1722.1 Proposal
One Time Passcodes

Ashley Butterworth
Apple Inc

What is it

- Typically our devices are not using encrypted transport of 1722.1 messages or need to be able to be setup out of the box in a potentially unfriendly environment
- We need a way to trigger an out of band, one time code that can be used with the AUTHENTICATE command to enable a controller to be able to authenticate without leaking a shared secret

How will it work

- New AEM Command is sent by the controller.
- Entity triggers the "display" of a code what form this takes is up to the manufacturer and may require additional tools from the manufacturer for the user to be able to decode. Examples include:
  - Presenting code on a built in display
  - Presenting code on a built in webpage
  - Flashing an LED with a decodable pattern
  - Generating a decodable audio signal
- User inputs the code into the controller which send AUTHENTICATE command