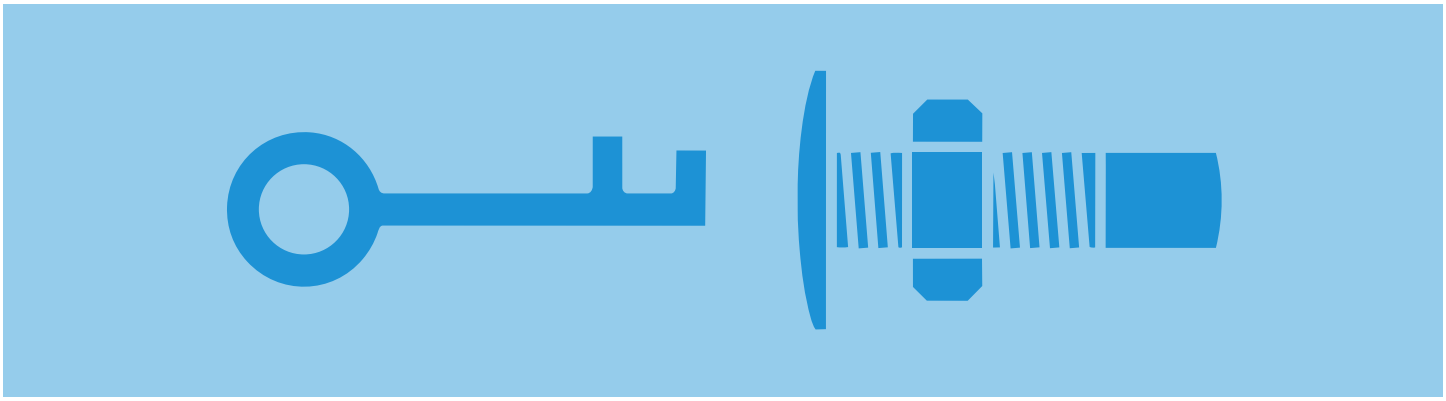
SECURITY OVERKILL: HOW NEXTCONNECT STAYS AHEAD OF QUANTUM HACKERS



Purpose

Quantum hackers are coming. The security on most wireless devices won't survive the computers of tomorrow. The NextConnect was built for that day. There isn't one lock guarding it. There are dozens on every device, each one different, and any of them can be changed without anyone ever laying a hand on the hardware. This paper explains the security that keeps NextConnect devices safe and secure.

5 Key Takeaways

01 Every NextConnect uses AES-256 encryption, the same standard trusted to protect classified U.S. government information.

02 Every key on every device is unique. There are no master keys and no shared keys.

03 Keys are created, stored, and rotated under strict controls, starting with a root key split across five physical titanium plates.

04 Even if one key were ever compromised, the damage would stop at one key on one device, and we can retire it remotely.

05 The NextConnect is built to stay secure for decades to come, including against the quantum computers of tomorrow.

We Obsess Over Security

> There's an old joke in our industry: the "S" in IoT stands for security. There isn't one.

Wireless utility devices get compromised more often than vendors like to admit. And a meter reading system touches more than water usage. It touches billing, personal data, and the trust between you and your customers.

We've taken security seriously from the beginning. Every generation of our devices has shipped with the strongest security we could build at the time. Our latest devices, including the NextConnect, carry our third generation of security, stacked on top of the first two. Because we control our entire architecture, we keep adding layers instead of starting over.

AES-256 Security, Everywhere

Every message a NextConnect sends or receives is encrypted with AES-256. AES is the encryption standard published by the National Institute of Standards and Technology [1], and AES-256 is the version the NSA requires for systems protecting information up to the Top Secret level [2]. It's the same encryption trusted by banks, governments, and militaries around the world.

