Tech 2021-05-11 Meeting notes

Date

11 May 2021, 8.30AM PT / 3.30PM UTC / 9.00PM IST

Meeting Link: https://zoom.us/j/97797520627?pwd=V2RiYzVXMG95eFh6VFpmZDNEOUc3Zz09

Attendees

- Tushar Behera
- John Kuriakose
- John Easterday (Intel)
- Randy Templeton (Intel)
- Prateek Chandrakar (Intel)

Goals

- Review FDO 1.0 release deliverables

Discussion items

Time	Item	Who	Notes
	Introduction	Tushar Behera	

	FDO 1.0 release deliverables	Tushar Behera	• client-sdk-fidoiot:
			  ◦ Add support for AES-GCM and AES-CCM support.
			  ◦ Rework based on security findings
			  ▪ Zeroize key material
			  ▪ L value in KDF
			  ◦ Update unit tests
			  ◦ Verifying compliance to FDO 1.0 spec
			  ◦ Defect fixes
			  ◦ (Stretch Goal) Support one ARM based platform
			  ▪ John Kuriakose It might be better to start with a generic ARM platform with Linux (e.g. RPI).
			• pri-fidoiot:
			  ◦ Rework based on security findings
			  ▪ Zeroise key material
			  ▪ L value in KDF
			  ▪ IV restriction for GCM mode
			  ◦ Increase unit test coverage
			  ◦ Verifying compliance to FDO 1.0 spec
			  ◦ Simplifying RVInfo blob handling
			  ◦ Fixing issue with Variable MTU (https://github.com/secure-device-onboard/pri-fidoiot/issues/250)
			  ◦ Defect fixes
			• ServiceInfo (Common for client-sdk-fidoiot and pri-fidoiot):
			  ◦ Use devmod:modules information while preparing ServiceInfo instructions.
			  ◦ Handling module:active true/false instructions
			  ◦ Add support for handling multiple device/owner ServiceInfo modules, prepare an example ServiceInfo module for validation, validate multiple rounds support.
			  ◦ **Note:** The objective is to validate the features mentioned in the specification, but this work item doesn't target towards creation of additional production ServiceInfo modules.
			• test-fidoiot:
			  ◦ Update to align with pri-fidoiot and client-sdk-fidoiot changes.
			• epid-verification-service:
			  ◦ A few defect fixes, creation of build script using Docker.

	FDO 0.5 Discussions		• fdo_sys documentation is available at https://secure-device-onboard.github.io/docs/0.5.0/fdo/fdo-serviceinfo-sys/

Action items

- [ ]