



Using Electronic Security to Protect your Revolutionary Medical Products

June 27–29, 2022 | San Jose, CA

#SensorsConverge

We live in an increasingly complex world



Pandemic



Political/Civil Issues



Inflation



Supply Chain / Shortages

Thought Experiment: If you could go back to a simpler time, would you?

Flourishing medical technology is one exciting area of hope in a difficult world



Explosive growth in new technologies



Greater access to larger portions of the population than ever before



Safety of products is paramount; No safety without security



Innovation is incubated and nurtured by incentives of reward for investment risk and hard work



Medical Device Trends

- **Medical Device Market Size : \$432.2B¹**
- **Medical Device Security Market 2021 : \$455.3M²**
- **CAGR 2021-2025: 8%**
- **Key Market Drivers:**
 - Growing number of patients and surgeries
 - Growing demand for innovative devices
 - Rising trend for connected devices requiring security for risk mitigation

Sources:

1. <https://www.fortunebusinessinsights.com/industry-reports/medical-devices-market-100085>

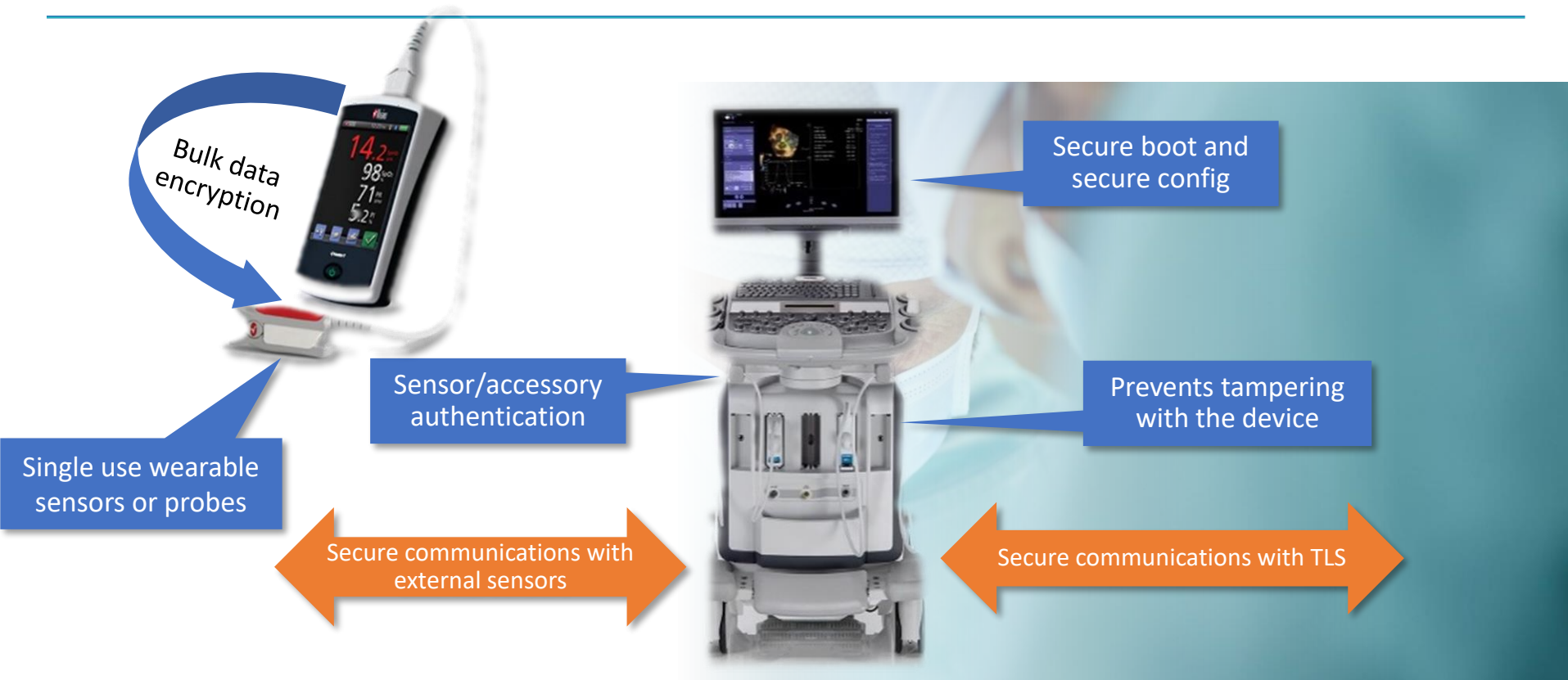
2. <https://www.vantagemarketresearch.com/industry-report/medical-device-security-market-1383>



