RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: BAC-R09

Using High-Entropy Encryption for Enterprise Collaboration

Aaron Turner
CEO – Hotshot
@AARONRTURNER

Jonathan Warren
CTO - HighSide

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

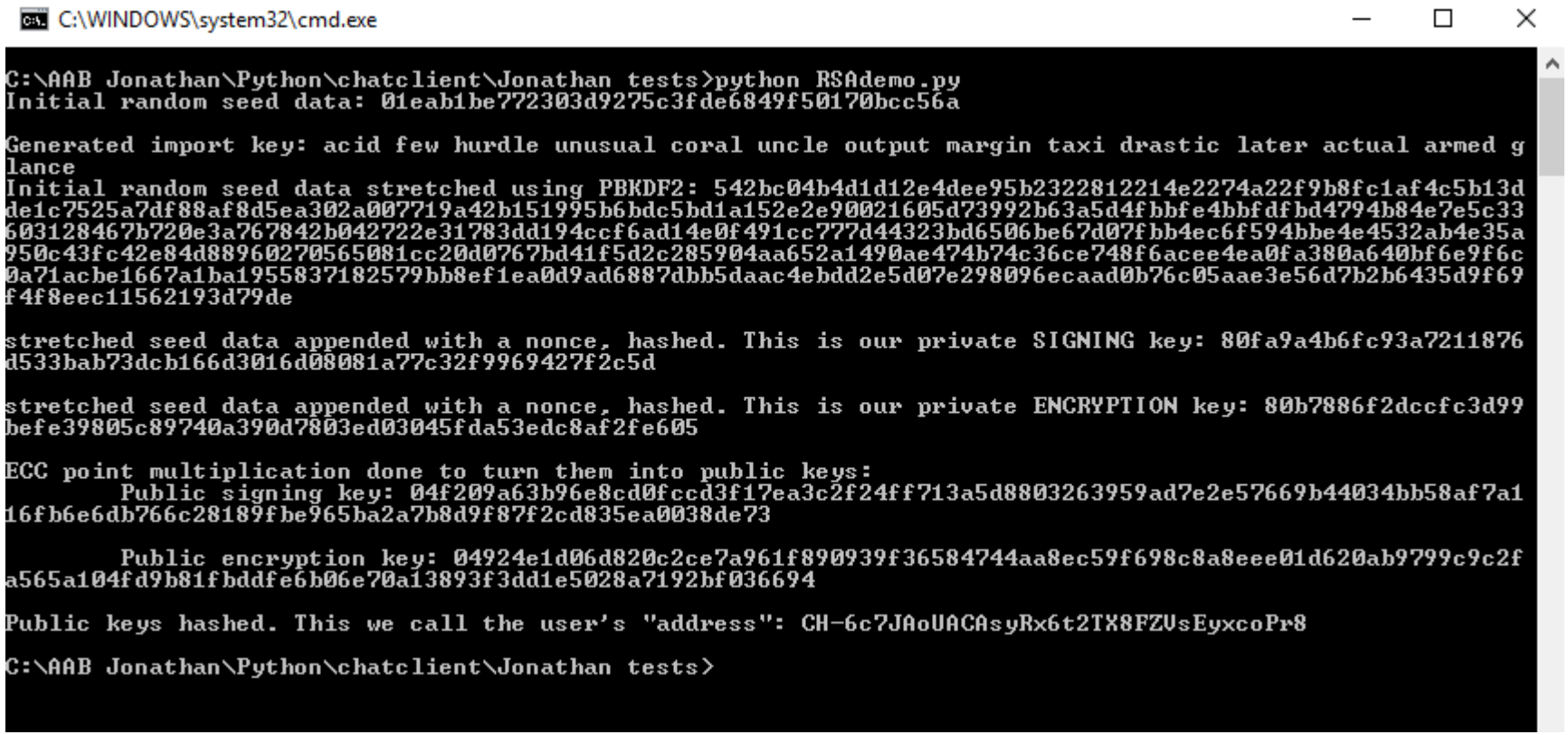
Enterprise Encryption Case Study – The Twist

