Device Identity Forum (DIF)

May 15, 2025
Introduction, Goals and Workplan

Agenda for 2025-05-15

- What is this forum about? (10min)
  - Why is this forum occurring now?
- What is it we are going to do? (10min)
- Who should be involved? (10min)
  - Are you the right person, or can you find the right person?
- How to get involved? (10min)
- Questions (20min)

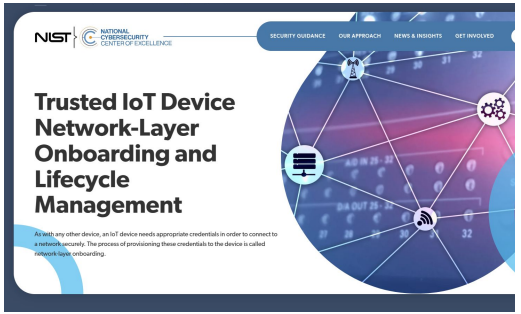
What is this forum about? What are Device Identities?

- Device Identities are cryptographically strong credentials that are installed into devices.
- They identify both the unique identity of the device (“serial number”), as well as point to the device type.
- The credential can be in a Secure Element, TPM, Trusted Execution Environment (or not).
- They credential can be used to sign Evidence for Remote Attestation (the “AK” in a TPM).
  - External Endorsements can be attached to this key
- They can be provisioned in the factory (IDevID), or in the field (LDevID) in both greenfield and brownfield situations.
- Today: RSA, EcDSA (EdDSA). Later on, we’ll need Quantum-Safe versions.

Why is the forum starting/occurring now?

- It was time. It took some in-person time to properly explain (vs COVID)
- The NIST NCCoE IoT Onboarding project identified a new for more understanding of factory installed identities.
- Maturation and deployment of: DPP (Wi-Fi EasyConnect), CSA MATTER, BRSKI, OPC UA and other onboarding protocols have **device identity** as a core requirement
    - This should be easy.
    - It is easy, but people don't know that.
- UK,California,CRA and other jurisdictions putting new requirements on IoT devices…
    - but how can operators know what device is which?

https://www.nccoe.nist.gov/projects/trusted-iot-device-network-layer-onboarding-and-lifecycle-management



Who is the IoT Security Foundation?

- Formed in 2015.
- Annual Fall Conference
- "help *make it safe to connect"* so the many benefits of IoT can be realized.
    - Through a dedicated program of guidance, reports, events, training, standards, advocacy and so much more, we represent a collaborative international response to the wicked challenge of IoT insecurity.
- Security Best Practice – Why & How?
- The IoT Security Assurance Framework
- IoT Security Self Certification
- No Universal Default Passwords
- Keeping Software Security Updated
- Vulnerability Reporting and Disclosure Policy

We are the Super Blue Team, and we're here to help. The Internet of Things Security Foundation (IoTSF) is a not-for-profit, global membership association working to make the connected world ever-more secure.

In unity we have strength. We each have a valuable role in keeping the digital world secure. Our stakeholders include IoT hardware and software product vendors, network operators, system specifiers, integrators, distributors, retailers, insurers, local authorities, academic institutions, government agencies security professionals, researchers and risk managers – anybody with an interest in cyber safety, security and privacy.

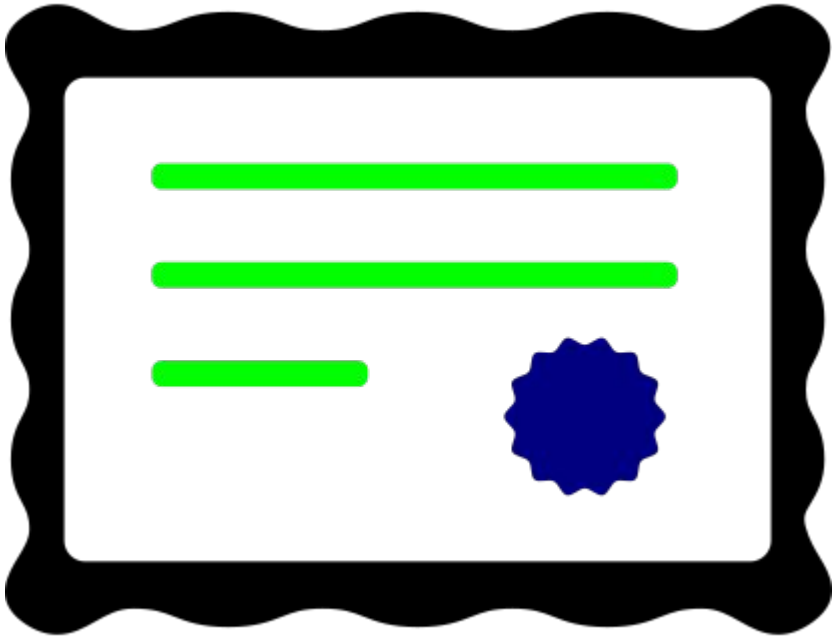
https://iotsecurityfoundation.org/

What is the forum going to do?

