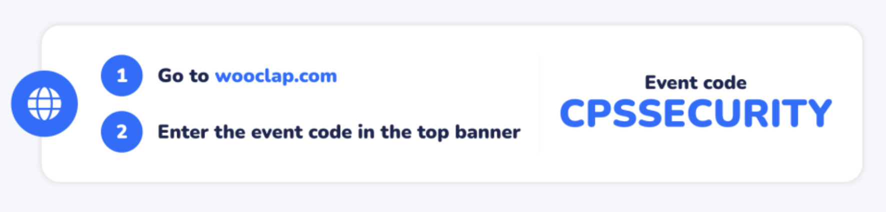
CE/CZ4055 Cyber Physical System Security

Anupam Chattopadhyay

CCDS, NTU



1 Go to wooclap.com

2 Enter the event code in the top banner

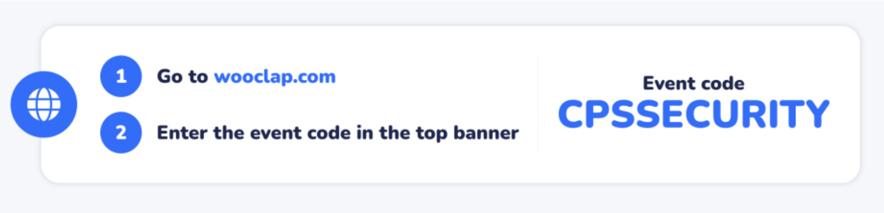
Event code

CPSSECURITY

NANYANG TECHNOLOGICAL UNIVERSITY

Contents

- *CPS/IoT: Again*
- Smart Cards
- Discussion



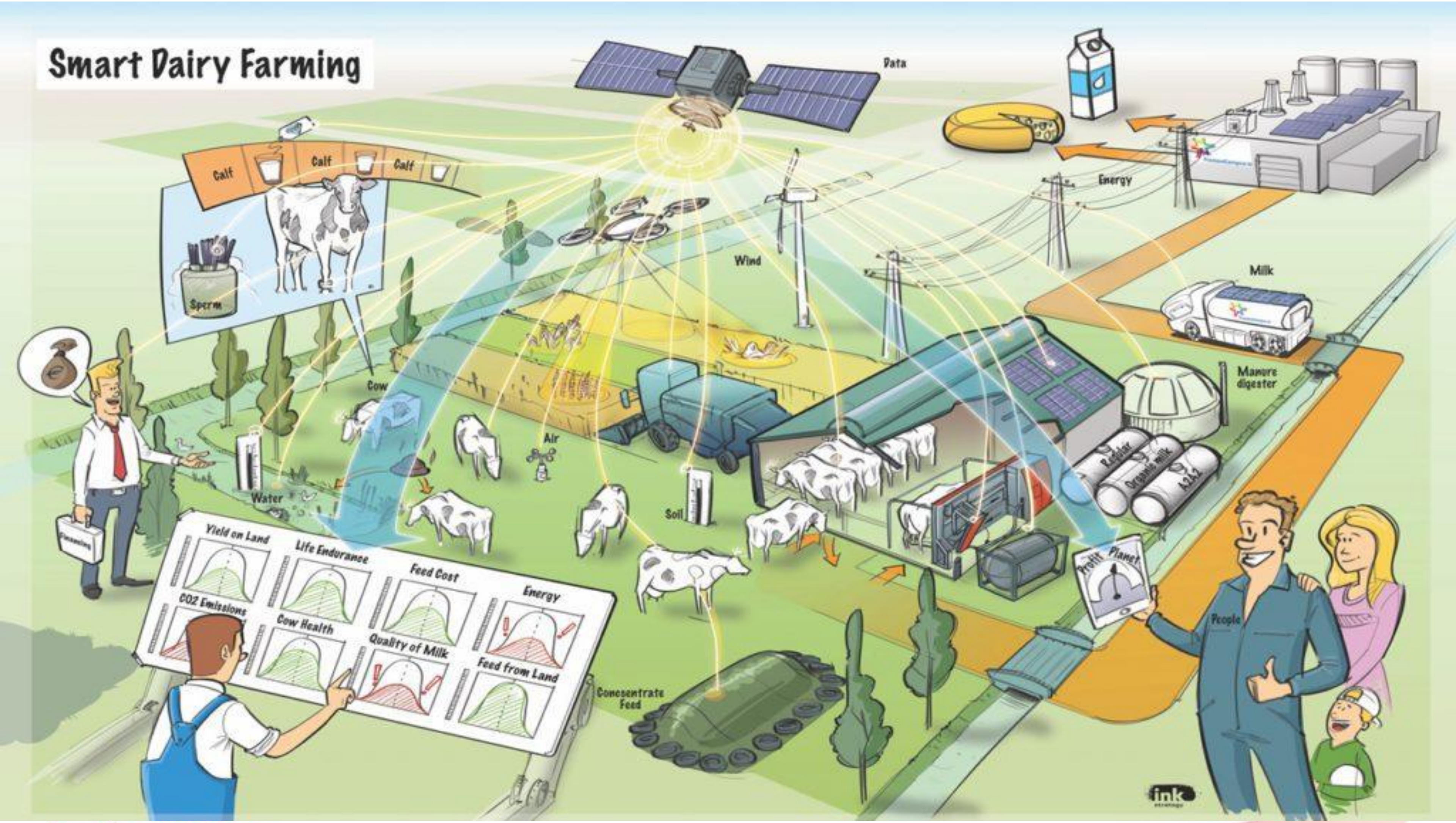
1 Go to wooclap.com

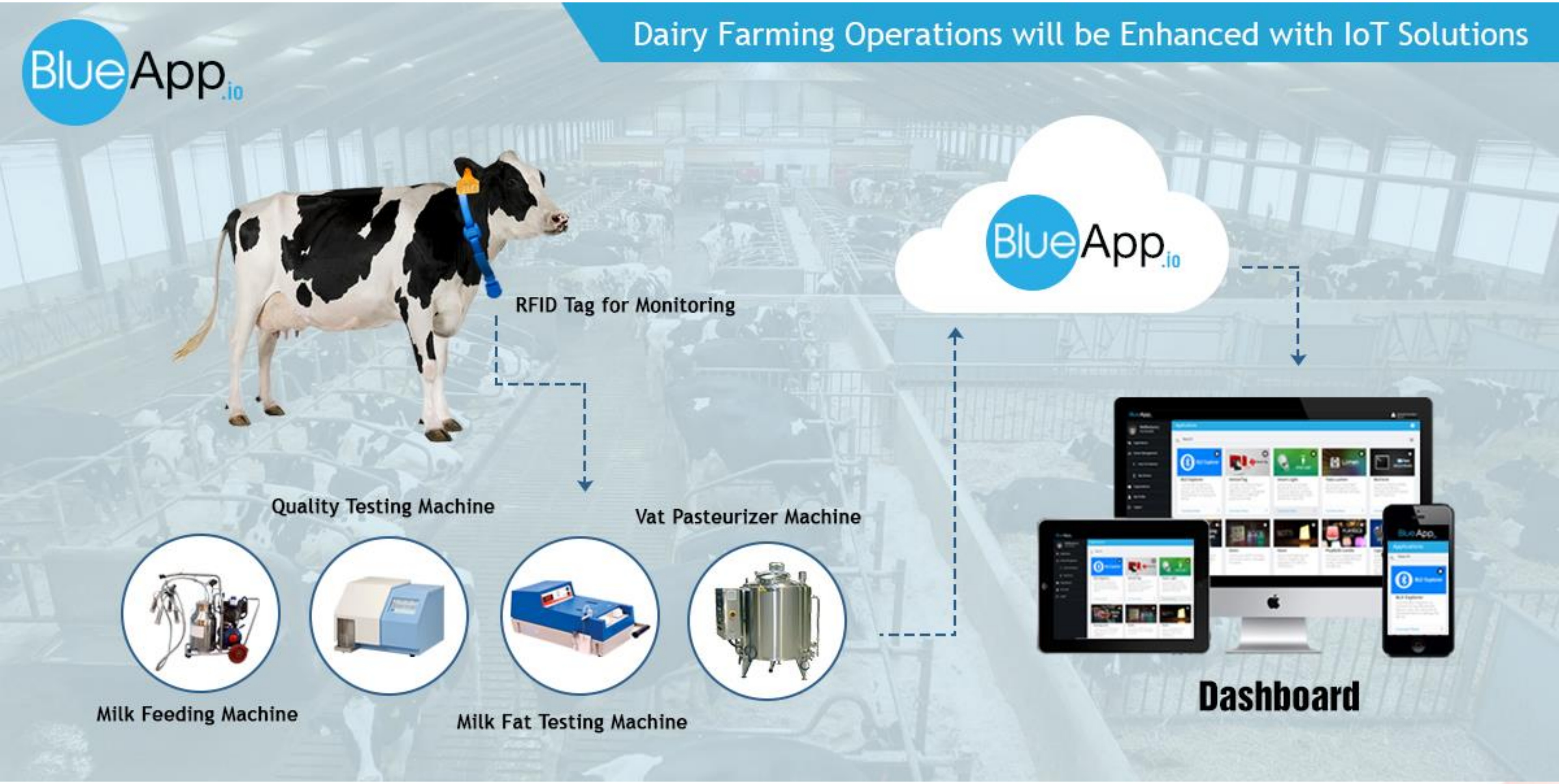
2 Enter the event code in the top banner

Event code

CPSSECURITY

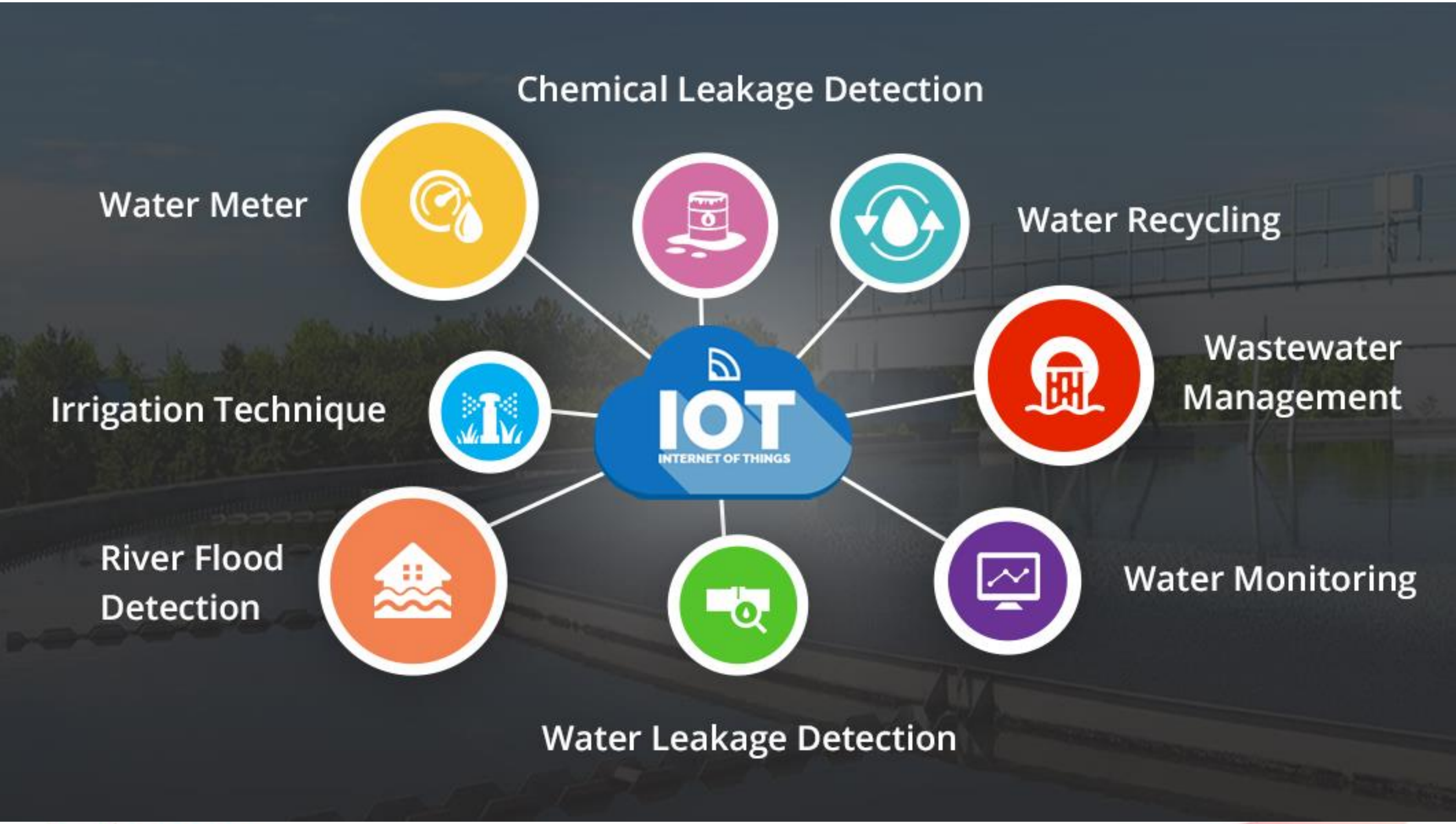
TARE 168 KG
STACKING:1+5
PROPERTY OF AL
TARA 41.1KG
2014
114003


