Immutable, digitally signed, verifiable attestations about the life of a device.

We can then answer ...

- Was the device made by a reputable manufacturer?
- Does the device have hardware based cryptography and secure key storage?
- Does the device have unique identity and cryptographic keys?
- Has the device been audited by a security auditing firm? Is there a signed audit proof?
- Are there any known vulnerabilities for the device hardware/software?
- Does the device produce signed data and signed firmware acknowledgements?
- Does the device have the latest firmware?
- Who installed the device? Who provisioned the device?

etc.