

# RSA<sup>®</sup>Conference2019

San Francisco | March 4–8 | Moscone Center



**BETTER.**

SESSION ID: BAC-R09

## Using High-Entropy Encryption for Enterprise Collaboration

**Aaron Turner**

CEO – Hotshot  
@AARONRTURNER

**Jonathan Warren**

CTO - HighSide

#RSAC

# Session Outline

- What are the attributes of enterprise-grade encryption?
- How many enterprises are actually using the right encryption?
- Enterprise encryption case study
- Enterprise encryption fundamentals
- Demonstration
- The intersection of encryption, security and compliance

# Enterprise-grade Encryption Attributes

- Cryptographic sovereignty – not subject to the whims of another party
  - Autonomous root authority
  - Total control over issuance
  - Policy enforcement upon use
  - Full revocability
- Problematic situations
  - SSL – too many Meddlers in the Middle
  - SaaS – whose root is this exactly?
  - Consumer-grade ‘secure’ messaging apps – enterprise loses all control

# State of the Market: Enterprise Encryption Madness

- Working on research with Digital Shadows on extent of SSL manipulation
  - How easy is it to purchase a \*.\* root from the underground and manipulate enterprise communications to/from SaaS platforms like Salesforce, Office365, etc.
    - Should have idea on results by next revision deadline
- iOS example of lack of control over SSL trusts
  - Updated graphic on iOS 12 roots of trust and how untrustworthy they are

# Enterprise Encryption Case Study - Background

- International professional & technical services firm
- 30,000 global employees, heavy use of WhatsApp because IT leadership believed it was 'secure'
- Regulator from Country X asks for company employee communications relating to a government services contract
- Company turns over all email e-discovery information



# Enterprise Encryption Case Study – The Twist

- Regulator is given WhatsApp messages by a whistleblower which contradict emails and show significant under-reporting by company
- Company fined millions due to inability to produce complete WhatsApp message history
- Bottom line: WhatsApp's encryption is better than SMS or email, but its use within the enterprise represents a significant data protection and compliance risk



Image credit:  
<https://www.ft.com/content/4fbf6c18-a501-11e7-b797-b61809486fe2>

# How should enterprise encryption work?

- Crypto Sovereignty – be master of your destiny

```
C:\WINDOWS\system32\cmd.exe

C:\AAB Jonathan\Python\chatclient\Jonathan tests>python RSAdemo.py
Initial random seed data: 01eab1be772303d9275c3fde6849f50170bcc56a

Generated import key: acid few hurdle unusual coral uncle output margin taxi drastic later actual armed g
lance
Initial random seed data stretched using PBKDF2: 542bc04b4d1d12e4dee95b2322812214e2274a22f9b8fc1af4c5b13d
de1c7525a7df88af8d5ea302a007719a42b151995b6bdc5bd1a152e2e90021605d73992b63a5d4fbbfe4bbf dfbd4794b84e7e5c33
603128467b720e3a767842b042722e31783dd194ccf6ad14e0f491cc777d44323bd6506be67d07fbb4ec6f594bbe4e4532ab4e35a
950c43fc42e84d88960270565081cc20d0767bd41f5d2c285904aa652a1490ae474b74c36ce748f6acee4ea0fa380a640bf6e9f6c
0a71acbe1667a1ba1955837182579bb8ef1ea0d9ad6887dbb5daac4ebdd2e5d07e298096ecaad0b76c05aae3e56d7b2b6435d9f69
f4f8eec11562193d79de

stretched seed data appended with a nonce, hashed. This is our private SIGNING key: 80fa9a4b6fc93a7211876
d533bab73dcb166d3016d08081a77c32f9969427f2c5d

stretched seed data appended with a nonce, hashed. This is our private ENCRYPTION key: 80b7886f2dccfc3d99
befe39805c89740a390d7803ed03045fda53edc8af2fe605

ECC point multiplication done to turn them into public keys:
Public signing key: 04f209a63b96e8cd0fccd3f17ea3c2f24ff713a5d8803263959ad7e2e57669b44034bb58af7a1
16fb6e6db766c28189f9be965ba2a7b8d9f87f2cd835ea0038de73

Public encryption key: 04924e1d06d820c2ce7a961f890939f36584744aa8ec59f698c8a8eee01d620ab9799c9c2f
a565a104fd9b81fbddfe6b06e70a13893f3dd1e5028a7192bf036694

Public keys hashed. This we call the user's "address": CH-6c7JAoUACAsyRx6t2TX8FZUsEyxc0Pr8

C:\AAB Jonathan\Python\chatclient\Jonathan tests>
```