Smart Dairy Farming
Data
Calf
Calf
Calf
Sperm
Cow
Wind
Energy
Milk
Manure digester
Air
Water
Soil
Regular
Organic milk
A2A2
Profit
Planet
People
Yield on Land
Life Endurance
Feed Cost
Energy
CO2 Emissions
Cow Health
Quality of Milk
Feed from Land
Concentrate Feed
ink



Dairy Farming Operations will be Enhanced with IoT Solutions

IOT in Agriculture
DreamzTech Solutions
Diagnosis of Diseases
Variable rate of Fertility
Auto Spreading
Water Stress
Crop yield Analysis
Field Monitoring
Smart Data
Soil Erosion
SAMSUNG
Wednesday:
Hi: 90°F
Lo: 72°F
Thursday:
Hi: 90
Lo: 72
83°F
So far today:
Hi: 88°F Lo: 71°F
Rain: 0"
Gust: 6mph S
Heat Index: 89°F
Humidity: 72%
Dew Point: 73°F



Chemical Leakage Detection

Water Meter

Water Recycling

Wastewater Management

Irrigation Technique

River Flood Detection

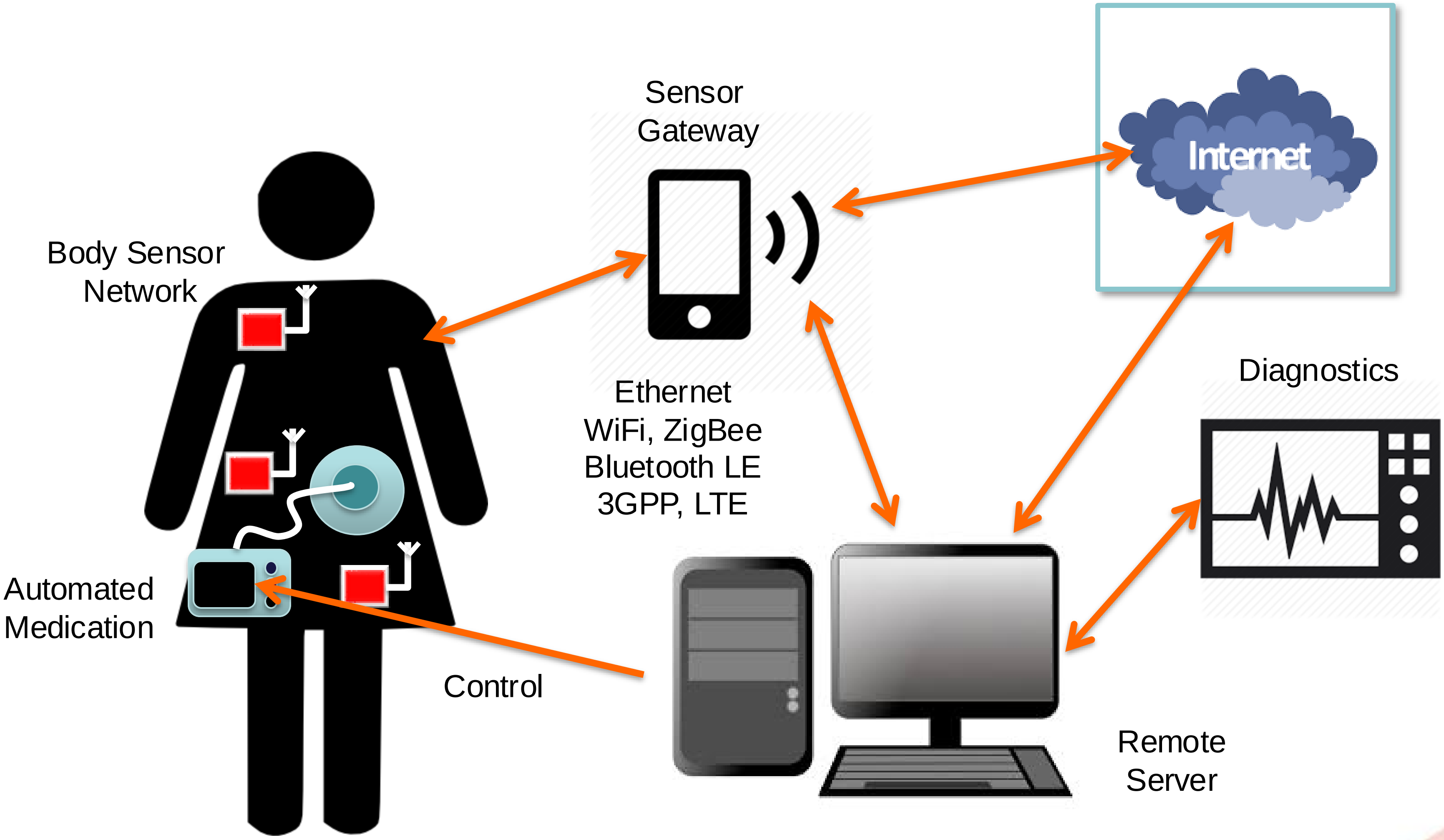
Water Monitoring

Water Leakage Detection

WAREHOUSE OPERATION

Tetley
SINCE 1837

CPS Example: Personalized Healthcare



Sensor Gateway

Body Sensor Network

Ethernet
WiFi, ZigBee
Bluetooth LE
3GPP, LTE

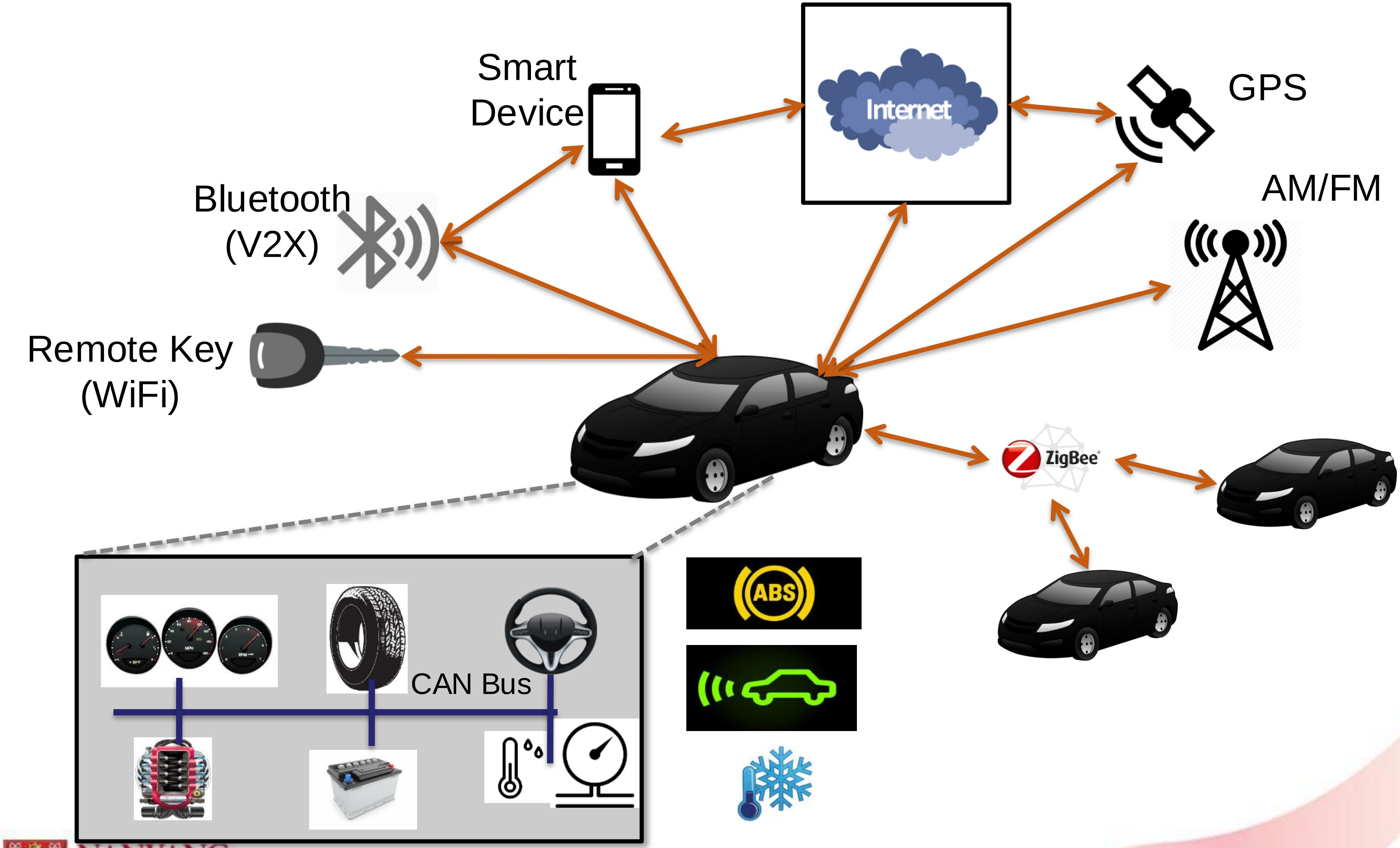
Diagnostics

Automated Medication

Control

Remote Server

CPS Example: Automotive



NANYANG TECHNOLOGICAL UNIVERSITY

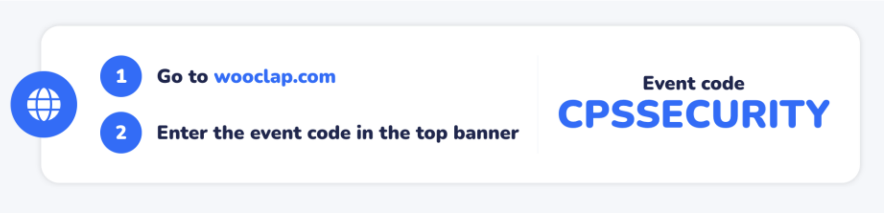
Contents

CPS/IoT: Again

- Security Issues
- Communication Security

- Smart Cards

- Discussion



1 Go to wooclap.com

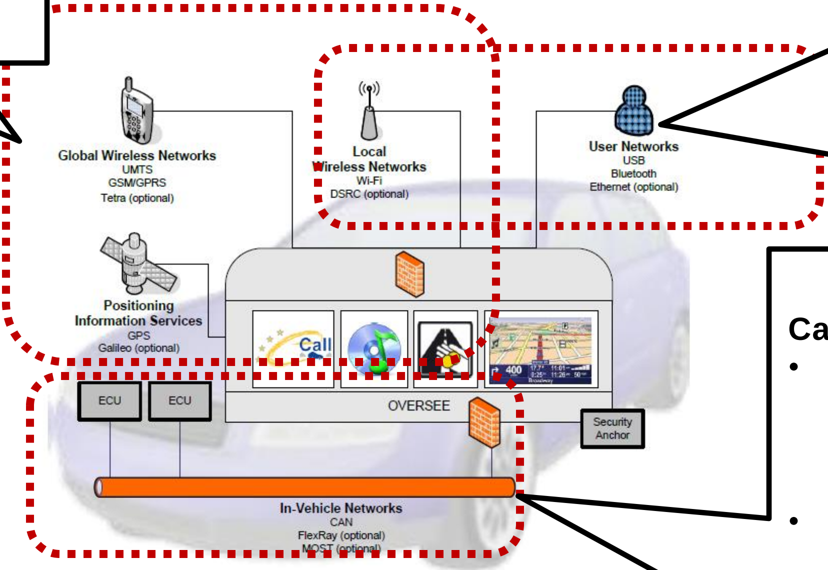
2 Enter the event code in the top banner

Event code

CPSSECURITY

CPS Security: Automotive

Car-to-Cloud
- Security, Privacy
- Identity management
  - public-key protocol
  - Authentication
- Real-time operations

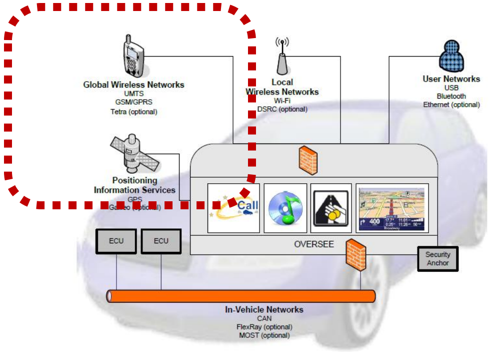


Car-to-X
- Security over Networks
  - Key pre-distribution
- Privacy
  - Untrusted Wireless network
- Information sharing
- Identity management
  - Meet-in-the-middle attack

Car Platform
- Security
  - Software stack
  - Storage
  - Network
- Electro-mechanical components
  - Novel attacks
  - Trojans
  - Sensors

