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 all items forming an HTTP request:

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

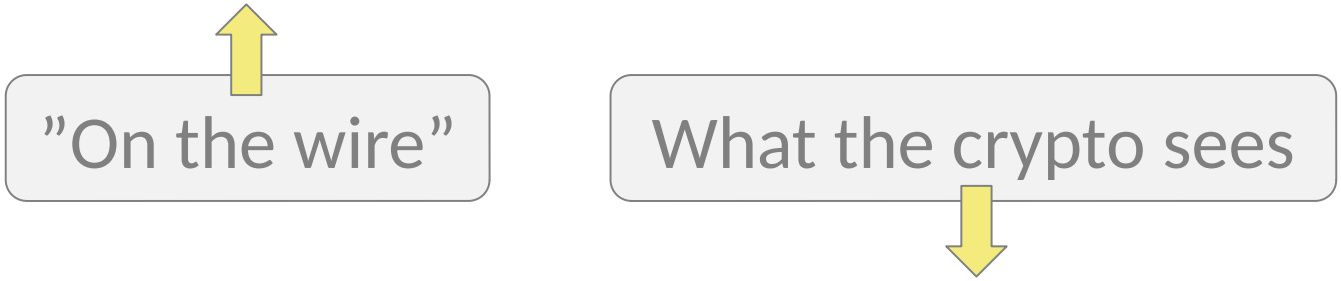
\+ Time Stamp

Other notable 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]
 }
```




```
{"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": "10000000000.99",
   "currency": "USD",
   ".secinf": {
      "uri": "https://example.com/transact/pay",
      "mtd": "POST",
      "iat": 1551361123,
      "jws": "eyJhbGciOiJI..VHVItCBCb849imarDt"
   }
}
```

SHREQ is worth a shot in the IETF?

https://github.com/cyberphone/ietf-signed-http-requests

It’s Alive…

POST using CURL:

```
curl -H content-type:application/json -d "{\"name\":\"Jane Smith\",\"profession\":
\"hacker\",\".secinf\":
{\"uri\":\"https://mobilepki.org/shreq/preconfreq\",\"iat\":1552152336,\"jws\":\"e
yJhbGciOiJFUzI1NiJ9..OfeBIeps4uzBdTksDLuTtYGR2Kip_1fNsx2AmIquRgqkcbo3SuZ7ea67YdHan
sxYCs0pAtMVP4f_Q_GMGubTyg\"}}" https://mobilepki.org/shreq/
preconfreq
```

GET using a Browser:

https://mobilepki.org/shreq/preconfreq/456?.jws=eyJhbGciOiJFUzI1NiJ9.eyJodHUiOiJqbFM2RzJiUk12LTZNalowNENVUUx0S25UNll6RWdkS2k1VE5LVGlnODd3IiwiaWF0IjoxNTUyMTUyMzM2fQ.1uaHMruRL9pW05UTKOjsH6atp4BC6RVCVpZFVPflBSGbAxeWmtmH_nZe1xRnHLr0jVRoY0HnDBrueW4LhQLTfA