Application Bridging for Federated Access Beyond Web (ABFAB) Architecture

draft-lear-abfab-arch-00.txt

Josh Howlett, Sam Hartmann, Hannes Tschofenig, Eliot Lear
What is a “federation”?

• Loosely defined as "An association compromising any number of relying parties and asserting parties."
• Enables inter-domain access management for subjects to relying parties.
• Consists of
  – Technical components
  – Policy components
Further Terminology

- Identity Provider
- Relying Party
- Subject
High-Level Architecture

Identity Provider

Federation

Relying Party

Host

User Alice

Authentication

Application Interaction

Host

User Bob

[optional]
Background: EAP for Network Access

Peer
- EAP peer (supplicant)
  - EAP lower Layer (e.g., 802.11i)
  - EAP MSK

Authenticator
- AAA
  - EAP lower Layer (e.g., 802.11i)
  - EAP method

EAP server
- EAP server
  - AAA
  - EAP MSK
Privacy

- IdP is the data controller and has responsibility for compliance in terms of Directive 95/46/EC.
- Personally identifiable data, e.g.
  - Subject identifier
  - Subject attributes
- Detailed privacy requirements are dependent on jurisdiction.
- WG responsibilities lie in providing technical measures to comply to high privacy standards, for those who have the obligations to fulfill them.
Work required

• Privacy & naming
• Security properties
• User experience considerations
• Terminology
We seek your Comments!

- Some further work needed to improve internal consistency.
- Would the WG adopt this document?