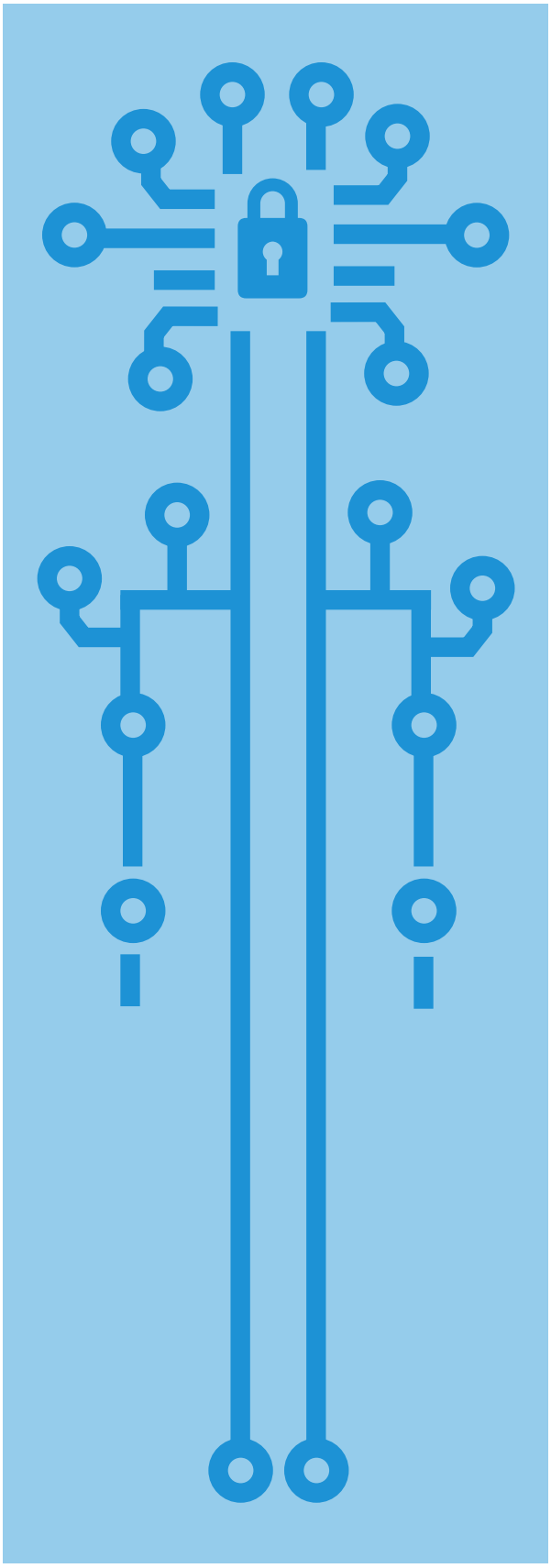
In practice, this means that if someone intercepted a reading on its way to the cloud, all they'd see is scrambled data with no way to read it without the exact key that created it.

Built-in tamper detection:
Every message also carries an integrity check. If anyone grabs data out of the air and changes even one piece of it, the receiving end knows immediately and rejects it. That check can't be faked or recalculated without the original keys.

Unique Keys for Every Device

Some metering systems use a single shared key across every device they sell. If that one key ever leaks, every device in the field is exposed at once. Worse, some of those systems have no way to replace the key after it's been compromised. The NextConnect does it differently.

Unique at every level:
Each NextConnect carries thirty-two interface keys. Eight keys for each of its four communication interfaces (cellular, Bluetooth, RF, etc.), plus separate keys for data storage, secure boot, and debug access. No key is shared between interfaces. No key is shared between devices. Two NextConnects sitting side by side can't read each other's messages.



Ready for tomorrow's computers:
Quantum computers will change the math on older encryption. Agencies like CISA are warning about "harvest now, decrypt later" attacks, where encrypted data gets stolen today and cracked years later [3]. The NextConnect is already ahead of that with its quantum-resilient security keys. According to NIST, even Grover's algorithm, the best-known quantum shortcut for attacking encryption, leaves keys this size safe for decades [4].

Key Creation & Storage

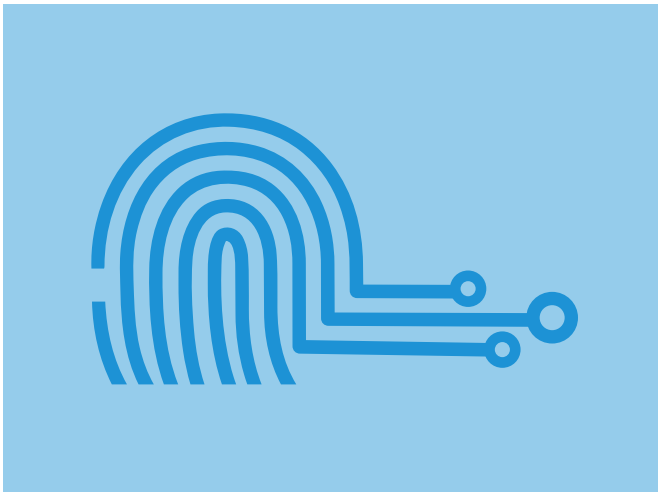
The titanium root key:
The master key behind all Next Meters device keys was generated on an air-gapped computer that has never touched the internet. Once its job was done, the key was split into five pieces and the original was destroyed, along with the machine that made it. Each piece is engraved on a fireproof titanium plate, held by different people in different locations. Any three plates can rebuild the key. One or two are worthless alone. Splitting a secret this way, so no single person or place holds all of it, is best practice.[5]

