The Asynchronous Remote Key Generation (ARKG) algorithm

John Bradley
Yubico

Emil Lundberg
Yubico

ARKG

Draft 01 updates formatting
https://www.ietf.org/archive/id/draft-bradleylundberg-cfrg-arkg-01.html

The need for a technique to generate multiple public keys from a seed has been motivated by verifiable credentials use cases, that require individual proof keys for each VC instance to prevent correlation.

ARKG is one of several techniques under consideration by large scale pilots in the EU. (EWC and DC4EU)

A prototype is under development for wwWallet using a Fido extension for raw signing of VP.

Review and feedback appreciated.