Car-to-Cloud Security

- **AV critically depends on Remote Center for navigation, traffic update**

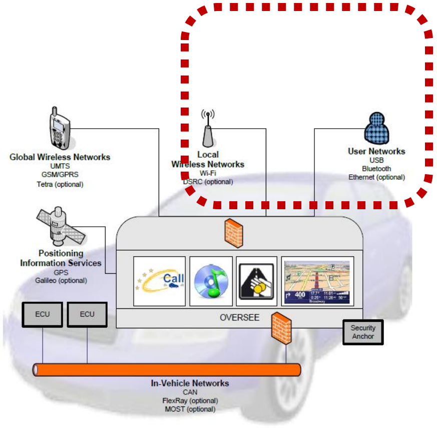


- 3rd Party Cloud service provider
  - Data privacy, integrity is vulnerable
  - GPS spoofing
  - Violation of real-time deadlines
  - Identity theft
  - DoS
- Often reduces problem complexity by offering car-to-car sharing
  - Malicious car

Car-to-X Security

- **AV shares information with cars, local user network, traffic system**

- Malicious AV/Traffic/User
  - Spoofing attack
  - Data Integrity violation
  - Network jamming
  - LIDAR blocking
  - Meet-in-the-middle



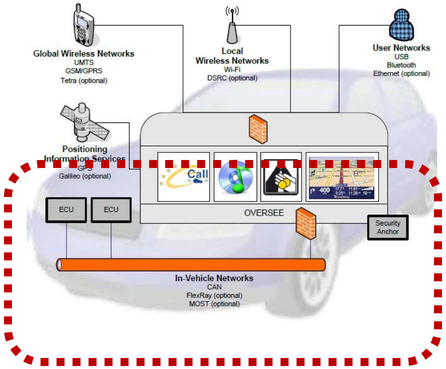
- To be addressed by public-key cryptosystem/distributed key-management techniques

Car Platform Security

- **AV is a complex electro-mechanical system**

- Remote as well as "*stealthy*" physical attacks possible
  - Protocol violation (*real-time deadlines*)
  - Passive/Active side-channel attacks
  - Replay attacks
  - Software virus
  - Hardware Trojan

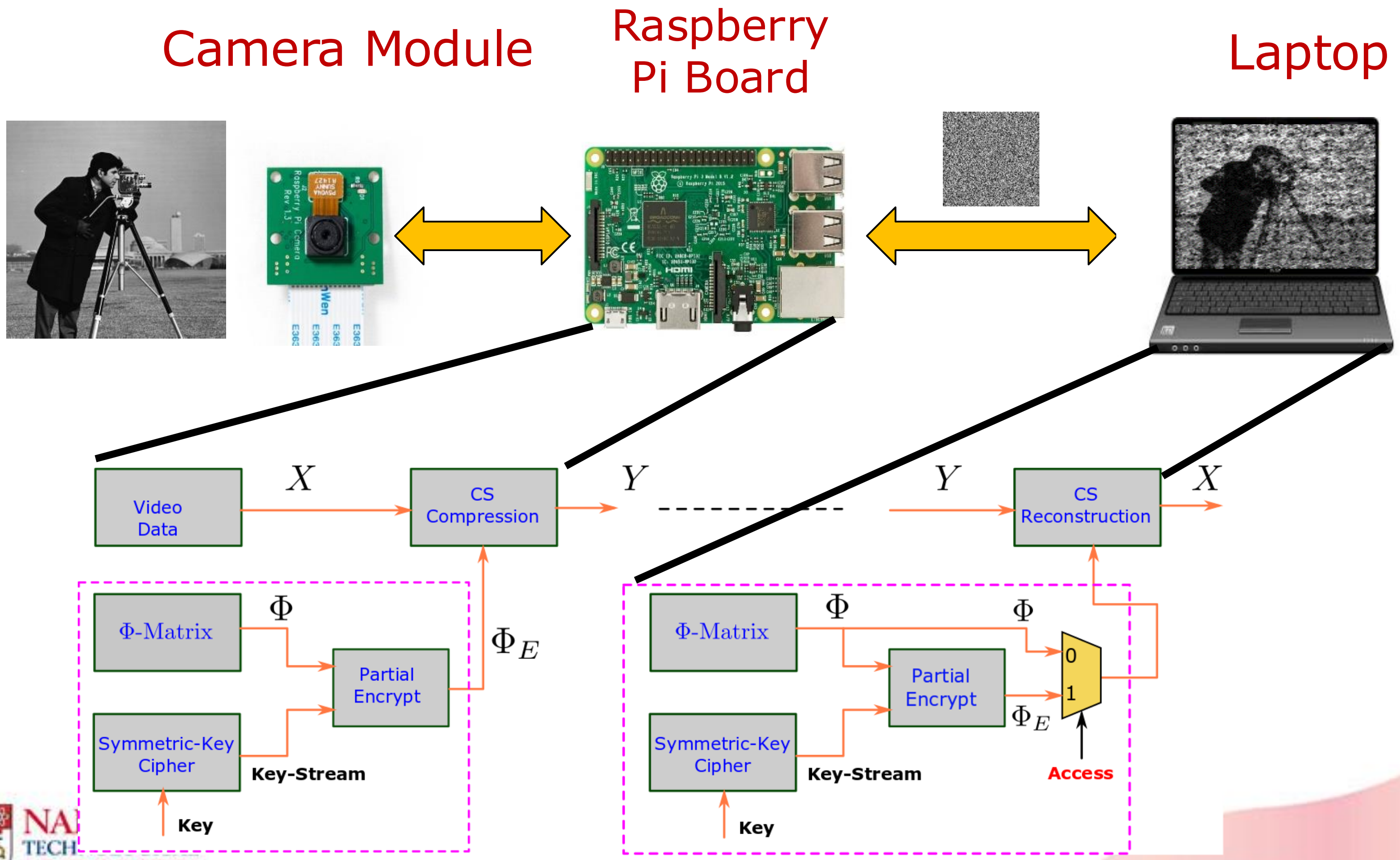
- To be addressed by techniques based on ***Root-of-Trust***



Privacy

- **Categories of *Individual Privacy***
  - **Internal**
    - Thoughts/Feelings, Bias, Preferences
  - **External**
    - Financial, Career, Medical, Ethnicity, Biographical
  - **Territorial**
    - Tracking, Daily habits, Location visits
  - **Social**
    - Communication, Family, Friends, Information Dissemination