A vault inside each chip:
During manufacturing, every NextConnect receives its own one-time programmable key, burned into a walled-off section of the chip called the secure engine. The processor can ask the secure engine to use that key, but never read it. If someone tampers with the secure engine, it erases everything before giving anything up.

Keys stored as gibberish:
Before any key is saved to the device's memory, the secure engine runs it through a one-way encryption process called wrapping. What's stored is a scrambled "blob" that's useless without the one-time key, which itself can never be read back out. Even if someone went to the extreme of desoldering the memory chip and reading every byte, they'd walk away with nothing they could use.

Locked debug ports:
The port used to program a NextConnect is locked with a key unique to that device. Even our own engineers cannot access it without permission granted from our servers, through the same authenticated cloud system that protects everything else.

Encrypted storage, end to end:
Everything the NextConnect saves, including meter read history and update files, is encrypted with a key unique to that device. If two million NextConnects stored the exact same data, no two memory chips would look alike. Data is protected both while it's moving and while it's sitting still.



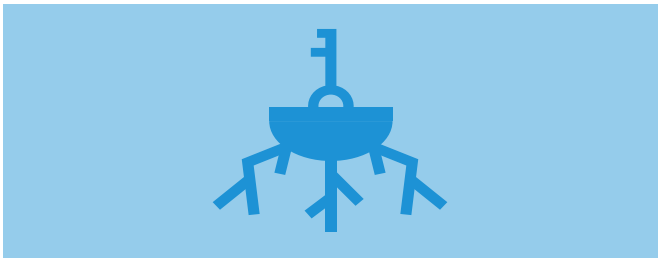
Security That Fights Back

> Good security plans for the worst scenario. So we built the NextConnect to resist and respond.

Key rotation:
If we ever suspect a key has been compromised, we can tell that device to retire it remotely and rotate to the next one. We can even push out new keys. And because every key we send carries a cryptographic fingerprint that proves it came from our servers, the device won't accept keys from anyone else.

Secure boot:
Every time a NextConnect powers on, the secure engine checks the firmware against a device-specific signature before it lets anything run. If the firmware didn't come from Next Meters, the device refuses to boot. It would rather not run at all than run code it can't trust.

Small windows:
Even standard brute-force calculations assume a target that's always on. The NextConnect isn't. Its cellular radio is active for a few minutes a day. Its RF radio, a few seconds. Bluetooth only turns on when someone activates it on site. There's barely a door there to knock on.



The Next Meters Difference

With many security systems, vendors can't explain how things work, because telling you would get you halfway to breaking in. With the NextConnect, we can walk you through every layer, every key, and every safeguard in this paper. Because knowing how it all works won't get you any closer to cracking it.

Quantum hackers are coming. Maybe not this year, and maybe not next, but attackers are already collecting encrypted data today so they can crack it later. The only question is whether your system will still be standing after they try.

These cybercriminals, and whatever comes after them, will find NextConnect is already lightyears ahead.

For more information:

www.nextmeters.com

sales@nextmeters.com



Sources

Standards and research behind our security

01 National Institute of Standards and Technology, FIPS 197: Advanced Encryption Standard (AES) — https://csrc.nist.gov/pubs/fips/197/final

02 National Security Agency, Commercial Solutions for Classified Program FAQ (CNSA suite, AES-256 for systems up to Top Secret) — https://www.nsa.gov/resources/commercial-solutions-for-classified-program/faq

03 Cybersecurity and Infrastructure Security Agency, Post-Quantum Cryptography Initiative — https://www.cisa.gov/topics/risk-management/quantum

04 National Institute of Standards and Technology, Post-Quantum Cryptography FAQs (Grover's algorithm and AES) — https://csrc.nist.gov/projects/post-quantum-cryptography/faqs

05 National Institute of Standards and Technology, NIST IR 8214: Threshold Schemes for Cryptographic Primitives — https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8214.pdf