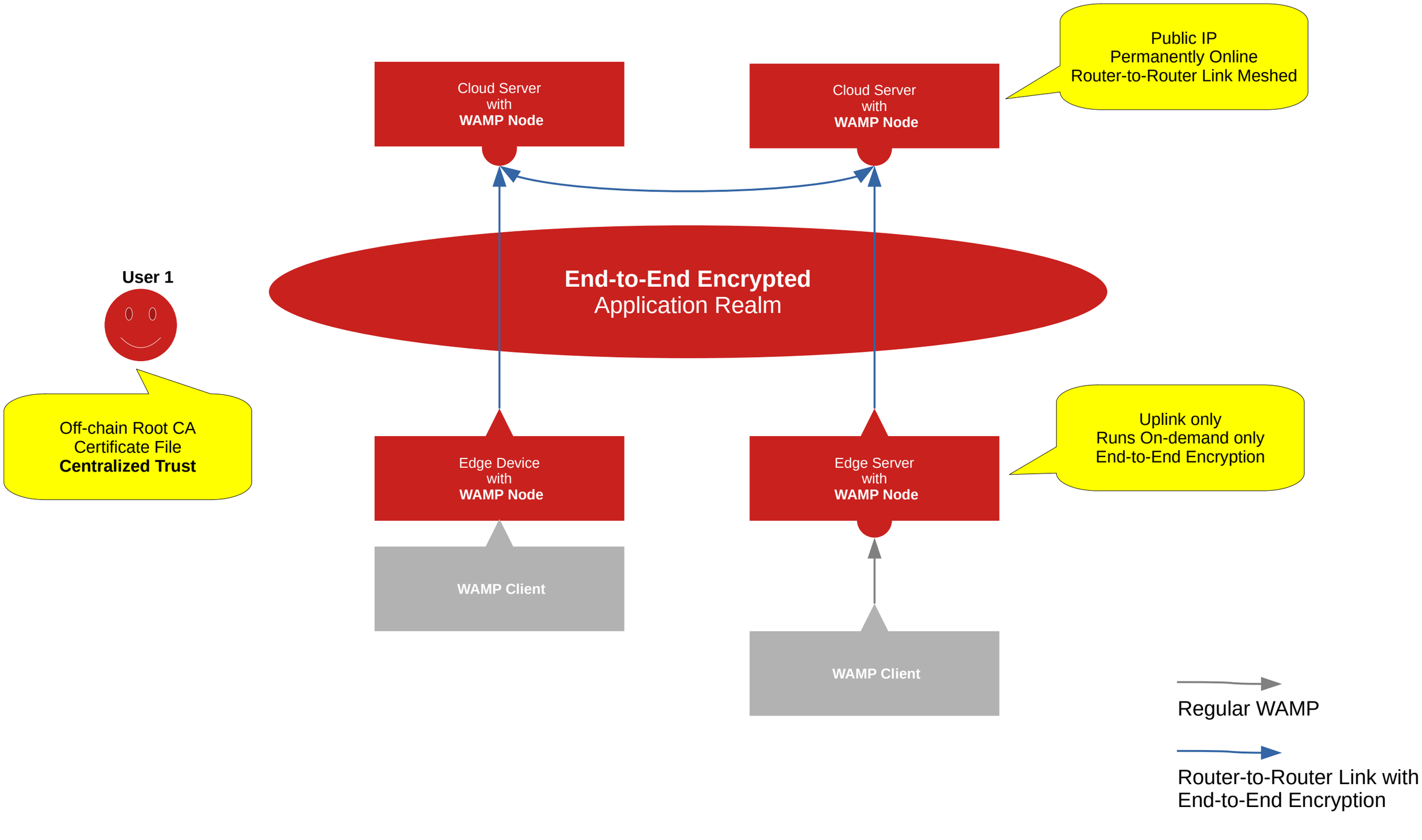
EIP712DelegateCertificate

Issuer: Delegate B
Pubkey: Pubkey B

