Minimal G-IKEv2 Client

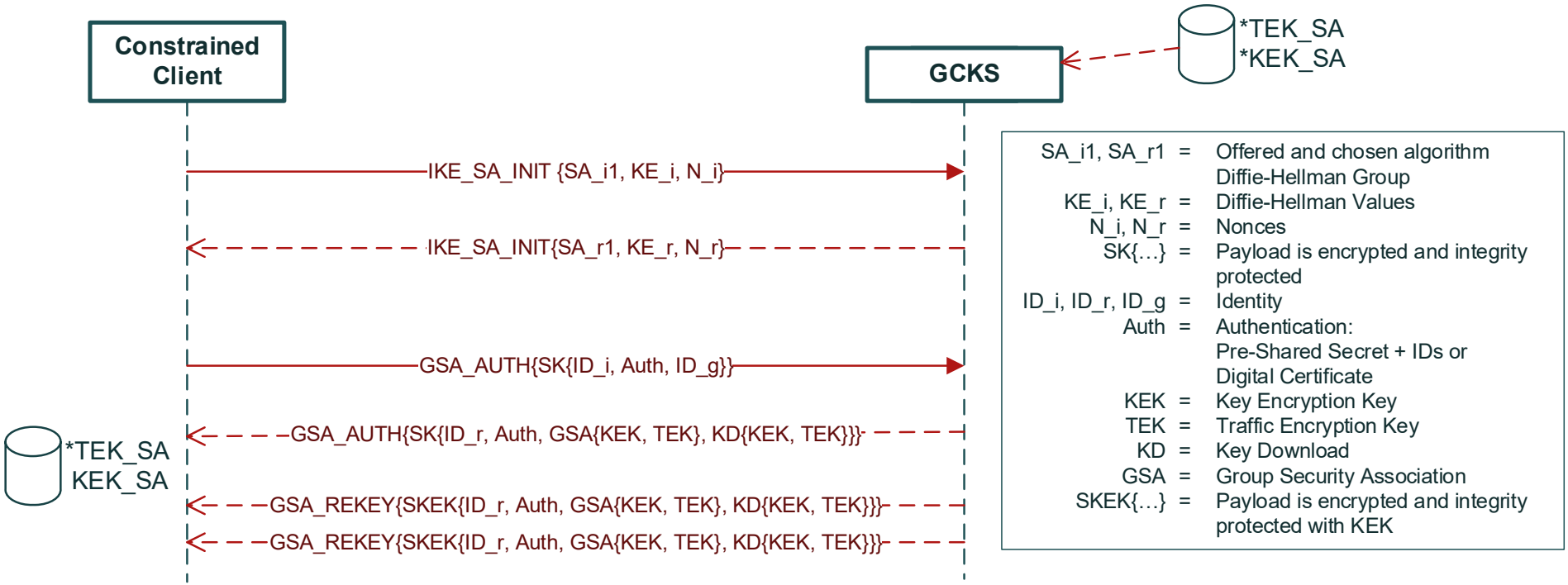
IETF99, 21.07.2017

Nils gentschen Felde Tobias Guggemos
Tobias Heider Dieter Kranzlmüller

`https://tools.ietf.org/html/draft-yeung-g-ikev2-11`

MNM TEAM
Munich Network Management Team

The Group IKEv2 Protocol

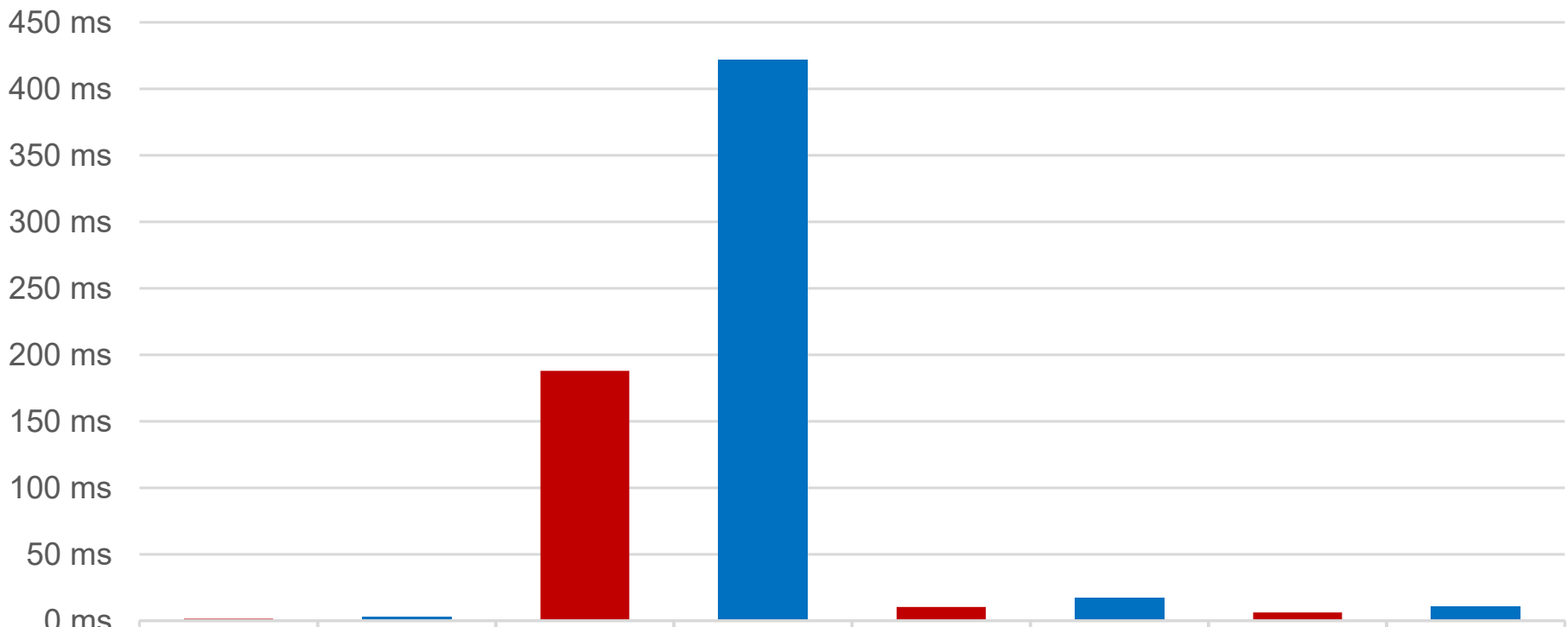


Implementation

Feature	**Required Memory**
RIOT kernel (incl. stack)	2,560 Byte
RIOT IPv6 stack	1,024 Byte
RIOT UDP stack	1,024 Byte
RIOT net cache	928 Byte
RIOT packet buffer	1,280 Byte
IKE SA	$\sim$210 Byte
SAD for 1 group membership	$\sim$100 Byte
SPD for 1 group membership	40 Byte
$\sum$	6,142 Byte

Options	Arduino Uno	Arduino M0	Arduino Due
symmetric cipher (native RIOT support)			
Encryption (AES128)	✔	✔	✔
