Selective Content Disclosure using Zero-Knowledge Proofs

Nikos Fotiou and George Xylomenos

Background of this talk

- D. Boneh, X. Boyen, H. Shacham "Short Group Signatures," In Annual International Cryptology Conference, 2004 (https://iacr.org/archive/crypto2004/31520040/groupsigs.pdf)
- J. Camenisch , M. Drijvers, A. Lehmann "Anonymous Attestation Using the Strong Diffie Hellman Assumption Revisited," TRUST 2016 (https://eprint.iacr.org/2016/663.pdf)

Background of this talk

```
CFRG - Crypto Forum Research Group
IETF 114 in Philadelphia

Monday, July 25, 2022, 10:00-12:00 (UTC - 4)

Meetecho: https://meetings.conf.meetecho.com/ietf114/?group=cfrg&short=&item=1
Jabber: cfrg@jabber.ietf.org
Notes: https://notes.ietf.org/notes-ietf-114-cfrg

Chairs:  Stanislav Smyshlyaev, Nick Sullivan and Alexey Melnikov

10:00 - Chairs' update.

10:10 -  Tobias Looker, "The BBS Signature Scheme" (15+5 mins)
        https://identity.foundation/bbs-signature/draft-bbs-signatures.html

10:30 - Deirdre Connolly, “Two-Round Threshold Schnorr Signatures with FROST” (10+5 mins)

10:45 - Chris Wood, “Key Blinding for Signature Schemes” (10+5 mins)

11:00 - Frederic Jacobs, “RSA Blind Signatures” (10+5 mins)

11:15 - Bjoern Haase, "CPace" (5+5 mins)

11:25 - Sofia Celi, "Post-Quantum NIST Process" (10+5 mins)

11:40 - Bas Westerbaan, "Kyber" (5+5 mins)
        https://github.com/bwesterb/draft-schwabe-cfrg-kyber

11:50 - AOB
```

Background of this talk

SECOND

https://mm.aueb.gr/projects

Background of this talk

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

domx
IOT TECHNOLOGIES

Pleg.ma
Labs

NGI DAPSI

https://mm.aueb.gr/projects

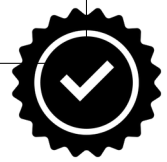
Motivation

- Caching of data on which computations can be made (vs bulk data)
  - Relational databases
  - Key-value encoded data streams
  - Append-only logs of a DL
  - Distributed social networks
  - …
- Selective disclosure without violating integrity
  - … and without sharing secret keys

Motivating example

/measurements/EA32B


```
{
   "deviceid":"22A",
   "temperature":"30",
   "humidity":"40%"
   "metadata"{
      "created" :"1 Jun. 2022",
   }
}
```

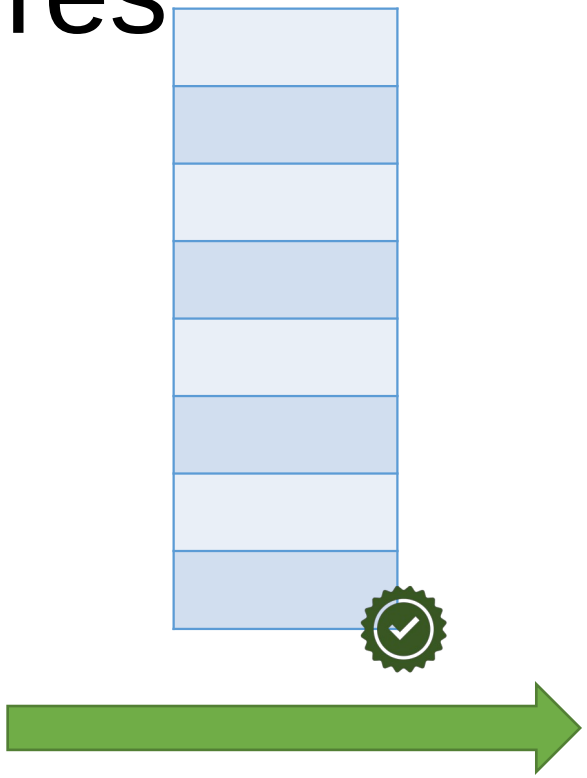



From "/measurements/EA32B" I want "temperature" from "device 22A"

...

