Common option compression

draft-amsuess-core-TBD

Christian Amsüss

2021-05-12
Single simple use case

“.well-known/*”

“.well-known/edhoc” eats 18 bytes
BCP190 says it needs to be /well-known/, and there’s a preference for descriptive names

- Define empty option 501 (critical, safe, cachekey; 3 bytes) to mean “/well-known/edhoc”
- Mutually exclusive with Uri-Path and Proxy-Uri
- Bycatch: can have uint value to give short version for “/well-known/core” too (4 bytes – fight!)
- Problem solved.
What else could this do
without actually doing it any different – if you were happy with the above, read things that way

Express as SCHC C/D rule (see pelov-lpwan-architecture)

Equivalence can become machine-readable and transformable

Generalization for whatever else could be needed (Uri-Host-Literal?)

Further potential in non-traditional responses (short-hands for Response-For)
Retroactive simplification of concepts
by example of oscore-edhoc, without needs for change

Alternative definition for EDHOC option: “invokes some SCHC rules”

\[
\begin{align*}
\text{POST, OSCORE: } & \text{ odat, EDHOC} & \iff & \text{ POST } & \text{/well-known/edhoc,} \\
& \text{ Payload: edat, odat2} & \iff & \text{ Payload: edat} \\
& & \iff & \text{ POST OSCORE: odat} \\
& & & \text{ Payload: odat2} \\
\end{align*}
\]

\[
\begin{align*}
\text{2.04 Changed, OSCORE,} & \iff \text{ 2.04 Changed} \\
& \text{ Payload: odat3} & \iff & \text{ 2.04 Changed, OSCORE} \\
& & \iff & \text{ Payload: odat3} \\
\end{align*}
\]

\[
\begin{align*}
\text{4.00 Bad Response} & \iff \text{ 4.00 Bad Response} \\
& \text{ Payload: edat2} & \iff & \text{ 4.01 Unauthorized} \\
& & \iff & \text{ Payload: edat2} \\
\end{align*}
\]

Note that C/D and F/R invoking rules on the request apply to both request and response.
Questions

- Urgency?
- Value in generalization?