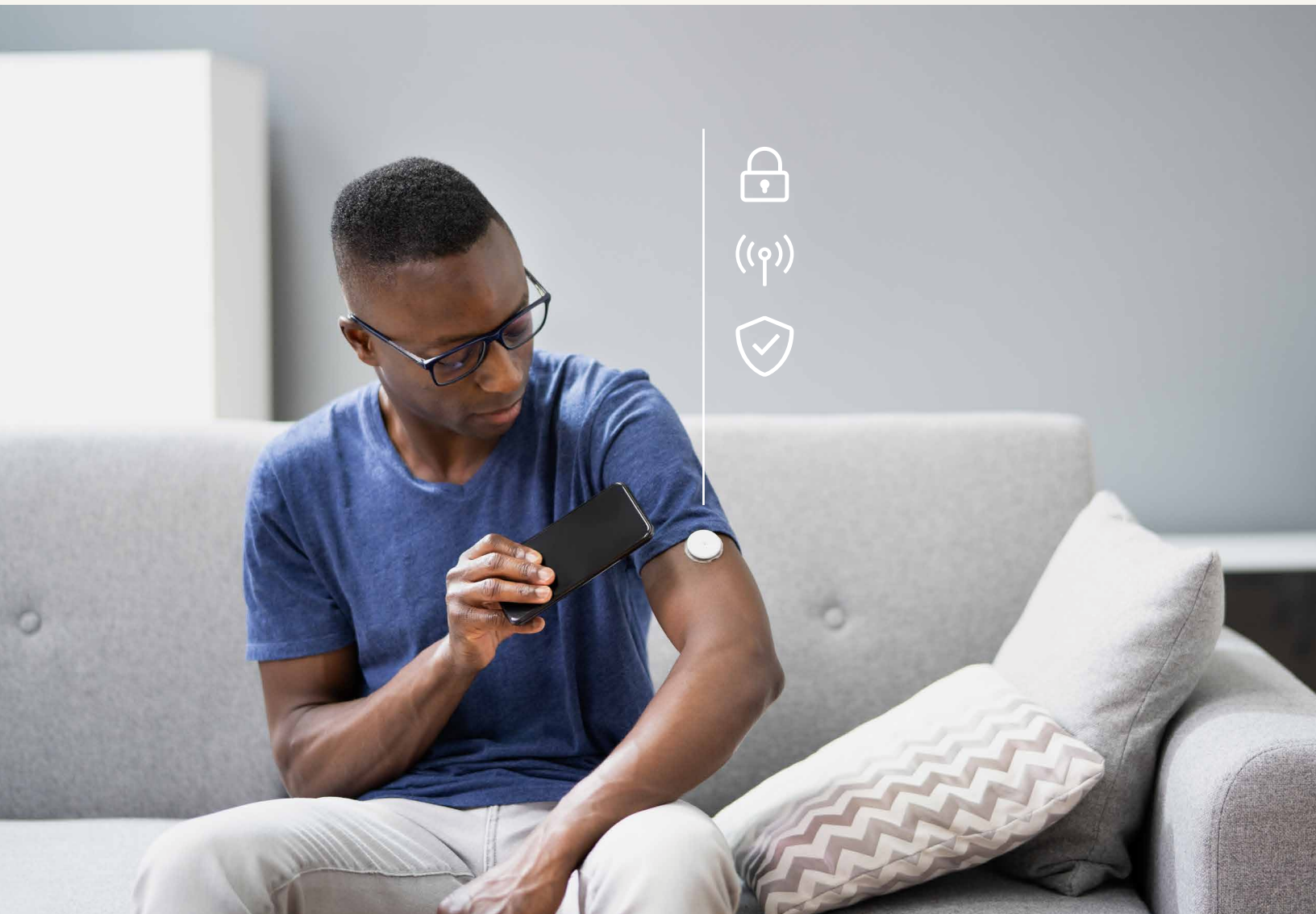
Use Case

EdgeLock® secure elements
and authenticators

Smart, Secure Medical Devices



Smart, Secure Medical Devices

In the Internet of Medical Things (IoMT), where doctors and healthcare staff use connected devices to treat patients in a whole new way, NXP provides a comprehensive, FIPS standard-compliant protection that safeguards privacy, secures data, and enables innovation.

