Securing Internet of Medical Things (IoMT) with Java Card Technology

Bryan Muehlmeier

Director & Product Manager, Oracle Cerner CareAware

Cristian Toma

Software Development Director, Oracle Java Platform Group, Java Card

ORACLE

December, 2023

Safe harbor statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Securing Internet of Medical Things (IoMT) with Java Card

#agenda

01 | **Medical Devices**

IoMT, Terminology, Architecture, …

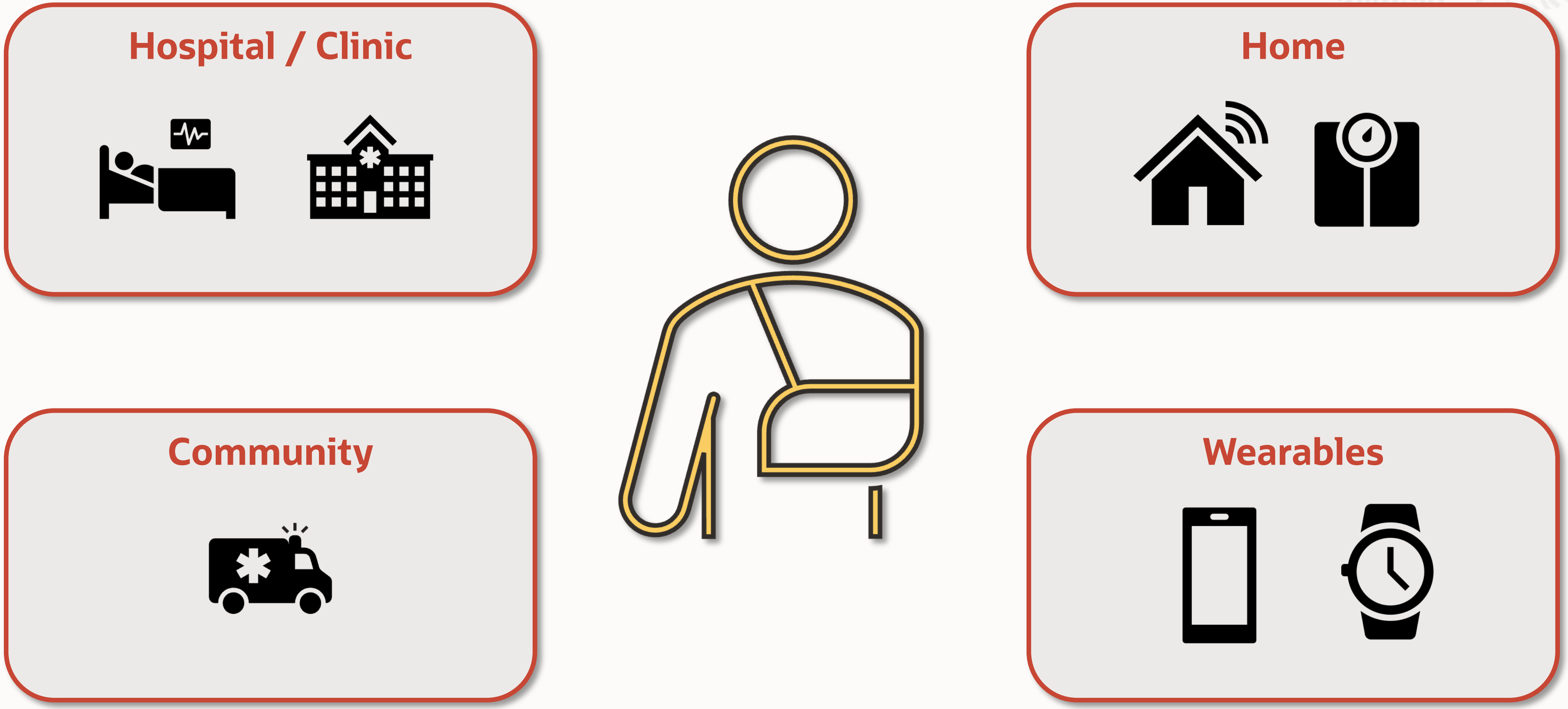
02 | **Java Card & IoMT Use-cases**

Java Card, IoMT, Use-cases, Healthcare Security Standards

03 | **Q&A**

Conclusions

Internet of Medical Things (IoMT)

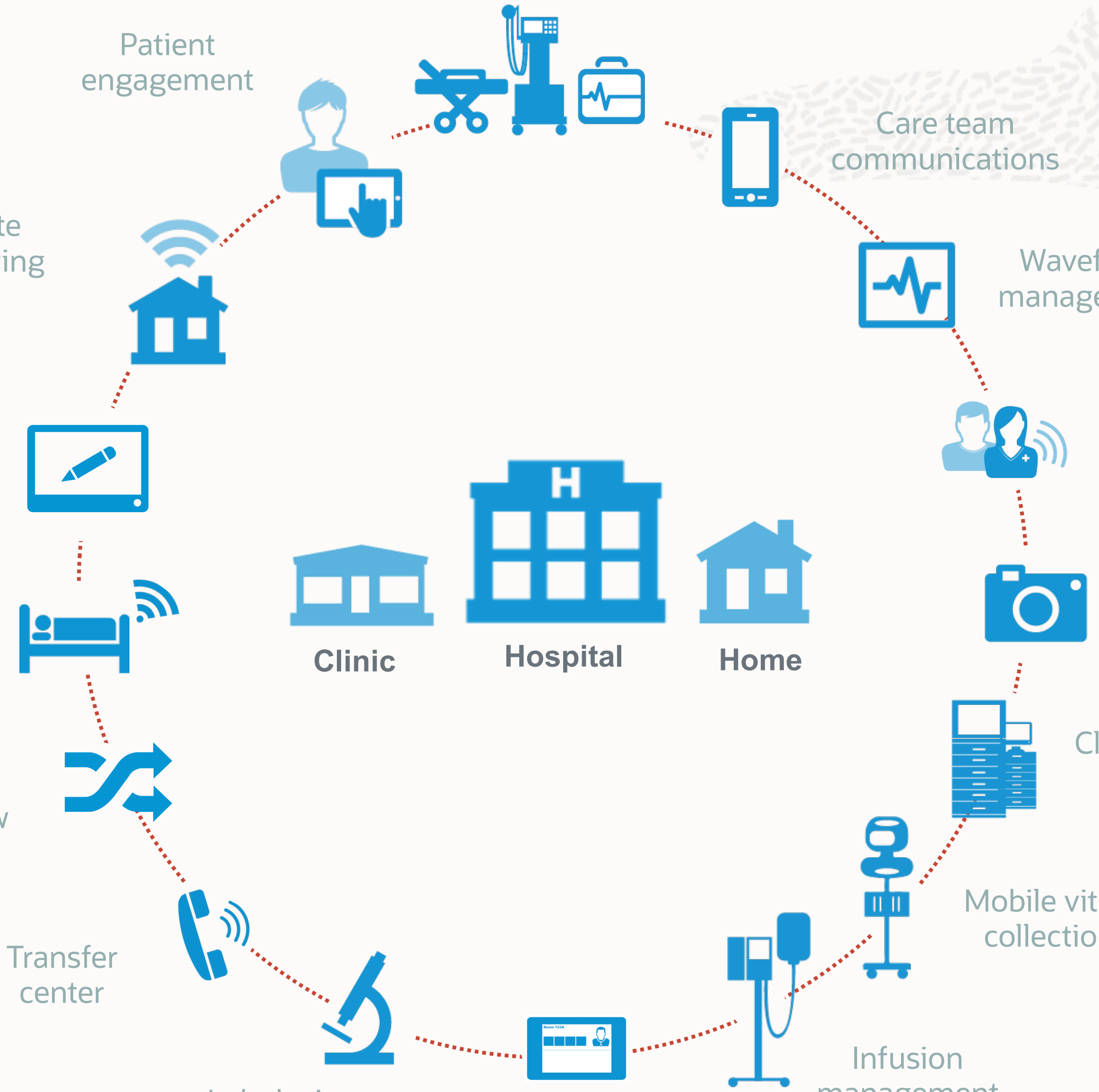


Hospital / Clinic

Home

Community

Wearables



Bedside medical device integration

Care team communications

Waveform management

Nurse call integration

Image capture

Closed loop meds dispensing

Mobile vitals collection

Infusion management

Digital room signage

Lab device integration

Transfer center

Patient flow

Location awareness

Digital unit whiteboard

Remote monitoring

Patient engagement

Clinic

Hospital

Home

AIRSTRIP®

ARC

sysmex

GE Healthcare

Baxter

BD

CareFusion

CENTRAK®

CompX

COPAN

COVIDIEN

critical alert

ACCELERATE DIAGNOSTICS™

Dräger

EarlySense

FRESENIUS KABI

FUKUDA DENSHI USA, INC.

