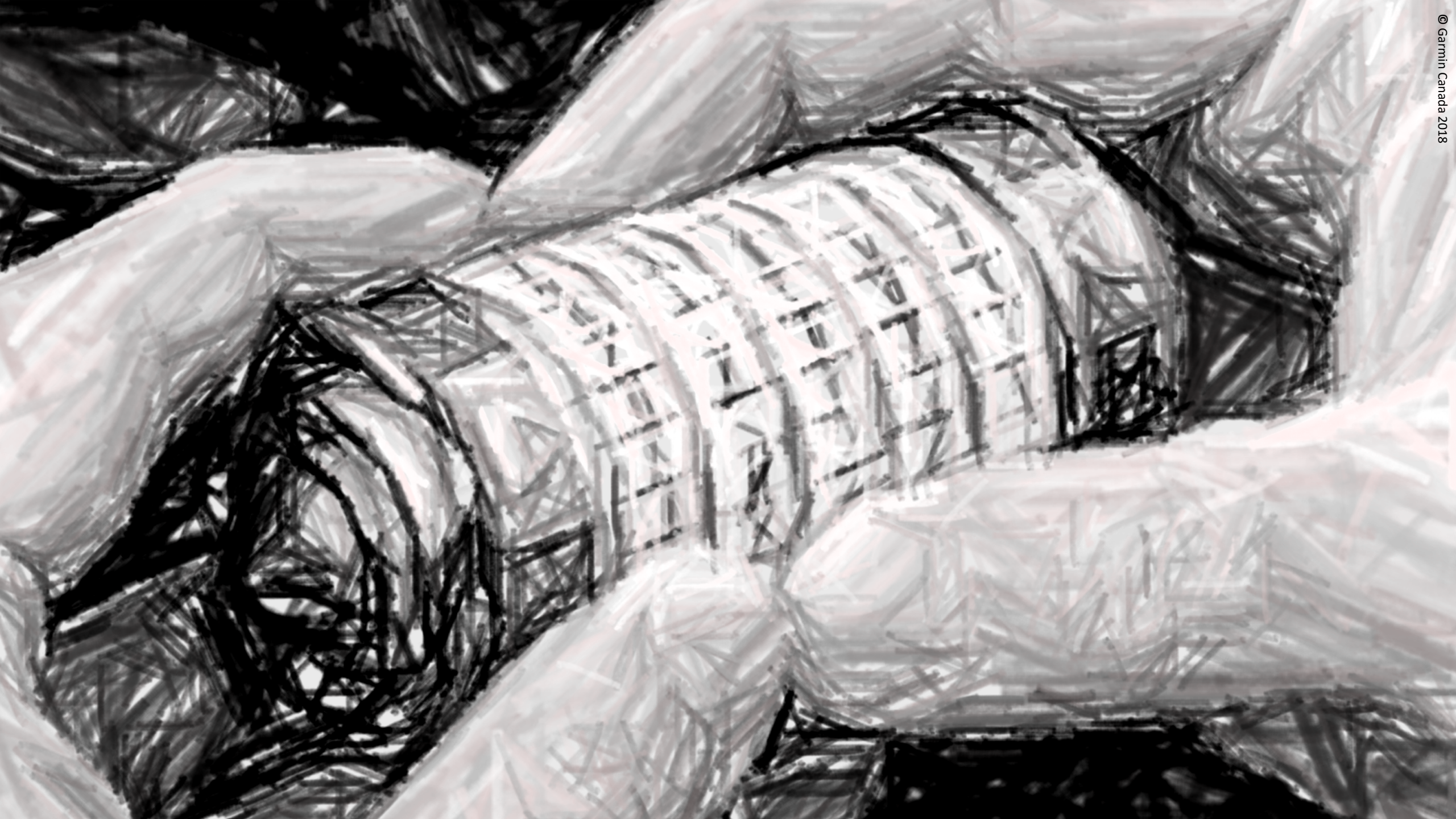