Traditional digital signature schemes

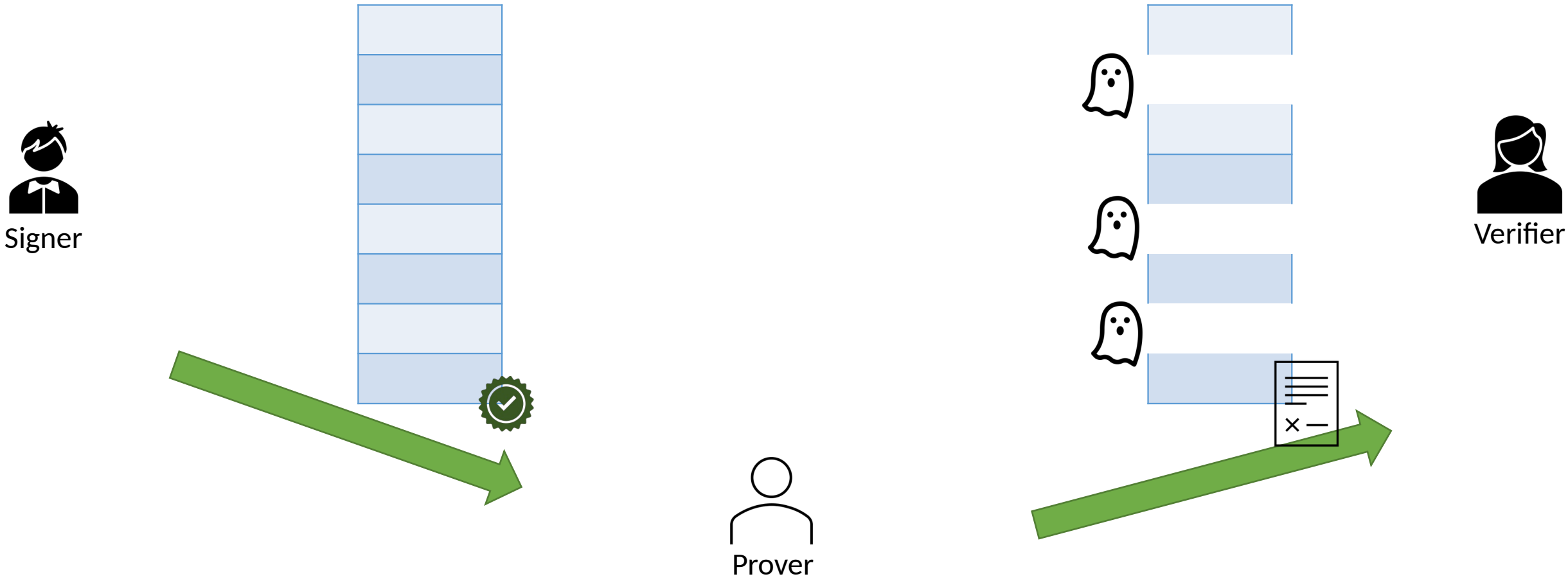
Group signatures



Signer

Verifier

Selective disclosure using ZKPs



Transforming JSON data into "group of messages"

- Canonicalization*

```
{
   "deviceid":"22A",
   "temperature":"30",
   "humidity":"40%"
   "metadata"{
      "created" :"1 Jun. 2022",
   }
}
```

"deviceid":"22A"
"temperature":"30",
"humidity":"40%"
"metadata.created":"1 Jun. 2022"

* V. Kalos, G.C. Polyzos "Requirements and Secure Serialization for Selective Disclosure Verifiable Credentials", IFIP Sec 2022

