TEE (Trusted Execution Environment) Combined Open Source/Standards Effort

Trusted Execution Environments based on hardware-assisted virtualization such as ARM's TrustZone™ have become a standard feature in many Android devices as well in Windows Phone.

It is also likely that this provably cost-efficient way of creating local security will be a core part of future IoT (Internet of Things) devices.

Although a traditional standards effort is possible, my personal experience is that such endeavors have lost some ground to Open Source efforts. However, Open Source typically also suffers from lack of documentation ("it's in the code").

Therefore it is imaginable running a combined standardization and Open Source effort. I'm not sure how you can do that (in an effective way) within a W3C context but it might be worth exploring the options.

I would also make sure that a number of TEE-based standard applications become a part of the plot to verify its usefulness. This could for example include FIDO Alliance's U2F.

Anders Rundgren
WebPKI.org

anders.rundgren.net@gmail.com

V0.5, 2014-07-18