B | BRAUN

getwell:)network

HAEMONETICS®

Hill-Rom

icumedical human connections

CareAware® VALIDATED

IDEAL LIFE

Leica

LINET®

Livongo®

MASIMO

mindray

MAQUET GETINGE GROUP

Medtronic

MIDMARK

BIOFIRE A BIOMÉRIEUX COMPANY

WestCall

Mortara

neoventa

NIHON KOHDEN

smiths medical bringing technology to life

Omnicell®

Polycom

PHILIPS Healthcare

Rauland

RICOH

Roche

seca®

SIZEWISE

sonitor® technologies

Sotera® WIRELESS

stryker®

SPACELABS HEALTHCARE An OSI Systems Company

spectralink

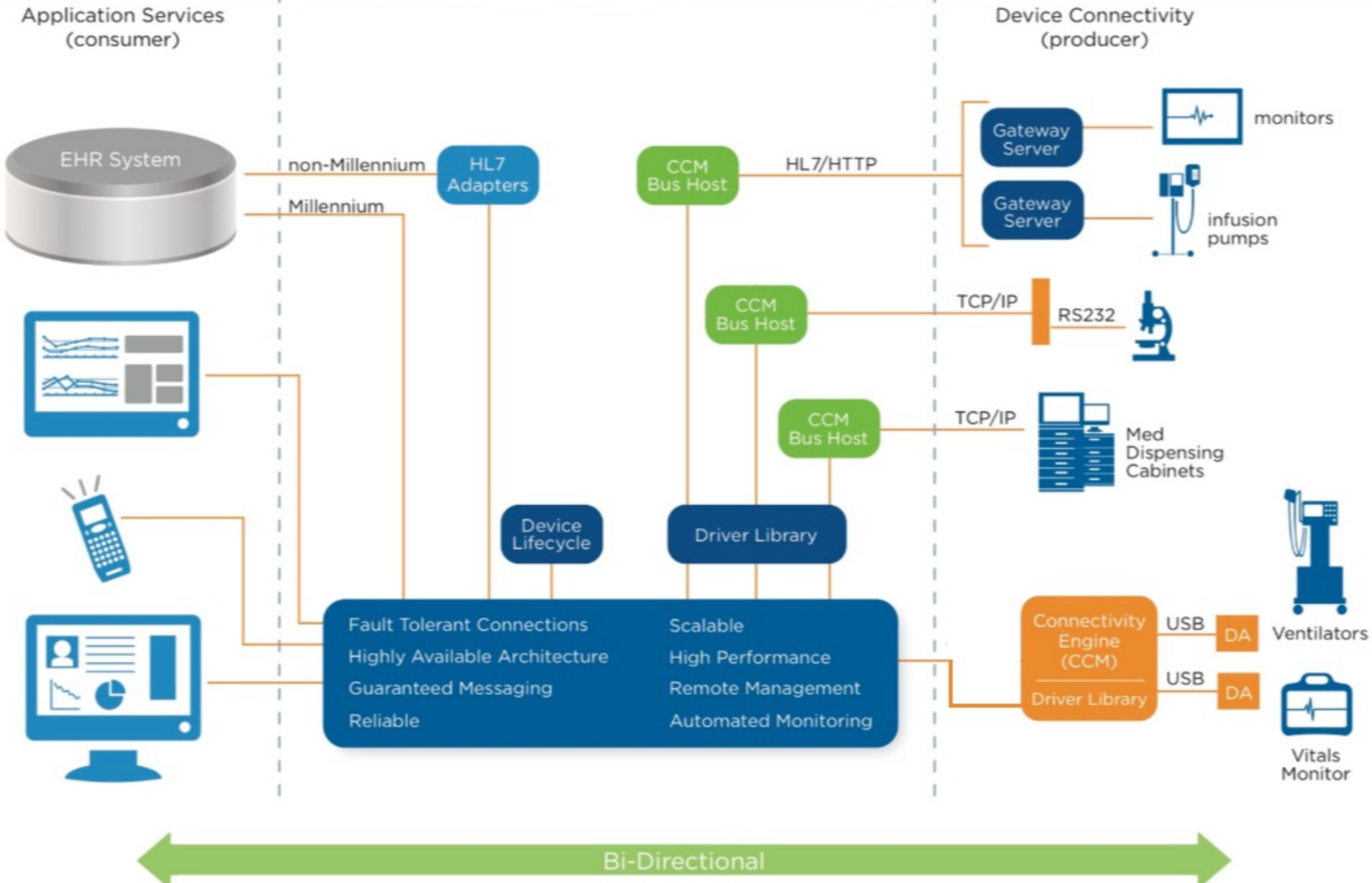
STANLEY. Healthcare

TALYST

vocera

Welch Allyn®

Over 50 validated members



Application Services (consumer)

Device Connectivity (producer)

EHR System

non-Millennium

Millennium

HL7 Adapters

CCM Bus Host

HL7/HTTP

Gateway Server

Gateway Server

monitors

infusion pumps

CCM Bus Host

TCP/IP

RS232

CCM Bus Host

TCP/IP

Med Dispensing Cabinets

Device Lifecycle

Driver Library

Fault Tolerant Connections

Highly Available Architecture

Guaranteed Messaging

Reliable

Scalable

High Performance

Remote Management

Automated Monitoring

Connectivity Engine (CCM)