Privacy through Lossy Compression



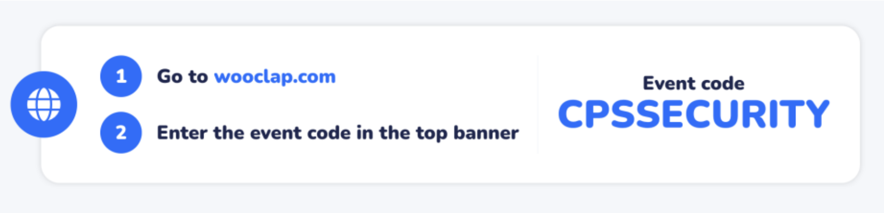
Contents

CPS/IoT: Again

  - Security Issues
  - Communication Security

- Smart Cards

- Discussion



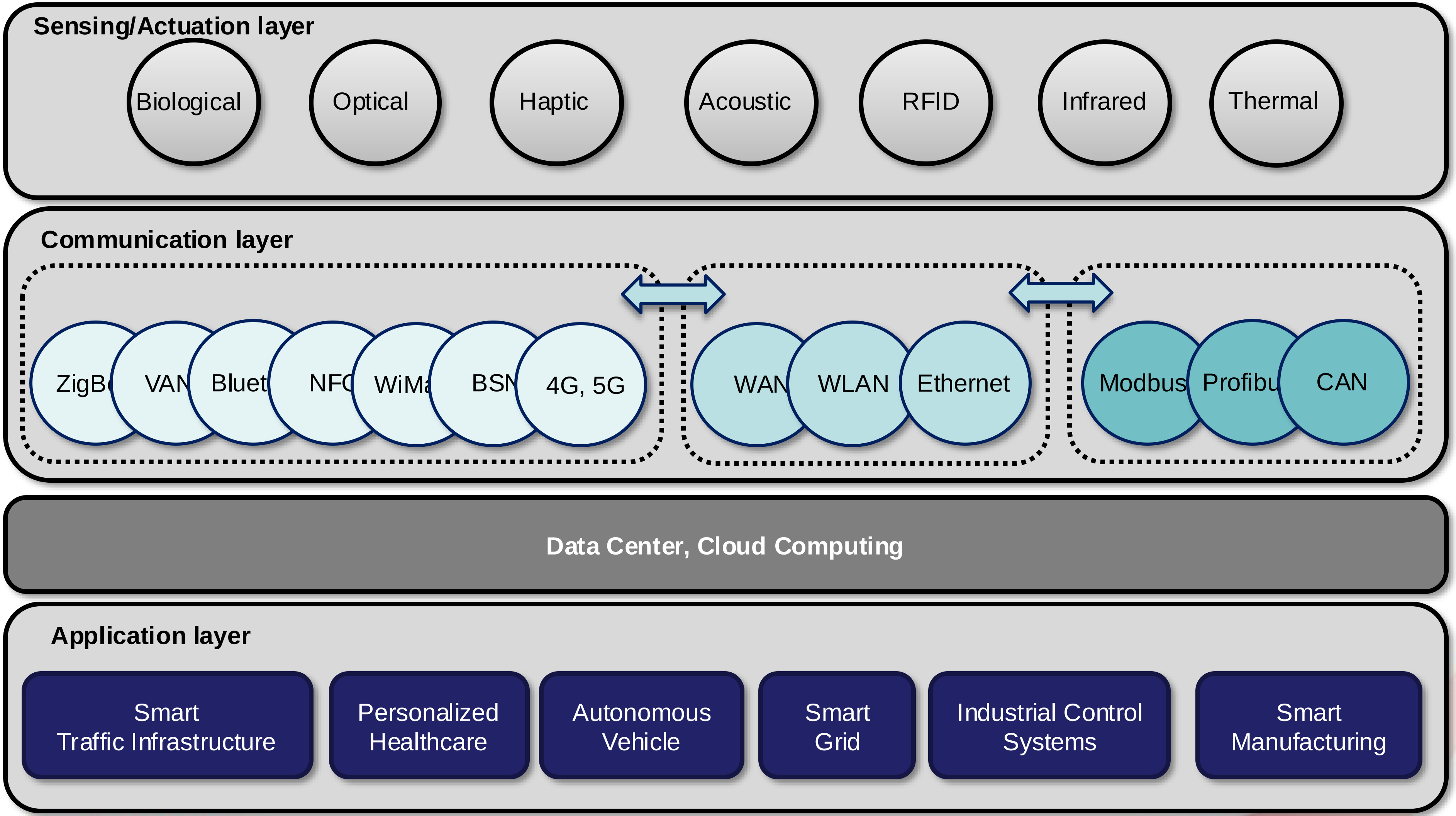
1 Go to wooclap.com

2 Enter the event code in the top banner

Event code

CPSSECURITY

CPS/IoT Layers



Sensing/Actuation layer

Biological

Optical

Haptic

Acoustic

RFID

Infrared

Thermal

Communication layer

ZigB

VAN

Bluet

NFC

WiMa

BSN

4G, 5G

WAN

WLAN

Ethernet

Modbus

Profibu

CAN

Data Center, Cloud Computing

Application layer

Smart Traffic Infrastructure

Personalized Healthcare

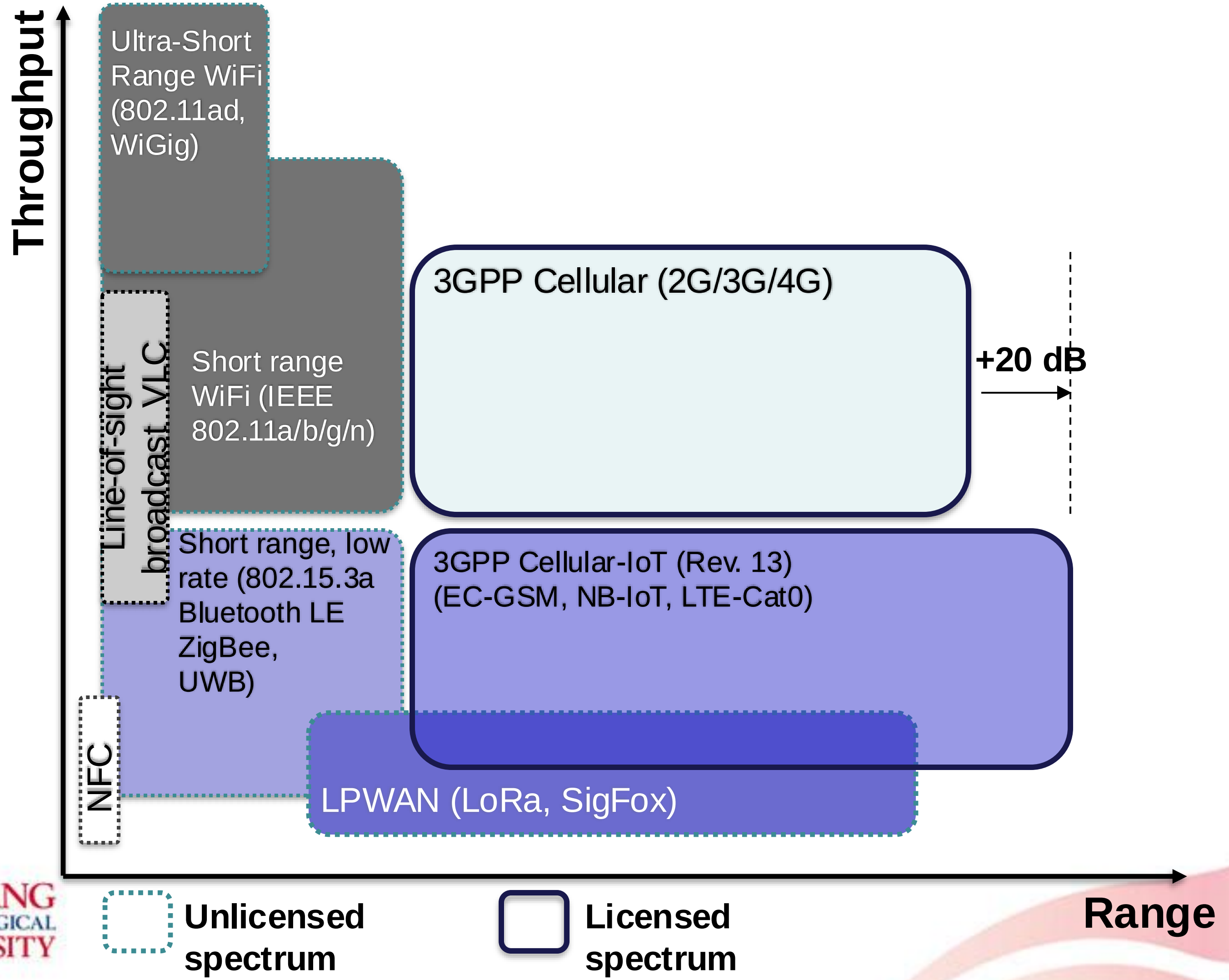
Autonomous Vehicle

Smart Grid

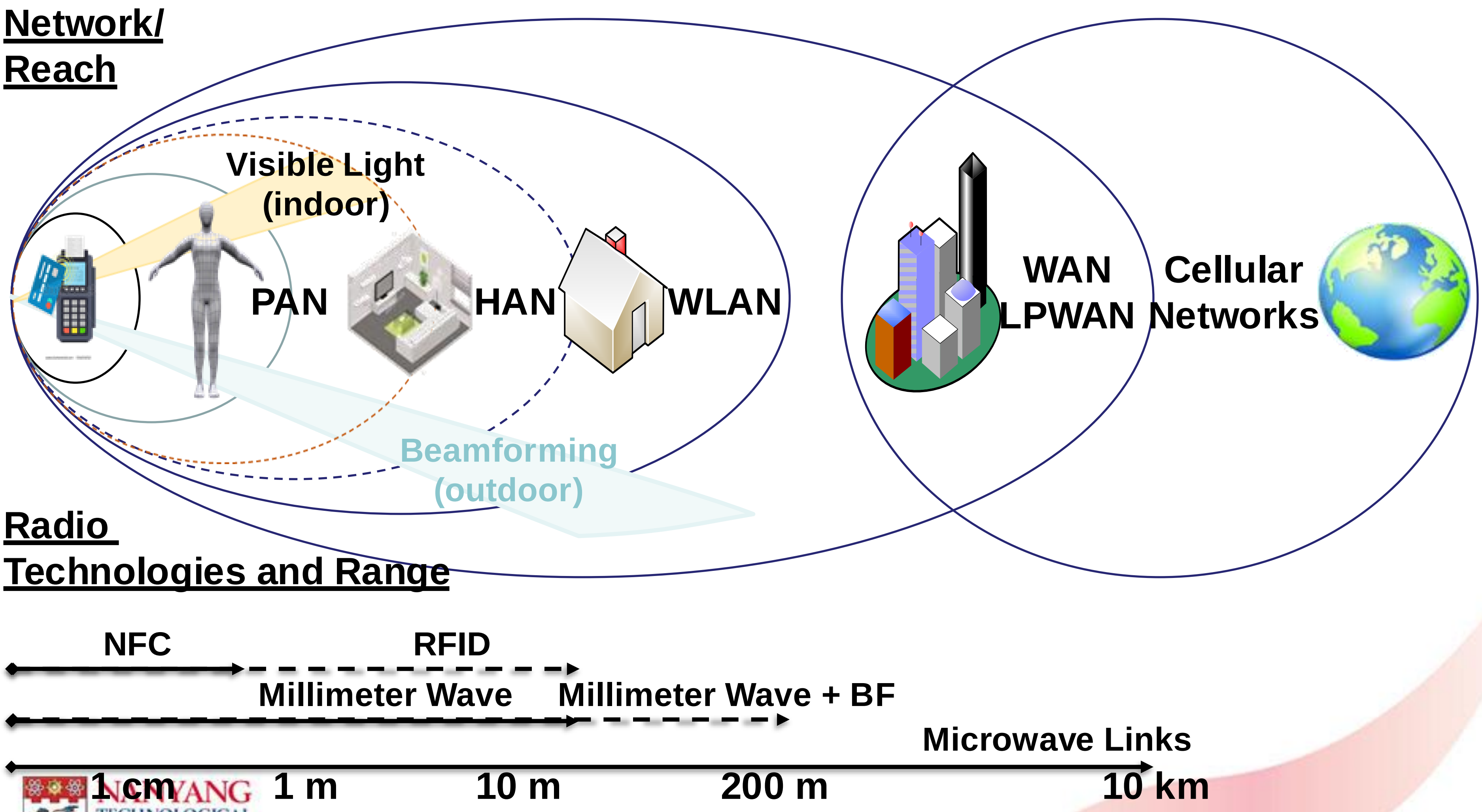
Industrial Control Systems

Smart Manufacturing

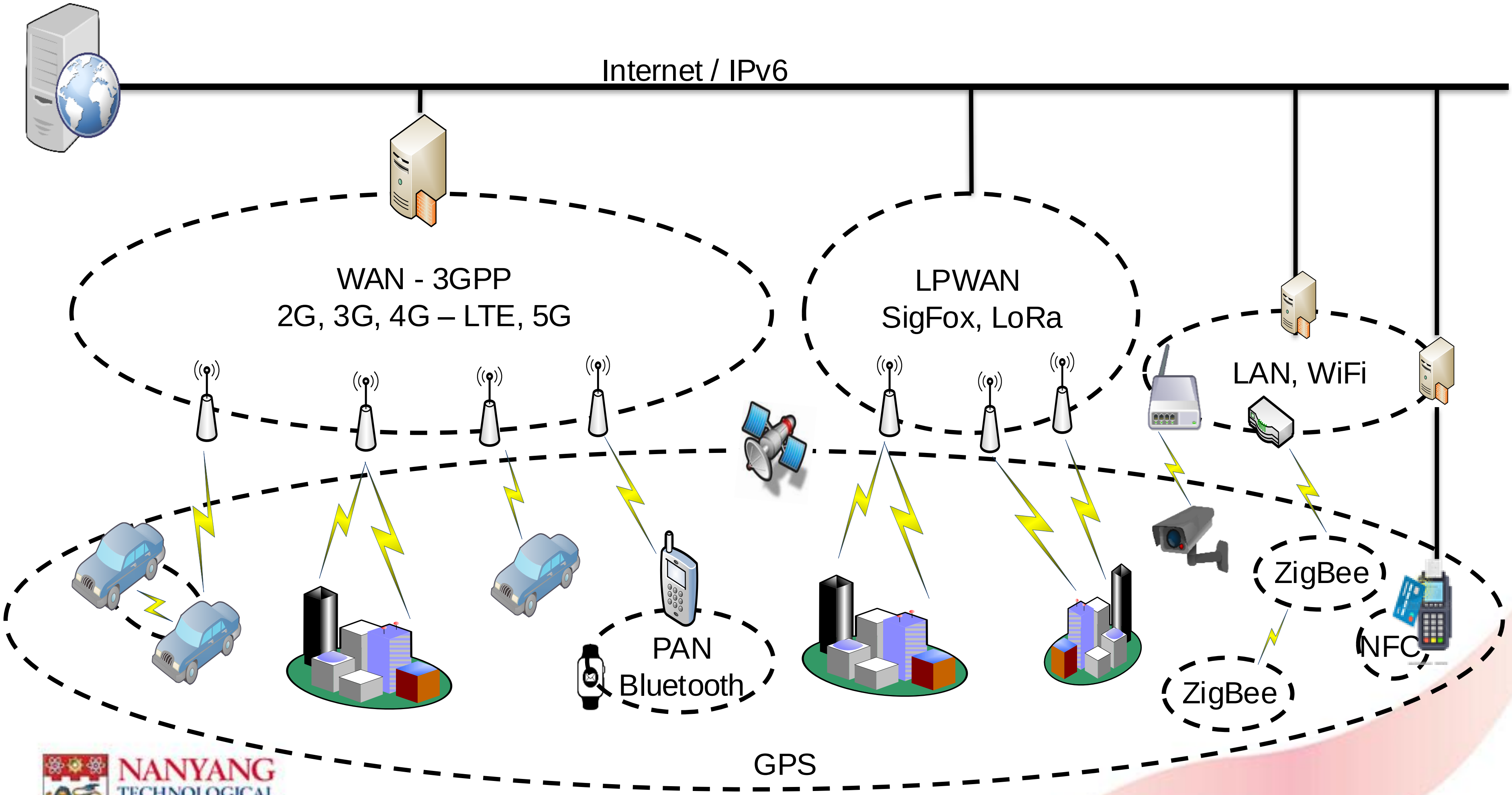
CPS/IoT: Spectrum Distribution


Throughput
Ultra-Short Range WiFi (802.11ad, WiGig)
Short range WiFi (IEEE 802.11a/b/g/n)
Line-of-sight broadcast VLC
3GPP Cellular (2G/3G/4G)
+20 dB
Short range, low rate (802.15.3a Bluetooth LE ZigBee, UWB)
3GPP Cellular-IoT (Rev. 13) (EC-GSM, NB-IoT, LTE-Cat0)
NFC
LPWAN (LoRa, SigFox)
Range
Unlicensed spectrum
Licensed spectrum

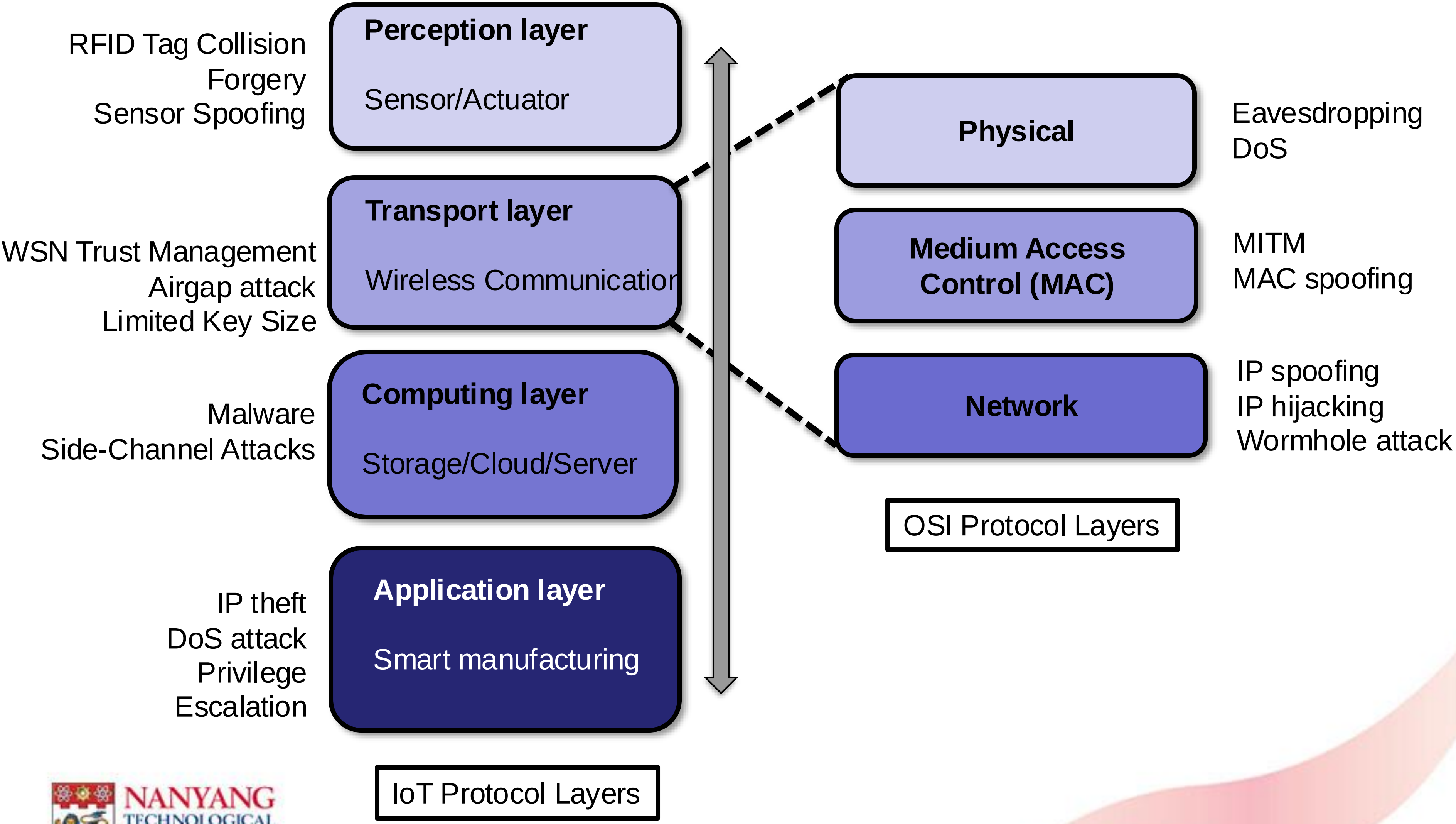
CPS/IoT: Across Standards



CPS/IoT: Heterogeneous Network



Attack Scopes across Layers



RFID Tag Collision
Forgery
Sensor Spoofing

Perception layer

Sensor/Actuator

WSN Trust Management
Airgap attack
Limited Key Size

Transport layer

Wireless Communication

Malware
Side-Channel Attacks

Computing layer

Storage/Cloud/Server

IP theft
DoS attack
Privilege Escalation

Application layer

Smart manufacturing

IoT Protocol Layers

Physical

Eavesdropping
DoS

Medium Access Control (MAC)