Integrity (HMAC-SHA256)	✔	✔	✔
PRF (HMAC-SHA1)	✔	✔	✔
asymmetric cipher (micro-ecc)			
Diffie-Hellman (SECP256R1)	✔	✔	✔
Flash Memory ($\geq$ 57 *KB*)	32 *KB*	256 *KB*	512 *KB*
RAM ($\geq$ 6.2 *KB*)	2 *KB*	32 *KB*	96 *KB*
Total	✘	✔	✔

Evaluation



	Due Prepare IKE_SA_INIT	M0 Pro Prepare IKE_SA_INIT	Due Process IKE_SA_INIT	M0 Pro Process IKE_SA_INIT	Due Prepare GSA_AUTH	M0 Pro Prepare GSA_AUTH	Due Process GSA_AUTH	M0 Pro Process GSA_AUTH
avg [ms]	1.62	2.62	187.92	421.94	10.29	17.41	6.32	10.53
std. dev. [ms]	0.00	0.00	0.11	0.13	0.00	0.00	0.40	0.00
min [ms]	1.62	2.62	187.72	421.71	10.29	17.41	6.15	10.52
max [ms]	1.62	2.62	188.11	422.18	10.29	17.41	7.26	10.53

Minimalization

→Specifying Minimal GSA_AUTH and GSA_REKEY
  →difference to IKE_AUTH is straightforward

