1) Working Group name: Native Application SSO

2) Purpose: To profile OpenID Connect 1.0 in order to enable a Single Sign On (SSO) model for native applications installed on mobile devices.

3) Scope

- define the role of an 'authorization agent' (AZA), a device resident software component that, once itself authenticated, can obtain OAuth access tokens for other native applications installed on the device
- define how an AZA might use an OAuth refresh token issued to it to obtain an access token for another native application – the access token issued by the same Authorization Server that issued the refresh token.
- define how an AZA might use an OIDC id_token issued to it to obtain an access token for another native application – the access token issued by a different Authorization Server than issued the id_token.
- define mechanisms by which an AZA can 1) be asked by a native application for an access token and 2) deliver an access token to another native application
- define a mechanism by which an Resource Server, on being presented with an access token by a native application (previously provided to that native application by an AZA), can determine how & where to validate that access token

4) Out of scope:

- How the user is initially authenticated (at time of issuance of tokens to the AZA)
- AZA client registration
- How an RS validates a reference style access token

5) Proposed specifications: Native Application SSO Profile of OpenID Connect 1.0.

6) Anticipated audience or users: Implementors of OpenID providers, relying parties, web browsers, and other non-browser applications.

7) Language: English

8) Method of work: E-mail discussions on the working group mailing list, working group conference calls, and face-to-face meetings at the Internet Identity Workshop and OpenID Foundation hosted summits.

9) Basis for determining when the work is completed: Rough consensus and running code. The work will be completed once it is apparent that maximal consensus on the draft has been achieved, consistent with the purpose and scope.

10) Background information

OAuth defines a model in which individual mobile native applications (ie those downloaded from an app store and installed into the OS) can be authorized and issued tokens to use on API calls to their corresponding servers. OpenID Connect adds to this model the ability for OAuth Clients to also receive identity information from the AS, but does not change the fundamental model of users authorizing individual applications one at a time.

As the popularity of native applications grows, and with that the number of native applications installed on an average user's device – the usability burden associated with individually managing the authentication & authorization of the set of apps will grow accordingly.

And so there is value in mitigating this usability burden by treating sets of applications *collectively* with respect to their authorization and token issuance. One manifestation of this would be to enable a Single SignOn (SSO) experience for users across some set of native applications.

The proposed model is to define the role of an 'authorization agent', a software component resident on the mobile device that obtains OAuth access tokens for some set of native applications- and so removes from the user the burden of individually authentication & authorization for those apps – and thereby makes possible an SSO experience for those apps.

11) Proposers

- Paul Madsen – pmadsen@pingidentity.com (editor)

- Chuck Mortimore – cmortimore@salesforce.com
- Ashish Jain – ashishjain@vmware.com
- John Bradley – jbradley@pingidentity.com
- Nat Sakimura - n-sakimura@nri.co.jp
- Nov Matake - matake@gmail.com

12) Anticipated contributions: 'OpenID Connect Native Authorization Agent Token Provisioning Profile 1.0' spec

(https://groups.google.com/forum/?fromgroups#!forum/native-authorization-agent)

under the OpenID Foundation's IPR Policy.