A GENERIC CIPHERTEXT FORMAT

Yaron Sheffer
Intuit
HotRFC, IETF-109
There are standards for "raw ciphertext", the direct result of encryption. This is not sufficient if you have trillions of ciphertexts, stored at rest. Long term goal: interoperability of encryption libraries and key management systems.

Standard format to denote key identity, key version...
Must be extensible
Allows automated detection and attribution of ciphertext
Supports granular key management: key wrapping and key derivation

Early draft [here](#)
NEXT STEPS

If you’re interested, let me know: yaronf.ietf@gmail.com

Meet informally at IETF-109

Then BoF, or submission to SAAG, or CFRG, or…
THANK YOU!

Yaron Sheffer,
yaronf.ietf@gmail.com