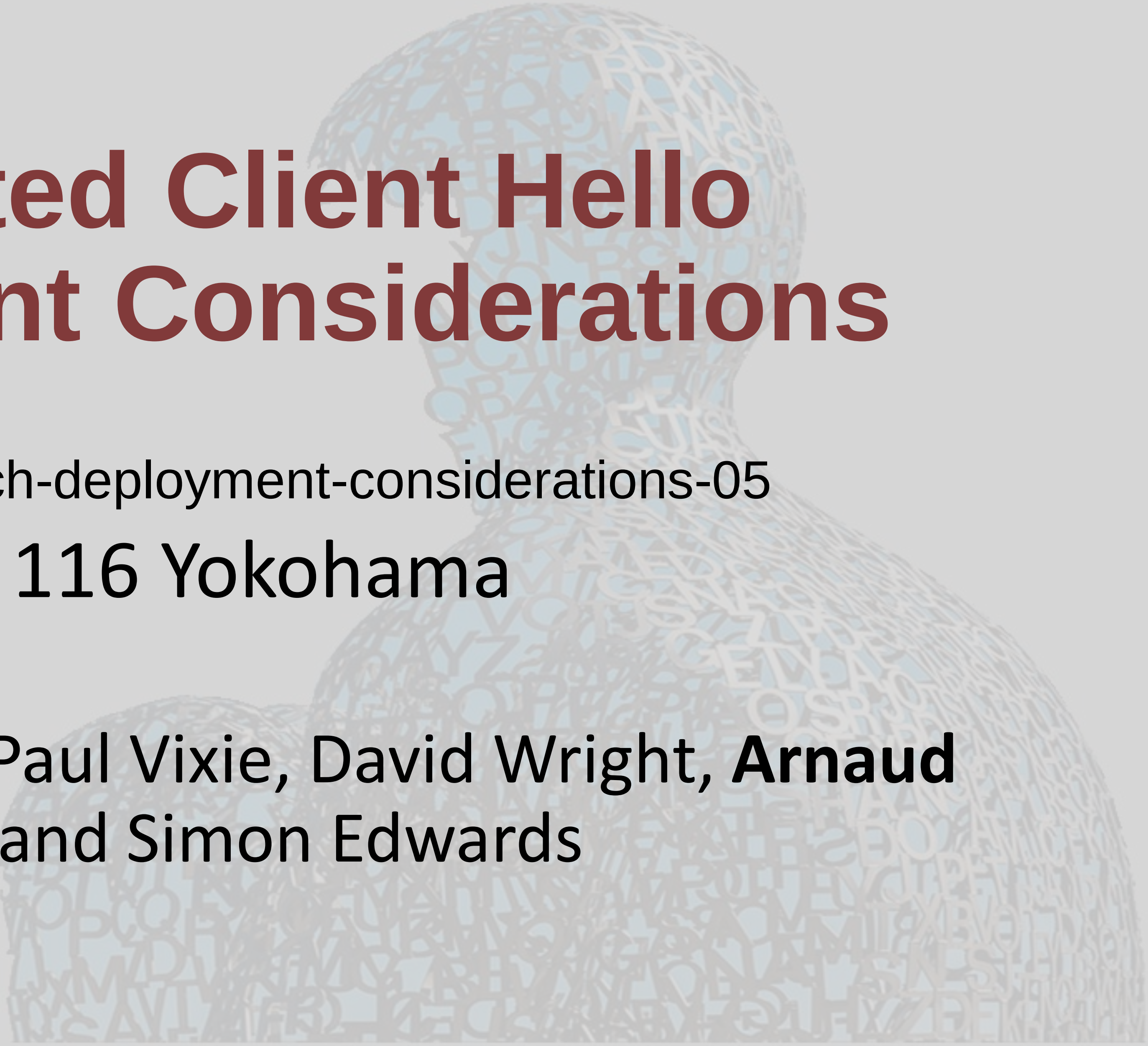
Encrypted Client Hello Deployment Considerations