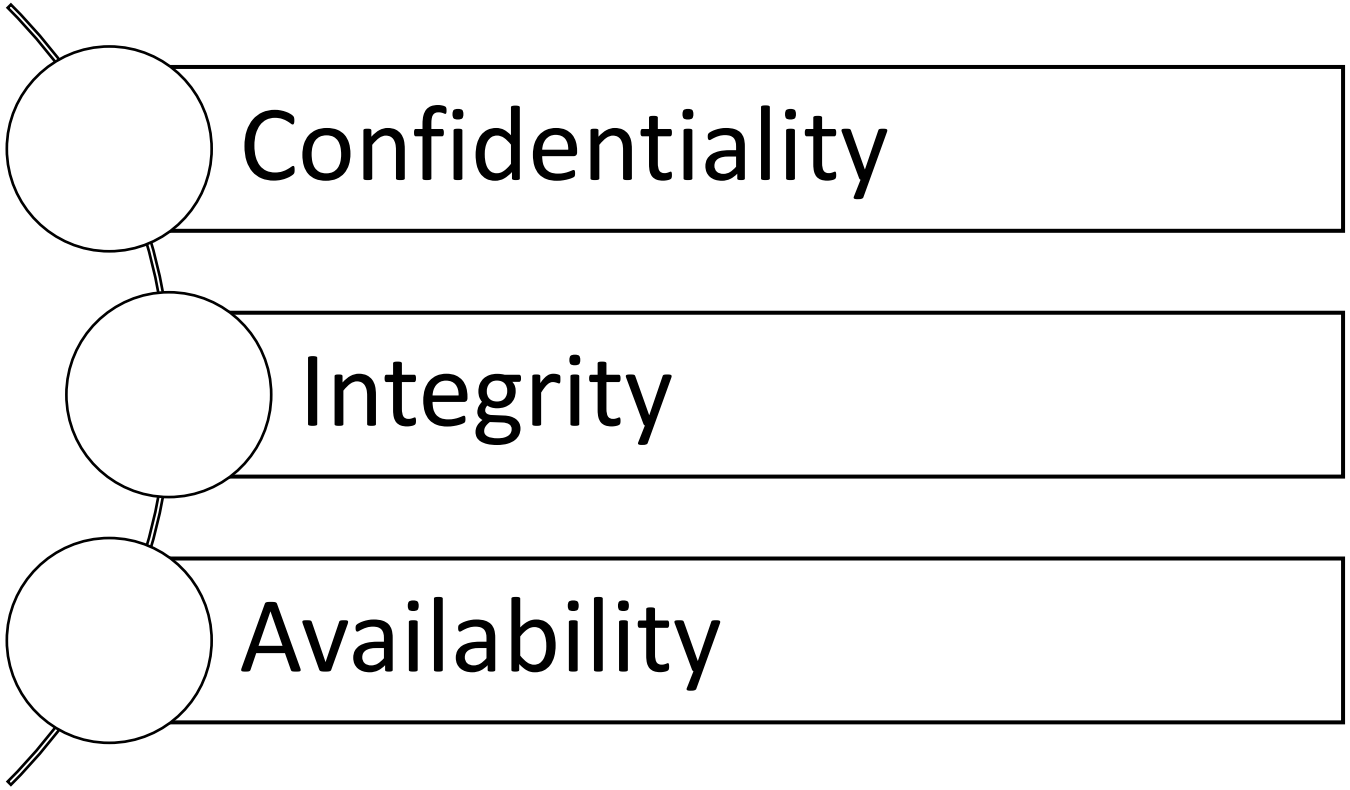