# Key Generation Demonstration

- How seeds can be used to generate subordinated keysets

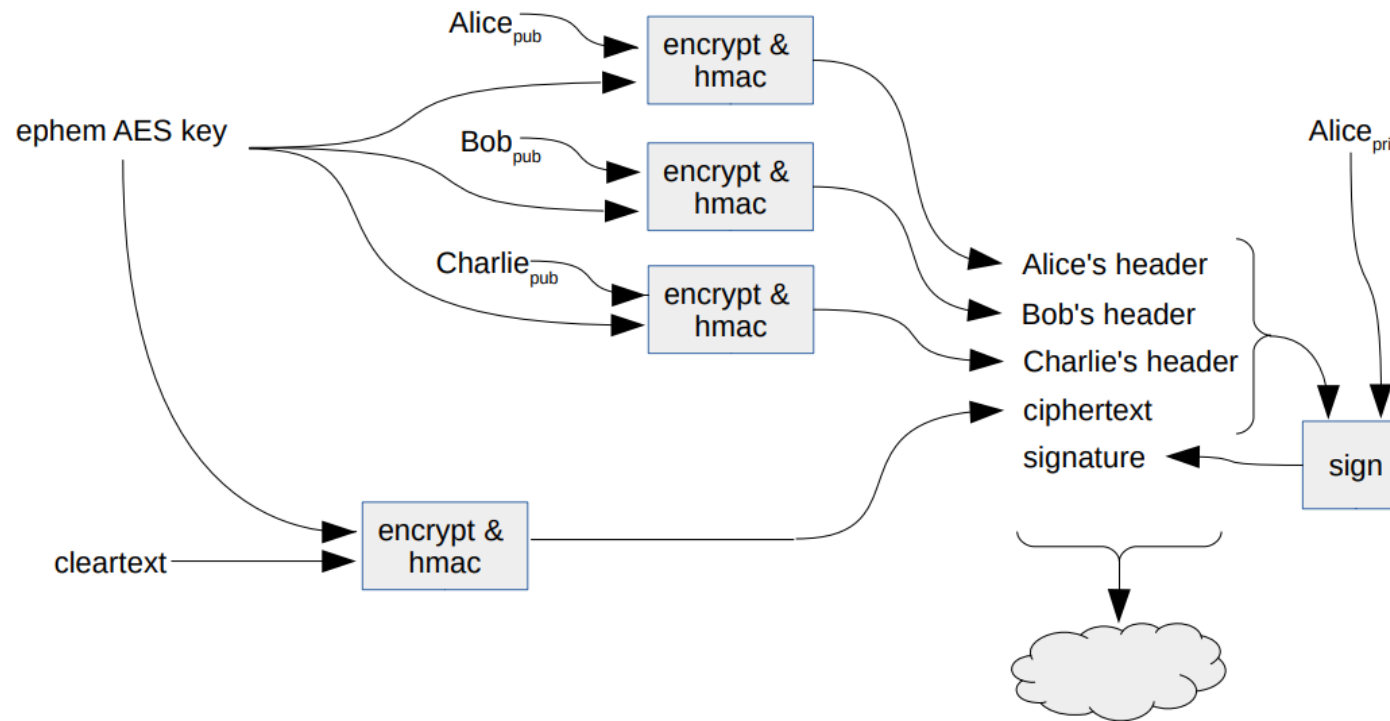
The screenshot shows a HighSide chat window titled "Data Room" (Private). The left sidebar lists channels and direct messages. The main chat area shows a conversation where Emily Newman asks for Q2 data, and Jeremy Thorpe provides a PDF file named "Q2 Fenson Report.pdf" (5.20 MB). Below the chat, a bar chart displays data for each month from January to December. The chart has two series: a light blue series and a dark blue series. The total height of the bars varies by month, with June and July having the highest totals.