Driver Library

USB

DA

USB

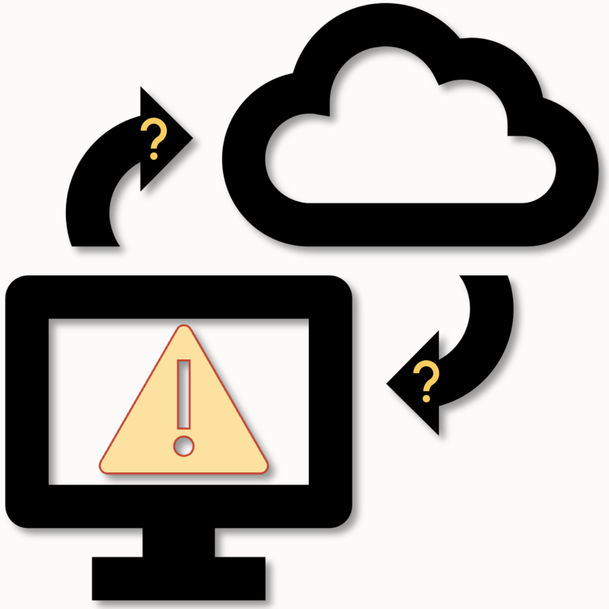
DA

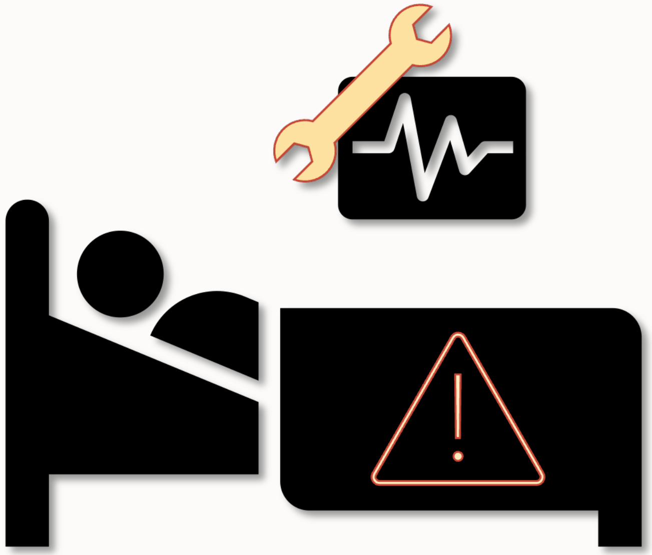
Ventilators

Vitals Monitor

Bi-Directional

Importance of Securing Medical Devices





Securing Internet of Medical Things (IoMT) with Java Card

#agenda

01 **Medical Devices**

IoMT, Terminology, Architecture, …

02 **Java Card & IoMT Use-cases**

Java Card, IoMT, Use-cases, Healthcare Security Standards

03 **Q&A**

Conclusions

Java Card Platform

Reference runtime for Secure Elements

Identification

Biometry

Data Confidentiality

Authorization

Secure communication

Access Control

Root of trust

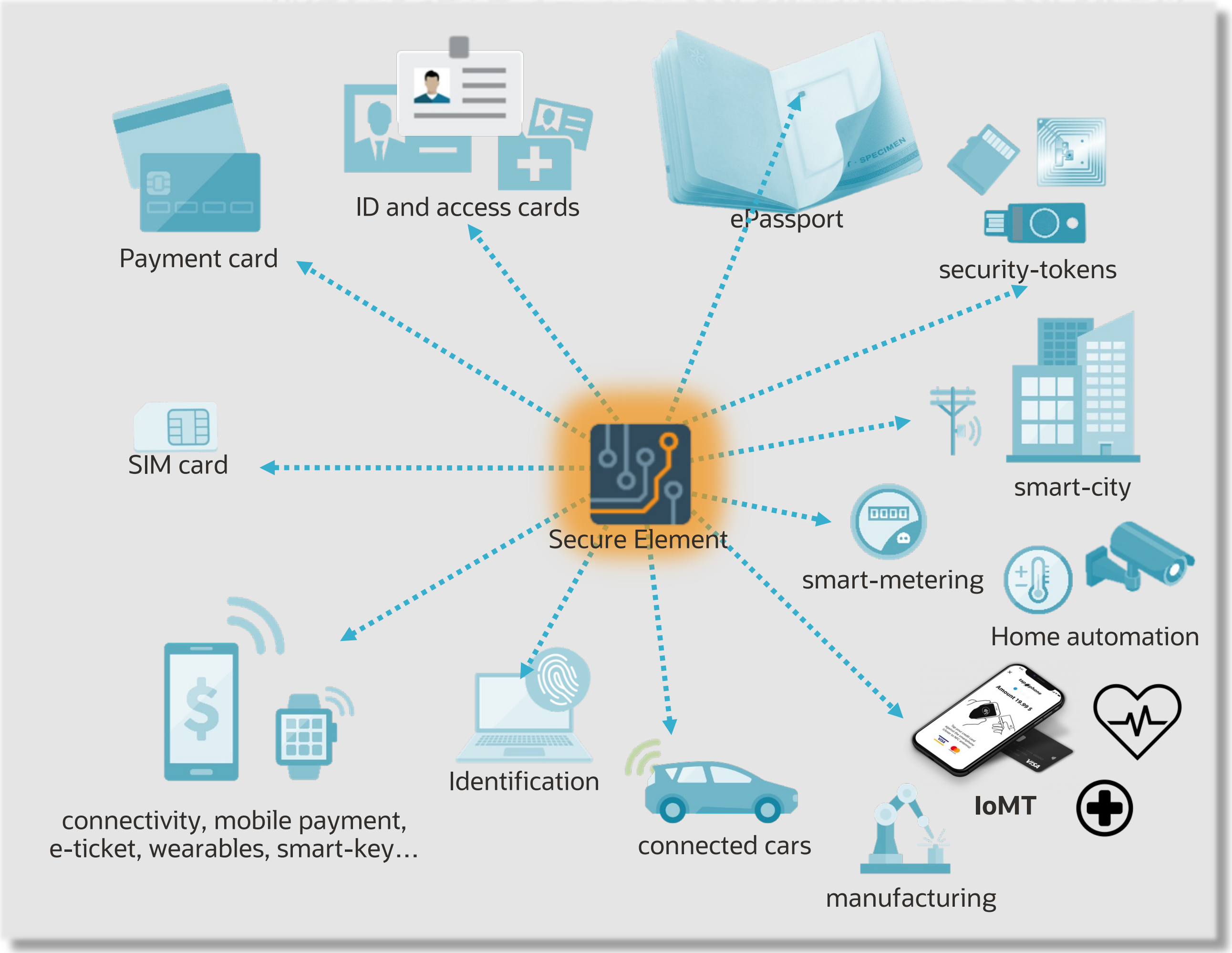
Data Integrity

Secure storage

Secure transactions

Authentication

Device Attestation

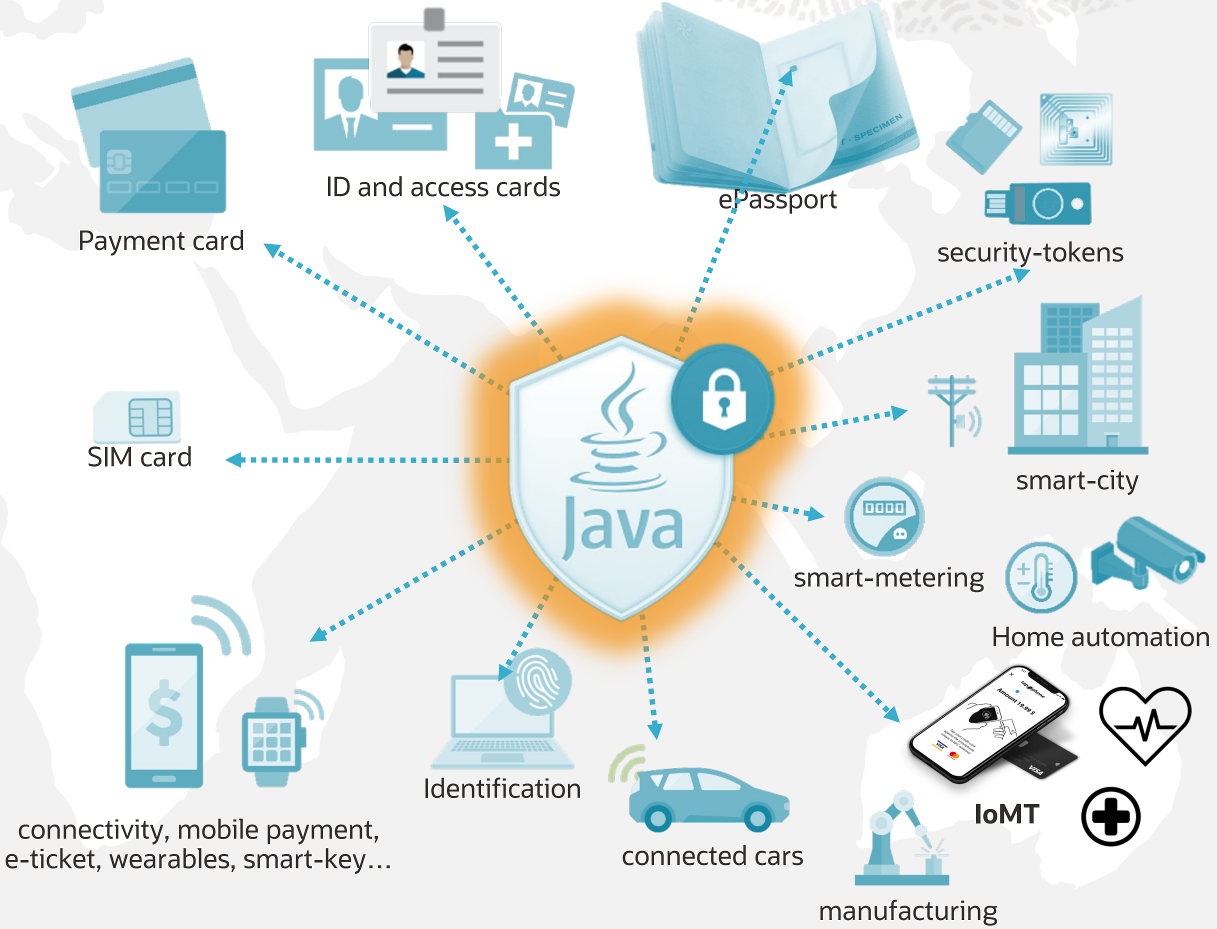


Java Card Platform

Reference runtime for Secure Elements

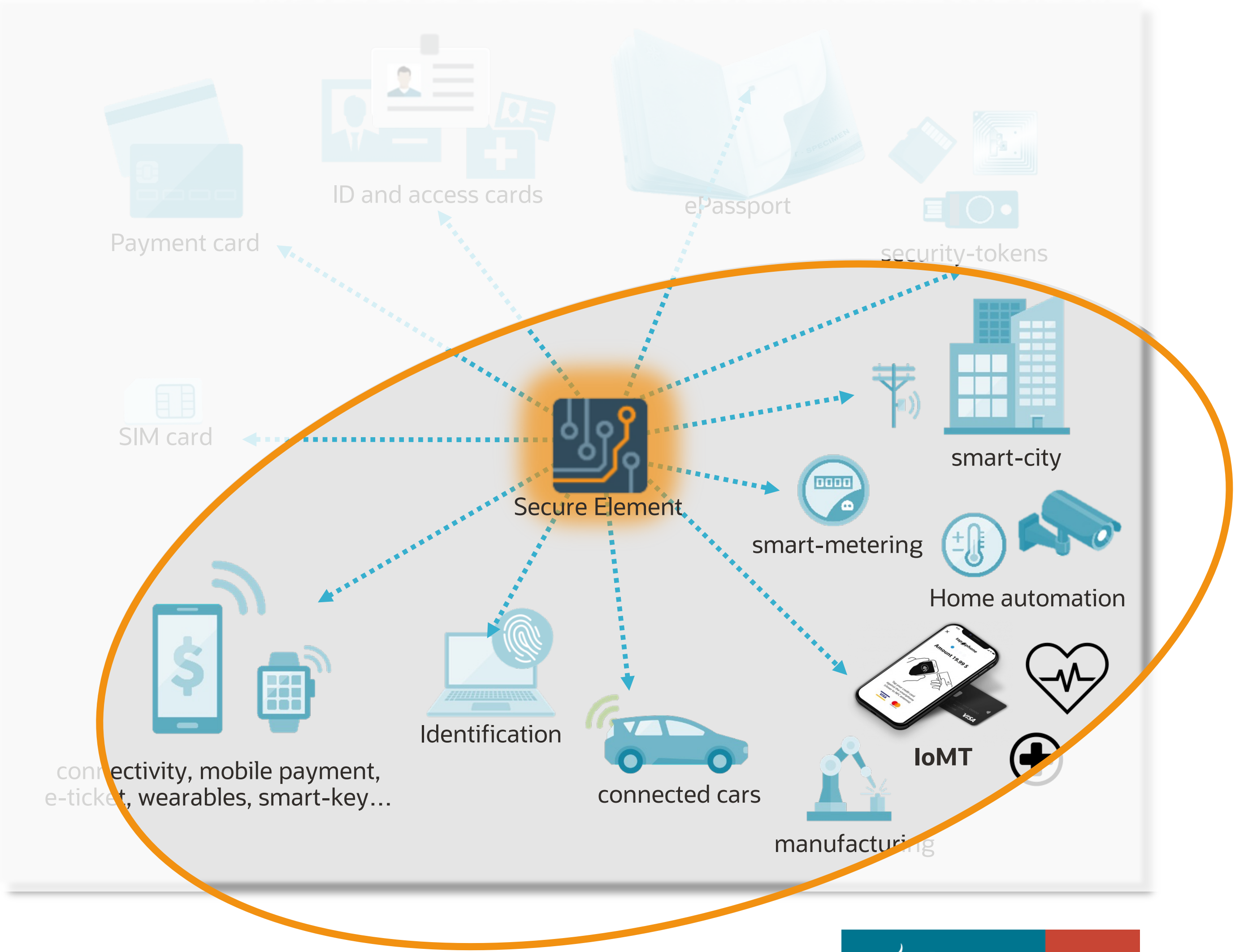
6 Billion

Secure Elements running Java Card are issued every year



Java Card 3.1, 3.2, … Release goals

- Continue to support traditional markets
- Address new use-cases (e.g. IoT, **IoMT**, Industry 5.0, Digital Twin, Non-Human Identity, Blockchain, A.I. – M.L., …)
- Support new secure hardware (SE, eSE, iSE)
- Fulfill broader security requirements



IoMT – Internet of Medical Things

Use Java Card Platform in SE to secure the healthcare data

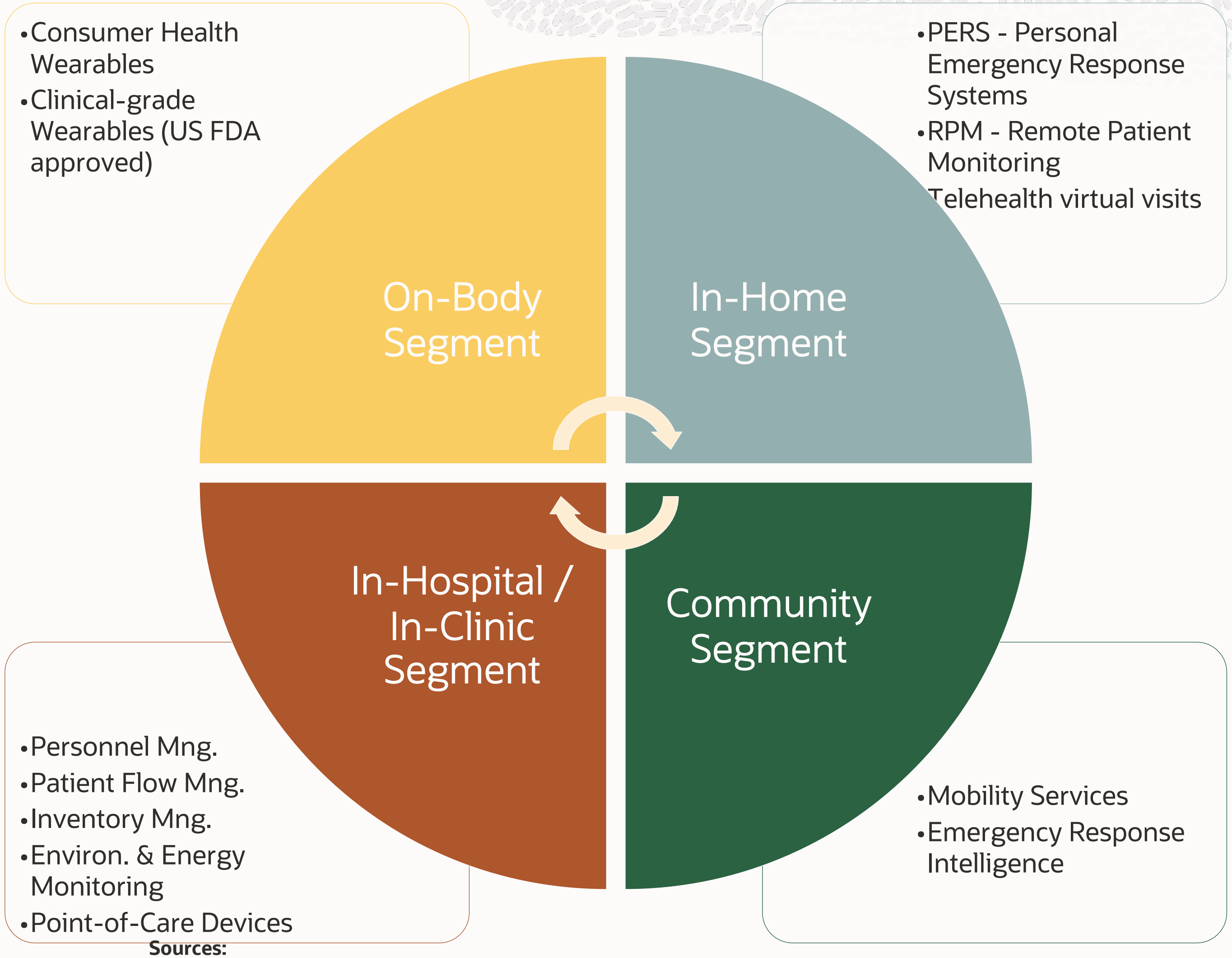
Dec 2022 – FDA authorized to regulate new medical device submissions to ensure security testing and controls

$543 billion - The expected size of the medical IoT devices market in 2025

It's concerning that **57% of healthcare security professionals don't fully understand the risks associated with unmanaged and IoT devices**, according to Armis report on IoT security.