"Framing" JSON data

```
{
   "deviceid":"",
   "temperature":"",
    "metadata"{
      "created" :"",
   }
}
```

```
{
   "deviceid":"22A",
   "temperature":"30",
   "humidity":"40%"
   "metadata"{
      "created" :"1 Jun. 2022",
   }
}
```

```
{
   "deviceid":"22A",
   "temperature":"30",
   "metadata"{
      "created" :"1 Jun. 2022",
   }
}
```

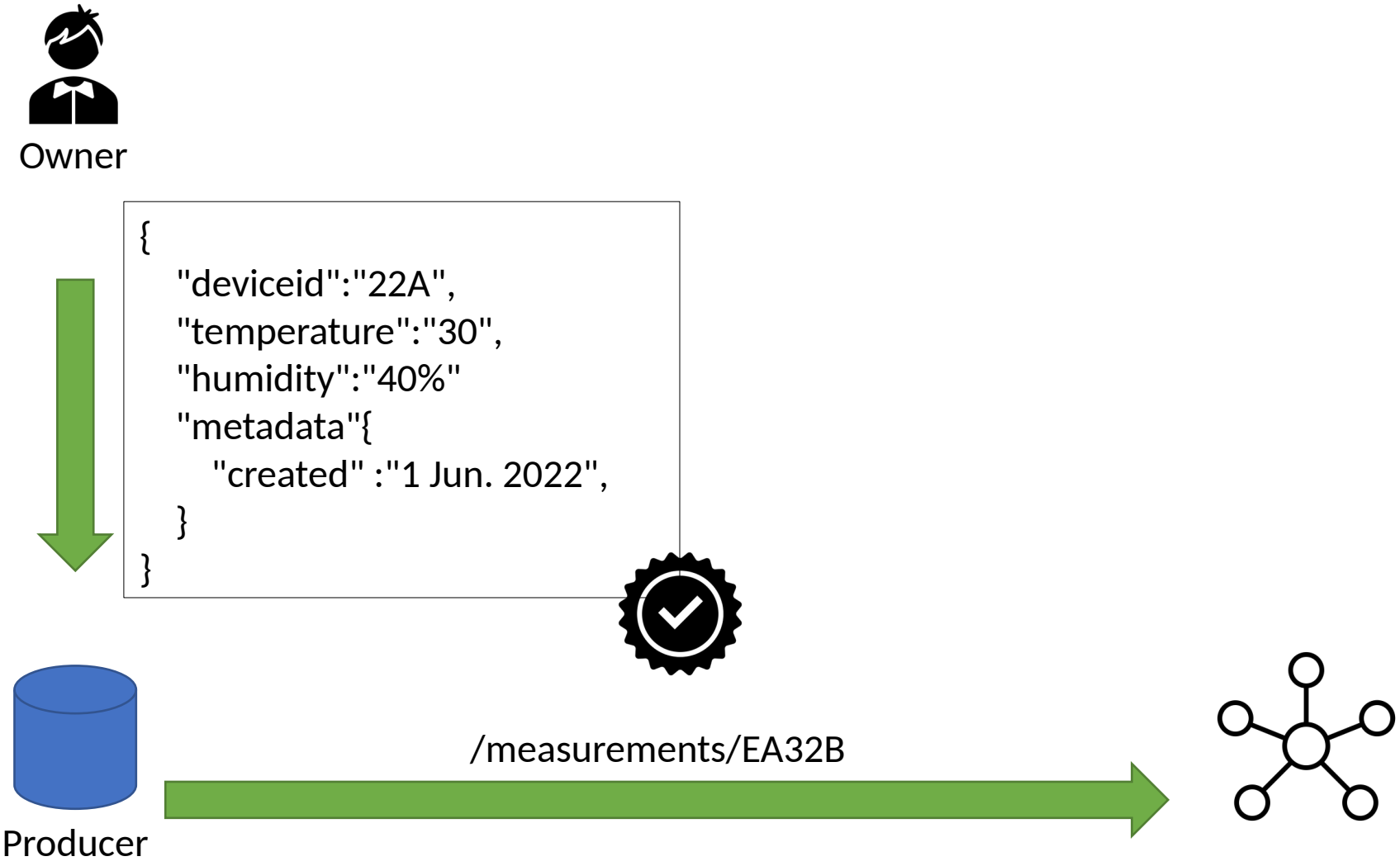
"Framing" JSON data

```
{
   "deviceid":"",
   "measurements":{
      "*":{
         "id":"temperature",
          "values":{"*":""}
   }
}
```

