Machine identity is hard.

- Every device, among billions, must be uniquely identifiable.
- Every device must have unique cryptographic keys that it can use to sign all data it produces.
- These cryptographic keys must be stored in secure hardware, like a TPM, that can run cryptographic operations in hardware. This way the secret keys never leave the hardware and cannot be stolen remotely using firmware vulnerabilities.
- There should be a record of exactly what hardware makes up a specific device.
- There should be a record of exactly what firmware is installed in a device and signed acknowledgments for every firmware update that is applied.
- Every message from a device must be cryptographically signed.

And a lot more.

We, the IoT community, must work together to drastically simplify device identity provisioning and management.