Authentication in ANT+ SMS

Beenish Khurshid, Applications Engineer | ANT Wireless

Fundamentals of Security



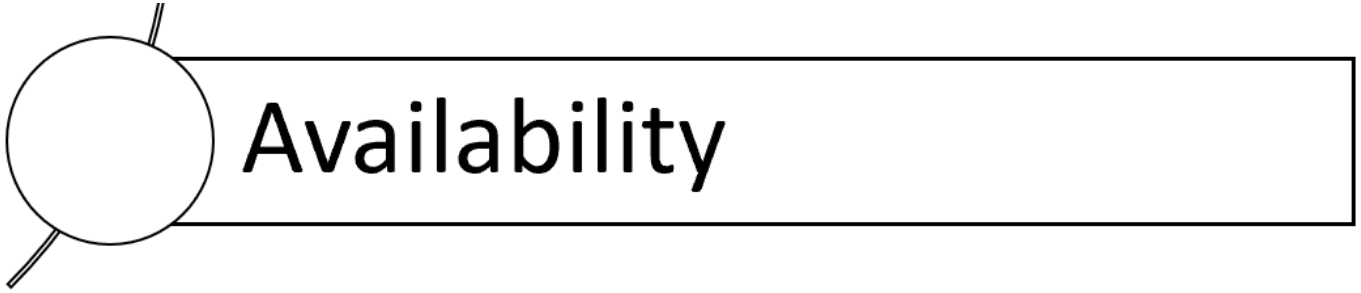
Confidentiality

“The state of keeping or being kept secret or private.”

Integrity

“that a message has not been tampered with or altered.”

“the ability of a user to access information or resources in a specified location and in the correct format”



The Hype

One Size Does Not Fit All

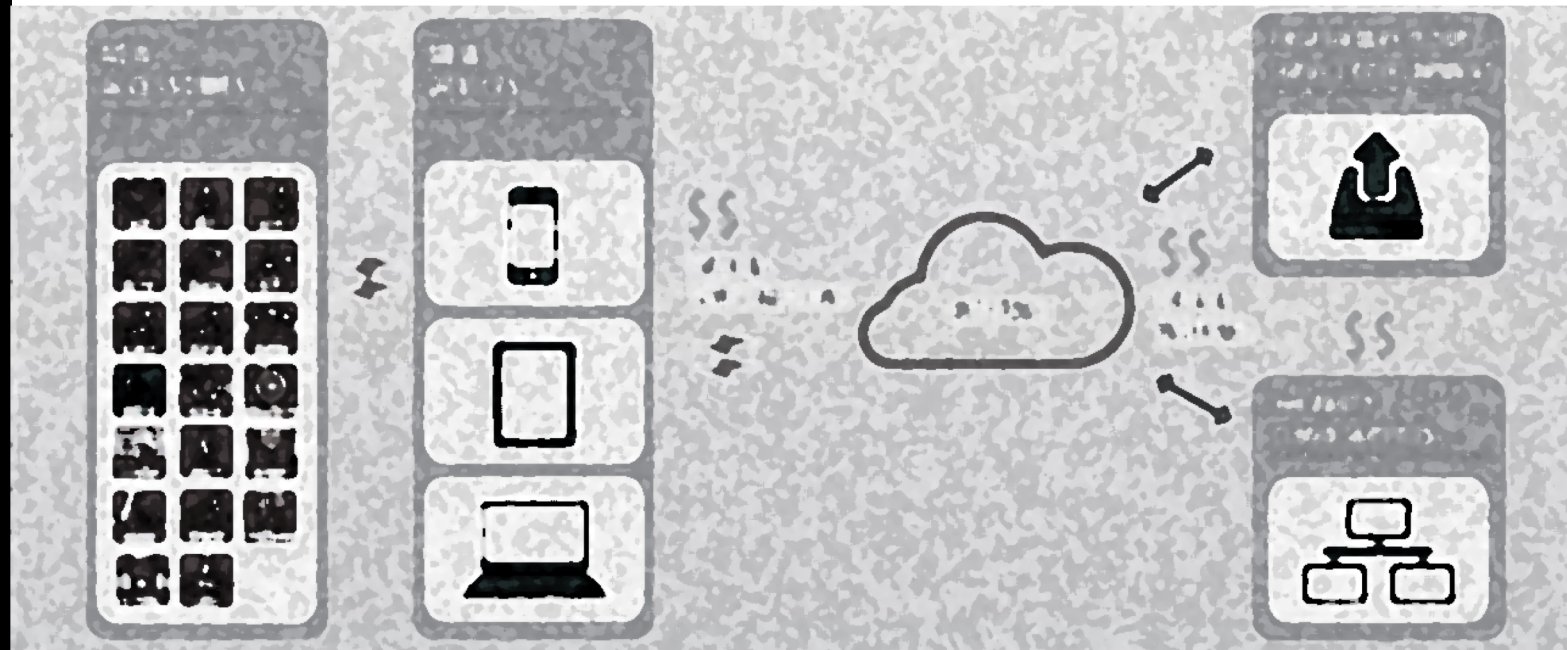
What is Best for Your Solution?