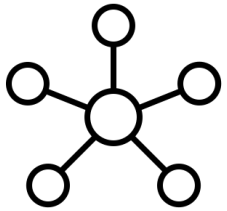
```
{
   "deviceid":"22A",
   "measurements":[
      {
        "id":"temperature",
        "values":[10, 20, 30]
      },
       {
        "id":"humidity",
        "values":["20%","30%"]
       }
    ]
}
```

```
{
   "deviceid":"22A",
   "measurements":[
      {
        "id":"temperature",
        "values":[10, 20, 30]
       }
  ]
}
```

Integration with NDN



Integration with NDN



/measurements/EA32B /.....

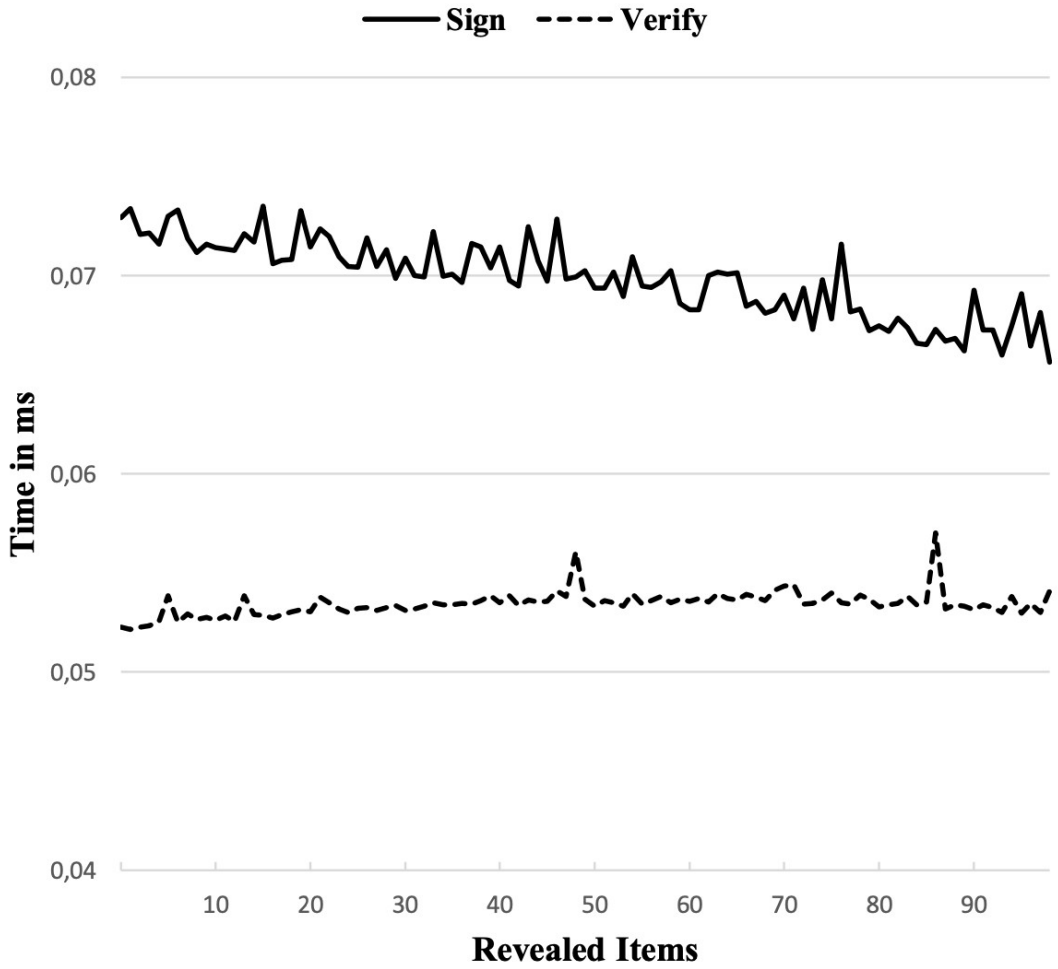