There's even a lack of understanding of what counts as Internet of Things in healthcare:

- 48% think that MRIs, X-ray, and ultrasound machines that connect to the network don't count as IoT technology.
- 41% think that biomedical devices (infusion pumps, ventilators, crash carts) that use Wi-Fi or Bluetooth don't count as IoT-enabled devices.



- Consumer Health Wearables
- Clinical-grade Wearables (US FDA approved)

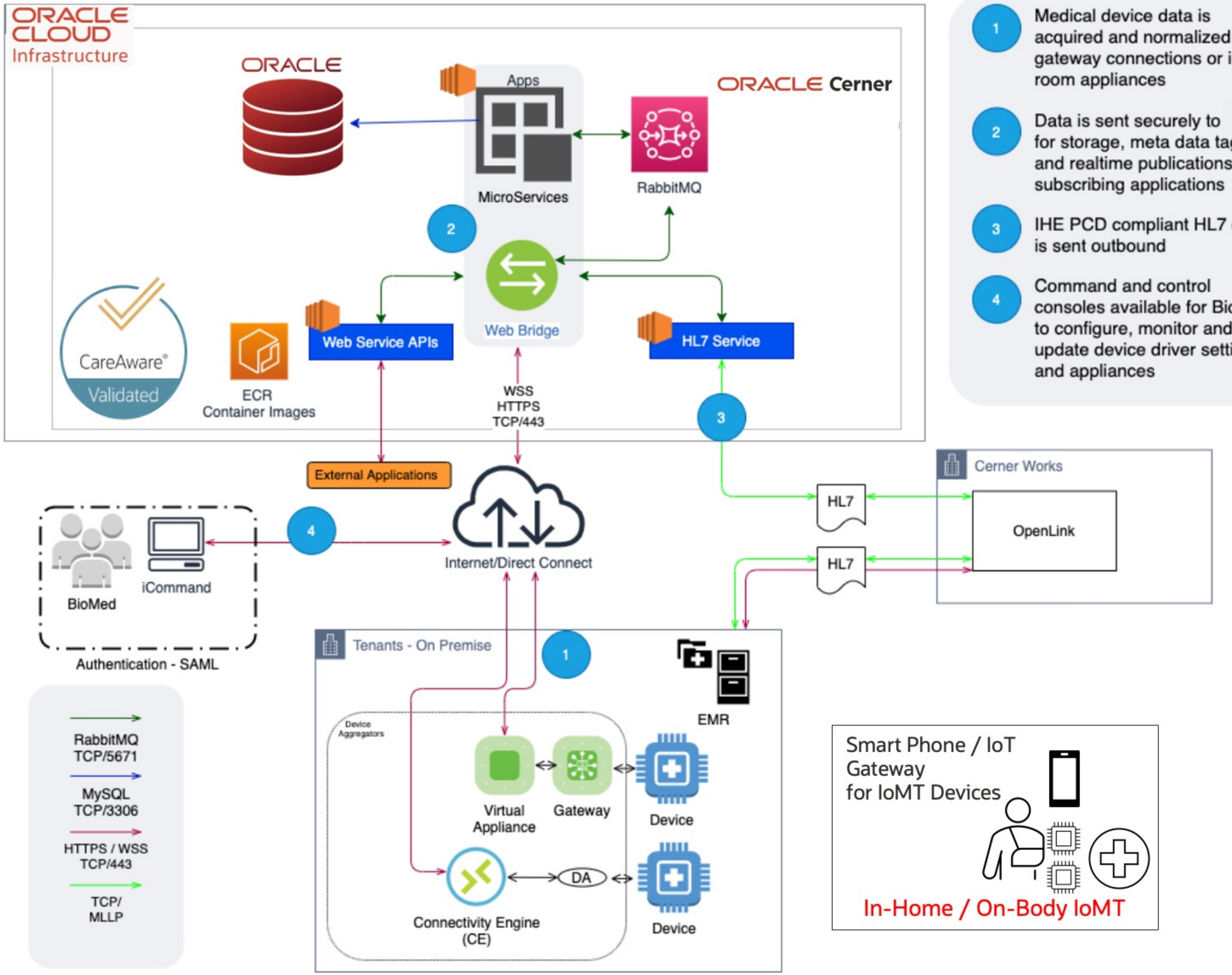
- PERS - Personal Emergency Response Systems
- RPM - Remote Patient Monitoring
- Telehealth virtual visits

- Personnel Mng.
- Patient Flow Mng.
- Inventory Mng.
- Environ. & Energy Monitoring
- Point-of-Care Devices

- Mobility Services
- Emergency Response Intelligence

Sources:
https://www.armis.com/analyst-reports/state-of-enterprise-iot-security-a-spotlight-on-healthcare/
https://www.armis.com/blog/chapter-1-how-to-innovate-in-healthcare-with-iomt-devices-without-exposing-the-expanding-cyber-attack-surface/
https://www.grandviewresearch.com/press-release/global-iot-in-healthcare-market
https://www.marketsandmarkets.com/Market-Reports/iot-healthcare-market-160082804.html

Oracle CareAware iBus Bedside & In-Home Medical Device Integration



1. Medical device data is acquired and normalized via gateway connections or in room appliances
2. Data is sent securely to OCI for storage, meta data tagging and realtime publications for subscribing applications
3. IHE PCD compliant HL7 data is sent outbound
4. Command and control consoles available for BioMed to configure, monitor and update device driver settings and appliances

CareAware® is Cerner's EHR-agnostic platform for integrating the Internet of Medical Things. Supporting EHRs include:

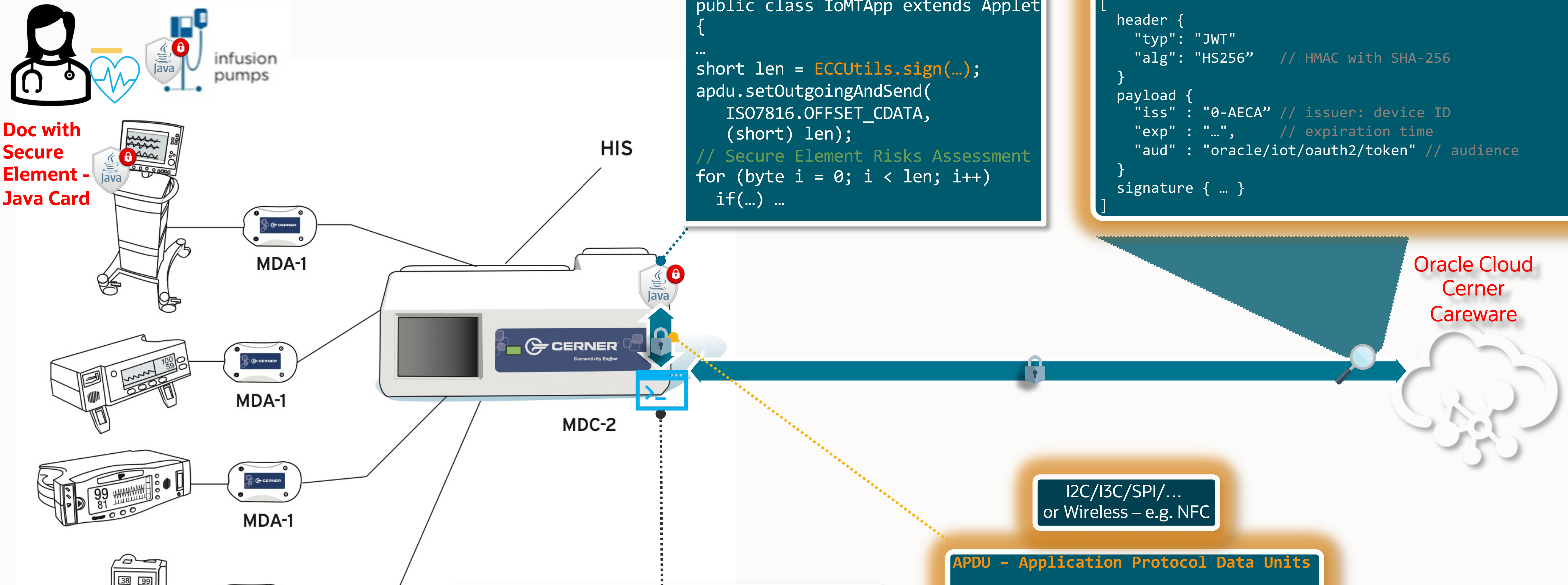
Cerner Millennium® Cerner Soarian® Cerner i.s.h.med® Cerner medico®	**Non-Cerner EHRs:** Epic Meditech Medhost Copra iMDsoft

IHE = Integrating the Health Enterprise
PCD = Patient Care Device
EHR = Electronic Health Register
EMR = Electronic Medical Records
SAML = Security Assertion Markup Language
DA = Oracle Cerner CareAware Device Adapter
MLLP = Minimum Lower Layer Protocol

OCI = Oracle Cloud Infrastructure
HL7 = Health Level 7

Use Case - In Hospital/Clinic Monitoring – Optional JC

Bedside Medical Device Integration



infusion pumps
Doc with Secure Element - Java Card
Java
HIS
MDA-1
MDA-1
MDA-1
MDA-1
MDC-2
CERNER Connectivity Engine
Oracle Cloud Cerner Careware

```
// Java Card Applet
public class IoMTApp extends Applet
{
…
short len = ECCUtils.sign(…);
apdu.setOutgoingAndSend(
    ISO7816.OFFSET_CDATA,
    (short) len);
// Secure Element Risks Assessment
for (byte i = 0; i < len; i++)
  if(…) …
```

```
Communications Protocols
HTTPs, MQTTs, gRPC, JMS ... with payload
- e.g. Authentication token(s)

[
  header {
    "typ": "JWT"
    "alg": "HS256”   // HMAC with SHA-256
  }
  payload {
    "iss" : "0-AECA” // issuer: device ID
    "exp" : "…",     // expiration time
    "aud" : "oracle/iot/oauth2/token" // audience
  }
  signature { … }
]
```