MITM
MAC spoofing

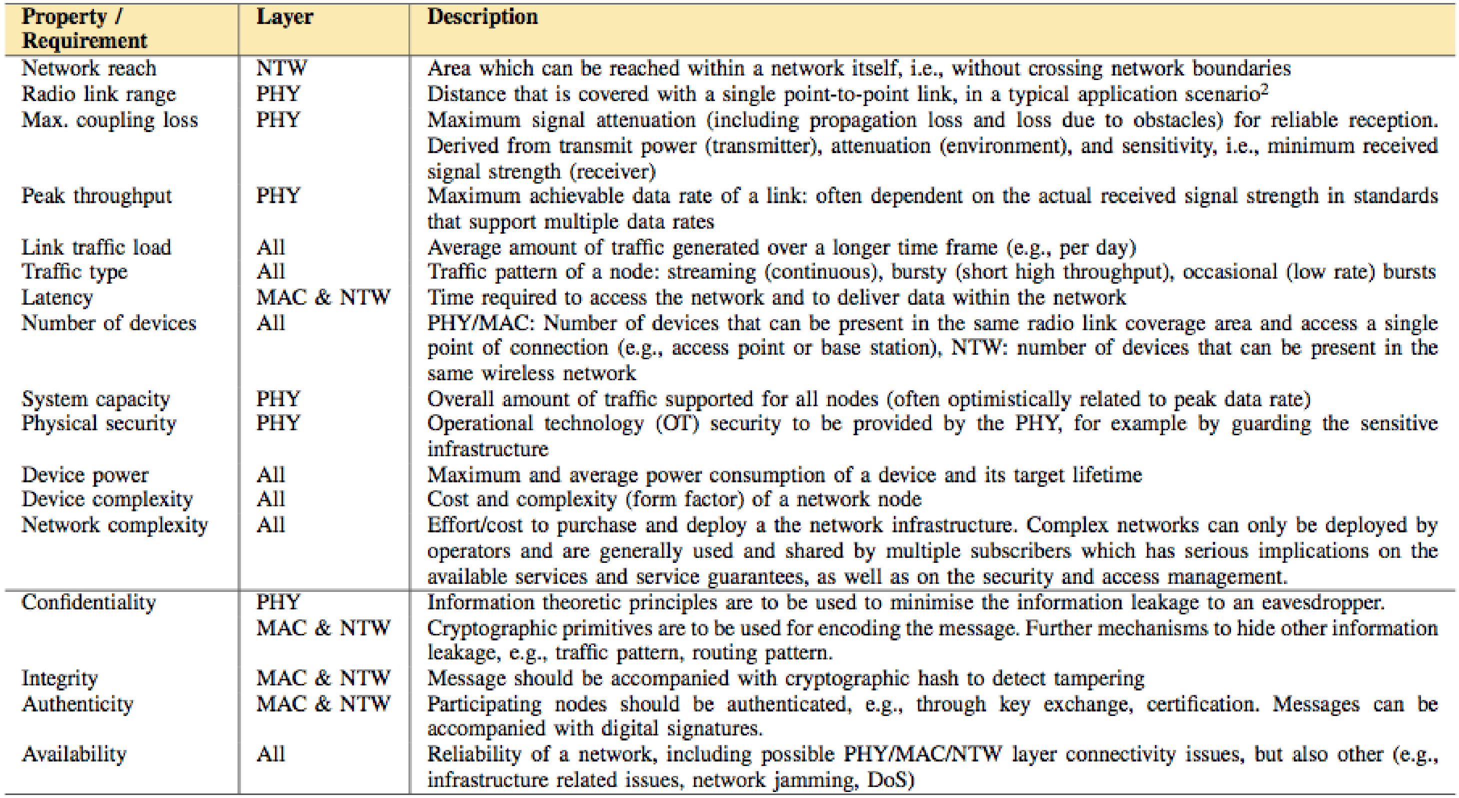
Network

IP spoofing
IP hijacking
Wormhole attack

OSI Protocol Layers

NANYANG TECHNOLOGICAL UNIVERSITY

Requirements for Wireless Communication in CPS

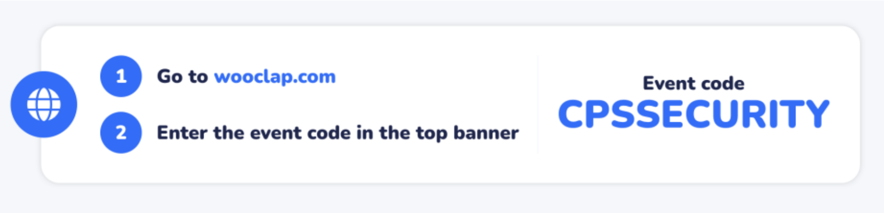


Property / Requirement	Layer	Description
Network reach	NTW	Area which can be reached within a network itself, i.e., without crossing network boundaries
Radio link range	PHY	Distance that is covered with a single point-to-point link, in a typical application scenario[2]
Max. coupling loss	PHY	Maximum signal attenuation (including propagation loss and loss due to obstacles) for reliable reception. Derived from transmit power (transmitter), attenuation (environment), and sensitivity, i.e., minimum received signal strength (receiver)
Peak throughput	PHY	Maximum achievable data rate of a link: often dependent on the actual received signal strength in standards that support multiple data rates
Link traffic load	All	Average amount of traffic generated over a longer time frame (e.g., per day)
Traffic type	All	Traffic pattern of a node: streaming (continuous), bursty (short high throughput), occasional (low rate) bursts
Latency	MAC & NTW	Time required to access the network and to deliver data within the network
Number of devices	All	PHY/MAC: Number of devices that can be present in the same radio link coverage area and access a single point of connection (e.g., access point or base station), NTW: number of devices that can be present in the same wireless network
System capacity	PHY	Overall amount of traffic supported for all nodes (often optimistically related to peak data rate)
Physical security	PHY	Operational technology (OT) security to be provided by the PHY, for example by guarding the sensitive infrastructure
Device power	All	Maximum and average power consumption of a device and its target lifetime
Device complexity	All	Cost and complexity (form factor) of a network node
Network complexity	All	Effort/cost to purchase and deploy a the network infrastructure. Complex networks can only be deployed by operators and are generally used and shared by multiple subscribers which has serious implications on the available services and service guarantees, as well as on the security and access management.
Confidentiality	PHY	Information theoretic principles are to be used to minimise the information leakage to an eavesdropper.
	MAC & NTW	Cryptographic primitives are to be used for encoding the message. Further mechanisms to hide other information leakage, e.g., traffic pattern, routing pattern.
Integrity	MAC & NTW	Message should be accompanied with cryptographic hash to detect tampering
Authenticity	MAC & NTW	Participating nodes should be authenticated, e.g., through key exchange, certification. Messages can be accompanied with digital signatures.
Availability	All	Reliability of a network, including possible PHY/MAC/NTW layer connectivity issues, but also other (e.g., infrastructure related issues, network jamming, DoS)

A. Burg, A. Chattopadhyay and K.-Y. Lam, "Wireless Communication and Security Issues for Cyber–Physical Systems and the Internet-of-Things", Proceedings of IEEE, 2018

Contents

- CPS/IoT: Again
- *Smart Cards*
- Discussion



1 Go to wooclap.com

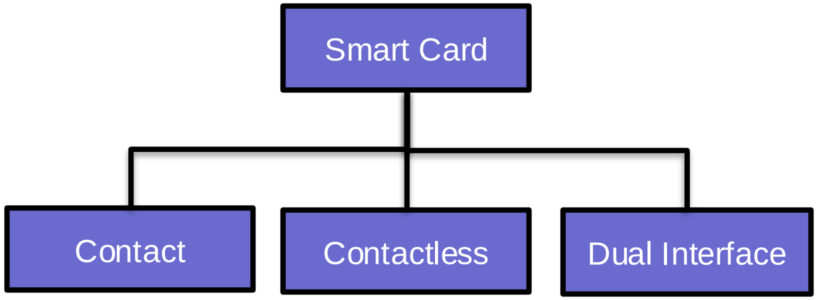
2 Enter the event code in the top banner

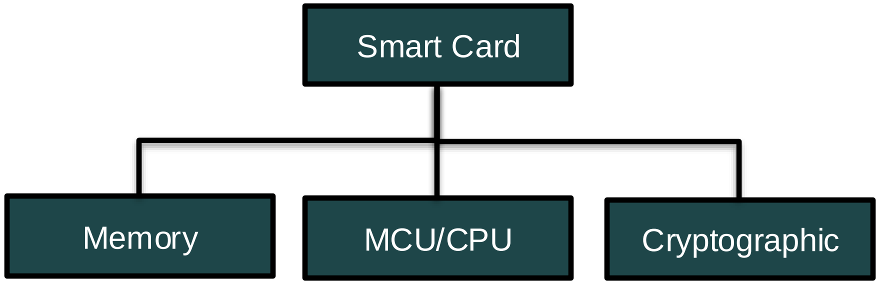
Event code

CPSSECURITY

NANYANG TECHNOLOGICAL UNIVERSITY

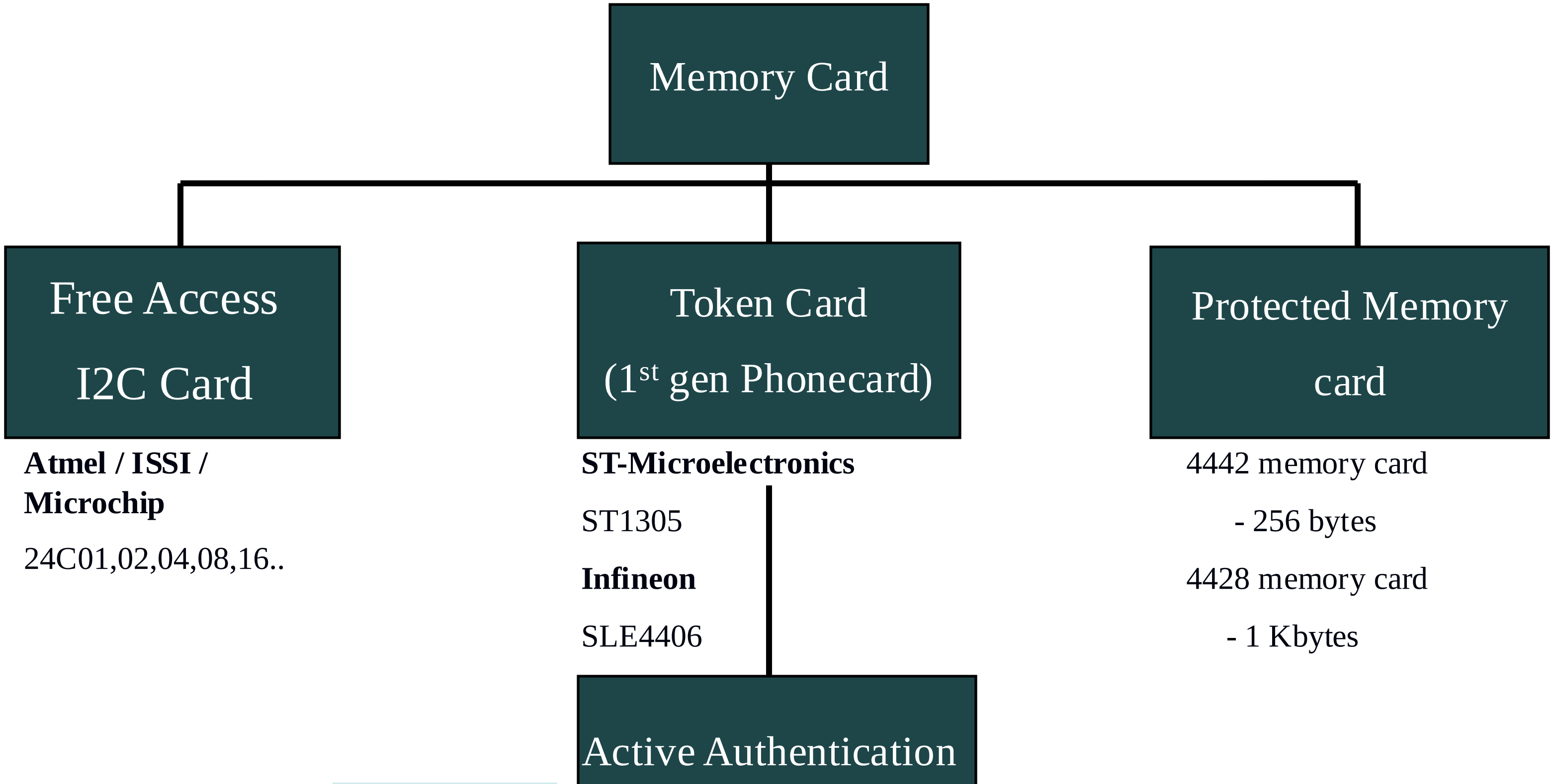
Smart Card / IC Card Family





- Contact **Memory** Card
  - Infineon & compatibles
- Contact **CPU** Card
  - GSM SIM, Smart Debit/Credit EMV Card
  - national smart card (banking / ID card)
- Dual Interface Card