How much will security cost?

What user story does security address?

Is security being done right?

The right technology for your use-case



inReach Mini

ANT+ SMS

Use Case:

- Allow a display device to send and receive message via a messaging gateway

Mis-Use Case

Goal:

- Protect user from a bad actor racking up bill, or triggering an SOS

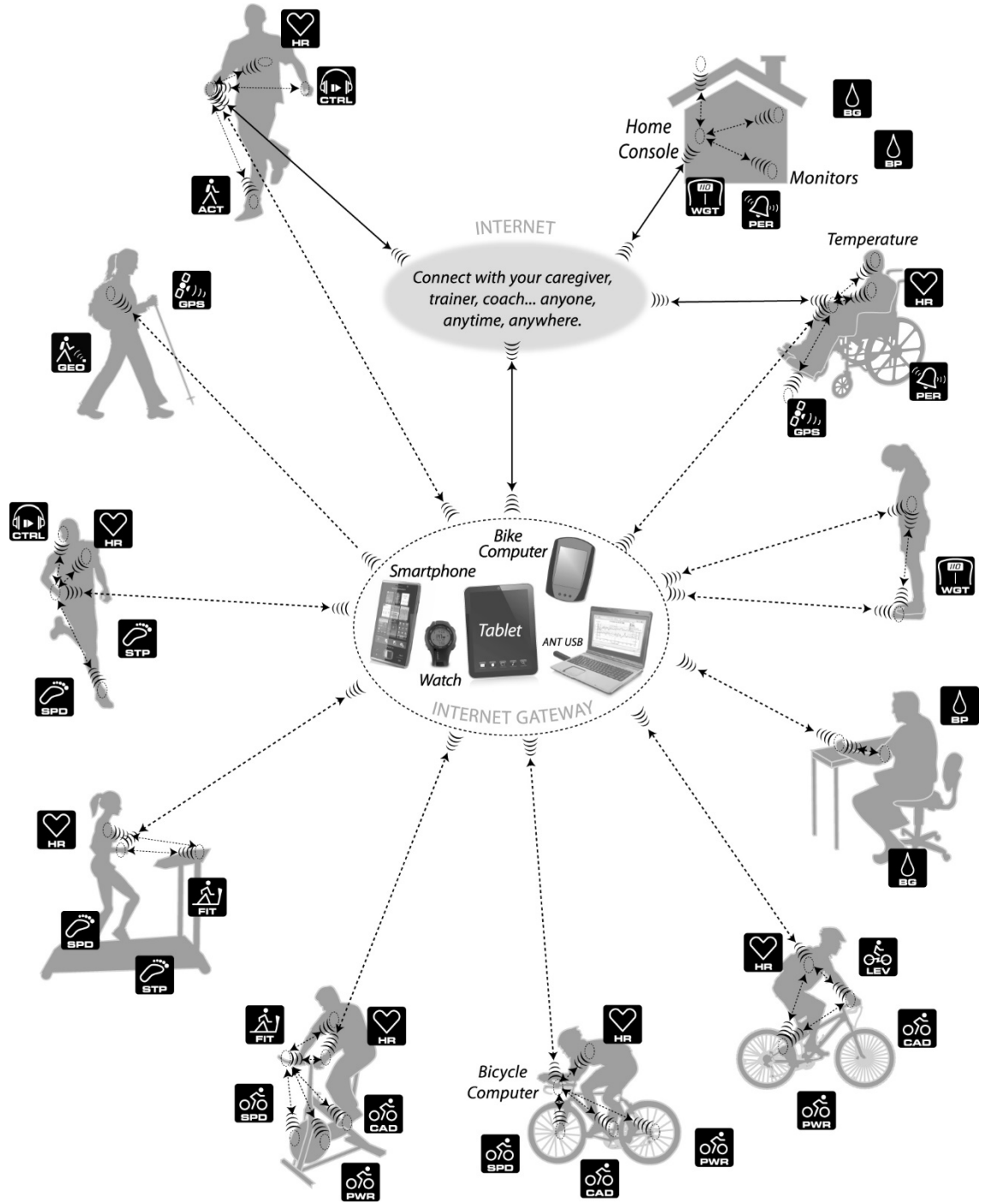
Solution:

- Authentication and Key Exchange

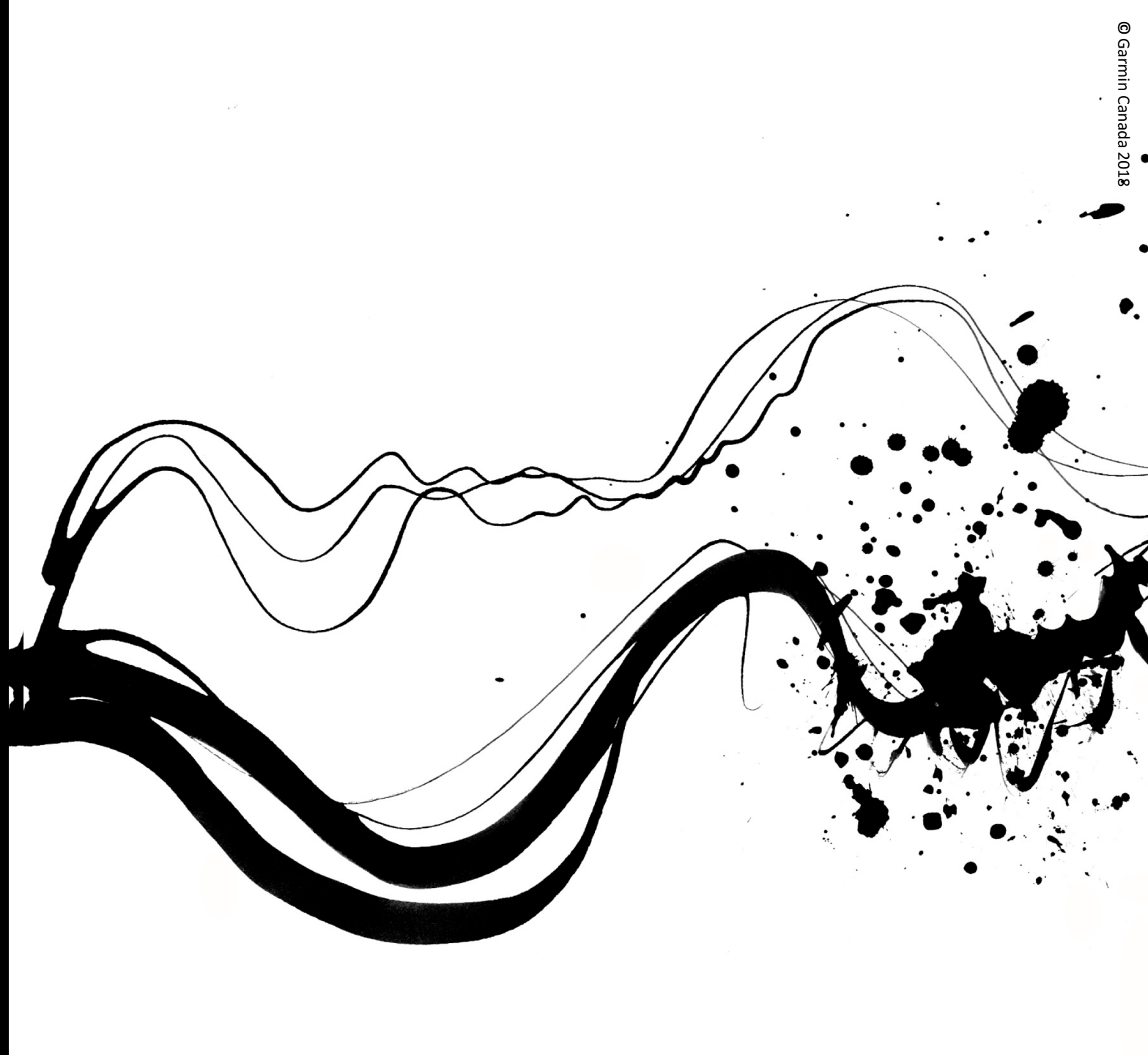
Demo!