1. White paper(s) explaining how to do device identities.
   a. This is likely in the form of success stories. Maybe like *The Goal* https://en.wikipedia.org/wiki/The_Goal_(novel)
   b. NDA-free Technical explanations of what to do, what the choices are. A menu of a few choices, rather than starting from scratch each time: “Yes, I’ll have the Quarter Pounder without onions”
   c. *Something something Quantum-Safe something.*
   d. Certificate, CA lifetimes, Brownfield updates, ways to connect to MUD
   e. The connection between device identities, IDS and asset management
2. Creating a common language to talk about device identities.
   a. English words and sentences.
   b. Elevator pitches suitable for C* Suites.
   c. Common icons for important ideas/things
   d. Some reusable slideware collateral for use in (outward) facing presentations
3. A common place to talk about limitations, confusions and other obstacles.
   a. With, ideally, Chapter House rules on attribution.

For Instance.

- I hate this using this icon.
- It’s a certificate.
  - No, it’s a diploma.
- What kind of certificate is it?
- Subordinate CA?
- EE certificate?
-



For Instance.

- What about this MS icon for PKI?
- Does it say Certification Authority to you?
- How would one represent that?
- How about a Subordinate CA?
- What if it’s on-prem, and not cloud?

For Instance: Trust Anchors!

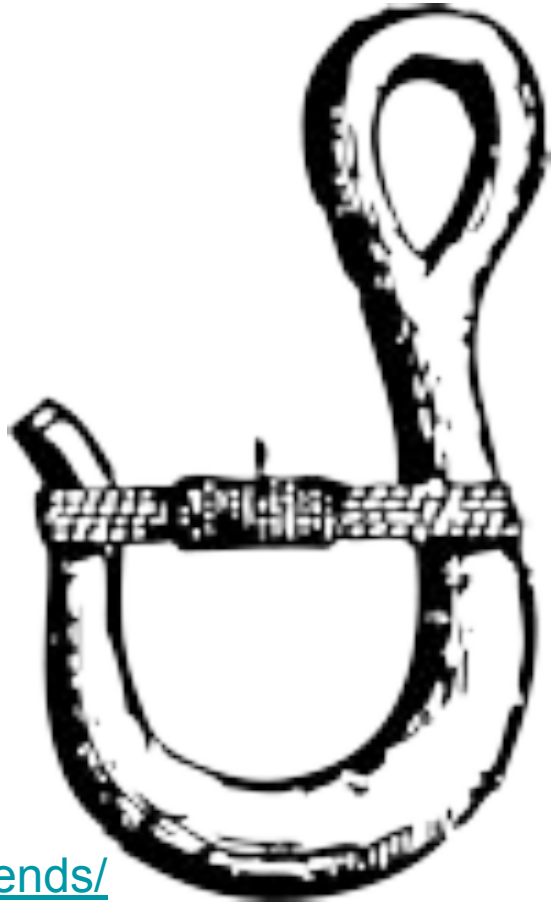
- What if the certificate is self-signed…
- So, it's really a Trust Anchor?
- Why do I care so much about icons?

65% of the world's population are visual learners. (Source)

>50% of human brain's surface is used to process visuals. (Source)

Humans can remember **65%** of visual information **after three days**. In comparison, **after three days**, people retain only **10-20%** of written or spoken information. (Source)

It takes the brain **13 milliseconds** to process an image. The brain can also see images that last for just **13 milliseconds.** (Source)



https://nikolaroza.com/visual-learning-statistics-facts-trends/
(lots of references)

NDA-free palette of choices

- A number of organizations that do provisioning have said (quietly) that they wind up with a *unique* workflow per customer.
  - A document describes the details, and it's then covered by NDA.
    - Even the existence of the document might be covered by NDA.
  - Aside from cost, there is the bug-tracking/fixing challenge, which is multiplied.

NDA-free palette of choices

- A number of organizations that do provisioning have said (quietly) that they wind up with a *unique* workflow per customer.
  - A document describes the details, and it's then covered by NDA.
    - Even the existence of the document might be covered by NDA.
  - Aside from cost, there is the bug-tracking/fixing challenge, which is multiplied.

- But, 90%+ of the workflows are the same.
  - Just some are without Onions, and others are without relish
  - Can not merge workflows, because NDA forbids sharing of document contents.
- If only they could cite some Forum documents for the 90% which is identical.
  - "Meat-like thing in a bread-like container"

Brownfields, LDevID and Operational Identities

Note every device out there can do zero-touch onboarding!

Some devices are already onboarding, but still need local identities.