- 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

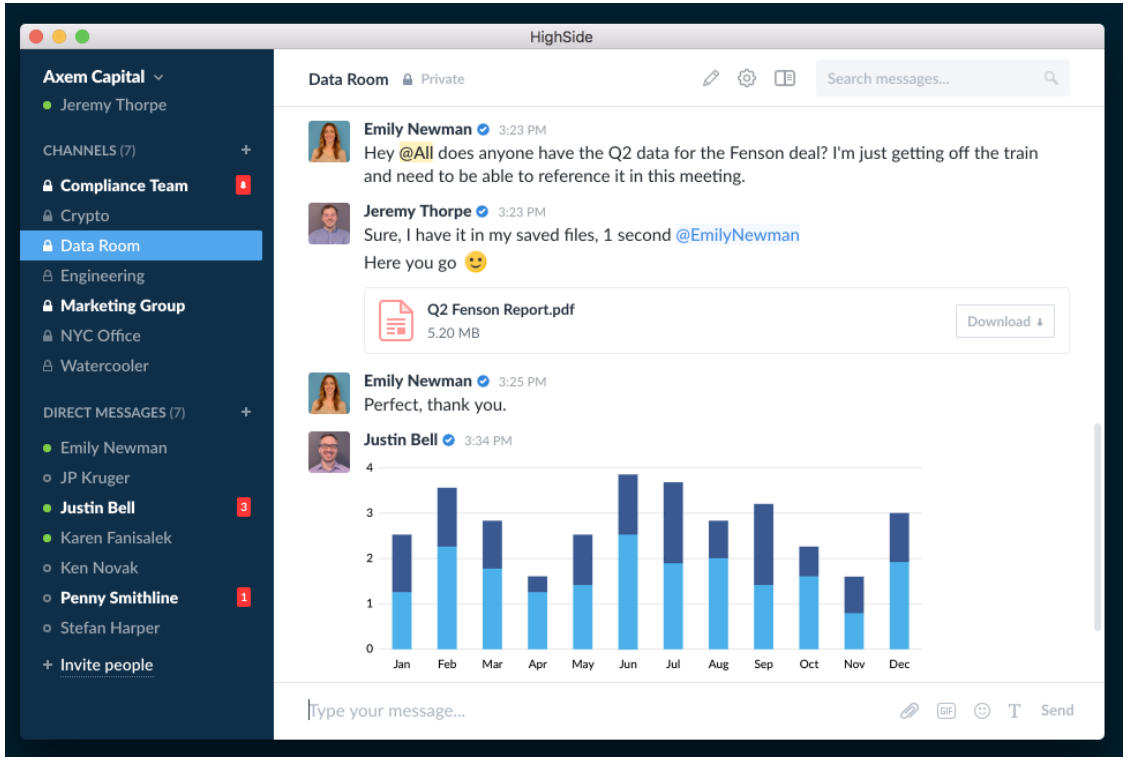
How should enterprise encryption work?

