



CREDIT: COURTESY OF DREAMWORKS ANIMATION

No, SHREQ is not an adorable ogre,  
it is rather a *boring Web Security System*

Anders Rundgren, IETF-104, Prague

## *Problem Statement:*

HTTP requests are used *Everywhere*

However, there is still no *Standard*  
for digitally signing HTTP requests

### “Rolling their own”

- FAPI (Financial API)
- Open Banking UK
- Open Banking France\*
- Amazon.com
- Other?

\* Or are using schemes have not reached standards status

# SHREQ – Signed HTTP Requests

*Signs these items:*

- HTTP URI
- HTTP Method
- HTTP Body (if applicable)
- Optional: Additional HTTP Headers

*Other characteristics:*

- JSON Oriented (for POST/PUT/PATCH)
- Signed Requests are Serializable
- Cryptography builds on JOSE-JWS

# SHREQ uses JSON Canonicalization

```
{  
  "statement": "Hello Si\u0067ned World!",  
  "otherStuff": [2e+3, true]  
}
```

"On the wire"



What the crypto sees



```
{"otherStuff":[2000,true],"statement":"Hello  
Signed World!"}
```

I-D: <https://tools.ietf.org/html/draft-rundgren-json-canonicalization-scheme-05>

# Yeah, the mandatory sample...

POST /transact/pay HTTP/1.1

Host: example.com

Content-Type: application/json

Content-Length: 1234

```
{  
  "payme": "100000000000.99",  
  "currency": "USD",  
  "$req.uri": "https://example.com/transact/pay",  
  "$req.mtd": "POST",  
  "$req.jws": "eyJhbGciOiJI..VHVItCBCb849imarDt"  
}
```

# SHREQ is worth a shot in the IETF?

<https://cyberphone.github.io/ietf-signed-http-requests>