Proliferating medical technology draws safety and security concerns

- Interconnection of sensors and devices requires trust
- IP copying, counterfeiting
 - Safety
 - ROI
- Usage Tracking
 - Some devices are approved for limited use, but how is that ensured?
- Feature Set Management
 - Electronically lock and unlock features
- Sterilization
 - Common sterilization techniques often hostile to electronics

Embedded Security in Medical Devices



Counterfeits and IP protection

- Accessories susceptible to cloning
- Safety: Clones may not have the same quality and pose safety risk
- Counterfeiters may copy entire bill of materials (BOM) of products
- Innovation may be in the Firmware and vulnerable to copying



Secure Use Management



Limited life/use medical peripherals (sensors, tools, catheters), system secure feature enablement



Bi-directional authentication, secure memory, non-resettable use counters



Devices electronically expire after the counter decrements to zero



Feature Control Management

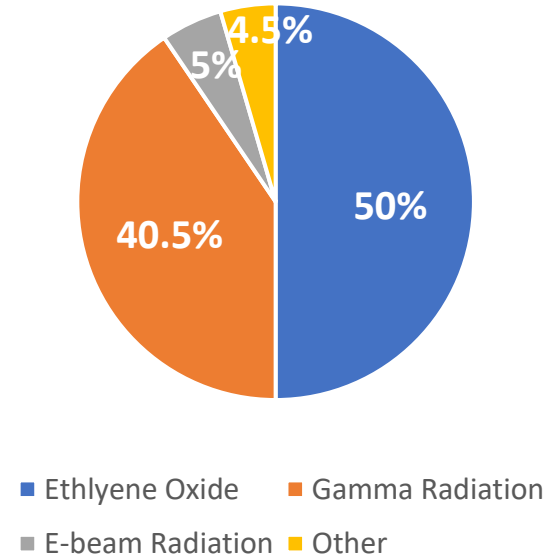
- For efficiency, hardware designed to support multiple usage options
- Options should be enabled / disabled only by authorized source
 - Factory options (set one time)
 - In-field use (i.e. subscription service, turn on/off)



Sterilization

- Medical devices most commonly sterilized by chemicals such as ethylene oxide (EtO) or radiation
 - EtO harmful for environment and dangerous to use
 - Radiation usually harmful to electronic non-volatile memory

Sterilization Methods



Source <http://large.stanford.edu/courses/2018/ph241/goronyz2/>

Solutions



Authentication vs. Encryption

Authentication = “Prove who you are”



Authentication

Anyone can read the data, but digital certificates and hashes prove the identity of the source and integrity of the data

Encryption = “Scrambled data”



Encryption

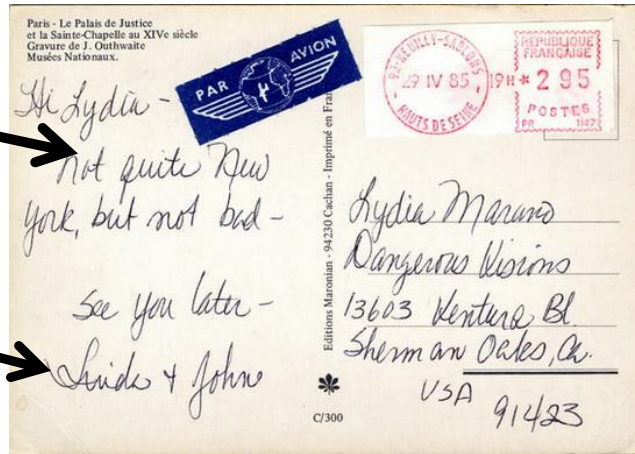
Nobody can read the data unless they know the secret to decrypt the data

Authenticity

- Proves it comes from whom you think it comes
- It is not confidential !!

Anyone can read it!

But only Linda and John could have signed it!