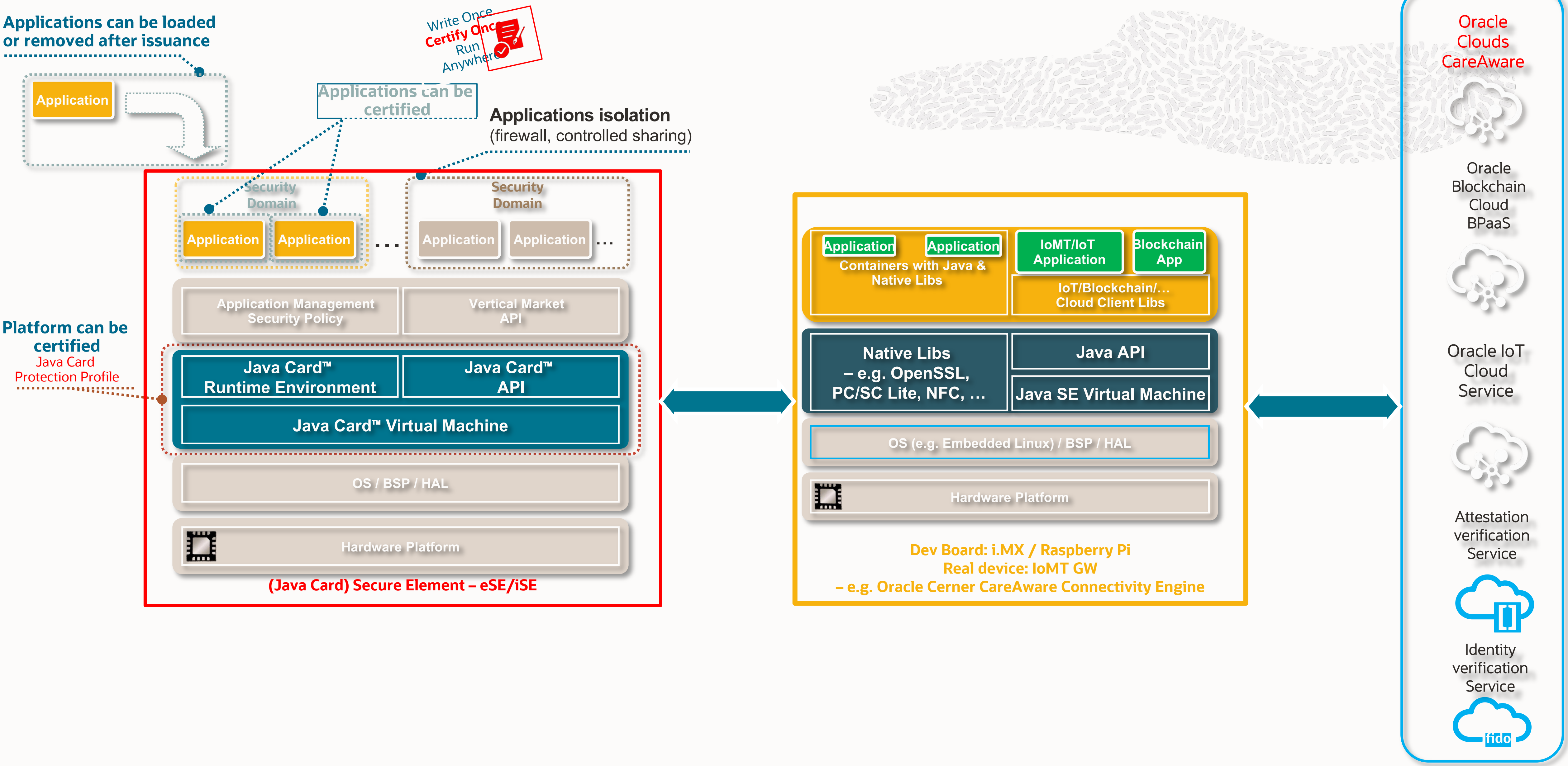
I2C/I3C/SPI/…
or Wireless – e.g. NFC

```
APDU – Application Protocol Data Units

APDU Command
CLA, INS, P1, P2, LC, …, LE

APDU Response
…, SW1, SW2
```

```
// IoT GW/CE Client application
try (CEngine gateway = client.connect()) {
  .
  HL7Proto netHL7 = gateway.getProtocol();
  ...
}
```

https://www.cerner.com/solutions/device-connectivity/cerner-validation

Java Card & IoMT



Applications can be loaded or removed after issuance

Application

Write Once
Certify Once
Run Anywhere

Applications can be certified

Applications isolation
(firewall, controlled sharing)

Security Domain

Application

Application

…

Security Domain

Application

Application

…

Application Management Security Policy

Vertical Market API

Platform can be certified
Java Card Protection Profile

Java Card™ Runtime Environment

Java Card™ API

Java Card™ Virtual Machine

OS / BSP / HAL

Hardware Platform

(Java Card) Secure Element – eSE/iSE

Application

Application

Containers with Java & Native Libs

IoMT/IoT Application

Blockchain App

IoT/Blockchain/… Cloud Client Libs

Native Libs – e.g. OpenSSL, PC/SC Lite, NFC, …

Java API

Java SE Virtual Machine

OS (e.g. Embedded Linux) / BSP / HAL

Hardware Platform

Dev Board: i.MX / Raspberry Pi
Real device: IoMT GW
– e.g. Oracle Cerner CareAware Connectivity Engine

Oracle Clouds CareAware

Oracle Blockchain Cloud BPaaS

Oracle IoT Cloud Service

Attestation verification Service

Identity verification Service

Use-case Remote patient monitoring

Heart-rate, Electrocardiogram (ECG), (non-invasive) Blood Glucose, Pressure, Oxygen & Temperature Monitoring

Remote patient monitoring is the most common application of IoT devices for healthcare. IoT devices can automatically collect health metrics like heart rate, blood pressure, temperature, and more (Electrocardiogram (ECG), Glucose, Blood pressure, Blood Oxygen) from patients who are not physically present in a healthcare facility, eliminating the need for patients to travel to the providers, or for patients to collect it themselves.

Today, a variety of small IoT devices are available for Heart-rate, Electrocardiogram (ECG), (non-invasive) Blood Glucose, Pressure, Oxygen & Temperature Monitoring, freeing patients to move around as they like while ensuring that their hearts are monitored continuously. ***Guaranteeing ultra-accurate results remains somewhat of a challenge, but most modern devices can deliver accuracy rates of about 90 percent or better.***

A major challenge with remote patient monitoring devices is ensuring that the highly personal data that these IoT devices collect is SECURE and PRIVATE.

https://ordr.net/article/iot-healthcare-examples/ | https://www.fruugo.ro/e500-blood-glucose-smart-watch-ecg-monitoring-men-womens-health-temperature-non-invasive-blood-sugar-smartwatch-ip68-waterproof/p-177962820-380091632

Use-case Parkinson’s disease monitoring

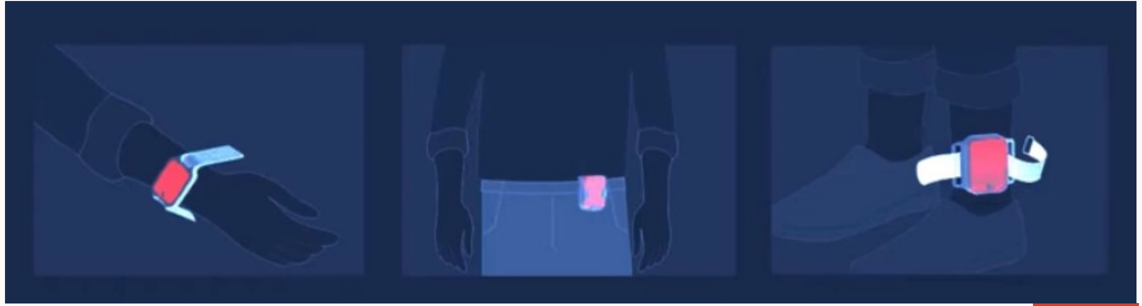
Parkinson’s Neuro Tech IoT Device Monitoring

Parkinson’s disease is the second most common neurodegenerative disease and a major cause of disability worldwide. Treatment is currently based on subjective questionaries and rare patient doctor interactions.

In order to treat Parkinson’s patients most effectively, healthcare providers must be able to assess how the severity of their symptoms (Tremor, Bradykinesia – lack of dopamine in the brain, Postural Instability, Gait Disturbance, Dyskinesia) fluctuate through the day.

IoT sensors promise to make this task much easier by continuously collecting data about Parkinson’s symptoms. At the same time, the devices give patients the freedom to go about their lives in their own homes, instead of having to spend extended periods in a hospital for observation.

Class IIa medical device according to Directive 93/42/EEC.

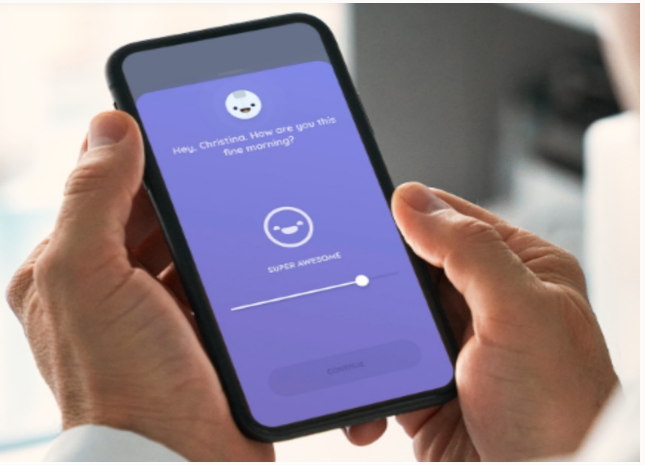


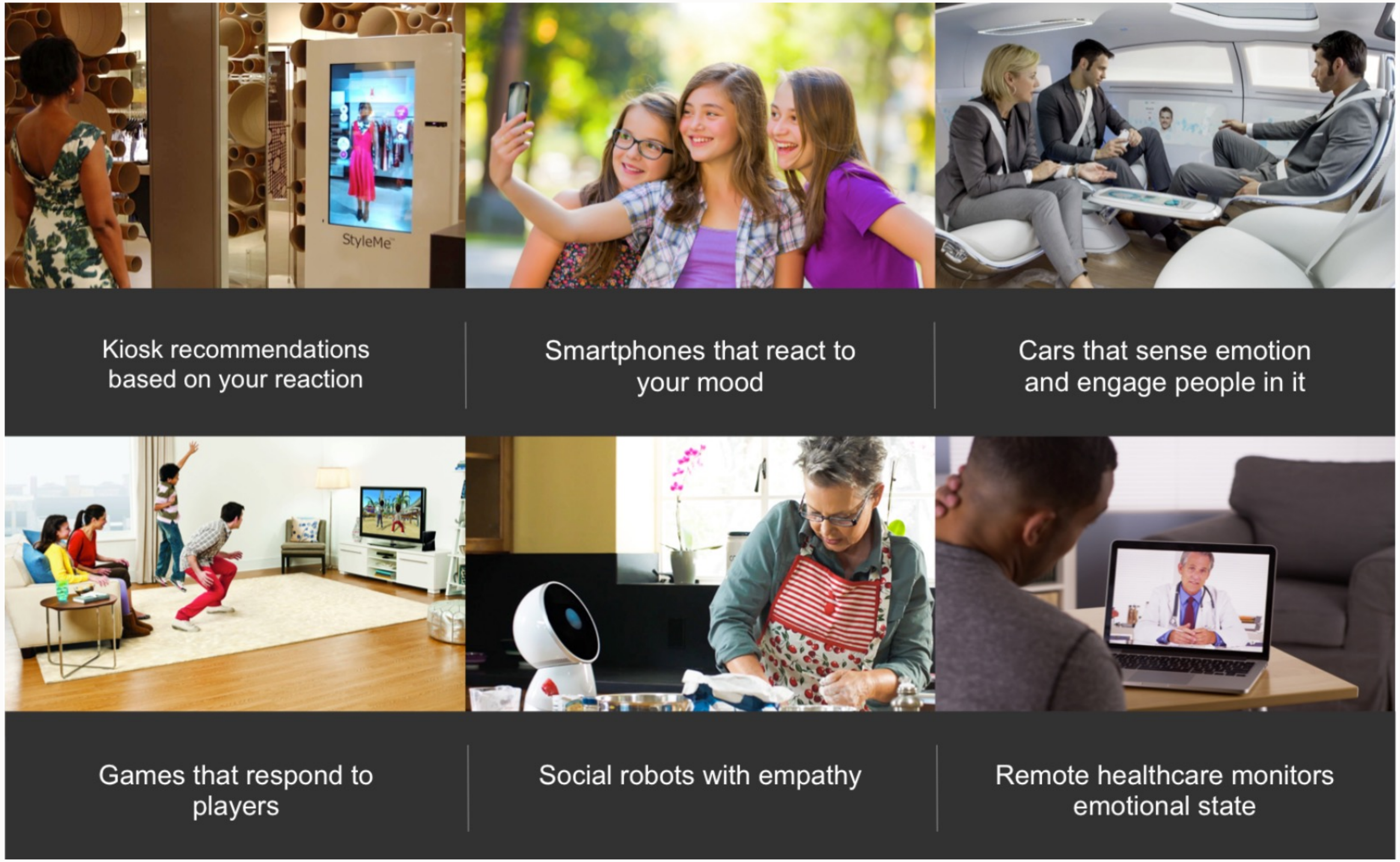
Accuracy, Anonymity and Confidentiality of the collected data is very important.