- Can we converge on a few good, well-supported protocols? Dealing with: Airgaps, copy&paste methods, and “factory” generated private keys.
- Operational certificates still need infrastructure. Trust anchors, HSMs, subordinate CAs, and lifetimes.

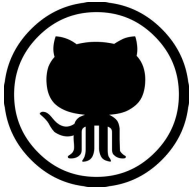
Private PKIs vs WebPKIs vs CABForum specified lifetimes

Most Device Identities will be from a private PKI.

Most Operational Identities will also be from a private PKI.

- MOST. Not all? It's hard for home/end users to run HTTPS at their homes. Not impossible through.
- Many larger Enterprise/Industrial users can deploy private trust anchors via MDM or other mechanism, and can do intranet/split-DNS for naming.
- But: are there users in between? Too big for no security, too small to be able to manage things themselves?

How will the forum operate?



- There will be an email-list.
- A stable place for results on iotsecurityfoundation.org
- There will be a git(hub) organization with documents (if using markdown)
- There will be a Google Drive folder with documents (if using Docs)
- Document and Presentation authoring/collaboration
- Existing IoTSF basecamp instance with planning, schedules (announcements)
- An approximately monthly teleconference (~9 times/year)
    - Some meetings will probably include presentations from participants about how they got to device identities. Lesson learned. What went well, what went poorly.
    - Most meetings will consist of recap of changes to documents, and will be working sessions
- Outward presentations/ambassadors to other SDOs/pseudo-SDOs/Interested parties

Who should be involved?

https://www.youtube.com/watch?v=TAJuBOtTpeQ
In 1970s, brilliant marketing from Rowntree turned the red-dye disaster into a plus.

- This effort is probably 40% (technical) marketing.
  - Product Line Managers (PLM)
  - People who code, and people who communicate about writing code
  - People who attend standards bodies, who write and review the standards
- It’s probably another 20% old-fashioned marketing
  - Marketing/Communications people
  - We need some artists/visually creative people
- The rest is technical work
  - Renewals, EST, CMP, SCEP.
  - Lifetimes, Quantum-Safety,
  - What’s possible. What’s easy. What’s not worth the effort.

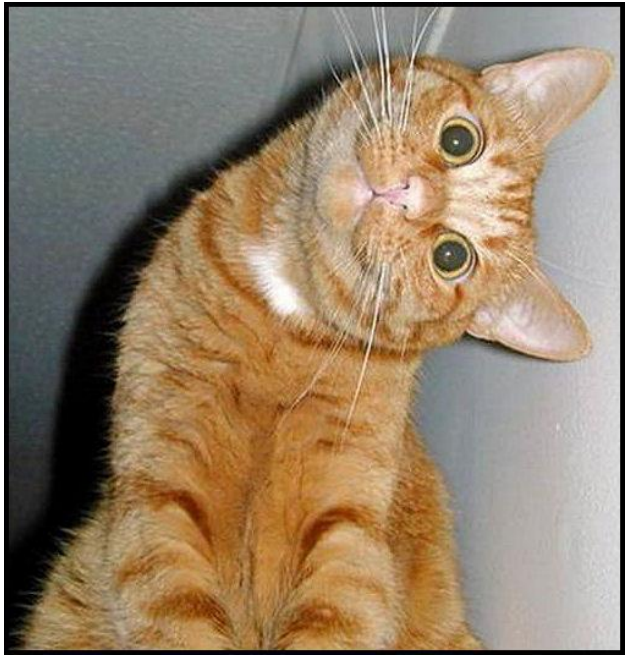
How to get involved?

- Are you the right person, or can you find the right person?
- We will send out a summary of today's meeting by email with next steps.
  - Please use the discussion time to say how you would prefer to interact.

- The IoTSF has some IPR policy, which you will have to agree to
  - Basically: you need to be aware of when you are contributing something you may have a claim to, and to let us know.
  - IoTSF membership is *not* required to join this WG
    - (but, encouraged)
- https://iotsecurityfoundation.org/constitution/
  - "*A Member (individual or representative of a member organisation), making a contribution which is designated as such in writing to an IoTSF collaborative project or works ("Contribution"), grants IoTSF a worldwide, irrevocable, nonexclusive, non-transferable, royalty-free and sub-licensable copyright license to reproduce, create derivative works, distribute, display and, perform the Contribution(s) solely for the purposes of IoTSF developing, publishing and distributing best practices or specification documents incorporating Contribution(s) to which such Contribution(s) was submitted.*
- IPR documents being revised/simplified right now, and are dealt with 1:1 for the moment, but that will get sorted.

Discussion!

- What is this forum about?
  - Why is this forum occurring now?
- What is it we are going to do?
- Who should be involved?
  - Are you the right person, or can you find the right person?
- How to get involved?
- Questions (20min)



DIF = Device Identity Forum