Authentication-Algorithm Type Comparison

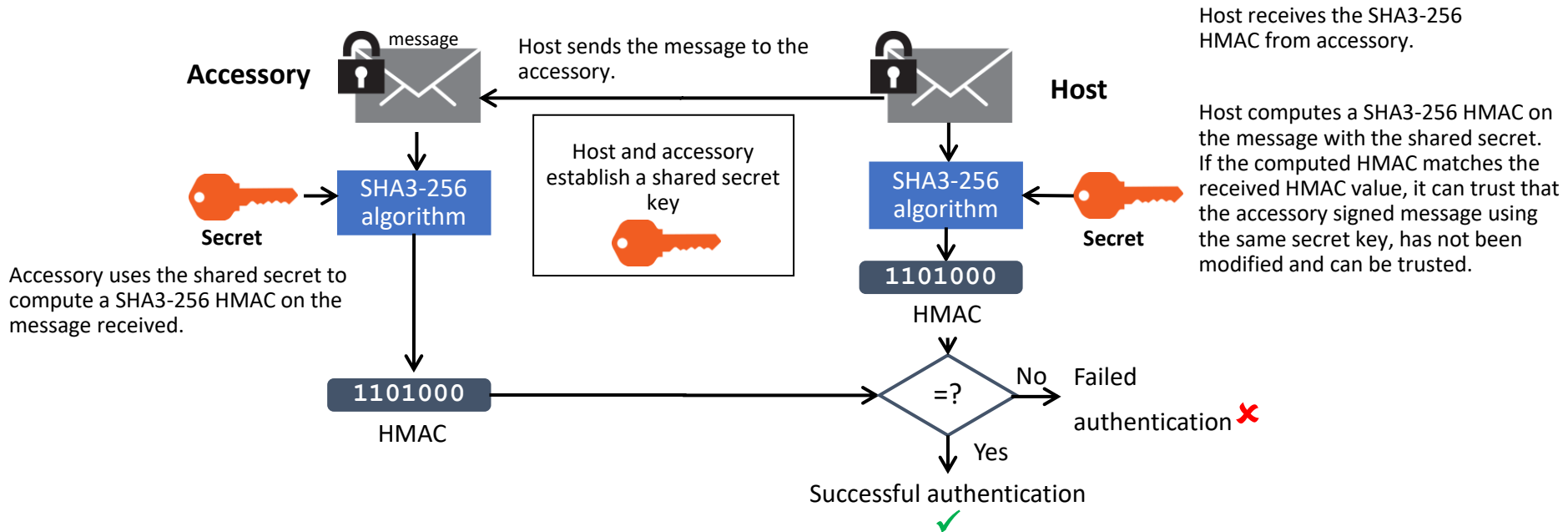
Symmetric Key (aka Secret-key)

- Host and accessory operate from same key/secret
- **Secret** must be **protected** from disclosure/replacement attack **on both sides**
- For comparable security level, **lower algorithm complexity, and faster**

Asymmetric Key (aka Public-key)

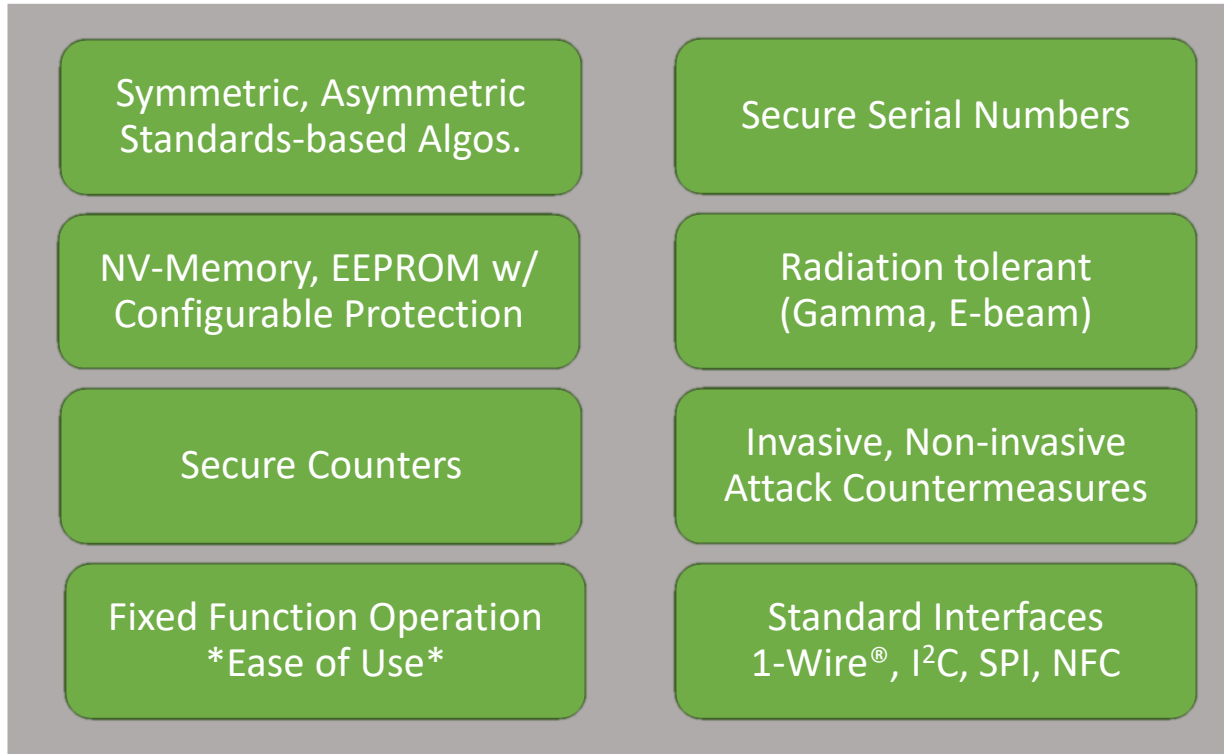
- Host operates with public-key; accessory with corresponding private-key
- **Two-step verification**: certificate then signature
- **Private key must be protected on the accessory side against disclosure**
- **Host certificate verification key must be protected against replacement**
- For comparable security level, **higher algorithm complexity, slower**

