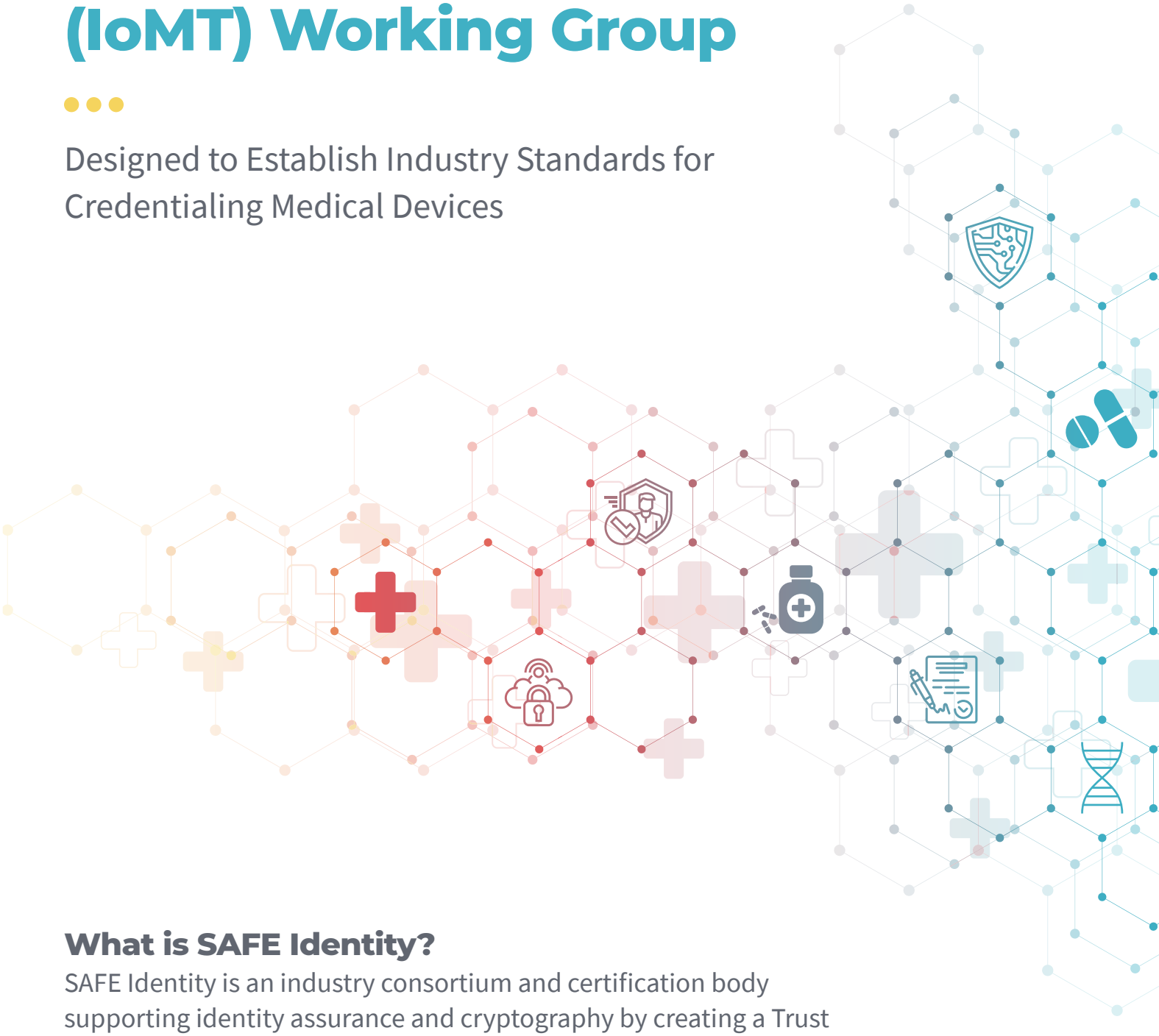
SAFE IDENTITY

Internet of Medical Things (IoMT) Working Group

Designed to Establish Industry Standards for Credentialing Medical Devices



What is SAFE Identity?

SAFE Identity is an industry consortium and certification body supporting identity assurance and cryptography by creating a Trust Framework for digital identities in healthcare.

The Challenge

Innovation is driving the growth and adoption of connected medical devices and evolving how these devices are used in patient care. Patients are receiving treatment from home through remote patient monitoring and sending PHI back to healthcare providers from their unprotected home networks. Counterfeit products are of increasing concern in healthcare both from a patient safety perspective and a regulatory perspective. Consumers of medical devices need a way to confirm what devices are on the network, know who manufactured the device and communicate sensitive data to and from the device. Each of these concerns can be addressed with a standards-based credential built into the medical device that consumers can interact with. The need for such a credential in today's healthcare environment becomes more apparent every day.

While the technology and standards exist for installing and interacting with standards-based digital credentials on medical devices, there remains a need for industry guidance that suggests strategies and best practices for issuing, enrolling and interacting with medical device identities at scale.

The IoMT Working Group

The SAFE Identity IoMT Working Group brings together digital identity experts and medical device subject matter experts to establish industry best practices and develop guidance for medical device manufacturers to credential and autoenroll their devices on the production line, at scale, in a federated environment.

Key Objectives of the SAFE Identity IoMT WG for Medical Device Manufacturers

Learn and develop best practices and strategies for choosing a PKI deployment methodology (build vs buy) to suit an organization's needs, including a cost/benefit analysis and various security considerations

Best practices for autoenrolling medical devices at scale on the production line

Develop industry policies and best practices for satisfying regulatory requirements in both the North American and European regulatory agencies

Alignment with industry-leading recommendations from NIST and ETSI

Key Objectives of the SAFE Identity IoMT WG for Healthcare Delivery Organizations (HDOs)

Develop strategic implementation guidance for interacting with medical device digital identities in today's healthcare environments

Develop procurement guidance to acquire IoT medical devices with built-in standards-based identities using a risk analysis methodology

The SAFE Identity IoMT Working Group calls upon the Medical Device Manufacturers, Healthcare Delivery Organizations and other stakeholders passionate about medical device security to represent their organization's interest and offer thought leadership in the working group's activities.

www.makeidentitysafe.com | info@makeidentitysafe.com | (703) 705-2920
1900 Reston Metro Plaza, Suite 303, Reston, VA 20190