https://www.pdneurotechnology.com/

Use-case Depression and mood monitoring

“Mood-aware” IoT devices




StyleMe
Kiosk recommendations based on your reaction
Smartphones that react to your mood
Cars that sense emotion and engage people in it
Games that respond to players
Social robots with empathy
Remote healthcare monitors emotional state

“Mood-aware” IoT devices collecting and analyzing data such as heart rate, face motions and blood pressure, they can infer information about a patient’s mood state. Advanced IoT devices for mood monitoring can even track data such as the movement of a patient’s eyes.

https://www.bgosoftware.com/blog/10-internet-of-things-iot-healthcare-examples/
https://blog.affectiva.com/the-mood-aware-internet-of-things

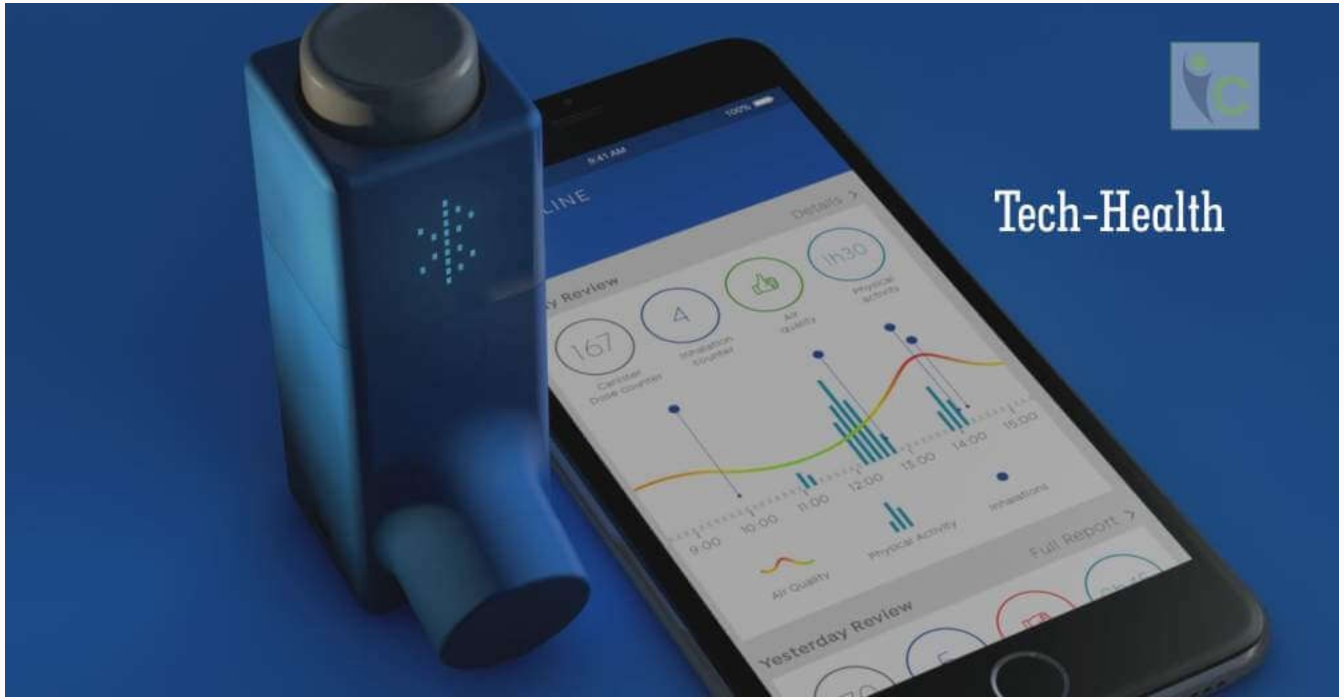
Asthma or Chronic Obstructive Pulmonary Disease (COPD) monitoring

Smart Connected Inhalers

Conditions such as asthma or Chronic Obstructive Pulmonary Disease (COPD) often involve attacks that come on suddenly, with little warning. IoT-connected inhalers can help patients by monitoring the frequency of attacks, as well as collecting data from the environment to help healthcare providers understand what triggered an attack.

In addition, connected inhalers can alert patients when they leave inhalers at home, placing them at risk of suffering an attack without their inhaler present, or when they use the inhaler improperly.

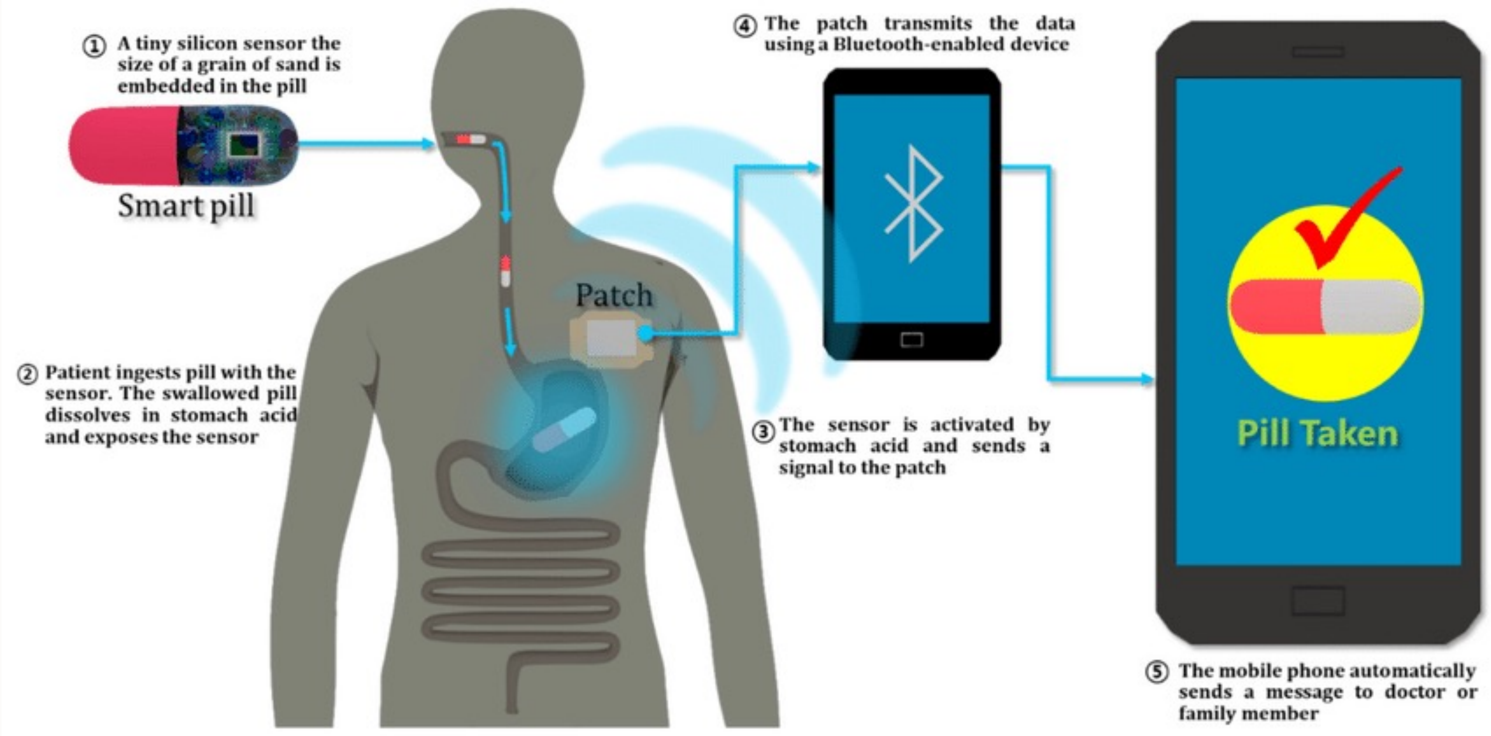
Security of the collected data is very important.



https://insightscare.com/smart-inhalers-tackling-respiratory-maladies-iot/

Use case of Collecting data from inside the human body

Smart Ingestible sensors
Ingestible-Micro-Bio-Electronic-Device (IMBED)



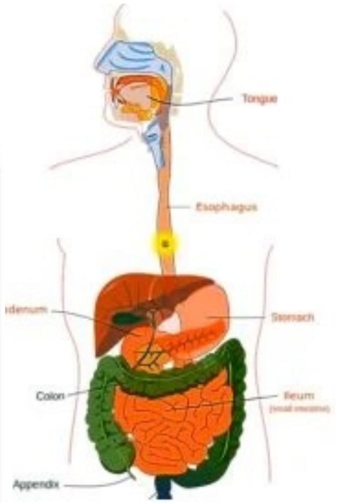
① A tiny silicon sensor the size of a grain of sand is embedded in the pill

