# Transcription for "Trusted IoT Onboarding: Updates to Draft NIST SP 1800-36" Webinar – Q&A Session

Date: Wednesday, July 10, 2024
Time: 10:00 a.m. to 11:30 a.m. (Eastern)

The NIST National Cybersecurity Center of Excellence (NCCoE) IoT Onboarding team would like to extend our sincerest thanks to each of you who attended our second webinar on Draft NIST Special Publication (SP) 1800-36. We received a number of insightful questions for an enriching and informative event!

We have prepared this Q&A response document to ensure all questions were addressed. This document encompasses all the questions submitted during the webinar and our comprehensive responses to each, along with the corresponding transcript and timestamps for those that were addressed live (see the post-event video). It is our hope that this further facilitates understanding and stimulates continued discussion. We greatly appreciate your engagement with our project and look forward to many more insightful conversations.

If you have any questions or comments or would like to help shape the scope of our future work, please contact us at iot-onboarding@nist.gov.

---

**[1:14:09]** Paul Watrobski. Principal Investigator, NIST NCCoE

**Q: So, first question: […] Are you strengthening authentication to an air gapped MFA tool? App-based auth is not secure. So, I think this is a general question to everyone. It does go back to the general architecture. We might come back to this one.**

Nick Allott, CEO, NquiringMinds

A: Authenticating what against what? That was the only reason I couldn't really answer that.

Paul: If [the commenter] wants to add additional information in the Q&A, we can answer this better.

Paul: Oh, let's see, [the commenter] said, I have found a root compromise in our present-day OSes […] We'll come back to this question.

**[1:15:47]** Paul Watrobski. Principal Investigator, NIST NCCoE

**Q: This was, I believe, during Build Four: […] As open source, are you continually running CVE scanners?**

Brecht Wyseur, Senior Product Manager and Product Strategy, Kudelski IoT

A: I'm not sure if this was a question towards Build 4, because it was asked around that same time. And I did mention during my introduction that we have built Four using Thread networking. And I mentioned that Thread is open source, so maybe that's why the question came.

Nick Allott, CEO, NquiringMinds

A: Build 5 is open source, as well. So, yes, we do it offline. I think the potentially interesting thing about Build 5 is we can interrogate the SBOM real-time at the point of network onboarding. So, the individual [...] or pledge device is implemented with software. There is an SBOM for that software, and using the protocols that we designed, you can pass the SBOM to the policy engine, and the policy engine will make that live CVE assessment. So, sort of, yeah.

**[1:17:06]** Paul Watrobski. Principal Investigator, NIST NCCoE

**Q: I think this was during Build 5: […] Are there restrictions to the size of the certificate as we migrate to stronger NIST standards?**

Nick Allott, CEO, NquiringMinds

A: I think Brecht partly answered this; I think this is similar to his answer. In theory, no. The abstract protocols will support arbitrary certificate sizes.

Paul: Right, and I imagine [...] any restrictions to the size would have to do with the storage space of that device.

Nick: The storage space or occasion – I mean for us because we're just negotiating over IP, it will handle it. If you've got a lower-level negotiation protocol, sometimes you'll hit over a frame or packet size, but for us, it's not a problem.

Brecht Wyseur, Senior Product Manager and Product Strategy, Kudelski IoT

A: The only limitation [is] the capability of the hardware root of trust that we have leveraged.

**[1:18:05]** Paul Watrobski. Principal Investigator, NIST NCCoE

**Q: Are you looking at CBOM tool sets as well? CBOM being Cryptographic Bill of Materials.**

Nick Allott, CEO, NquiringMinds

A: I think that the methods that we developed will be totally extensible to CBOM. I think there's probably a little bit more fine tuning to get the SBOM working perfectly first before we open the scope up, but [...] the abstract policy negotiation method, yes, it'd be very easy to do.

**[1:18:38]** Paul Watrobski. Principal Investigator, NIST NCCoE

**Q: [This question was submitted] during Build 6. The question is, aren't self-signed or generated certificates prohibited in federal environments?**

Steve Clark, Security Technologist, SEALSQ

A: So, the self-signed—that actually isn't what we did here. We actually had a certificate authority that was a publicly trusted authority potentially, or a custom certificate authority, doing the signing of our birth certificate. We did that through an online certificate management service, so there was an API that the Raspberry Pi called out and got a certificate that we actually had signed. So it wasn't self-signed at all.

