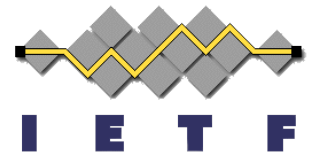


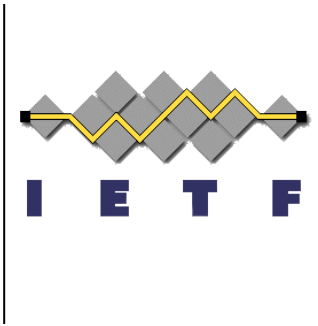
# JWK for PKIX Certificates

defining a JSON Web Key object to wrap PKIX certificate chains and/or individual certificates

**JSON Web Key (JWK) for PKIX Certificates**  
a.k.a. “the useful bag”  
**draft-miller-jose-pkix-key-01**

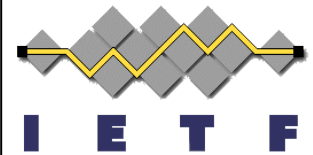
Brian Campbell  
Matt Miller  
IETF #86, March 2013





## Why Bother?

- There are some applications of JWK where it is highly desirable to have the additional security characteristics provided by PKIX within the context of JWK/JOSE
- There is already existing and widespread tool support for working with X.509 certificates

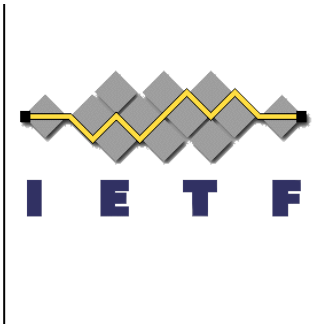


# What is it?

- A new JWK Key Type” representing a PKIX/X.509 certificate chain (or single certificate)
  - kty: PKIX
  - x5c: a JSON array of strings, each of which is base64 encoded DER certificate

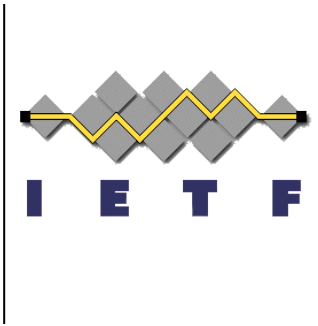
```
{ "keys": [
  { "kty": "PKIX",
    "x5c": [ "MIIE3jC...sXBTWVU+4=",
            "MIIE+zC...85j09VZw==",
            "MIIC5zC...y8W9ViH0Pd" ],
    "use": "sig",
    "kid": "somekeyid" } ] }
```

```
{ "keys": [
  { "kty": "RSA",
    "use": "sig",
    "kid": "1b94c",
    "n": "vrj0...unqsIo1vQ",
    "e": "AQAB" },
  { "kty": "PKIX",
    "use": "sig",
    "kid": "1b94c",
    "x5c": [ "MIIDQj...IVfOWA==" ] }
] }
```



# Where It's Useful

- OpenID Connect
  - Helped simplify the model for publication and rotation of public keys
- draft-miller-xmpp-posh-prooftype
  - Helped simplify the model for publication and rotation of service credentials



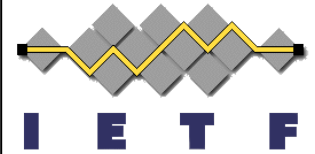
# Other ways to skin the cat

- x5c as a first order JWK member that serves as an alternative representation of the same key

```
{ "keys": [  
  { "kty": "RSA",  
    "use": "sig",  
    "kid": "1b94c",  
    "n": "vrj0...unqsIo1vQ",  
    "e": "AQAB",  
    "x5c": [ "MIIDQj...IVfOWA==" ] }  
]}
```

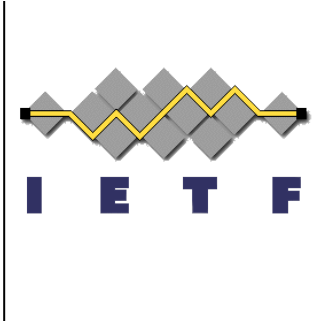
- x5u
- Others...?

# Detractors to the useful bag



- “... it turns JWK into a bag that is no longer strictly holding keys. It now holds PEM encoded certificate chains” - Tony Nadalin
- “... x5u doesn't fit in JWK at all. It'd stick out like a turd in a punch bowl.” – Me

# What's Next?



- Kill it?
- Explore alternatives?
- Consideration as a JOSE WG document?