Applications

Laboratory

Medical Facility

Residence

Challenge

Connected medical devices are already helping enhance healthcare delivery and improve patient outcomes. Hospitals and other care facilities are using IoMT devices to streamline operations, enhance efficiency, reduce human errors and enable easier access to real-time data provided by continuous patient monitoring. When patients return home, IoMT devices are reducing hospital readmission by providing remote healthcare staff with access to timely diagnostic information. IoMT devices are also helping people with chronic conditions track their health data and therapy adherence, in real time, for better overall health and improved quality of life. On a broader scale, IoMT devices generate data needed to identify trends, predict potential complications, and help personalize treatment plans.

As technologies continue to evolve, the IoMT has the potential to transform vital aspects of healthcare delivery, from patient care to population management. Before this transformation can take place, however, there are several cybersecurity challenges that need to be addressed. Whenever connected medical devices communicate and exchange information with other actors in the IoMT ecosystem, such as another medical device, a patient's or doctor's mobile phone or tablet, a cloud server, or other IT system, the transaction must be kept private and protected from tampering and spoofing. Also, medical devices might become entry point for cybercriminals aiming to disrupt the IT system or hospital network to perform Distributed Denial-of-Service (DDoS) attacks or ransom attacks. Real-time monitoring, used to detect health problems and issue automated notifications, can pose a risk, too, since always-on devices are an easy target for cybercriminals looking to disrupt operations or steal information.

As the healthcare industry becomes more interconnected, through the increasingly widespread use of IoMT devices, the need to formalize security becomes all the more urgent. Regulatory agencies worldwide are recognizing the importance of treating IoMT devices as cyber-physical items that must be designed in a secure way, to protect against the kinds of attacks that can compromise data privacy and patient health. In key markets, including the United States and the European Union, regulations that aim to safeguard sensitive patient data, prevent unauthorized access, and mitigate the risk of cyber threats, are already in place. What's more, as the separation between medical devices and other electronic devices, such as smartphones, tablets, and wristbands, begins to disappear, it's possible that IoMT devices will need to comply with regulations beyond the scope of traditional healthcare, such as the EU's General Data Protection Regulation (GDPR).

With so many regulatory requirements for IoMT device security either already here or on the horizon, manufacturers of IoMT devices need comprehensive, trusted security solutions that protect connectivity and ensure data privacy, not just today, but for the entire life of the product.

"the transaction must be kept private and protected from tampering and spoofing."

Solution

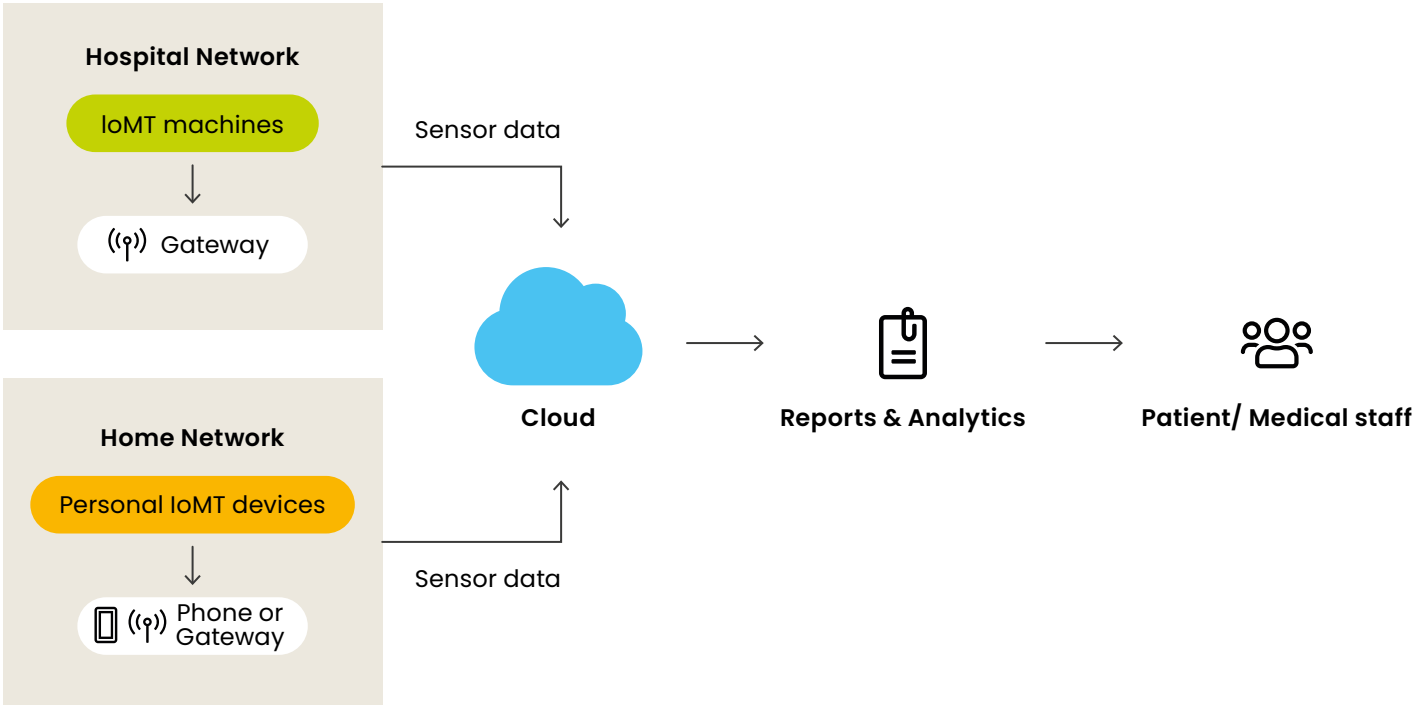
As a leading supplier of third-party certified security solutions for the Industrial IoT as a whole, NXP offers a range of security solutions ideally suited to IoMT devices. Our EdgeLock Discrete solutions, which are designed to prevent unauthorized access to connected devices while ensuring secure communication and authenticated transactions, help developers add high-level security to all kinds of medical devices, including those intended for deployment in regions with specific regulatory standard requirements.