Authentication Example with Symmetric Key SHA3-256

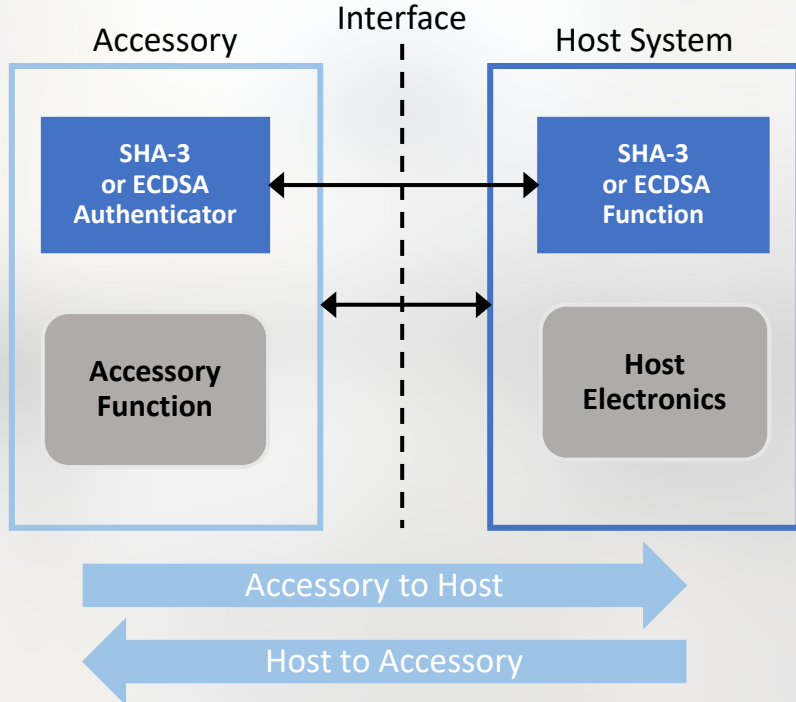


- Host and accessory need to use a **shared secret** to authenticate messages

Core Technologies of Secure Authenticators



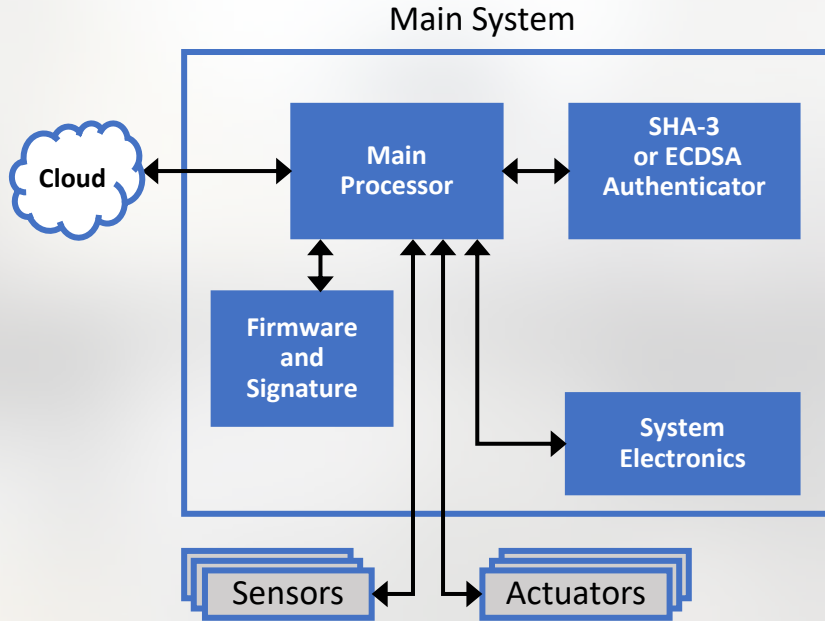
Typical Use: Counterfeit Protection and Secure Use Management



Use Scenarios

- Authenticate the accessory before use
- Securely update data in accessory authenticator
- Provide authenticated read of accessory operating parameters
- Securely count the number of accessory uses
- Expire additional uses of the accessory

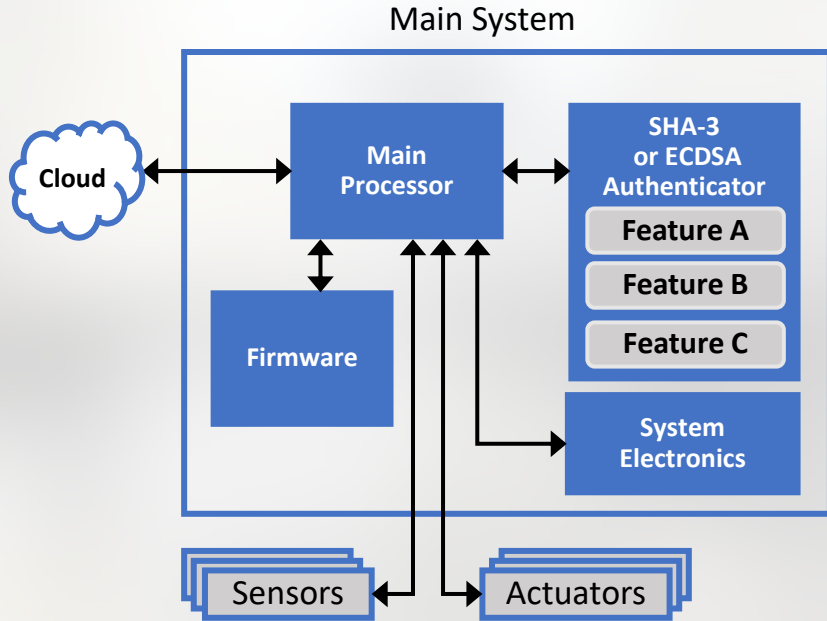
Typical Use: IP Protection



Use Scenarios

- Secure device is on BOM
- Device procurement not available to unauthorized parties
- Device provisioned only for use in system
- System performs authentication check, only authentic device will respond
- Authenticator can verify FW updates

Typical Use: Feature Control Management



Use Scenarios

- **Factory Setting:**
 - Options can be set and locked on one-time basis
- **In-field Use:**
 - Options can be enabled or disabled based on subscription
 - Possible use with activation via Cloud Host

Conclusion

- It's an exciting time for innovation in medical devices
- Safety and security are paramount
- Electronic authentication techniques can be used in a variety of ways to protect IP, block counterfeits, and enable feature control management in medical devices



Resources

Title	URL
Best Practices: Access Controls for Medical Devices	https://www.welchallyn.com/en/education-and-research/research-articles/access-controls-for-medical-devices-part-1.html
How to tackle device authentication and data security in the healthcare industry	https://www.entrust.com/blog/2019/05/how-to-tackle-device-authentication-and-data-security-in-the-healthcare-industry/
New Memories Breaking the Gamma Barrier for Medical Consumables	https://www.maximintegrated.com/en/design/technical-documents/app-notes/6/6075.html
Secure Authentication for Medical Disposables	https://www.maximintegrated.com/en/design/technical-documents/app-notes/6/6891.html
Easily Add Memory, Security, Monitoring, and Control to Medical Sensors and Consumables	https://www.maximintegrated.com/en/design/technical-documents/tutorials/4/4702.html