A Framework for MetaNet Based P2P IM Communication

I propose a draft of a frame work for MetaNet based P2P IM communication. Based on this framework, a MetaNet based P2P IM application or an email similar system can be easily developed. It includes two protocols, IM protocol and N protocol. IM protocol transmits massages between users. N protocol maps user names to addresses.

The IM protocol format is shown as follows.

[IM Protocol Identifier][source user name][massage type][encryption type][message][other information][time stamp][signature]

IM Protocol Identifier(IMPI)=17KUVffFHVpxueePCBzp5gJWAJsz9nx5cr

source user name is the name of who send this message. It can be mapped to an address by N protocol. The name can be replaced by an address directly.

massage type is type of the massage. For example, text, image, audio, video, html.

encryption type denotes which encryption algorithm is used to encrypt the message. For example, plain, ECC, RSA, AES.

Message is the data to be send. Message can be encrypted.

Other information. Leave it empty if no other info. Do not remove the bracket.

Time stamp is unique and increased for [IMPI][source user name][massage type][encryption type][message][other information]. Any two M protocol op_returns with the same [IMPI][source user name][massage type][encryption type][message][other information], their time stamps should be different. If two or more M protocol op_returns are the same, the first verified one is valid.

signature is the signature of [17KUVffFHVpxueePCBzp5gJWAJsz9nx5cr][source user name][massage type][encryption type][message][other information][time stamp] by the secret key of the address mapped by the [source user name]. The public key of the address must be known. The signature is used to validate the message op_return.

N protocol please refer to *a Framework for MetaNet Pages* (https://github.com/wy000000/A-Framework-for-MetaNet-Pages).

If Bob wants to send message to Alice, they should register their names by N protocol. Then the names of Bob and Alice are mapped to unique addresses respectively. Bob send a transaction to the address mapped by the name of Alice with the op_return [IMPI][Bob][massage type][encryption type][message][other information][time stamp][signature]. Alice listen to her address and receives the IM op_return. Since the IM op_return is signed by Bob's secret key, it can be verified the message comes from Bob.