Signed JWK Sets

Richard Barnes, Sharon Goldberg
Normal JWT lifecycle

What if JWK Set is unavailable?
- Key has been rotated
- Server is down

Issue

JWT
"Iss": "https://issuer.example"

GET /.well-known/...
Host: issuer.example
Normal JWT lifecycle

Issue

Signed JWK Set
“x5c”: [...]/* issuer.example */ [...]  
“iss”: “https://issuer.example”
“keys”: [...]/* JWK Set */

JWT
“iss”: “https://issuer.example”

No validate-time dependency
Not a new idea ... except!

Signed JWK Set
“x5c”: [... /* issuer.example */ ...]
“iss”: “https://issuer.example”
“keys”: [... /* JWK Set */ ]

JWT
“iss”: “https://issuer.example”

Issue

Proof of authority for domain