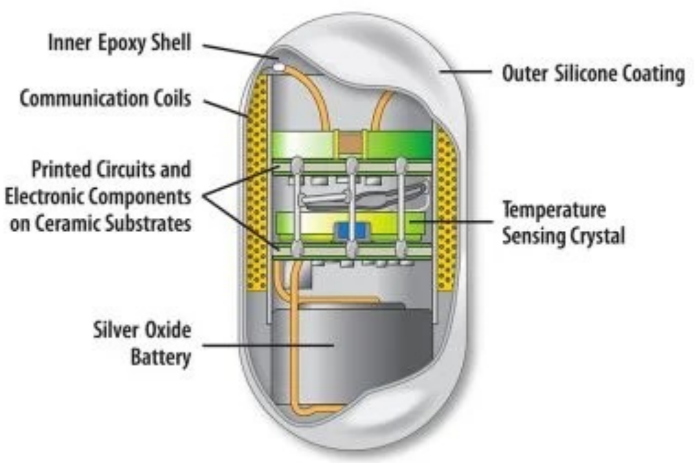
② Patient ingests pill with the sensor. The swallowed pill dissolves in stomach acid and exposes the sensor

③ The sensor is activated by stomach acid and sends a signal to the patch

④ The patch transmits the data using a Bluetooth-enabled device

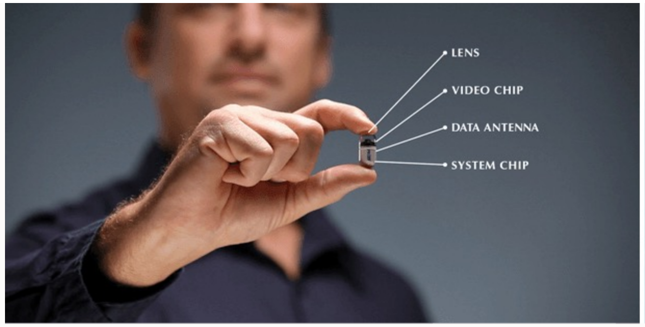
⑤ The mobile phone automatically sends a message to doctor or family member





Inner Epoxy Shell
Communication Coils
Printed Circuits and Electronic Components on Ceramic Substrates
Silver Oxide Battery
Outer Silicone Coating
Temperature Sensing Crystal

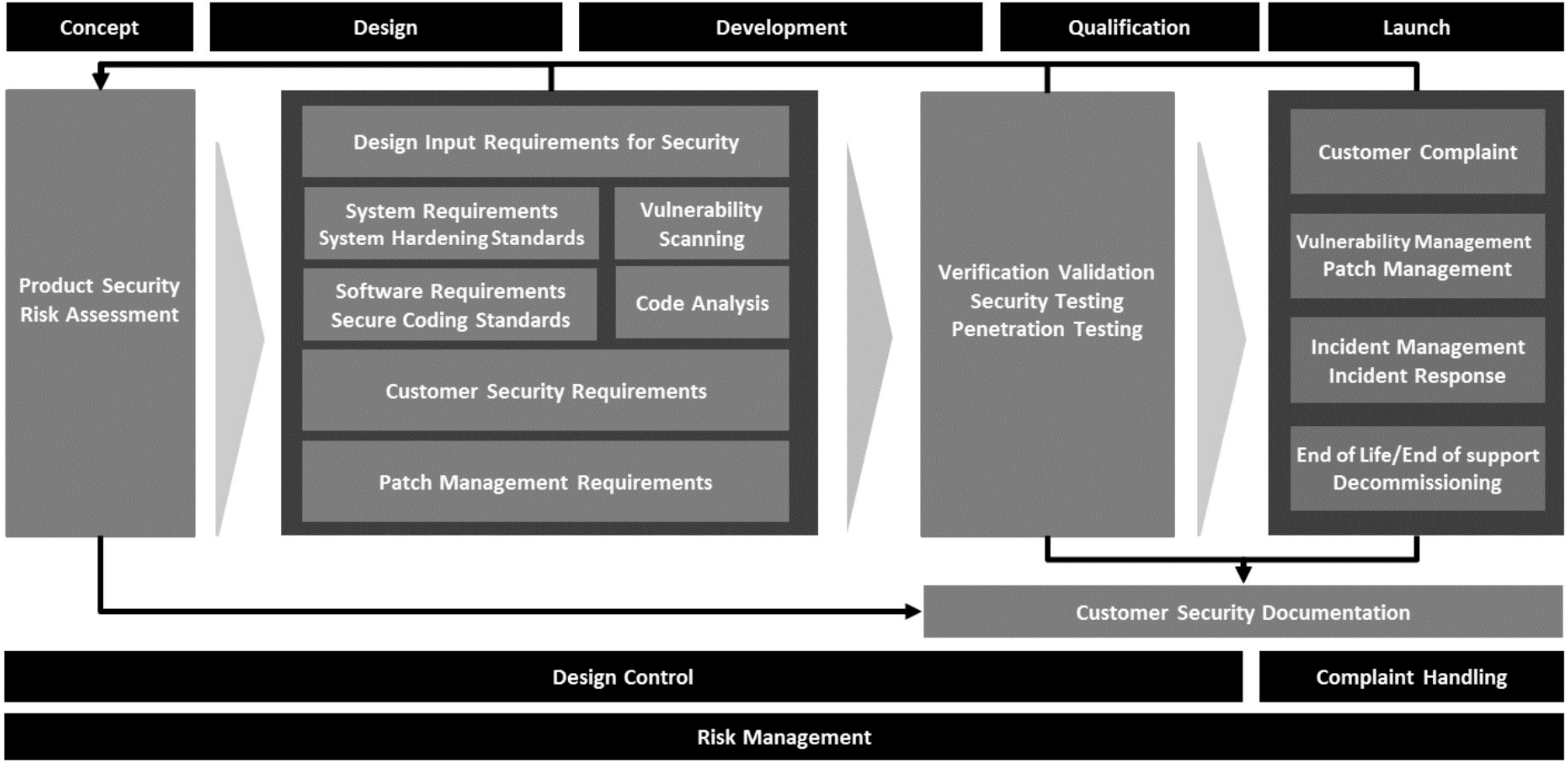
Collecting data from inside the human body is typically disruptive and difficult for the patients. Camera or probe stuck into the patient digestive tract is disturbing.
With ingestible sensors, it’s possible to collect information from digestive and other systems in a much less invasive way. They provide insights into stomach PH levels, for instance, or help pinpoint the source of internal bleeding.
The idea of putting tiny microchips and cameras into the human body might make some consumers uncomfortable. There’s no doubt that numerous scientific, legal and ethical questions will be raised in the next few years. The jury’s still out as questions about privacy, data sharing and *side effects* continue to be raised.



https://www.marsdd.com/news/ingestibles-smart-pills-revolutionize-healthcare/ | https://ee.cdnartwhere.eu/
https://www.researchgate.net/figure/Overview-of-ingestible-pill-sensor-system_fig5_333472144

Security Standardization for the Healthcare Sector

Healthcare and Public Health Sector Coordinating Council (HSCC) Joint Security Plan (JSP)



Concept

Design

Development

Qualification

Launch

Product Security Risk Assessment

Design Input Requirements for Security

System Requirements
System Hardening Standards

Vulnerability Scanning

Software Requirements
Secure Coding Standards

Code Analysis

Customer Security Requirements

Patch Management Requirements

Verification Validation
Security Testing
Penetration Testing

Customer Complaint

Vulnerability Management
Patch Management

Incident Management
Incident Response

End of Life/End of support
Decommissioning

Customer Security Documentation

Design Control

Complaint Handling

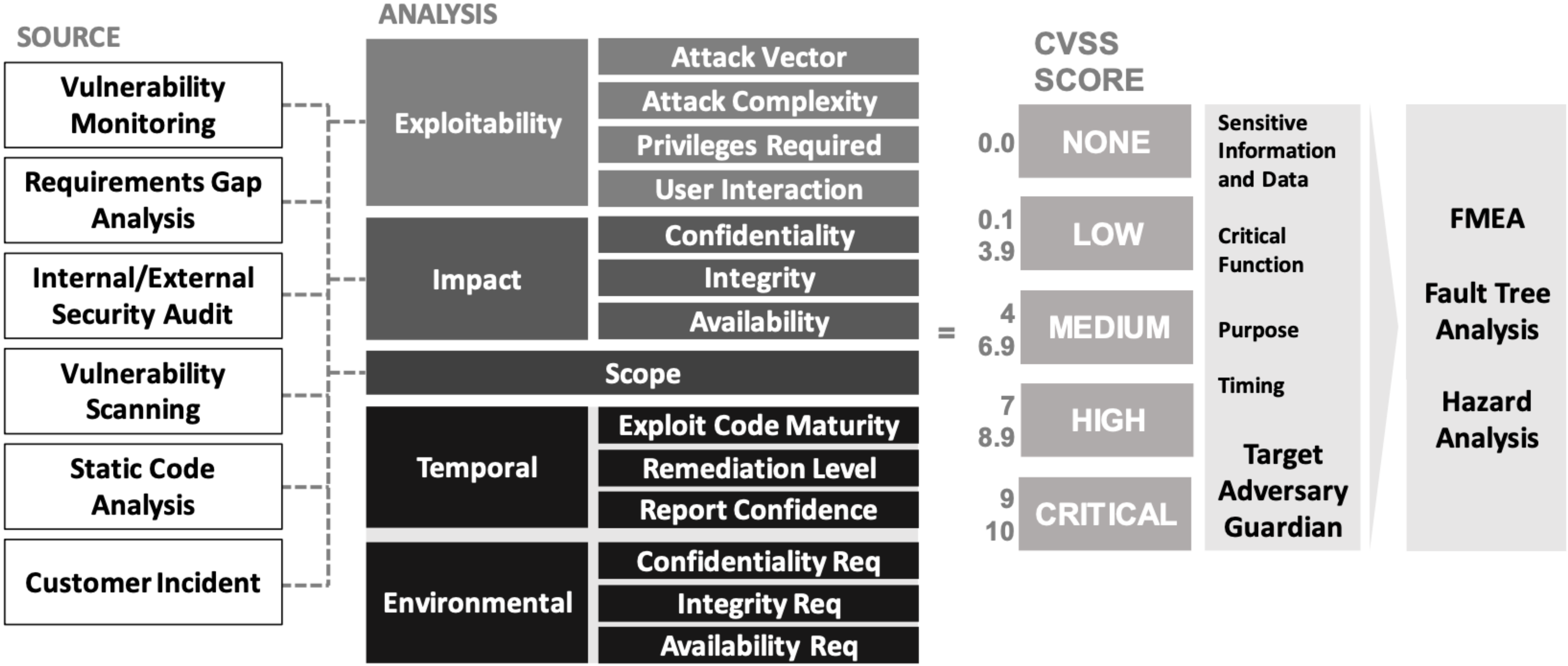
Risk Management

Product Security Framework

HSCC JSP: https://healthsectorcouncil.org/wp-content/uploads/2021/11/HSCC-MEDTECH-JSP-v1.pdf

Security Standardization for the Healthcare Sector

Healthcare and Public Health Sector Coordinating Council (HSCC) Joint Security Plan (JSP)



SOURCE

Vulnerability Monitoring

Requirements Gap Analysis

Internal/External Security Audit

Vulnerability Scanning

Static Code Analysis

Customer Incident

ANALYSIS

Exploitability: Attack Vector, Attack Complexity, Privileges Required, User Interaction