→Providing guidelines for minimal server configuration

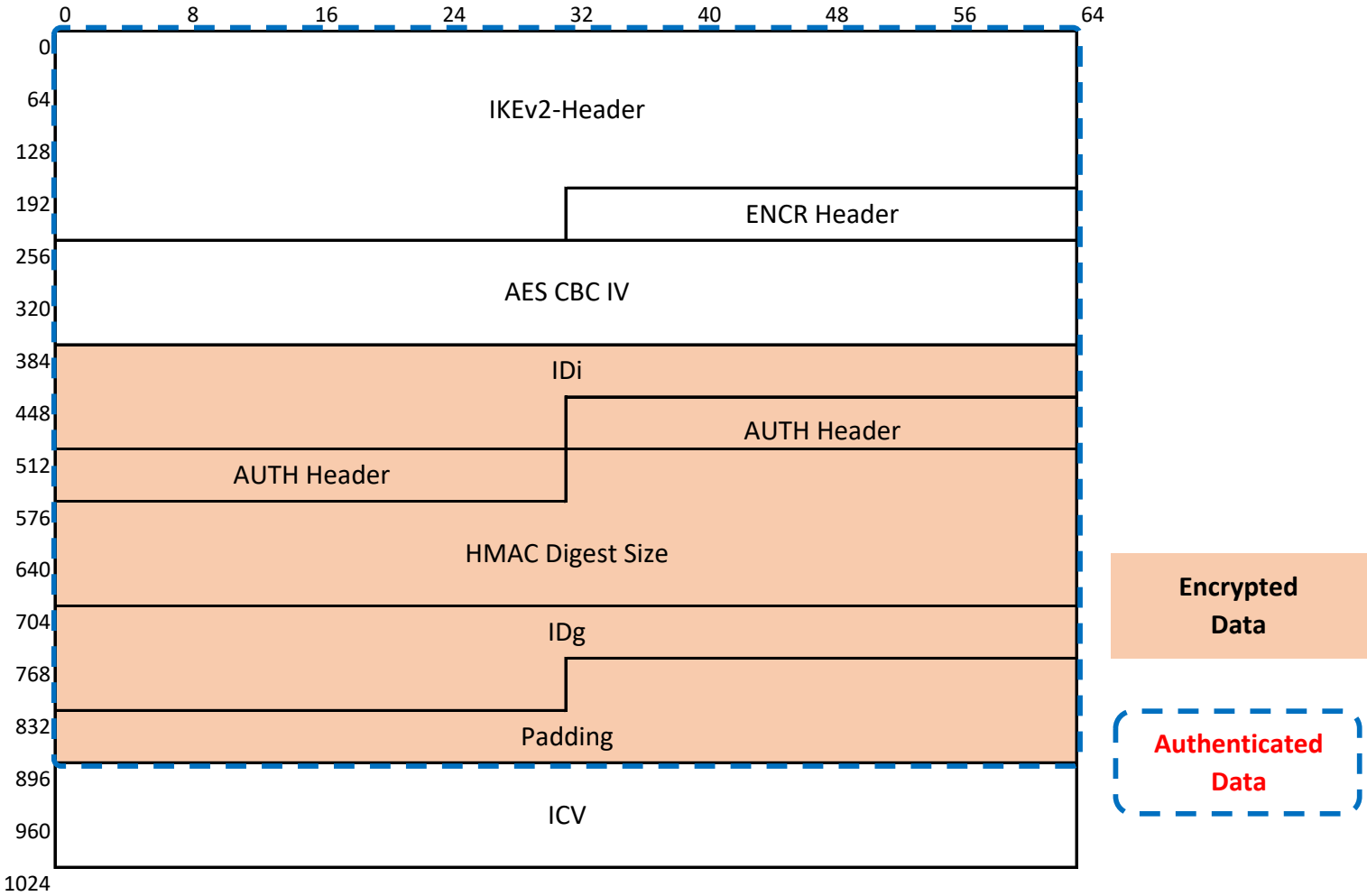
End

Implementation will be available open source
for RIOT OS

Is the WG interested in designing a Minimal G-IKEv2
(a la RFC 7815)?

Backup

GSA_AUTH request



GSA_AUTH response