- Crypto Sovereignty – be master of your destiny



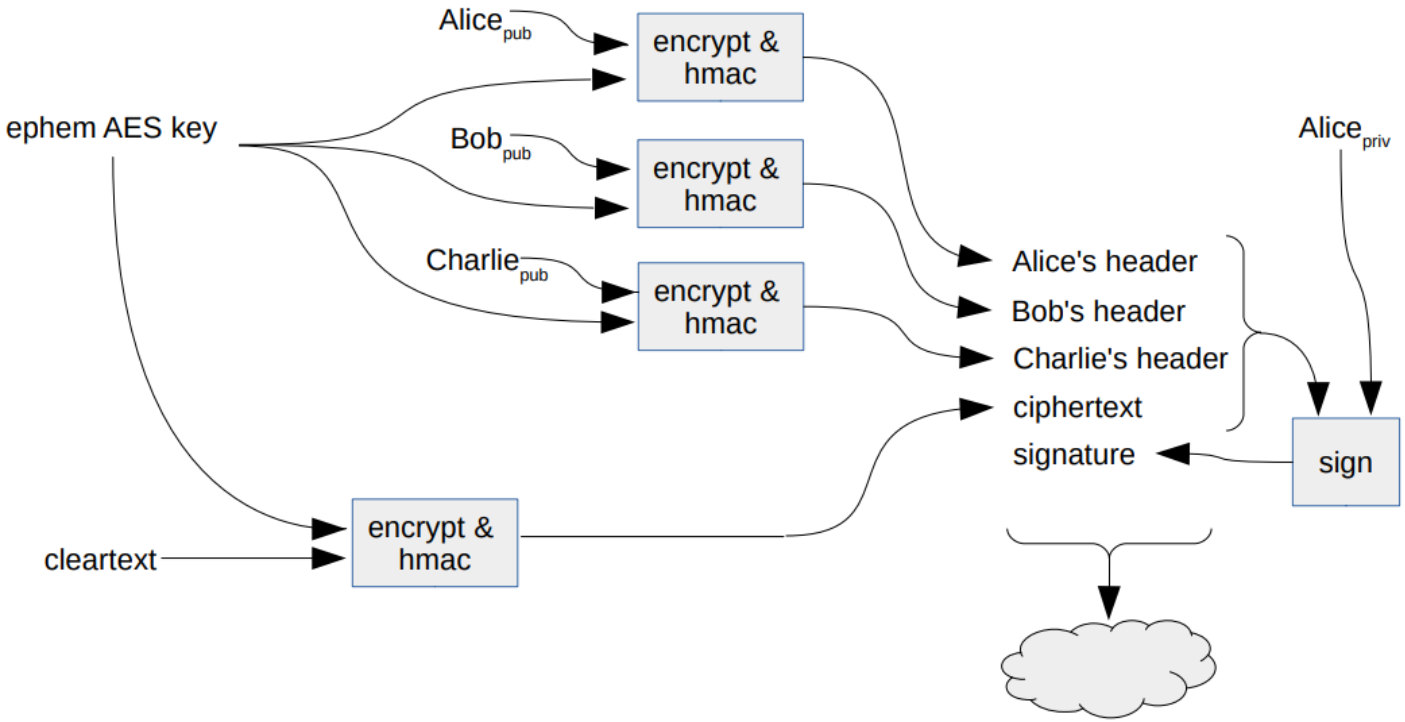
Key Generation Demonstration

- How seeds can be used to generate subordinated keysets



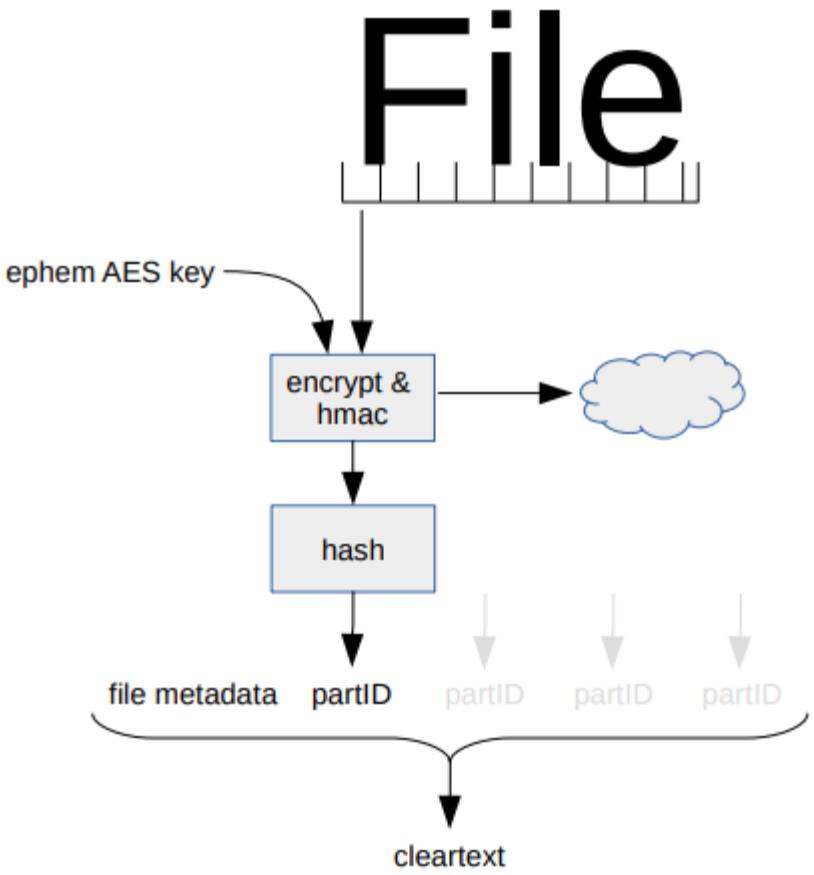
Enterprise Encryption: Ephemeral keys

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



High-efficiency encryption: file sharing demonstration

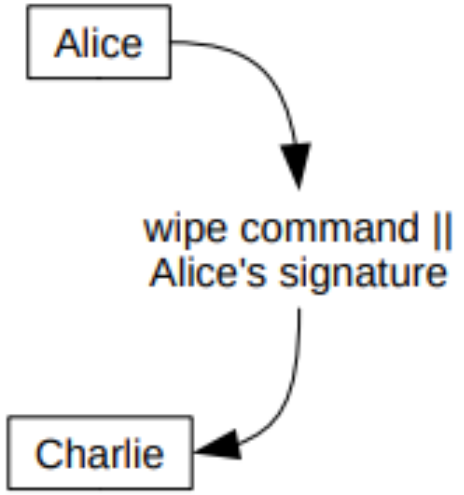
- File chunking prior to encryption speeds up data transfer over slow connections



Enterprise Encryption: Data ownership demonstration

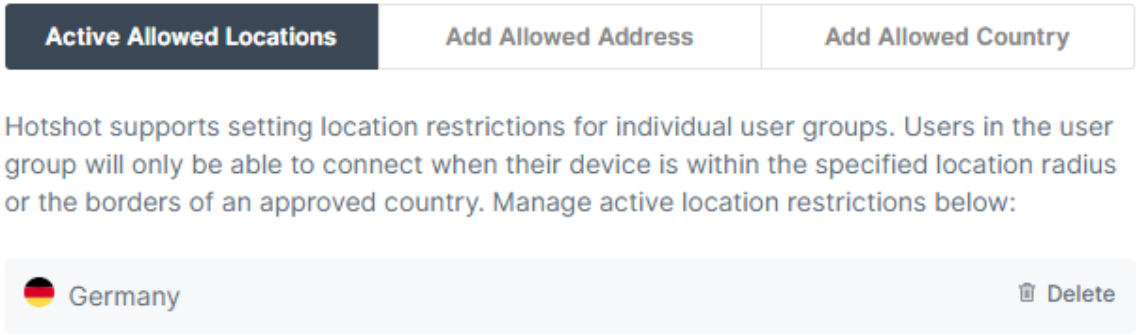
- Easy lifecycle management: how to maintain control over data

- How enterprise ownership of keys facilitated data lifecycle management



Enterprise Encryption: where & when matters

- Hotshot data restriction policies demonstration



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