JOSE Security
Parameters Index
Alice and Bob agree on kid -> key

- alg: "A256KW"
- enc: "A128CBC+HS256"
- kid: "dHJ5c3Rlcm8"
- key: [...] content: [...]

- alg: "A256KW"
- enc: "A128CBC+HS256"
- kid: "dHJ5c3Rlcm8"
- key: [...] content: [...]

"kid"
IPsec

IKE negotiation (establish SA)

SPI: 5e6e6641
IV: ef20fc54
[encrypted packet]

SPI: 5e6e6641
IV: 7adaa97a
[encrypted packet]
PRE-NEGOTIATE
ALL THE PARAMETERS
Save on octets!

**JWS**

```
{"typ":"JWS","alg":"HS256","kid":"dHJ5c3R1cm8"}
```

base64url: 67B

```
{"typ":"JWS","spi":"dHJ5c3R1cm8"}
```

base64url: 45B

33% savings!

**JWE**

```
{"typ":"JWE","alg":"RSA-OAEP","enc":"A256GCM","kid":"dHJ5c3R1cm8"}
```

base64url: 89B

```
{"typ":"JWE","spi":"dHJ5c3R1cm8"}
```

base64url: 45B

49% savings!