Paul: I believe that may be the case for federal environments. [...] But another point to bring up about this project is it's not necessarily just for federal environments; this also has to do with consumer use case and enterprise as well. So, there may be other applications where that may be appropriate, but yeah, excellent. Thank you for that answer, Steve.

**[1:20:01]** Paul Watrobski. Principal Investigator, NIST NCCoE

**Q: Another question here: […] Will you be able to update the firmware as required, as securely as bed of nails? I think this was during Build 6.**

Steve Clark, Security Technologist, SEALSQ

A: Yeah, so basically what you would be doing is a different process that would be more at the application layer. You would provide a secure platform, secure update facility – some kind of ability along those lines it would be. Secure boot would verify whatever firmware that you have. You could use our secure element for that, or the TPM, or whatever platform hardware that you have, can verify the firmware at boot time and at update time, so that would be more of an application layer leveraging this particular secure element and capability. So, yeah, that's absolutely possible.

**[1:21:10]** Paul Watrobski. Principal Investigator, NIST NCCoE

**Q: I think the next questions were for Build 1, so this was to Dan – the comments on the US Cyber Trust Mark. Does this help bring or enable trustworthiness? […] Does the Cyber Trust Mark bring or enable trustworthiness, or does what was done in Build 1 bring trustworthiness?**

Dan Harkins, Fellow, HPE Aruba

A: I think it's the other way around. […] What DPP does is provide trustworthiness and the [...] robust onboarding of a device that will provide the trustworthiness of the resulting network.

Steve Clark, Security Technologist, SEALSQ

A: The Cyber Trust Mark has a bunch of different requirements that include things like secure identities and secure communication. So, there's a whole host of requirements, and secure onboarding is among those requirements.

Paul: We have gotten some questions before this webinar regarding the relationship between the Cyber Trust Mark and this project. In our practice guide we do reference the Cyber Trust Mark and essentially the work that supports that. And I think vice versa, as Steve had mentioned, secure onboarding is something that is mentioned in the Cyber Trust Mark, [or] rather, NIST IR (Internal Report) 8425, which is the basis for that Cyber Trust Mark. That said, it's not like you have to be able to implement everything that's done in our architecture that we have in this project in order to […] earn that trust market. There's kind of, there are two separate things that, in a way, do interconnect, but it's not a requirement of any kind.

**[1:23:34]** Paul Watrobski. Principal Investigator, NIST NCCoE

**Q: Next question: […] Is Wi-Fi 6 supported [for Build 1], or [are] there plans to support that?**

Dan Harkins, Fellow, HPE Aruba

A: It is, yes. Of course, you need an access point that supports Wi-Fi 6, but yeah, DPP is Wi-Fi agnostic; it'll work over any band. It does have independent discovery mechanisms for different bands because there are different regulatory requirements for each of them, but there is a different way for devices to be discovered using DPP.

**[1:24:16]** Paul Watrobski. Principal Investigator, NIST NCCoE

**Q: Next question is for Build 2: […] Is there any instantiation also envisioned in relation to FIDO onboarding approach?**

Andy Dolan, Senior Security Engineer, CableLabs

A: The short answer is "not presently." We haven't expanded on this, and we don't have plans to. But to expand on […] what I discussed in the application section of Build 2, any onboarding methodology would be possible as long as you're exchanging […] some type of metadata. So, if you wanted to loop in a secure token as part of that, or a hardware token, that's a possibility, right. […] For example, in OCF—not that this is FIDO-token specific—there is a challenge response method of onboarding that involves […] entering a one-time passphrase or one-time code that's generated by the device, right. So, there are other alternatives and ways that you could integrate this that I could foresee where you could include a hardware token. That's my take on it. I hope that answer to that question helps.

Dan Harkins, Fellow, HPE Aruba

A: One of the nice things about DPP is that the provisioning protocol is extensible, and you can pass […] other bits of information. And if you wanted to pass, for instance, a FIDO token, that could be done so that your device could then host DPP to do whatever sort of specific application-layer onboarding it wants to do.