draft-campling-ech-deployment-considerations-05

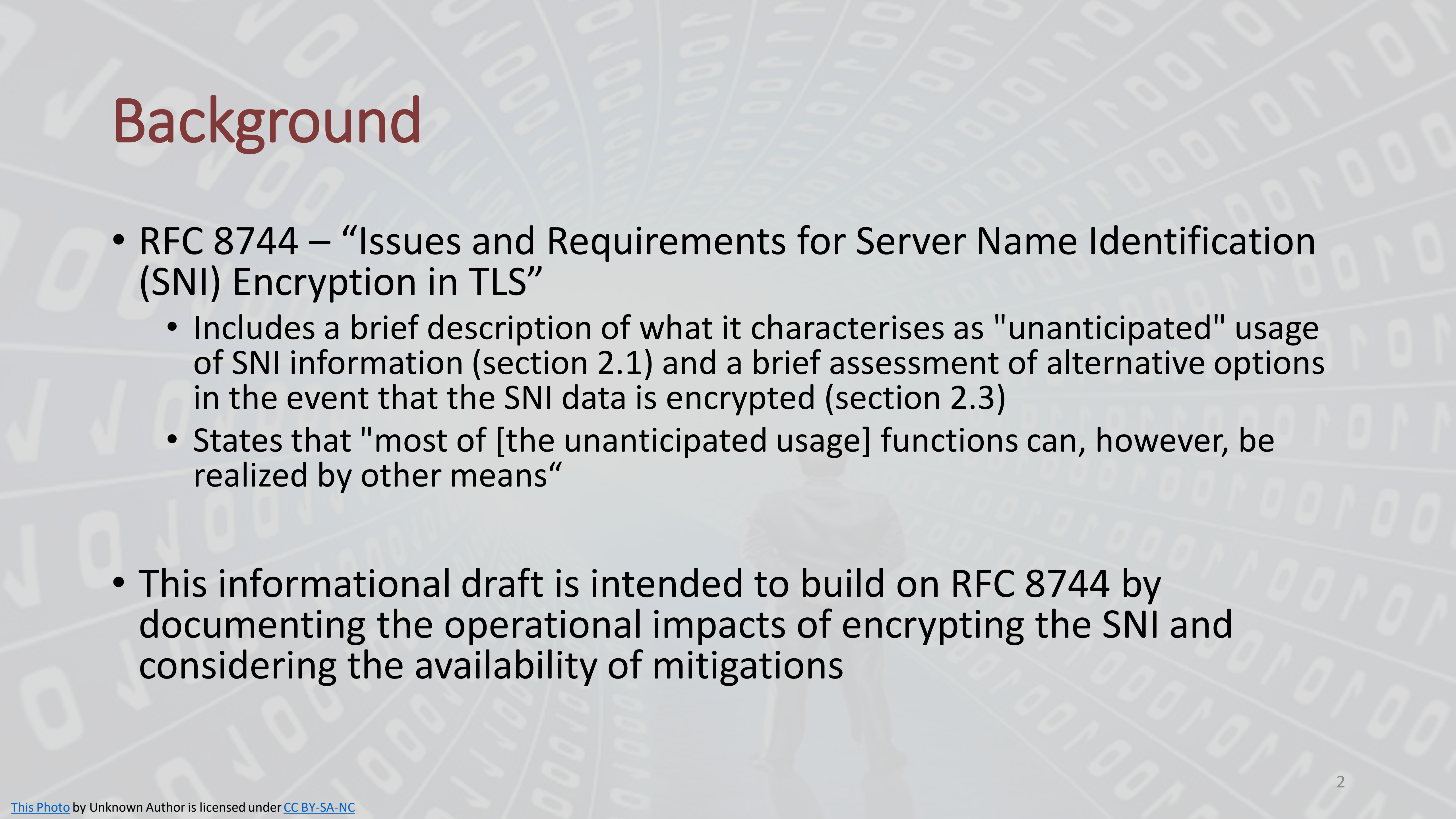
IETF 116 Yokohama

Andrew Campling, Paul Vixie, David Wright, **Arnaud Taddei** and Simon Edwards

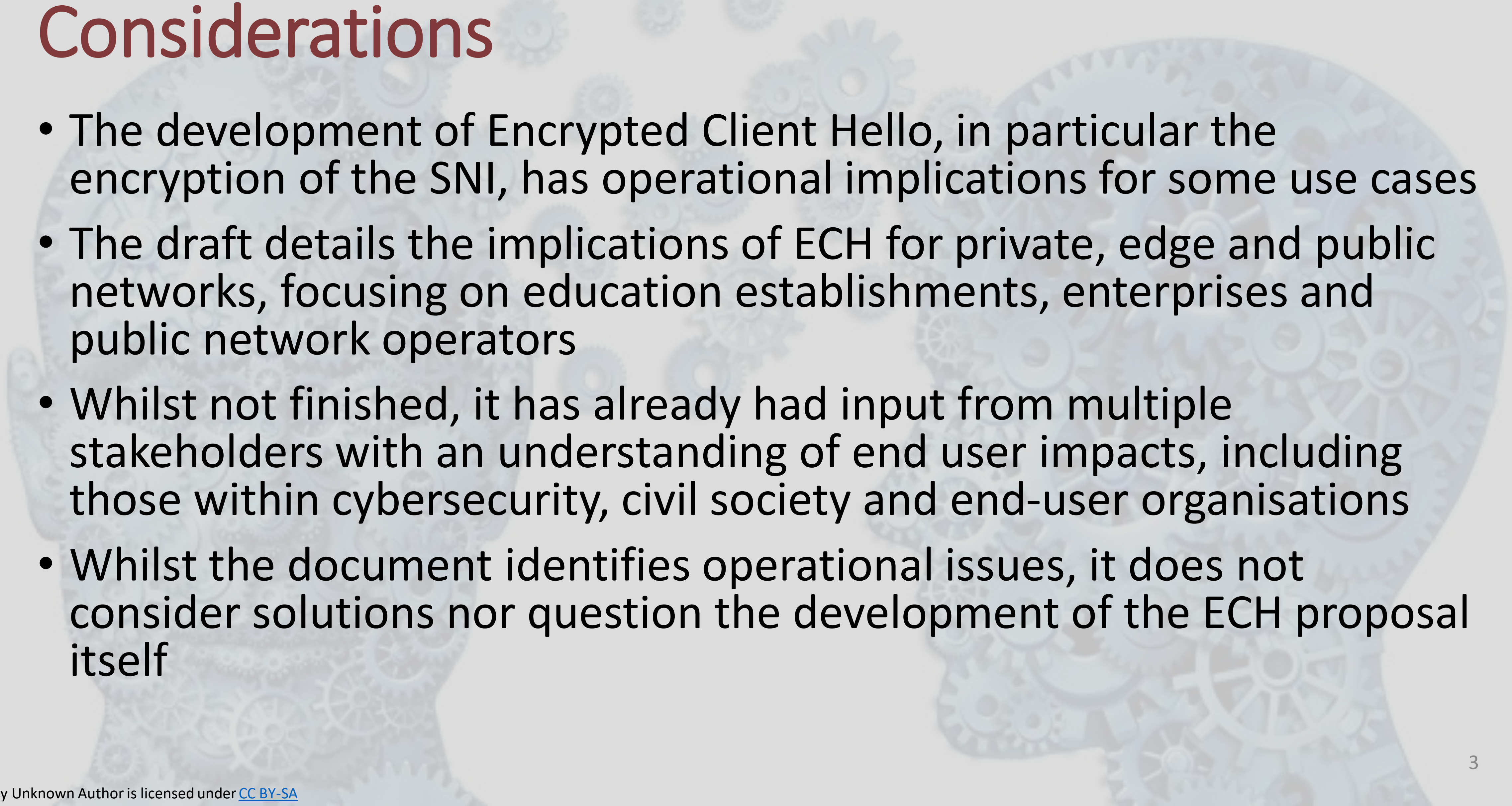


Background

- RFC 8744 – “Issues and Requirements for Server Name Identification (SNI) Encryption in TLS”
  - Includes a brief description of what it characterises as "unanticipated" usage of SNI information (section 2.1) and a brief assessment of alternative options in the event that the SNI data is encrypted (section 2.3)
  - States that "most of [the unanticipated usage] functions can, however, be realized by other means“
- This informational draft is intended to build on RFC 8744 by documenting the operational impacts of encrypting the SNI and considering the availability of mitigations