Types Of Contact Memory Card



Memory Card

Free Access

I2C Card

Atmel / ISSI / Microchip

24C01,02,04,08,16..

Token Card

(1st gen Phonecard)

ST-Microelectronics

ST1305

Infineon

SLE4406

Protected Memory card

4442 memory card

- 256 bytes

4428 memory card

- 1 Kbytes

Active Authentication Token Card

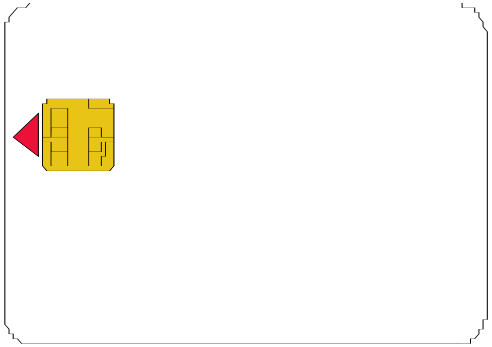
ST-Microelectronics

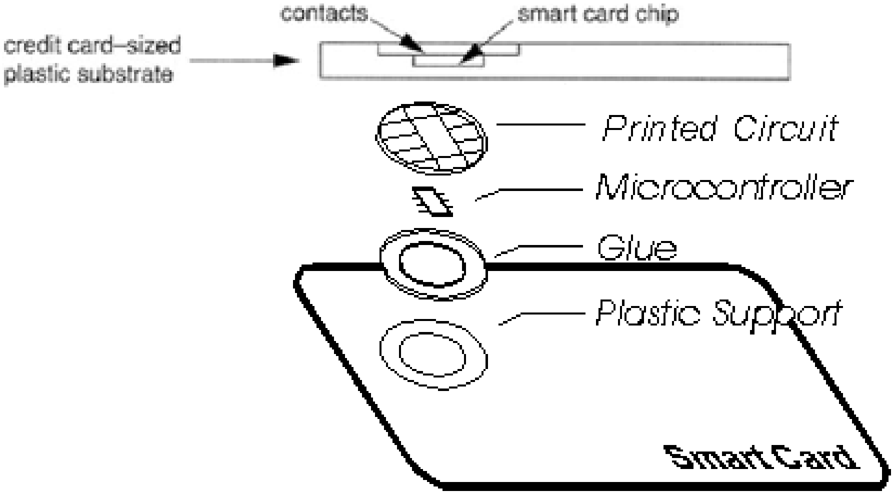
ST1333,ST1335

Infineon

SLE4436,SLE5536

What Is A Contact Smart Card



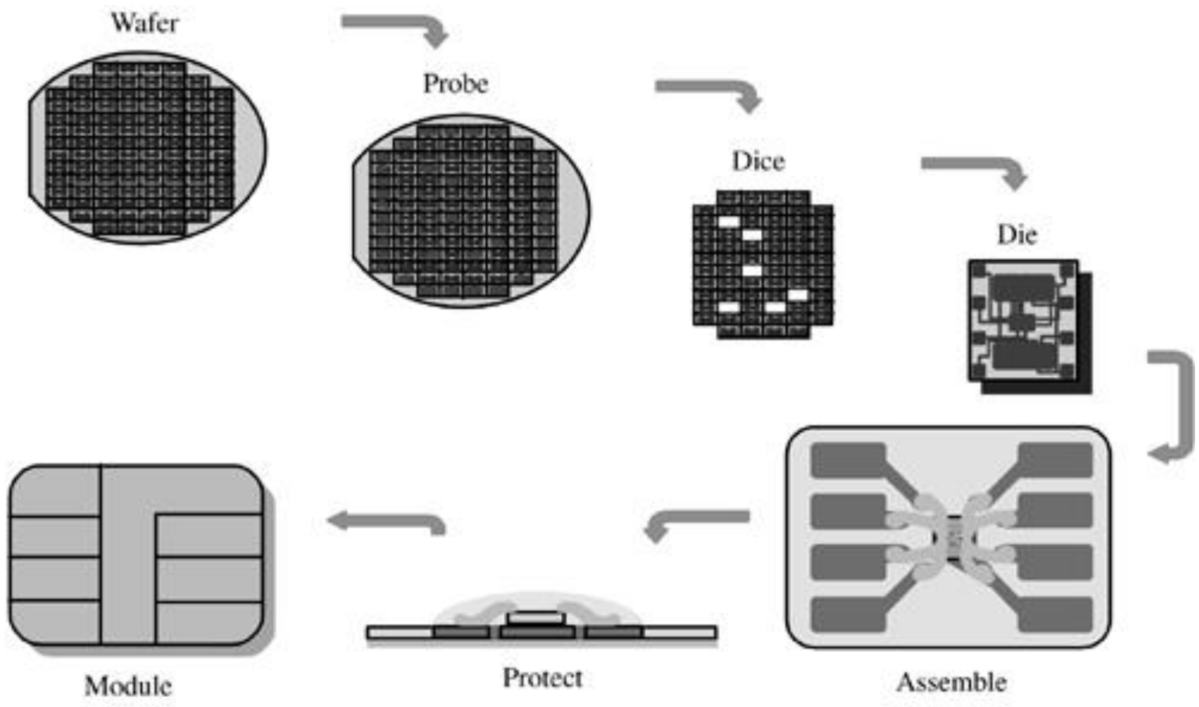


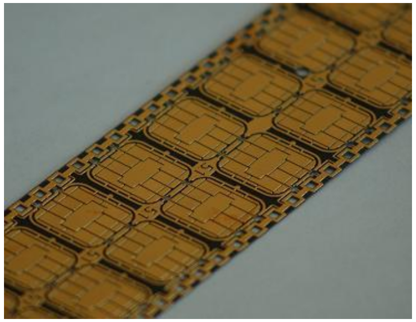
- a credit card size (ID-1) plastic with a single IC chip on board and conforms with ISO-7816
- a smart card comprises of 3 parts
  - contact disc
  - chip
  - plastic body with cavity

Contact Disc

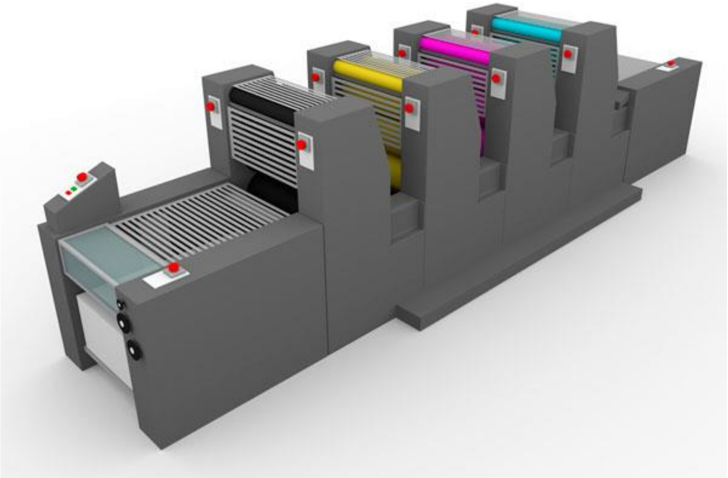
- Contact disc with the chip is called a micro-module
- 6 or 8 contacts – cost difference of fraction of a cent
- Contact position complies with ISO-7816-2
- *Visually* cannot tell the type of cards from the contact disc
  - Answer-To-Reset says that it is a CPU card

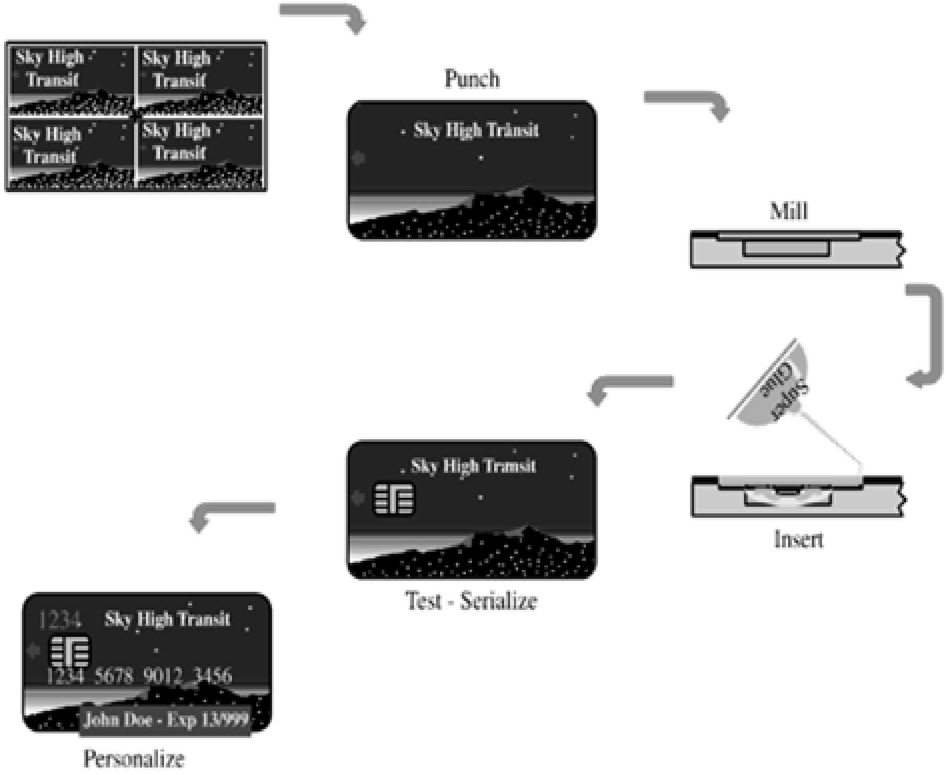
Micro-Module Manufacturing





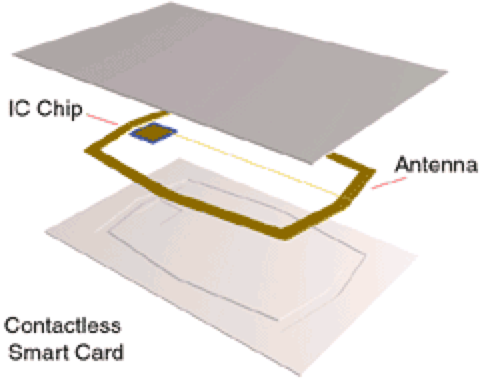
Card Manufacturing





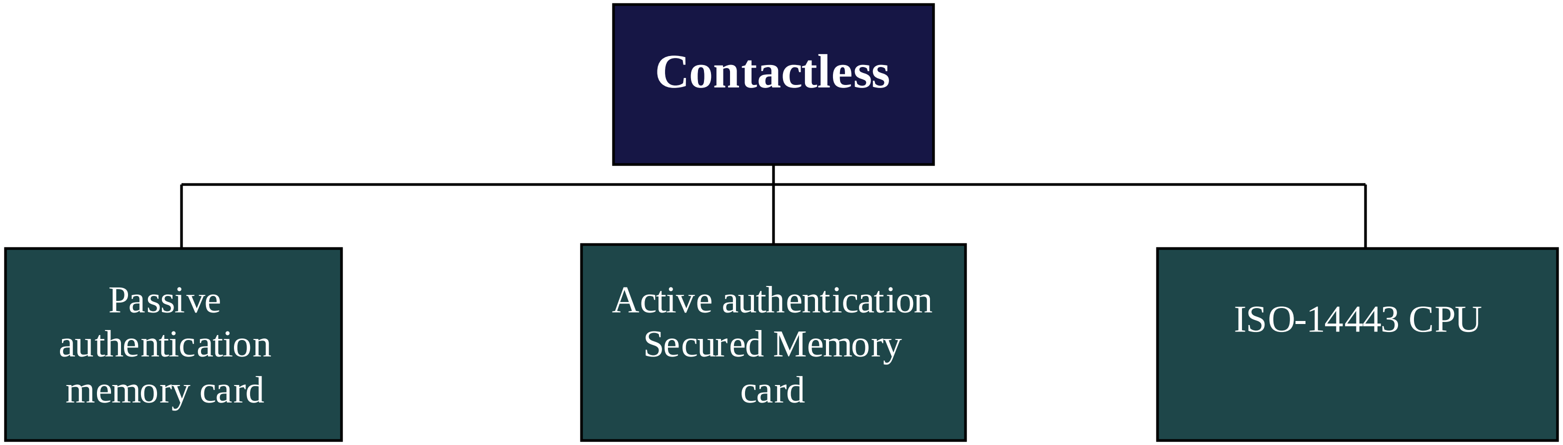
What Is A Contactless Smart Card

- Smart card → credit card size card with memory capable of self protection
- If other form factor, referred to as a RF Tag
- Various standards ISO-14443, ISO-15693, ISO-18000-6C (EPC), NFC



NANYANG TECHNOLOGICAL UNIVERSITY

Types Of Contactless Cards



Contactless

Passive authentication memory card

Active authentication Secured Memory card

ISO-14443 CPU

e.g.