The Current Ecosystem

- Open Ecosystem
- Easy access to data
- Smooth user experience
- Ideal for:
  - Non-controllable sensors
  - Personally non-identifiable data



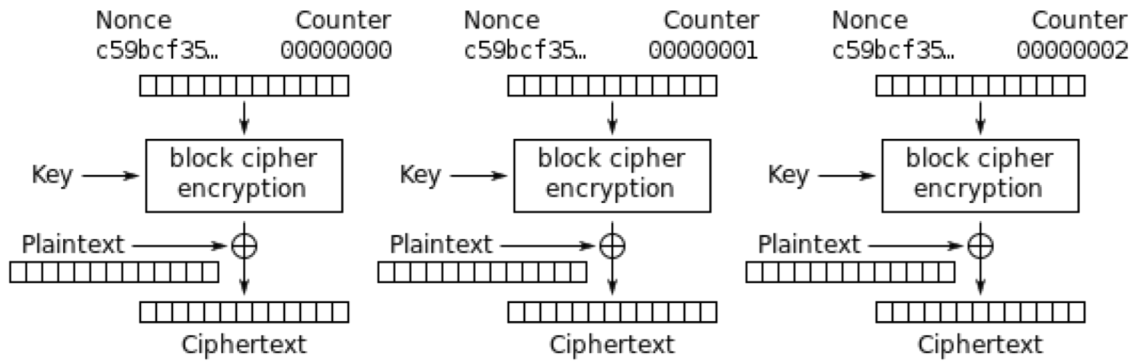
Enabling Secure Use-Cases



What's Already There

Encrypted Channels

- Handled natively by the ANT stack
- One master to many slaves possible



Counter (CTR) mode encryption

Trade-offs:

- 3% increase in battery consumption

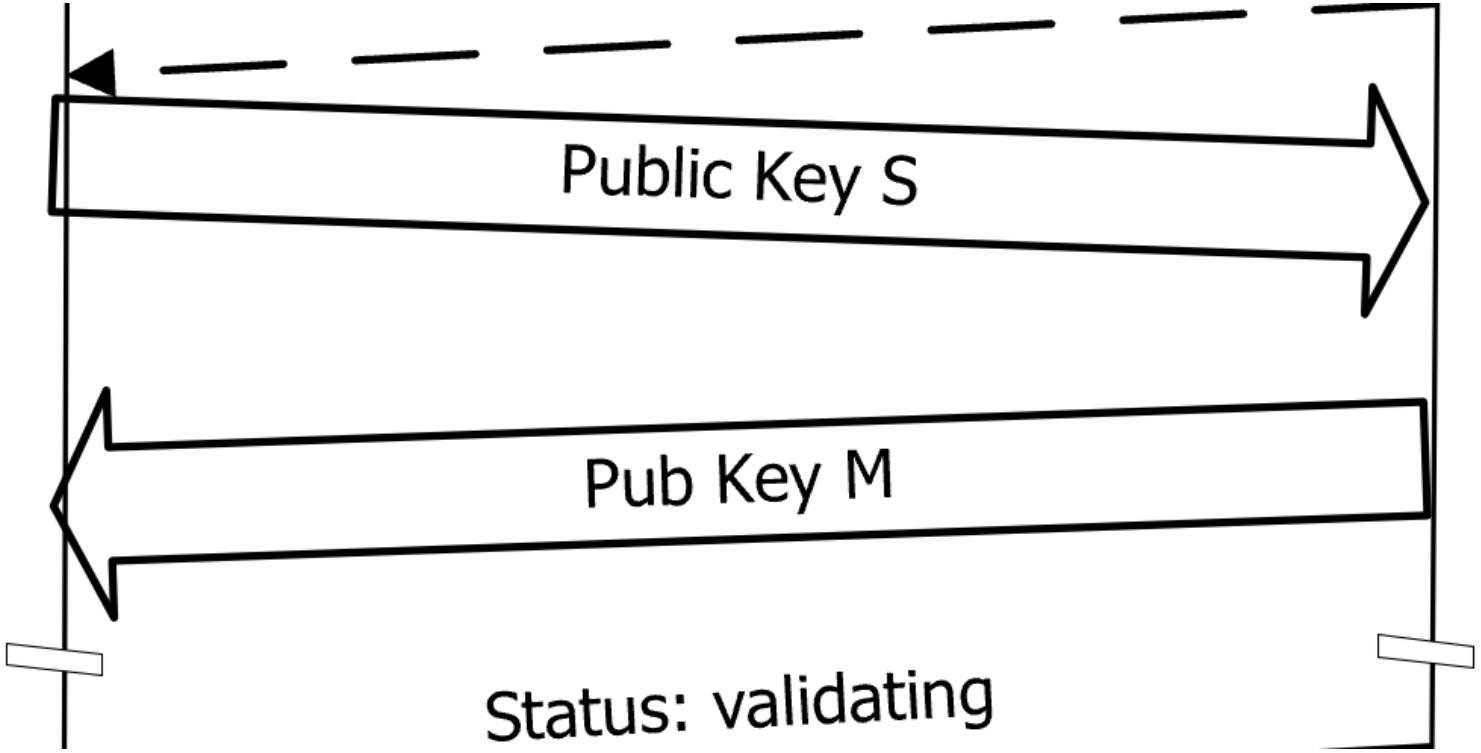
Limitations:

- Not supported on older chips
- No way to exchange shared secret

What's New

Key Exchange

- Ability to establish a shared secret between two devices
- Shared Secret can be used as an authentication key



Trade-offs:

- Increased code size

What's New

Authentication

- Standardized method for a master device to validate a slave as a trusted controller
- Ability for a slave to send authenticated commands
- Support for multiple authenticated slaves

Trade-offs:

- 6 digit display required on both devices

Why ANT?

Expert Reviewed, and Standardized

- Vetted by world-renowned security expert
- Certification of implementations
- Standardized protocol (key exchange and authentication)
- Comes with stack (Encrypted Channels)

Low Resource Cost

- Minimal RAM/ROM hit
- Low Power

Built for the Future

- Device report’s security version number
- Requirements to support firmware update