Craig Pratt, Lead Software Engineer, CableLabs

A: Yeah, and […] in case it wasn't obvious, that was the technique being used to convey the credentials for layer four onboarding that Andy used for OCF.

**[1:26:32]** Paul Watrobski. Principal Investigator, NIST NCCoE

**Q: We have a few questions that have come up during the Q&A, so these may be more generalized questions […] Can these techniques be adapted to existing networks with large scale IoT device deployments? So, I think we can kind of open it up to each of the builds to address.**

Dan Harkins, Fellow, HPE Aruba

A: Yeah, definitely. So that's what I was trying to highlight, is that the DPP adapts the network you have. It doesn't require you to re-architect your network, just start using it. So, depending upon how your existing IoT devices are connected, you can use DPP to onboard devices using the same types of credentials, or a different credential if you want. So, it allows you to basically grow as new technology does.

Nick Allott, CEO, NquiringMinds

A: I think, just to follow on from our perspective, some of them yes, some of them no. You can get away with sort of upgrading your network relatively easily, but if you want the real benefits of, you know, unique identities and unique networking credentials on the IoT device. Clearly that IoT device needs that capability, which probably isn't the case at the moment. To answer that question is probably quite nuanced because you have to look at the individual security features. Certainly, there are subsets of them from our perspective which could be retrofitted on a pre-existing network, especially if you can upgrade the end device.

Craig Pratt, Lead Software Engineer, CableLabs

One thing […] I would add to that is one thing that's not generally known, is that Wi-Fi, in general, devices can have unique credentials. The challenge is whether a device is […] Wi-Fi-enterprise-enabled, or personal-profile-enabled. If you want to go back and look at the paper, a little bit, I would say, we came up with a somewhat unique way to deal with that that allows existing Wi-Fi devices with WPA 2 personal to be provided unique passphrase credentials that enables the ability for device management, as I kind of touched on in my presentation. So, adapting the network's great. If you can't adapt the devices, there's answers for that, too, which […] I covered in the publication.

**[1:29:40]** Paul Watrobski. Principal Investigator, NIST NCCoE

**Q: I do see another question that came up from during the Q&A […] So, "code signing as per White House requirements next year?" So, I'm guessing this has to do with verifying firmware updates or that sort of thing as part of the continuous process. Is that something that's being implemented in any of the builds?**

Nick Allott, CEO, NquiringMinds

A: So, Build 5 does part of it, not all of it. So obviously, the whole point about doing the negotiation is allowing you to establish some of the benefits of […] verifying the software service at point of onboarding. In our current implementation, we don't do the sort of trusted boot for firmware attestation, but if you add those pieces in, then pretty much you've got the complete stack to allow you to implement […] a code signing validation at point of onboarding. But it's tricky to do end-to-end.

**[1:31:02]** Paul Watrobski. Principal Investigator, NIST NCCoE

**Q: So I see there's a follow up. This was directed to Craig, concern being with "Wi-Fi continues to be sidelobe vulnerabilities." Is that being addressed in any sense?**

Craig Pratt, Lead Software Engineer, CableLabs

A: No, that's not really in the context of what we're working on. But it'd be great to hear a little more about that, but I don't know. We can flip the script on the person who posted the question, but no, […] that was out of scope for what we were doing.

**[1:34:19]** Paul Watrobski. Principal Investigator, NIST NCCoE

**Q: Firmware update and code signing; CLM is an overused meaning. I'm not sure if anyone is able to address that. If that provides more context regarding cert. life cycle tools. So, I'll give a quick moment here, and we may have to follow up.**

Steve Clark, Security Technologist, SEALSQ

**A:** I think I could address that a little bit. The certificate management tool that we are using actually provides enrollment over secure transport, which is a standard way of doing the certificate lifecycle management. And the way that works is the birth certificate is used as a foundational identity for the device, and at enrollment time for network layer, any other certificates that you need, the authenticity is—the IoT device actually calls home and gets a certificate, or whatever it needs to get a certificate for. And as you want to push out new certificates or reissue certificates, or that sort of thing, throughout its life cycle, you can manage the certificates using this secure connection enrollment over secure transport, and that capability is enabled in the certificate management service that we have. So that may be useful.