Internet Financial EXchange (IFEX)

Searc

Our Proposals > IFEX Protocol >

Open Issues List

- **Cryptography**
    - Cryptographic features within IFEX are all *optional*.
        - This is because some deployment environments may not want them, eg. those that may be highly latency sensitive.
    - The IIBAN registry, which should be managed by IANA, will include cryptographic keys for IIBAN allocating institutions, which can act as an initial trust anchor for IFEX transactions.
    - Most deployments are expected to require some cryptographic features:
        - message integrity, encryption, signatures, non repudiation.
    - Given the JSON structure of the basic messages, what is the best way to integrate these features?
        - Message Integrity
            - Can be provided by signatures.
        - Non Repudiation
            - Can be provided by signatures.
        - Signatures
            - It is easier if signatures are part of the message itself.
            - It should be possible to strip the signature and verify the rest of a message against that signature.
            - Conclusion: desirable to include in IFEX messages, though optionally not as part of the core but rather an extension specification (this would necessitate an extension negotiation mechanism)
        - Encryption
            - Encrypted messages are wholly unintelligible to IFEX nodes other than the intended recipient. This makes providing meaningful feedback from such nodes difficult.
            - If a single encryption strategy is not specified (beneficial for both the flexibility and longevity of the protocol, yet impacting poorly on the potential for interoperability amongst initial adopters), then a pre-messaging link establishment phase may be required
                - This all adds complexity... not so pretty. Therefore, perhaps message encryption should be shelved as part of IFEX and deployed as a transport-layer concern using encryption that links somehow to IFEX-negotiated party identities?
- **JSON Schema**
    - Need to create/finalize JSON Schema for various parts of each message type
        - Can do by hand (error prone) or use http://www.jsonschema.net/ - though that doesn't support subschemas (referencing) which are a requirement given duplicate objects (party specifiers, etc.)
- **Link or Extension Negotation**
    - Potentially useful for defining which vocabularies (eg. Assets within specific Asset Registries), cryptographic features, etc. may be supported
    - Could occur within RFQ/QUO messages or within an as yet undefined, still-earlier message type `HELO` (sent when initiating an IFEX Link) .. though another message-passing stage would likely harm latency

Comments

You do not have permission to add comments.