App-Identity Authorization Flow

Jeff Disher (Copyright 2013 Open Autonomy Inc.)
*Date: 2013-08-22*
Version: 1

Introduction:

Normal web applications connect to their owning identity's other applications using the following method.

NOTE: Applications using the "native" PreTrust tokens do NOT use this mechanism since the user acts as the trusted medium to set the key directly.

Steps:

1. App generates a token which it stores.

2. App contacts Identity by calling the identity.authorizeNewApplication RPC method, passing its URL and the token. Identity does not return call yet.

3. Identity contacts App by calling its application.getInFlightToken RPC. App returns the token it sent to the identity in step 2.

4. If these tokens match, the identity returns success as a packed authentication string (of the form "VERSION-KEY-STRIDE") to the caller.
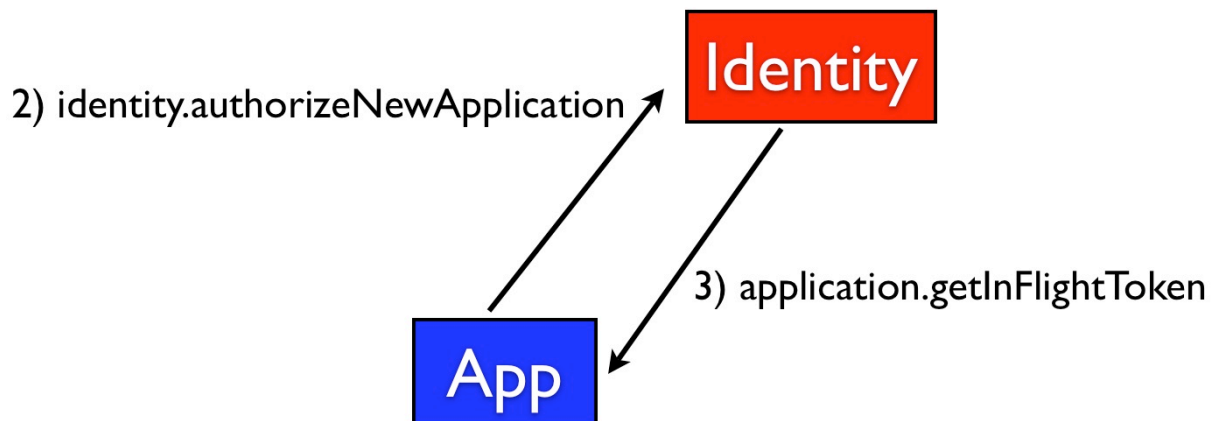
Note: This same flow is used for identity.reauthorizeApplication as the only difference is that fewer arguments are sent (since the identity already knows this application).