DISPATCH
Multiformats @ IETF 116

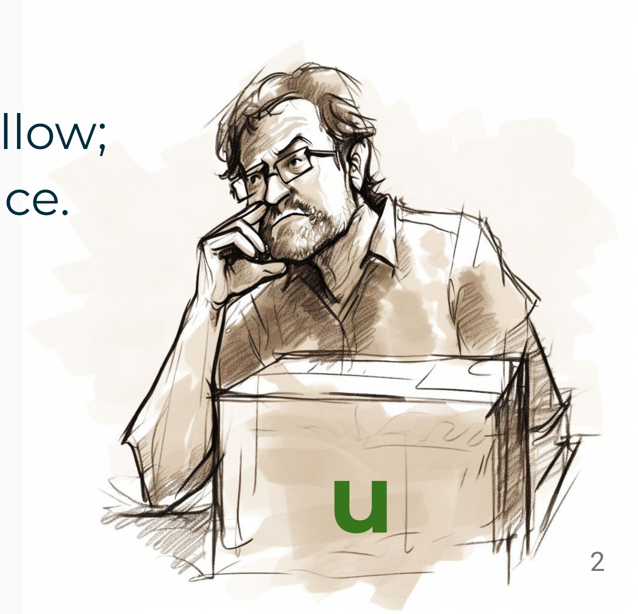
Monday 27 March 2023 9:30am (local time)

Internet Engineering Task Force

Production by Meetecho

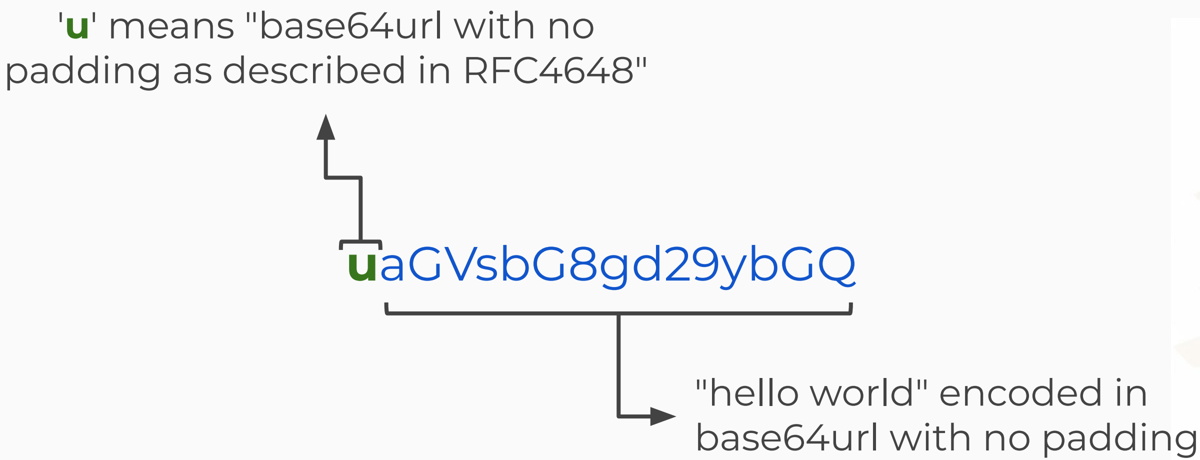
What are Multiformats?

- A self-describing data value,
- that starts with a byte header,
- that identifies the format of the bytes that follow;
- the byte headers share ONE global namespace.



Example: uaGVsbG8gd29ybGQ

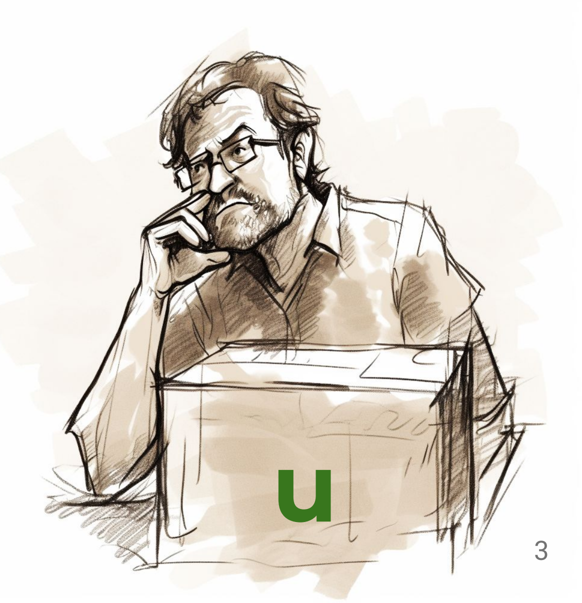
An Example of a Multiformat Value



'**u**' means "base64url with no padding as described in RFC4648"

uaGVsbG8gd29ybGQ

"hello world" encoded in base64url with no padding

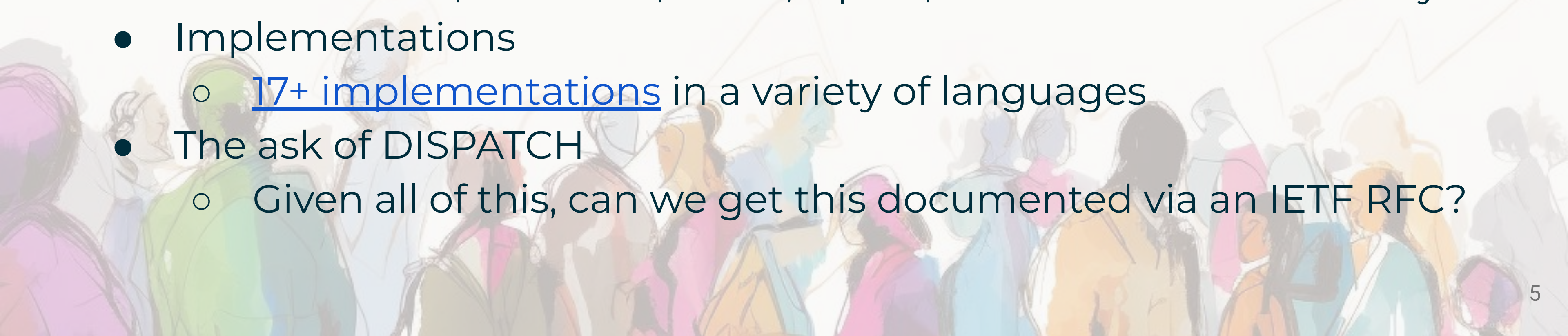


Why are Multiformats useful?

- "A label that lets you know what's in the box."
- Can be used in text and binary formats
- Used to identify:
  - Base encodings (base16, base32, base64)
  - Hashes (SHA-2-256, SHA-3-256, SHAKE-256, BLAKE2b-256)
  - Public Keys (ed25519, x25519, secp256r1, secp256k1)
  - Codecs (cbor object, raw git object, protobuf object)

Who uses Multiformats?

- W3C Working Groups
  - Verifiable Credentials, Decentralized Identifiers, Data Integrity
- Vendors
  - Cloudflare, Microsoft, Brave, Opera, and the IPFS Community
- Implementations
  - 17+ implementations in a variety of languages
- The ask of DISPATCH
  - Given all of this, can we get this documented via an IETF RFC?



What is Multibase?

`zStV1DL6CwTryKyV` (base58-btc)
`uaGVsbG8gd29ybGQ` (base64url no pad)
`bNBSWY3DPEB3W64TMMQ` (base32 no pad)
`F68656C6C6F20776F726C64` (base16 hex upper)

- draft-multiformats-multibase-07
- Identifies base-encoding for a string
- Useful in text-based formats like JSON and YAML

What is Multihash?

SHA-2 256-bit	0x12a948904f2f0f479b8f8197694b30184b0d2ed1c1cd2a1ec0fb85d299a192a447
SHA-3 256-bit	0x16a8009a7a528d87778c356da3a55d964719e818666a04e4f960c9e2439e35f138
SHAKE-256	0x194b7b2eafa0af610fce30bc6fdcdc44adb08999b1db43b366e62996d7a0f01d3e
Multibase-encoded	z6YXWkNzZjmZaM3coEnisJdFuCXXGeX371a41SPzt37Wgn

- draft-multiformats-multihash-06
- Identifies type and length of hash
- With Multibase, useful in text-based formats like JSON and YAML

Where does this fit at IETF?

- Multibase and Multihash; preferred path: **AD Sponsored**
  - 2-4 page specs are documenting mature implementations
  - Most content contained in IANA Registries
- Alternatives: *Maybe CFRG?*
  - Heavily used in security architectures and systems
- Future potential path: Multiformats WG
  - If there is enough Multiformats community interest
  - NOT NOW: Will require more cat herding and time