Encrypted Client Hello Deployment Considerations

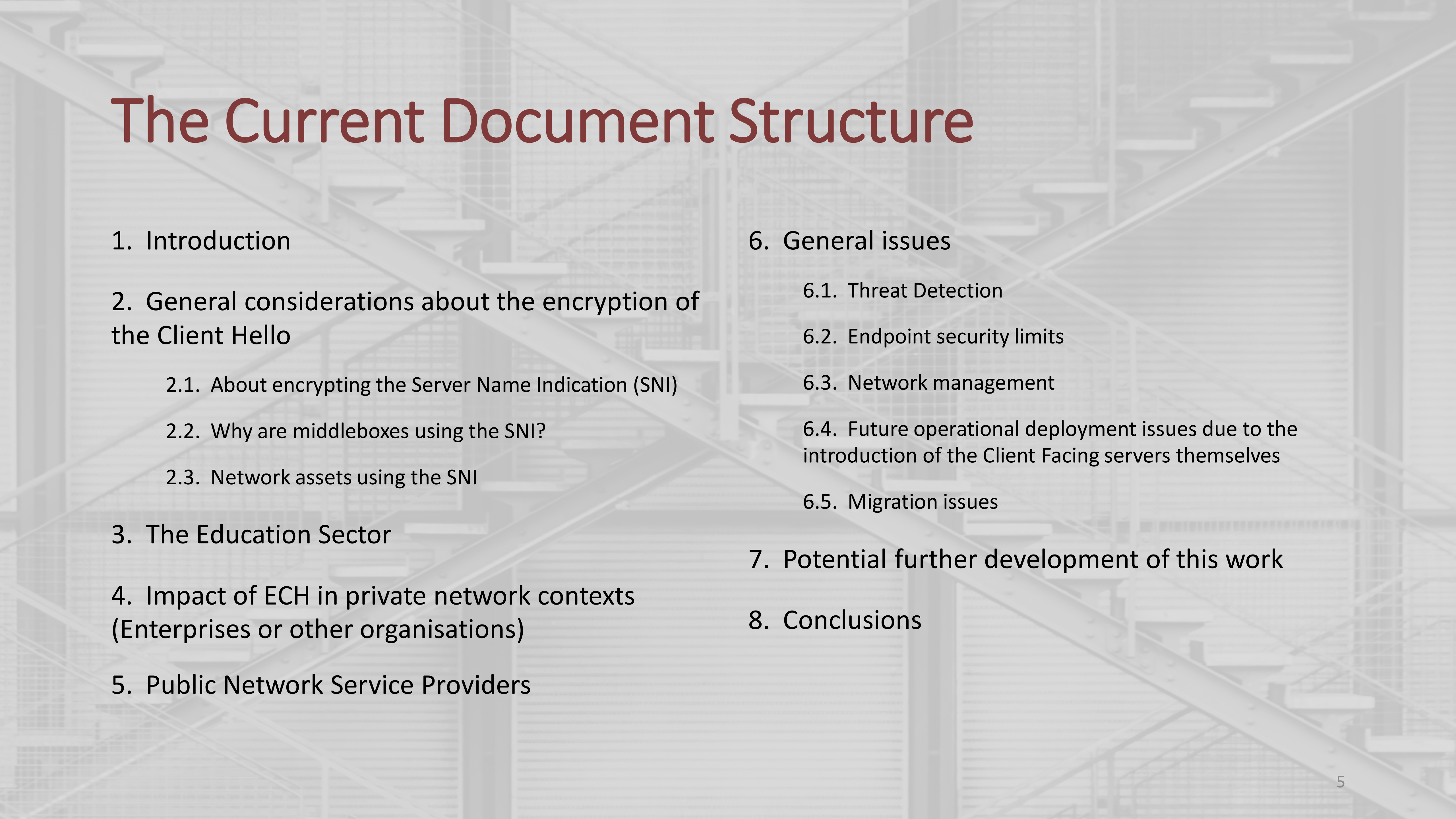


- The development of Encrypted Client Hello, in particular the encryption of the SNI, has operational implications for some use cases
- The draft details the implications of ECH for private, edge and public networks, focusing on education establishments, enterprises and public network operators
- Whilst not finished, it has already had input from multiple stakeholders with an understanding of end user impacts, including those within cybersecurity, civil society and end-user organisations
- Whilst the document identifies operational issues, it does not consider solutions nor question the development of the ECH proposal itself

Use of the SNI

- The SNI encapsulated by ECH is of legitimate interest to on-path security actors including those providing:
  - Inline malware detection
  - Firewalls
  - Parental controls
  - Content filtering to prevent access to malware and other risky traffic
  - Mandatory security controls (e.g. data loss prevention) etc.

- Beyond network security, there are various operational impacts of different types e.g. network management, general content filtering, etc.



The Current Document Structure

1. Introduction
2. General considerations about the encryption of the Client Hello
   - 2.1. About encrypting the Server Name Indication (SNI)
   - 2.2. Why are middleboxes using the SNI?
   - 2.3. Network assets using the SNI
3. The Education Sector
4. Impact of ECH in private network contexts (Enterprises or other organisations)
5. Public Network Service Providers
6. General issues
   - 6.1. Threat Detection
   - 6.2. Endpoint security limits
   - 6.3. Network management
   - 6.4. Future operational deployment issues due to the introduction of the Client Facing servers themselves
   - 6.5. Migration issues
7. Potential further development of this work
8. Conclusions

End-User Impacts

Education

- Schools, for example in the US and UK, are required to operate content filtering, use the SNI data for this purpose
- Enterprise solutions may be beyond their financial or operational capabilities
- Mitigations include
    1) Disabling ECH in client software (where possible) or removing that software
    2) Abandoning BYOD

Enterprises

- BYOD is often implemented using transparent proxies, alternatives are generally more complex and more invasive of user privacy
- SNI aids content filtering in enterprises, including the blocking of access to malicious content via phishing
- Loss of visibility of SNI data as a key indicator of compromise weakens cybersecurity
- Small enterprises lack the financial and operational capabilities of multinationals

End-User Impacts contd

Public Network Operators

- Both voluntary and legally mandated blocking, filtering and takedown of illegal internet content
- Techniques include use of the DNS, SNI field or the Uniform Resource Locator (URL)
- There may be legal consequences for operators that do not comply with blocking orders

Why the Opsec Working Group?

- The draft is a good fit with the charter, covering operational issues and the potential revision of operational security practices.

- A opportunity to improve the draft:
  - Broadening the scrutiny of the content
  - Providing additional input

- Adoption?

Questions?