Our EdgeLock Discrete portfolio, including secure elements and secure authenticators, provides scalable, flexible, and secure products that help to fulfill the security and connectivity requirements recommended by the Food and Drug Administration (FDA) in the US and the Medical Device Regulation (MDR) in the EU. The EdgeLock SE052F, for instance, is the industry's first hardware secure element validated to the Federal Information Processing Standards (FIPS) 140-3 standard Level 3, as issued by the National Institute of Standards and Technology (NIST) in the US. By providing out-of-the-box FIPS compliance, the EdgeLock SE052F's functionality can quickly be leveraged for use with other certification efforts, including FDA submissions.

The EdgeLock Discrete portfolio also includes the EdgeLock A30 secure authenticator, an optimized, dedicated authentication product designed to complement the EdgeLock secure element family. With Common Criteria EAL 6+ certified security, the EdgeLock A30 is designed to support secure authentication for medical devices, enabling manufacturers to quickly deliver secure solutions that comply with regulatory requirements for traceability, authentication and data protection.

IoMT devices equipped with NXP EdgeLock secure elements or secure authenticators work seamlessly with NXP's EdgeLock 2GO cloud service, which lets customers securely manage the credentials of already-deployed medical devices and update devices in the field as needed to address new security requirements, for full device lifecycle protection. The EdgeLock 2GO service makes it easy to create and manage secure objects, such as symmetric roots of trust, as well as asymmetric keypairs and certificates, which are then securely provisioned (either remotely or locally) to the EdgeLock SE05x secure element or EdgeLock A30 secure authenticator.

Block diagram



NXP Delivers the Comprehensive Protection that Enables IoMT Innovation

Learn more

The NXP Design Community site offers helpful hints, easy-to-follow how to's, and detailed application notes for use with the EdgeLock secure elements and authenticators, while our product pages link to detailed specs, designs tools & software, training & support, and more.

NXP Design Community
community.nxp.com/community/identification-security/secure-authentication/overview

Application Code Hub
Integrating EdgeLock SE05X to FRDM-MCX-N development boards

Application Note
Secure Medical IoT Application with NXP Secure Devices (AN14252)

Webinar
How to Address Cybersecurity Requirements in Healthcare: Deep Dive into FDA and EU MDRs

EdgeLock SE050 Secure Element
nxp.com/SE050

EdgeLock SE051 Secure Element
nxp.com/SE051

EdgeLock SE052F Secure Element
nxp.com/SE052F

EdgeLock A30 Secure Authenticator
nxp.com/A30

EdgeLock 2GO
nxp.com/EdgeLock2GO

nxp.com/iotsecurityusecase

NXP, the NXP logo and EdgeLock are trademarks of NXP B.V.
All other product or service names are the property of their respective owners. © 2025 NXP B.V.

Document Number: SMARTSECMEDDEVCS REV 1