NFC tags from ST-Micro, NXP, Infineon;

Single Trip Ticket (recyclable)

e.g.

Mifare, Mifare compatible

Mifare Ultralight C

e.g.

DESFire,

PBOC 2.0 & 3.0

CEPAS

Paypass, Paywave EMV

ICAO passport

Smart Card Acceptors

Card Acceptor

Card Acceptor Contacts

Plug-In Card Acceptor

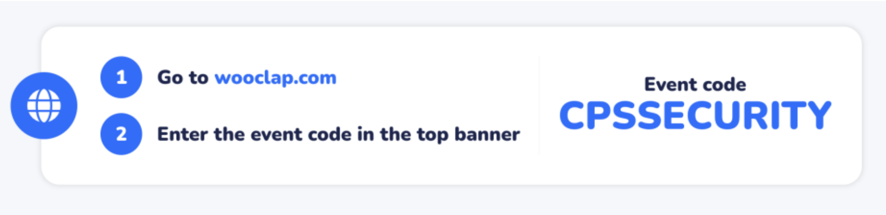
ISO 14443-1 – Physical Characteristics

This standard defines

- Card dimensions (refer to ISO 7810 for ID-1 cards)
- Surface quality for printing
- Mechanical resistance
- UV and X-ray resistance
- Sensitivity to surrounding magnetic fields

Contents

- CPS/IoT: Again
- *Smart Cards*
  - Chip Security
  - Plastic Card Security
  - Communication Security
- Discussion

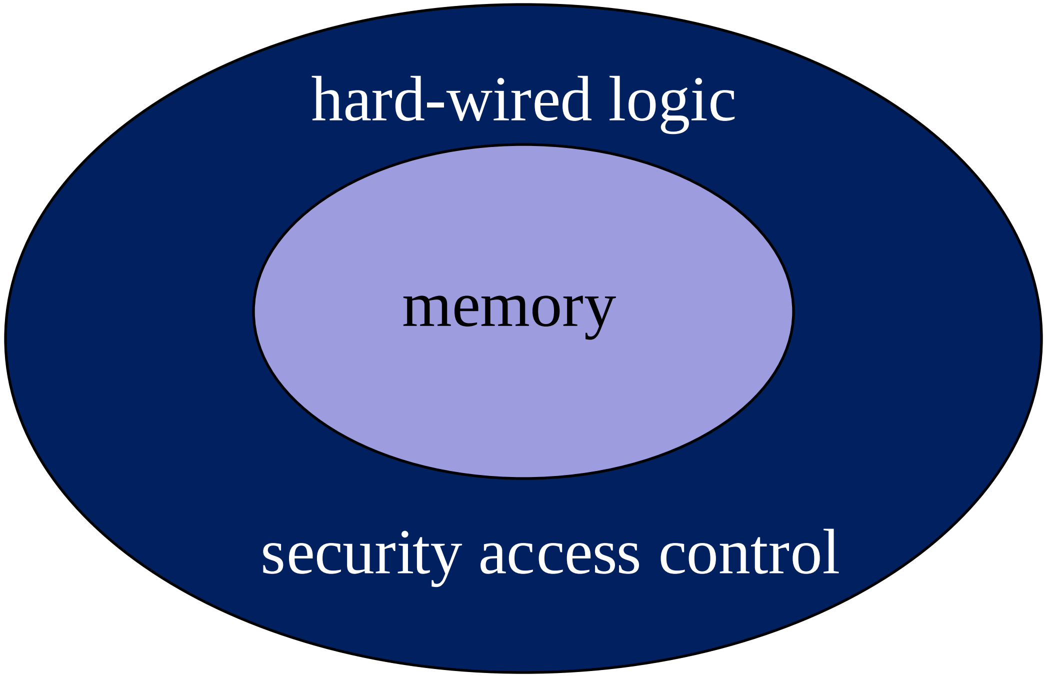


1 Go to wooclap.com

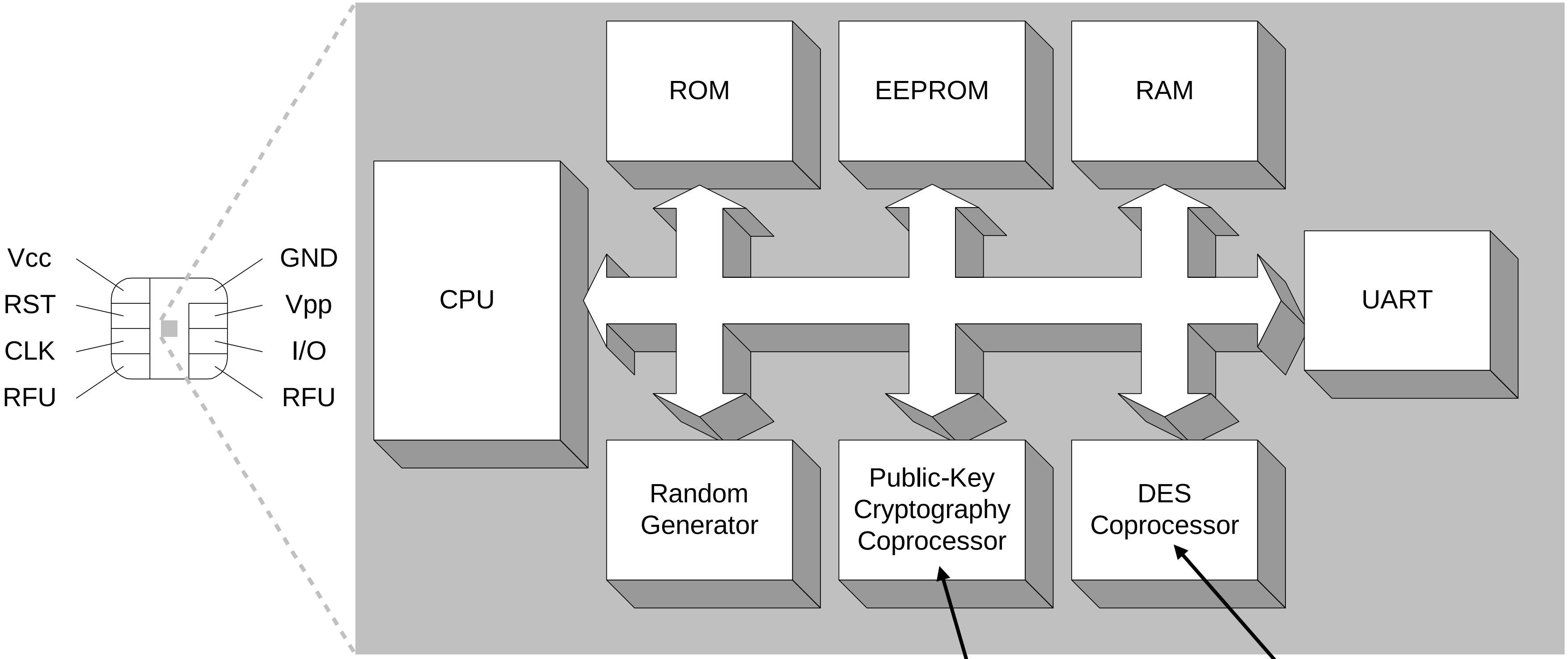
2 Enter the event code in the top banner

Event code
CPSSECURITY

Memory Card Security Architecture



CPU Card Architecture



DES *replaced by* AES

(arriving!) Post-Quantum Cryptography

Chip Security

- Goals of attack
  - Extract or clone sensitive data (codes, cryptographic keys)
  - Tamper with s/w execution, bypass security mechanism, modify data

- Typical Security Features of smart card chip
  - Chip hardware
  - Chip OS

- Essential that the application system security design fully exploits the security features and patch up any security limitations and weaknesses, if any

Physical Attacks, Countermeasures

- Physical or invasive attack methods
  - Chip modification, signal probing, memory content or secret retrieval
  - Fault injection – power supply disturbance, clock frequency, temperature, light, laser

- Physical / invasive attack countermeasures
  - Security sensors – voltage, frequency, passivation layer, power supply glitch sensors
  - Memory scrambling, memory encryption, bus encryption, glue logic layout, dynamic shield covering entire die surface, EEPROM 2 page destroy mechanism
  - RAM integrity check, EEPROM double READ, Code integrity check for critical routine

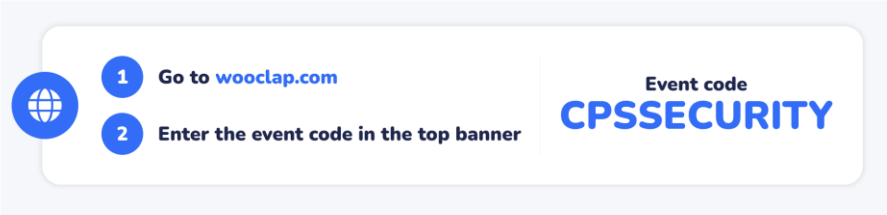
Side Channel Attacks, Countermeasures

- Taking advantage of side channel information that leaks secret
  - Timing attack, power consumption, magnetic, electrical analysis

- Countermeasures against side-channel attack
  - Hardware internal jittered clock mode to add random delays
  - Software adding random dummy clocks
  - Scrambling, Encryption

Contents

- CPS/IoT: Again
- *Smart Cards*
  - Chip Security
  - Plastic Card Security
  - Communication Security
- Discussion



1 Go to wooclap.com

2 Enter the event code in the top banner

Event code
CPSSECURITY

NANYANG TECHNOLOGICAL UNIVERSITY

Secure Printing

Main Goal of Secure/Security Printing

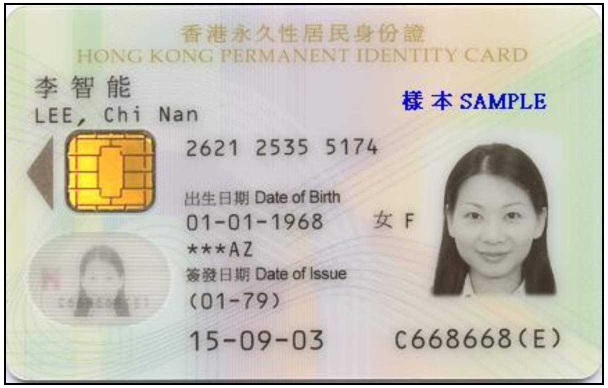
Prevent forgery or counterfeiting

Typical Application

National ID cards, passport, banking card

Typical Examples

- UV Printing
- Microtext
- Multiple laser image (MLI)
- Watermark
- Hologram



香港永久性居民身份證
HONG KONG PERMANENT IDENTITY CARD

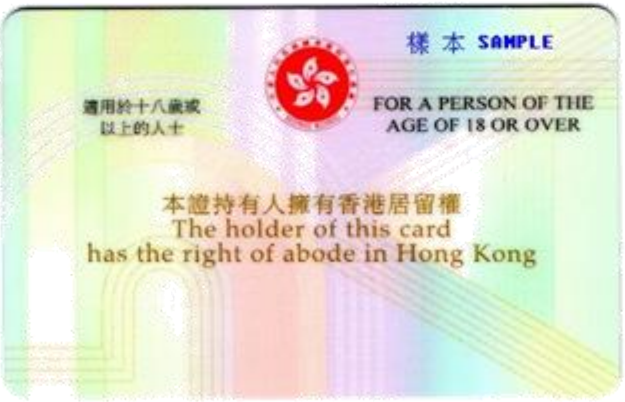
李 智 能
LEE, Chi Nan

樣 本 SAMPLE

2621 2535 5174

出生日期 Date of Birth
01-01-1968 女 F
***AZ

簽發日期 Date of Issue
(01-79)
15-09-03 C668668(E)