Impact: Confidentiality, Integrity, Availability

Scope

Temporal: Exploit Code Maturity, Remediation Level, Report Confidence

Environmental: Confidentiality Req, Integrity Req, Availability Req

=

CVSS SCORE

0.0 NONE

0.1 – 3.9 LOW

4 – 6.9 MEDIUM

7 – 8.9 HIGH

9 – 10 CRITICAL

Sensitive Information and Data

Critical Function

Purpose

Timing

Target Adversary Guardian

FMEA

Fault Tree Analysis

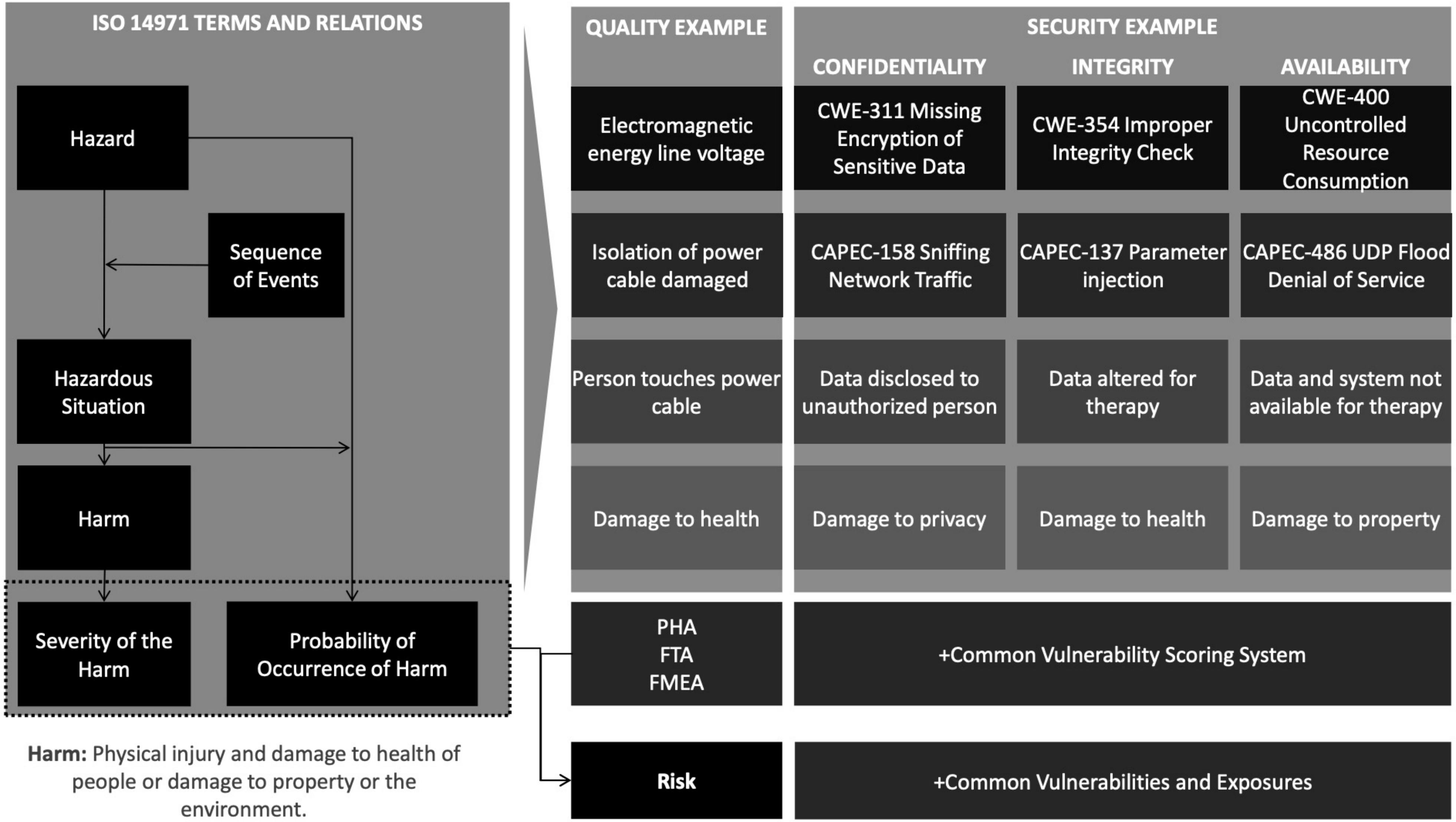
Hazard Analysis

Risk Assessment Sources

HSCC JSP: https://healthsectorcouncil.org/wp-content/uploads/2021/11/HSCC-MEDTECH-JSP-v1.pdf

Security Standardization for the Healthcare Sector

Healthcare and Public Health Sector Coordinating Council (HSCC) Joint Security Plan (JSP)



QUALITY EXAMPLE	SECURITY EXAMPLE		
	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
Electromagnetic energy line voltage	CWE-311 Missing Encryption of Sensitive Data	CWE-354 Improper Integrity Check	CWE-400 Uncontrolled Resource Consumption
Isolation of power cable damaged	CAPEC-158 Sniffing Network Traffic	CAPEC-137 Parameter injection	CAPEC-486 UDP Flood Denial of Service
Person touches power cable	Data disclosed to unauthorized person	Data altered for therapy	Data and system not available for therapy
Damage to health	Damage to privacy	Damage to health	Damage to property
PHA FTA FMEA	+Common Vulnerability Scoring System		
Risk	+Common Vulnerabilities and Exposures		

Harm: Physical injury and damage to health of people or damage to property or the environment.

Risk Assessment Mapping

HSCC JSP: https://healthsectorcouncil.org/wp-content/uploads/2021/11/HSCC-MEDTECH-JSP-v1.pdf

Security Standardization for the Healthcare Sector

Health Level 7 (HL7) Fast Healthcare Interoperability Resources (FHIR)

Fast Healthcare Interoperability Resources (FHIR) is not a security protocol, nor does it define any security related functionality. However, FHIR does define exchange protocols and content models that need to be used with various security protocols defined elsewhere. This section gathers all information about security in one section. A summary:

1. Time Keeping
2. Communications Security
3. Authentication
4. Authorization/Access Control
5. Audit
6. Digital Signatures
7. Attachments
8. Labels
9. Data Management Policies
10. Narrative
11. Input Validation
12. Security / Privacy Event Reporting

HL7 FHIR: https://hl7.org/fhir/documentation.html

Securing Internet of Medical Things (IoMT) with Java Card

#agenda

01 **Medical Devices**

IoMT, Terminology, Architecture, …

02 **Java Card & IoMT Use-cases**

Java Card, IoMT, Use-cases, Healthcare Security Standards

03 **Q&A**

Conclusions

Addressing evolving security requirements

A comprehensive set of API for security services

Security assets

- Key generation and key storage API
  to securely store and use symmetric or asymmetric keys
  and easily configure the key generation 3.1
- PIN code API
  for secure handling of PIN codes
- Biometry API
  to securely enroll and verify biometric templates
- Certificate API
  to optimize storage and certificate parsing 3.1

Cryptography

- Digital Signature API 3.1
  to sign and verify using DES, AES, DSA, RSA, HMAC, ECDSA, Additional ISO9796 digital signature with message recovery paddings, EdDSA… 3.2
- Encryption/Decryption API 3.1
  to encrypt or decrypt using DES, AES…
  with ECB,CBC,CFB, CTR, XTS modes,
  Authenticated Encryption AEAD GCM, CCM,
  Configure RSA-OAEP cipher scheme, … 3.2
- Digest API
  to create a hash of data using SHA1, SHA256, SHA3, SM3, RIPEMD160, …
- Random numbers API
  true random (TRNG) or deterministic (DRBG)
- Big Numbers API
  to perform operations on big integers.

Security Protocols

- Key Agreement API 3.1
  to perform Diffie-Hellman key exchange (including ECDH with curves X25519, X448)
- Key Derivation Functions API 3.1
  to derive keys (X9.63, NIST SP800-108, HKDF, IEEE1363, TLS1.1, TLS1.2, …)
- Monotonic Counter API 3.1
  for anti-replay functions
- Security assertions API
  for control-flow integrity
- TLS1.3 and DTLS1.3 key schedule 3.2

Java Card key features for IoT/IoMT

Programmable Secure Runtime

To develop new applications and securely run them in a secure element

Portable

To deploy and operate services on multiple hardware platforms, from different vendors, at lower cost

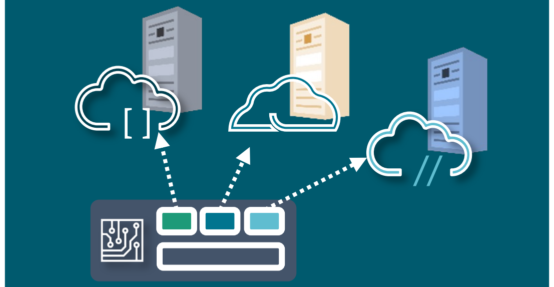
01110
10011
01110

Manageable

To deploy new services, update or upgrade code and ensure up-to-date security

Extensible

To extend the platform or upgrade services to remain compliant with fast evolving security requirements



More Information

https://www.oracle.com/java/java-card/

Java Card Platform Specification 3.2

Latest release of the Java Card specification and the reference for Java Card products.

Java Card Development Kit Tools

The Java Card Development Kit Tools are used to convert and verify Java Card applications.

Java Card Development Kit Simulator

The Java Card Development Kit Simulator includes a simulation component and Eclipse plug-in.
Combined with the Java Card Development Kit Tools, it provides a complete, stand-alone development environment.

Java Card IoT and Security blog

This Blog covers the latest Java technology for small devices and security in the IoT, Mobile, ID and Payment.

contact: https://www.oracle.com/java/contact-form.html

ngiyabonga
рахмат
danke
謝謝
spas
teşekkür ederim
Баярлалаа
mersi
kia ora
barka
welalin
tack
mahalo
tapadh leat
спасибо
faafetai lava
vinaka
спасибі
blagodaram
dank je
misaotra
matondo
paldies
grazzi
kiitos
dankie
nanni
nandri
dhanyavad
thank you
gracias
хвала
asante
manana
obrigada
tenki
bedankt
bayarlalaa
gràcie
hvala
mauruuru
köszönöm
aciú
dankon
akun
djiere dieuf
tau
mochchakkeram
murakoze
enkosi
dziękuję
дякую
mamnun
chokrane
chnorakaloutioun
grafias ago
gràcies
sulpáy
go raibh maith agat
sobodi
dėkuji
sagolun
sukriya
kop khun krap
taiku
obrigado
mèsi
didi madloba
ありがとう
tanemirt
grazie
arigatô
takk
dakujem
trugarez
najis tuke
kam sah hamnida
terima kasih
rahmat
rahmet
ευχαριστώ
diolch
dhanyavadagalu
shukriya
merce
мерси
তোমাকে ধন্যবাদ
감사합니다
xièxie
merci

ORACLE