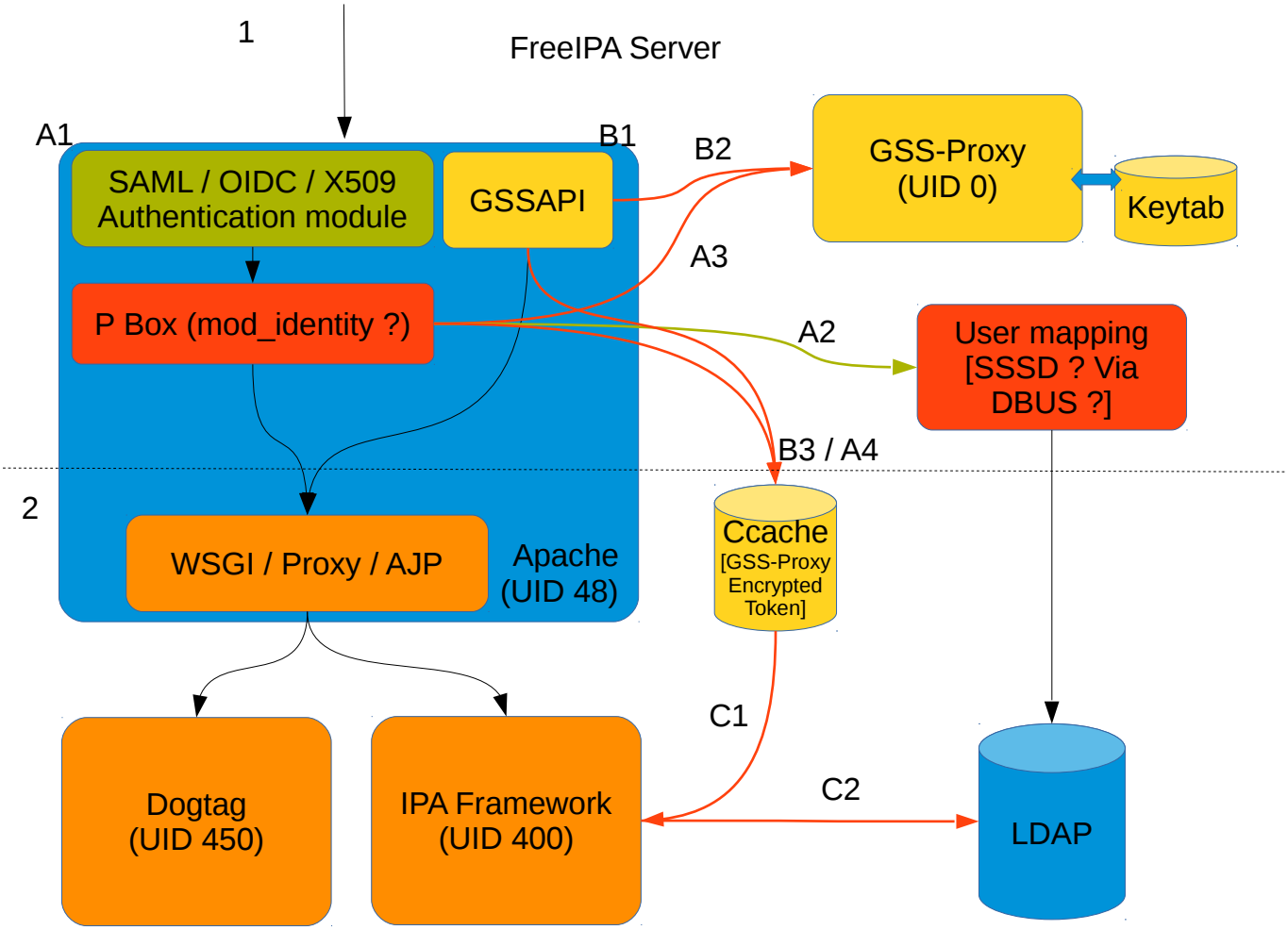

P-Box draft1

1. a web clients connects and wants to authenticate, it may be using Negotiate (B) or an alternative SSO module (A)

A1. Clients is authenticated by an apache module, no krb credentials available
A2. The “P-Box” module is used to map the incoming user to a kerberos principal
A3. The “P-Box” requests GSS-Proxy to perform a s4u2self operation and impersonate the user [GSS-Proxy must allow s4u2self only by UID 48]
A4. The returned encrypted credential token is stored in a ccache

B1. The client is authenticated by mod_auth_gssapi
B2. mod_auth_gssapi is intercepted by GSS-Proxy
B3. An encrypted credential token is stored in a ccache [ms_auth_gssapi is unaware of this]

2. At this point the user has been authenticated and a kerberos credential has been made available through GSS-Proxy

C1 The IPA Framework is interposed by GSS-Proxy and ccache and authentication via SASl/GSSAPI to the LDAp server is mediated by GSS-Proxy that allows S4u2proxy operations to obtain LDAP/host tickets from HTTP/host tickets.

NOTES:

- Only GSS-Proxy has access to the HTTP/host keytab
- All the components in the picture MUST be interposed by GSS-Proxy
- The framework and other scripts MUST be extracted and run as a different user id, mod_wsgi, mod_proxy, mod_ajp all allow this mode of operation.
- GSS-Proxy allow different operations based on the connecting client UID.
    - Ex. Apache can impersonate any user, but the IPA Framework cannot, althoguh they are all using the same credentials

With session checking/storage built into apache: