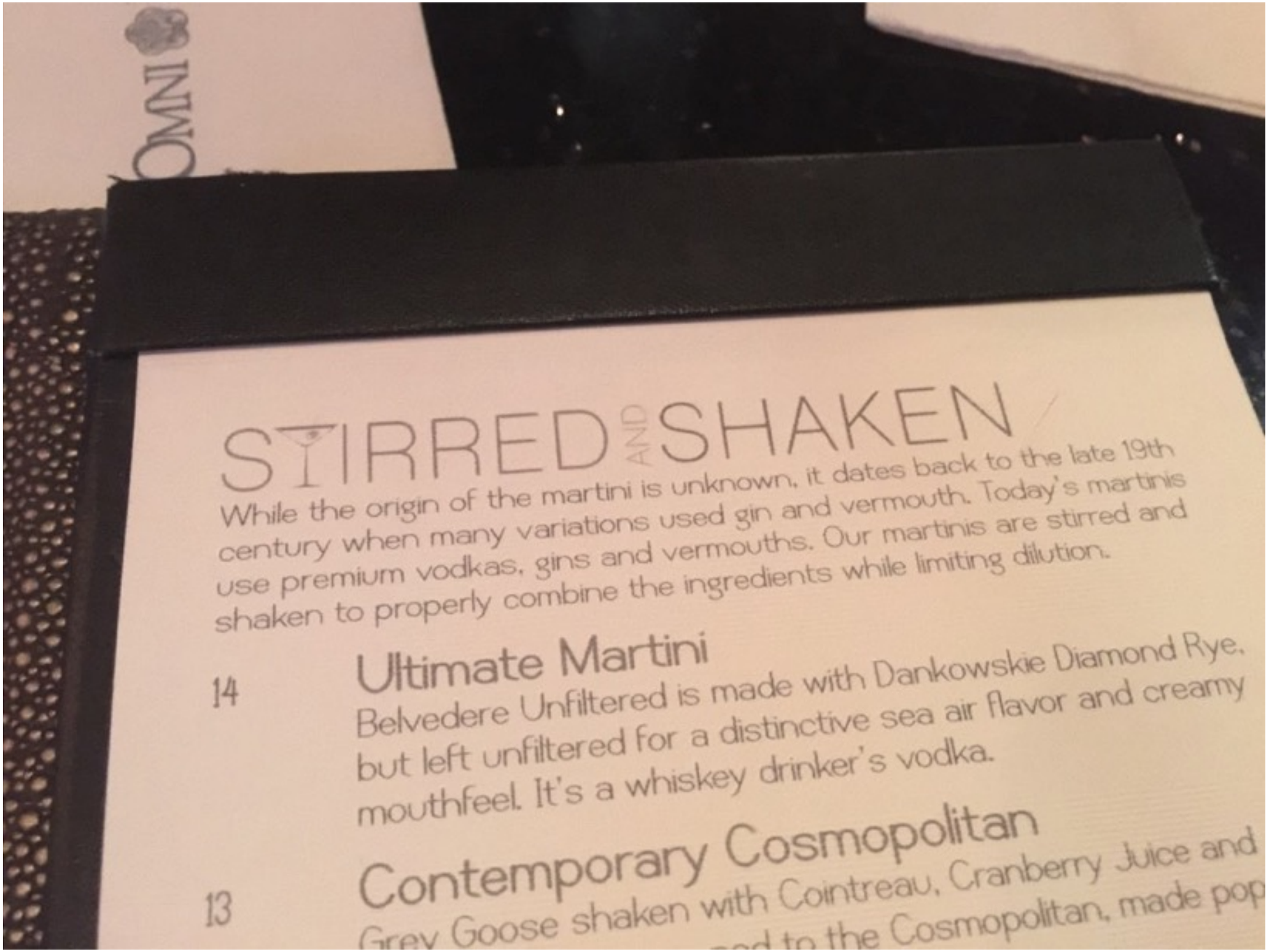
verified token

chris wendt



wednesday evening at the omni in DC

overview

- expands and changes some assumptions from 4474bis
- focus on the token and the security and digital signature, use cases, certificate infrastructure and SIP signaling specific specification would follow
- allow for flexible implementation potentially using multiple signatures/tokens and certificate associations or multiple actors along the path
- allow flexibility from validation of authorized routing agent vs authorized identity
- with separation of the token to signaling specific attributes, additional benefit, potential applicability to future RTC applications and signaling protocols

token overview

- tokens have become a popular and convenient way to encapsulate a set of information with a cryptographic hash or signature for various internet applications

- JWT is one canonicalization that has emerged and has had a lot of support from both usage and implementation availability.

- It provides a flexible framework to support many digital signatures and cryptographic algorithms

- It also defines a flexible “claim” framework which allows for JSON key value pairs that consist of both standard keys as well as application defined customized keys.

token header

- Within the JWT framework, the JWS token uses a JOSE header to define the token type as well as the cryptographic algorithm used.

- Example:
```
{ "typ":"JWT",
  "alg":"RS256"}
```

- The suggestion is to use digital signatures related to X.509 PKI with the following crypto algorithms

- RS256 or ES256

- but could include RS384, RS512, ES384, and ES512

token claim

- JWT defines a set of claims as well as supports custom claims

- Verified token is required to include the following standard claims

"**iss**" - required - principal that issued and signed the JWT. This is an https URL with the domain of the authorized originator of the token (e.g. "https://pstn.example.com)
"**jti**" - required - unique identifier of the JWT, useful for both tracking and avoiding replay of JWT
"**iat**" - required - issued at, time the JWT was issued, used for expiration

- Verified token is required to include the following custom claims

"**orig**" - required - the identity claimed by the originating party. (e.g. for SIP, the FROM or PAI associated e.164 telephone number, TEL or SIP URI) This MAY be in URI format as defined in [RFC3986] or an application specific identity string.
"**term**" - required - the terminating identity claimed by the originating party. (e.g. for SIP, the TO associated e.164 telephone number, TEL or SIP URI) This MAY be in URI format as defined in [RFC3986] or an application specific identity string.

token claim example

- Example claim would be as follows:

```
{ "orig":"+12155551212",
  "term":"sip:+12155551213@example.com",
  "iss":"https://pstn.example.com",
  "jti": “FAhNaPk0onffyJvykJZC2A==",
  "iat": 1443208345 }
```

token signature

- The JWS signature would fully correspond to the specification
- Both the header and claim are signed and the signature is placed at the end of the token and is Base64 encoded per spec.
- Basic JWT compact format “header.claim.signature”
- The “iss” claim would be used to link to the domain associated with X.509 public key certificate

security

- There is a number of required claims that must be associated with signaling specific fields for avoidance of cut and paste and replay types of attacks

- These include:

"iat" claim should closely correspond to a date/time the message was originated. It should also be within a relative delta time that is reasonable for clock drift and transmission time characteristics associated with the application using the verified token.

"jti" claim could be used to exactly correspond to a unique identifier (e.g. INSIPID for SIP)

"term" claim is included to prevent the ability to use a previously originated message to send to another terminating party

SIP signaling

- Currently the thought is to use similar SIP header association claims as 4474bis
- Token(s) would be carried in Message body as a multi-part MIME, RFC5621

Signature associations

- General framework build around validating both:
  - authorized routing agents signing INVITES over NNI
  - device or telephone number “special” use case where devices have certificates or for example “notification” services that are authorized to vouch for authenticity of the call to guarantee delivery.
- Likely first case would always be used, and second would be used for special cases.
- Additional use cases will likely be identified, but the important thing is to provide a simple mechanism to extend the claims to support new use cases.