# GSSAPI-EAP mechanism

Janet’s Moonshot architecture is based on the ABFAB architecture. The ABFAB architecture, Application Bridging for Federated Access Beyond Web, describes an architecture for providing federated access management to applications using the Generic Security Service Application Programming Interface (GSS-API) and Simple Authentication and Security Layers (SAML). This specifications provides the core mechanism for bringing federated authentication to these applications.

Blabla

RFC3748 discusses security issues surrounding EAP. RFC5247 discusses the security and requirements surrounding key management that leverages the AAA infrastructure. These documents are critical to the security analysis of the mechanism.

RFC2743 discusses generic security considerations for the GSSAPI. RFC4121 discusses security issues surrounding the specific permessage services used in this mechanism.

This mechanism may introduce multiple layers of security negotiation into application protocols. Multiple layer negotiations are vulnerable to a bid-down attack when a mechanism negotiated at the outer layer is preferred to some but not all mechanisms negotiated at the inner layer. One possible approach to mitigate this attack is to construct security policy such that the preference for all mechanisms negotiated in the inner layer falls between preferences for two outer layer mechanisms or falls at one end of the overall ranked preferences including both the inner and outer layer. Another approach is to only use this mechanism when it has specifically been selected for a given service. The second approach is likely to be common in practice because one common deployment will involve an EAP supplicant interacting with a user to select a given identity. Only when an identity is successfully chosen by the user will this mechanism be attempted.

The security of this mechanism depends on the use and verification of EAP channel binding. Today EAP channel binding is in very limited deployment. If EAP binding is not used, then the system may be vulnerable to phising attacks where a user is diverted from one service to another. These attacks are possible with EAP today although not typically ith common GSS-API is definitely use with trusted-third-party mechanisms such as Kerberos.