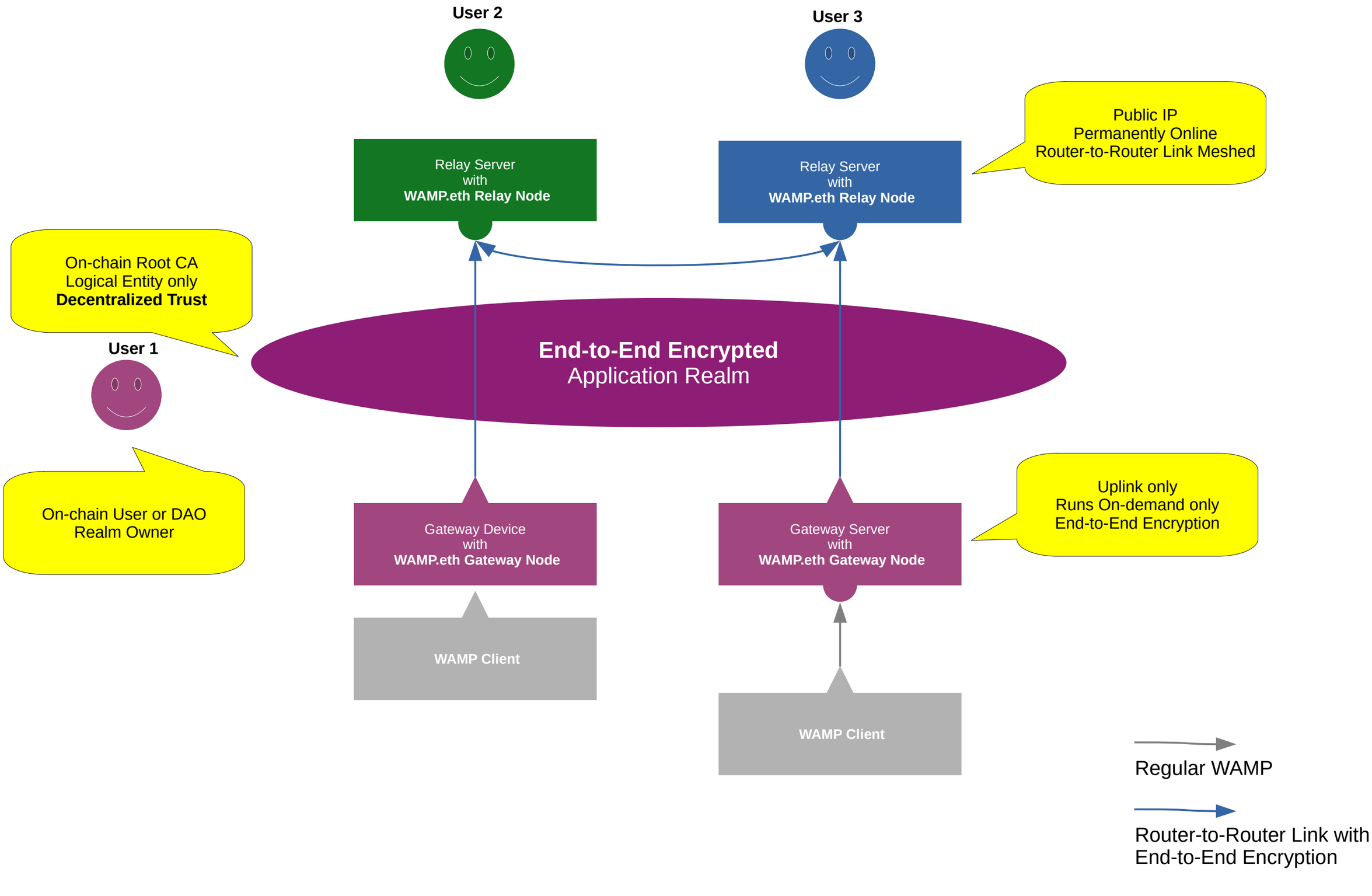
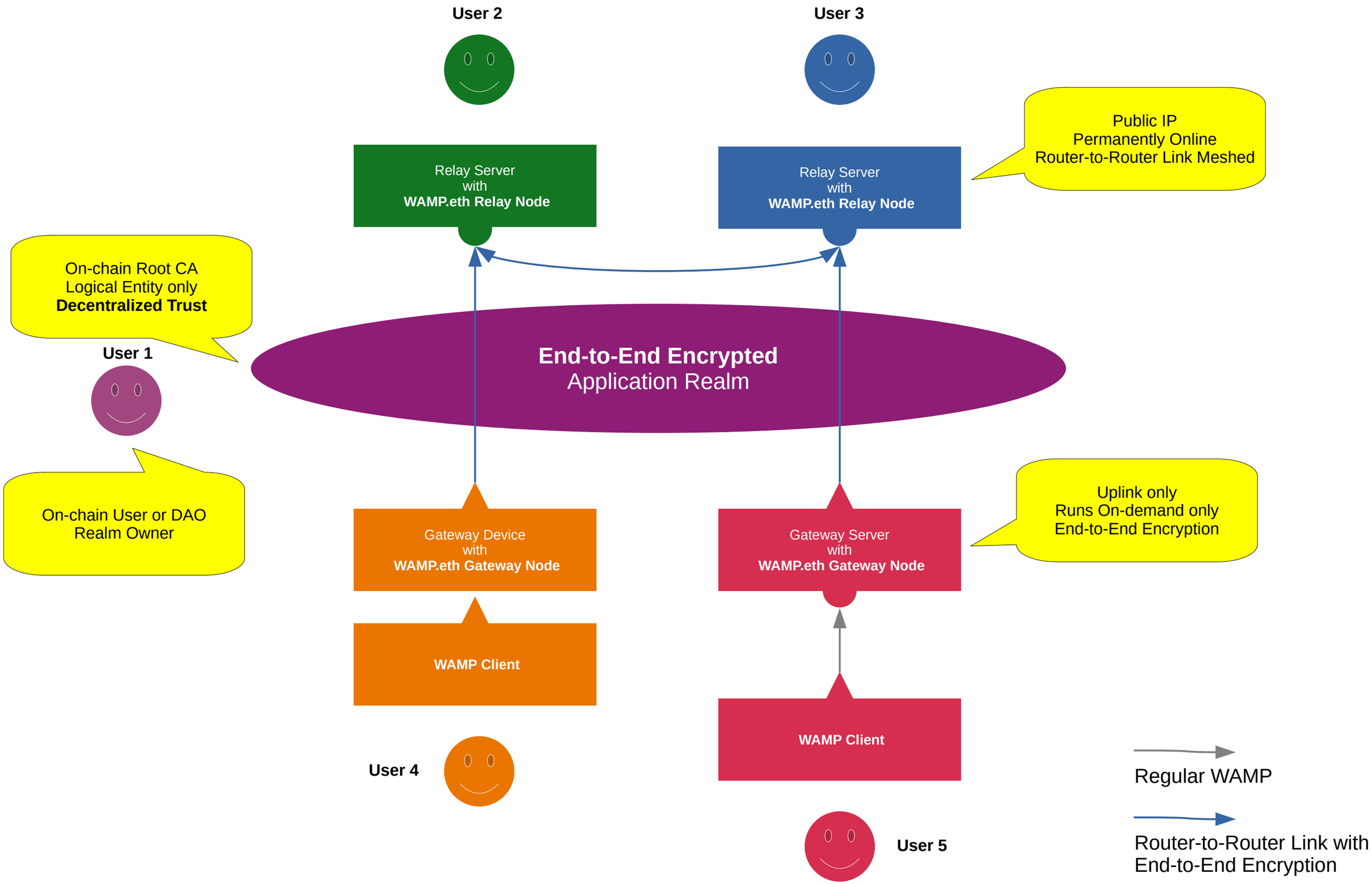
User 2 Authority Domain

User 3 Authority Domain

Scenario 0: Standalone Realm



Scenario 1: Private Realm



Scenario 2: Shared Realm