Thinking Ahead

Linking Key Exchange and Encryption

- A standard that uses ANT Key Exchange to enable ANT Encrypted channels

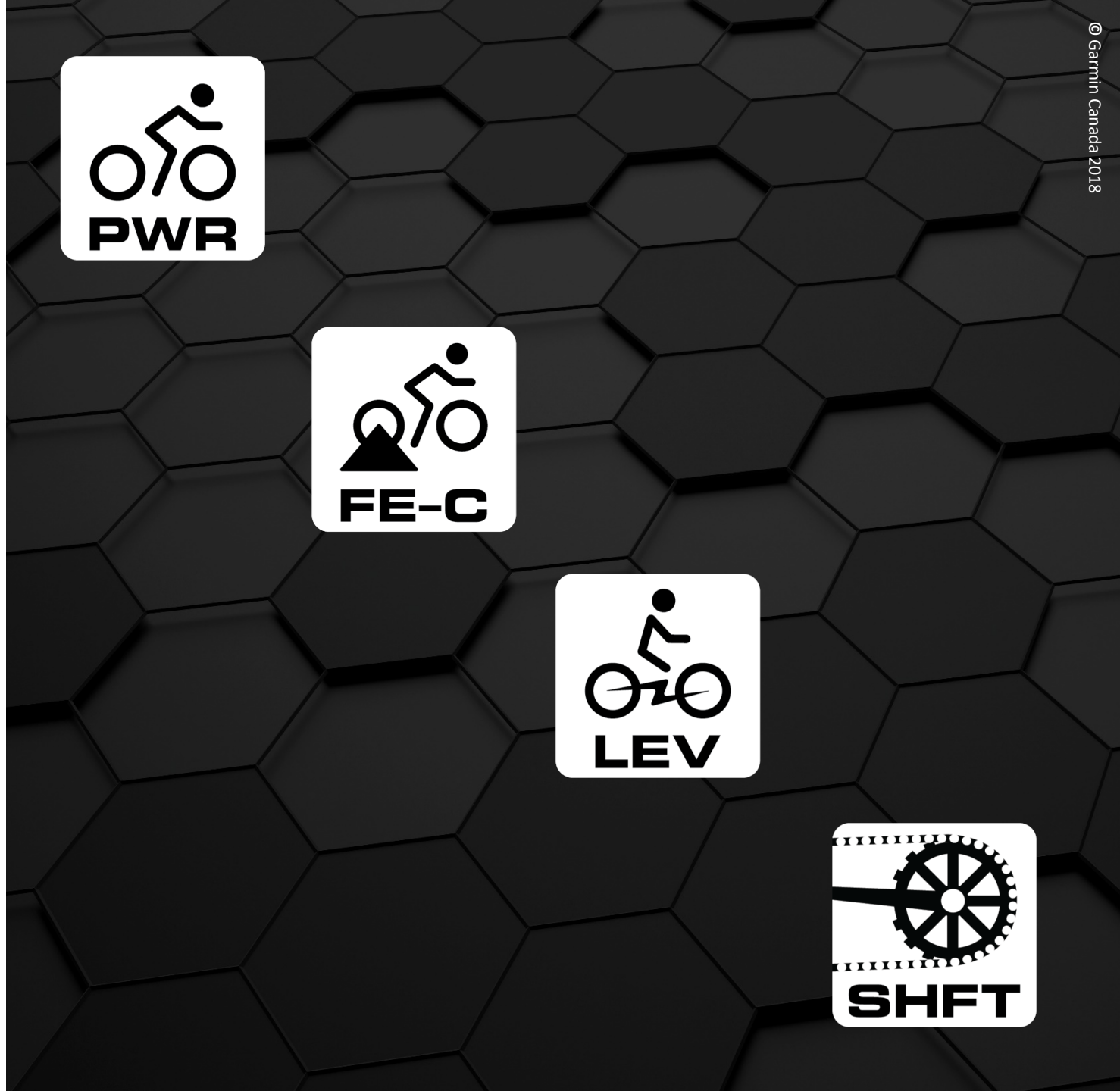
No-Display Authentication

- A standard for authenticating sensors that don’t have displays (needed right now to display auth codes)

Thinking Ahead

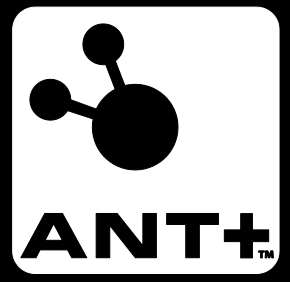
Addressing Existing Profiles

- TWG driven
  - We won’t build until there is a market need
- Considerations:
  - Backwards compatibility
  - Indicating compatibility to end user
  - Requirements of the TWG



Thinking Ahead

- It’s an ecosystem.
- Let’s build it together.



Beenish.Khurshid@THISISANT.COM

THANK YOU