Consumer

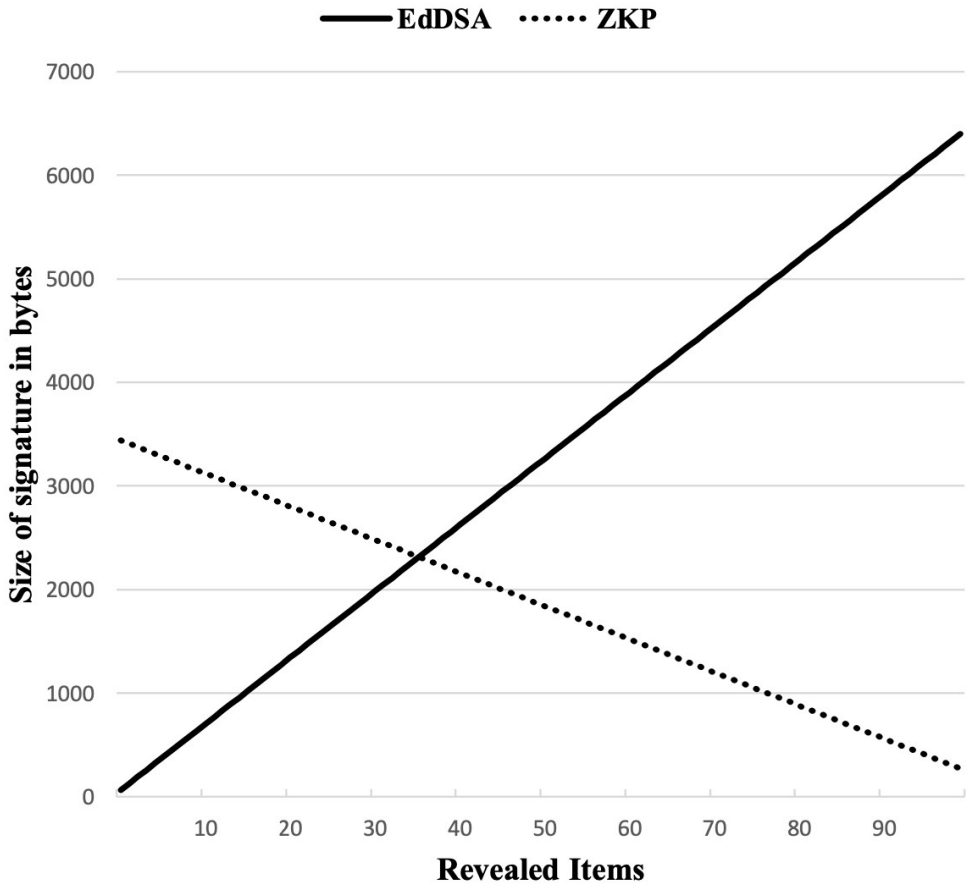
App. Parameters

```
{
   "deviceid":"",
   "temperature":"",
    "metadata"{
      "created" :"",
   }
}
```

Producer

Some performance results





Next steps

- Define encodings
  - A new key type
  - Two new signature types
- Define framing protocols
  - Not only for JSON-encoded data
- Co-operation with other WGs
- More use cases (e.g., in routing protocols?)

Thank you

https://mm.aueb.gr

fotiou@aueb.gr xgeorge@aueb.gr