Month	Light Blue Series	Dark Blue Series	Total
Jan	1.2	1.3	2.5
Feb	2.2	1.3	3.5
Mar	1.8	1.0	2.8
Apr	1.3	0.3	1.6
May	1.4	1.1	2.5
Jun	2.5	1.4	3.9
Jul	1.9	1.8	3.7
Aug	2.0	0.8	2.8
Sep	1.4	1.7	3.1
Oct	1.5	0.7	2.2
Nov	0.8	0.8	1.6
Dec	1.9	1.1	3.0



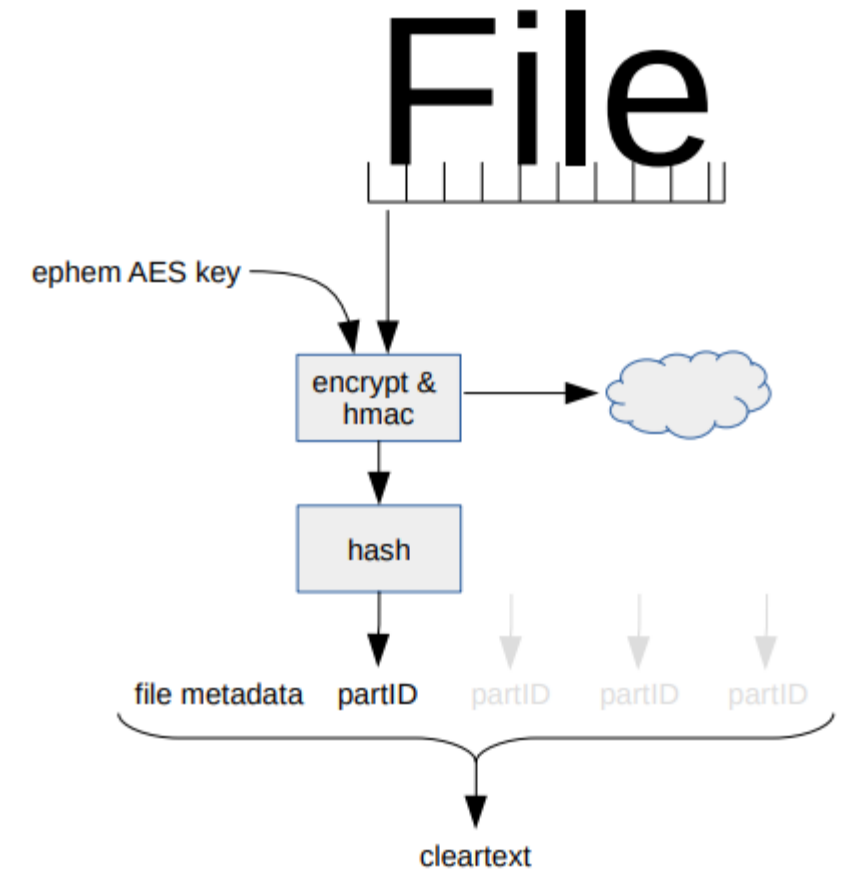
# Enterprise Encryption: Ephemeral keys

- Encryption flexibility: avoiding the use of pre-used keys



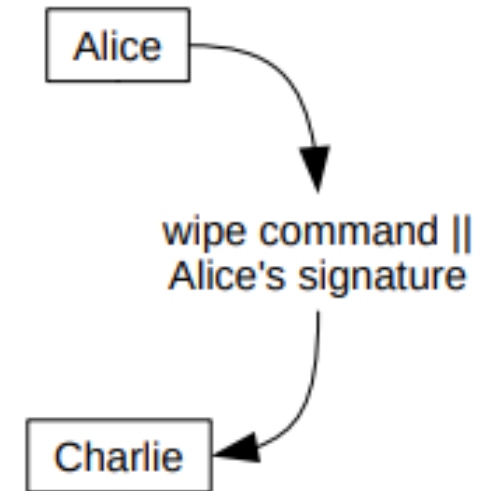
# High-efficiency encryption: file sharing demonstration

- File chunking prior to encryption speeds up data transfer over slow connections



# Enterprise Encryption: Data ownership demonstration

- Easy lifecycle management: how to maintain control over data
- How enterprise ownership of keys facilitated data lifecycle management




# Enterprise Encryption: where & when matters

- Hotshot data restriction policies demonstration

Active Allowed Locations    Add Allowed Address    Add Allowed Country

Hotshot supports setting location restrictions for individual user groups. Users in the user group will only be able to connect when their device is within the specified location radius or the borders of an approved country. Manage active location restrictions below:

 Germany 🗑️ Delete



# How to assure proper use of encryption in the enterprise

- Assure appropriate cryptographic infrastructure which facilitates crypto sovereignty
- Look for tools which allow administrators to easily manage all aspects of the encryption lifecycle
  - Issuance
  - Use restrictions
  - Revocation
- Implement encryption tools which reduce the risk of data disclosure and regulatory risks