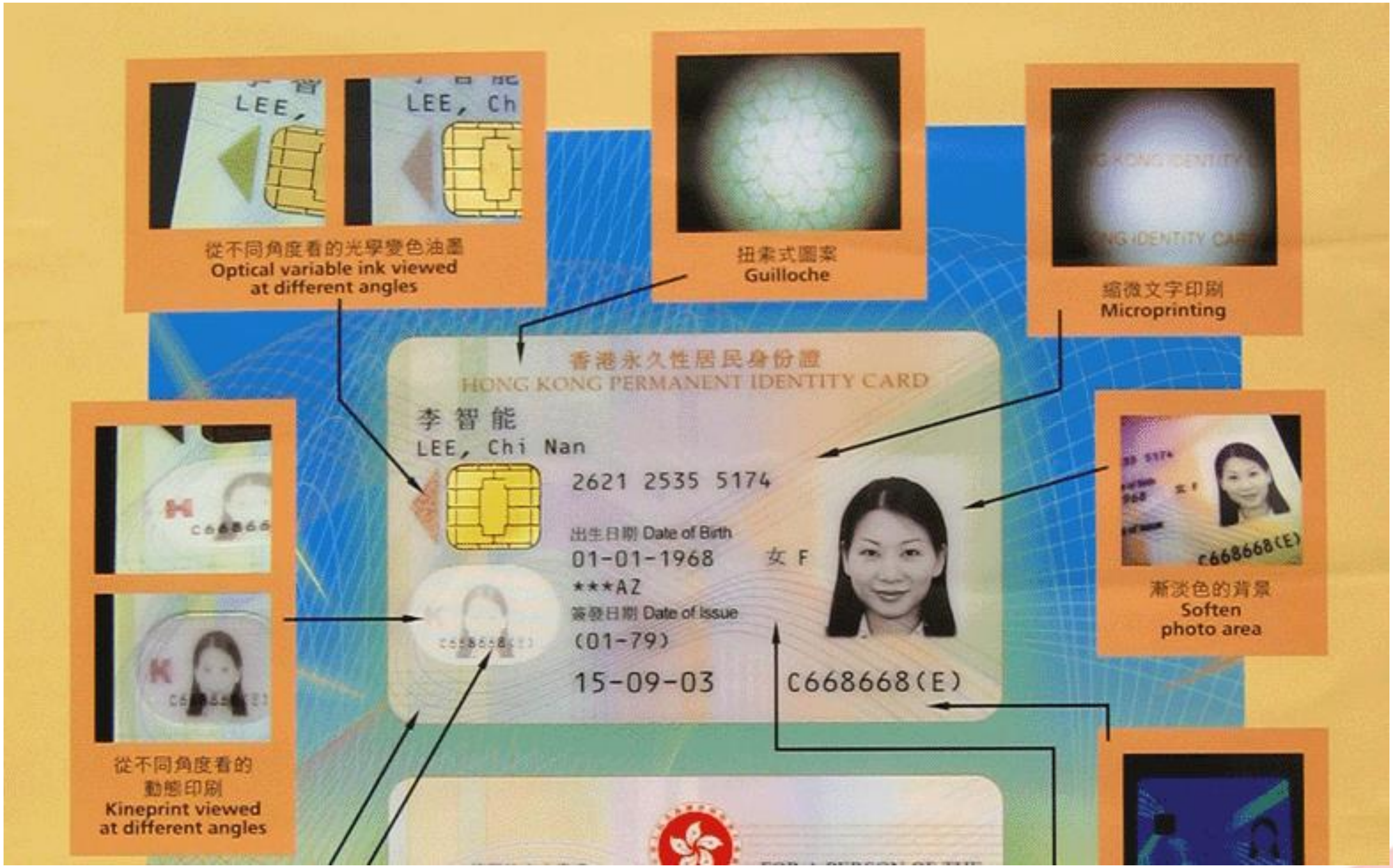
樣 本 SAMPLE

適用於十八歲或
以上的人士

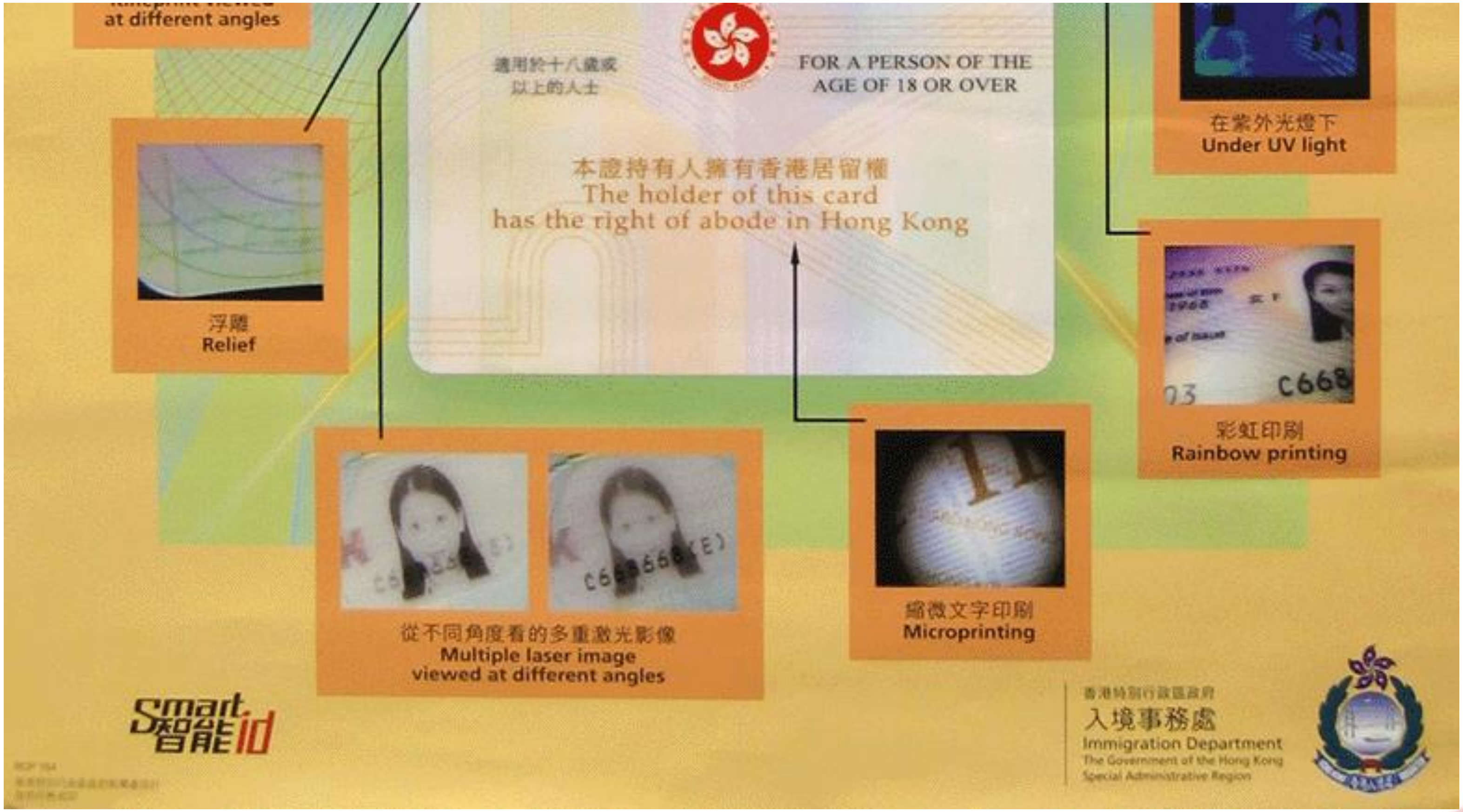
FOR A PERSON OF THE
AGE OF 18 OR OVER

本證持有人擁有香港居留權
The holder of this card
has the right of abode in Hong Kong

Secure Printing

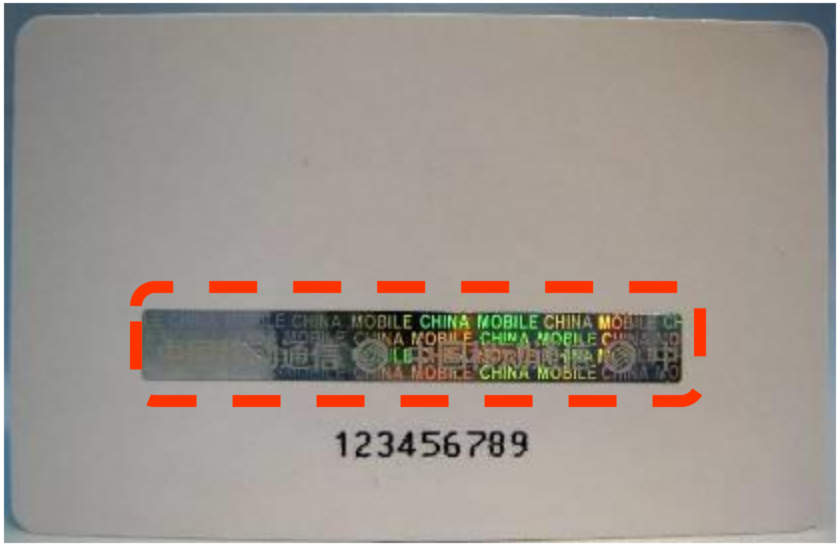


Secure Printing

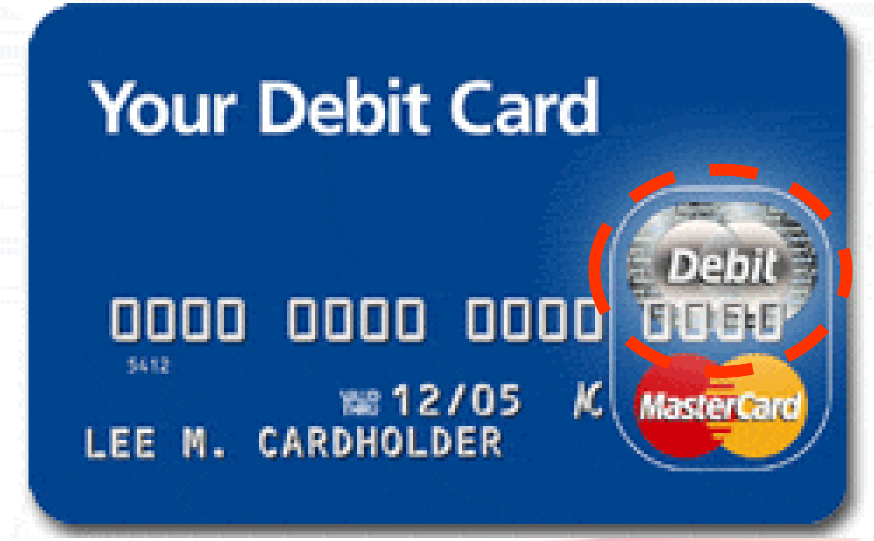


(Source: HK Immigration Department)

Secure Printing – *more examples*



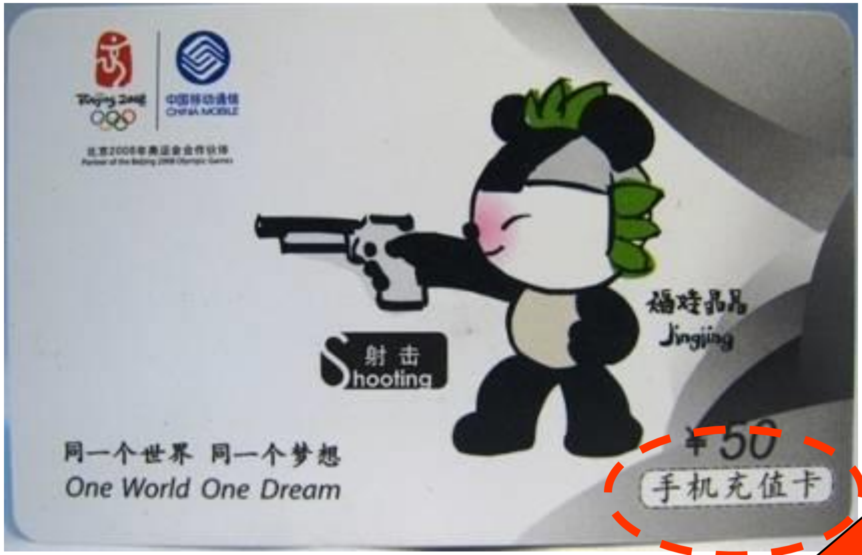
<u>HOLOGRAM</u>



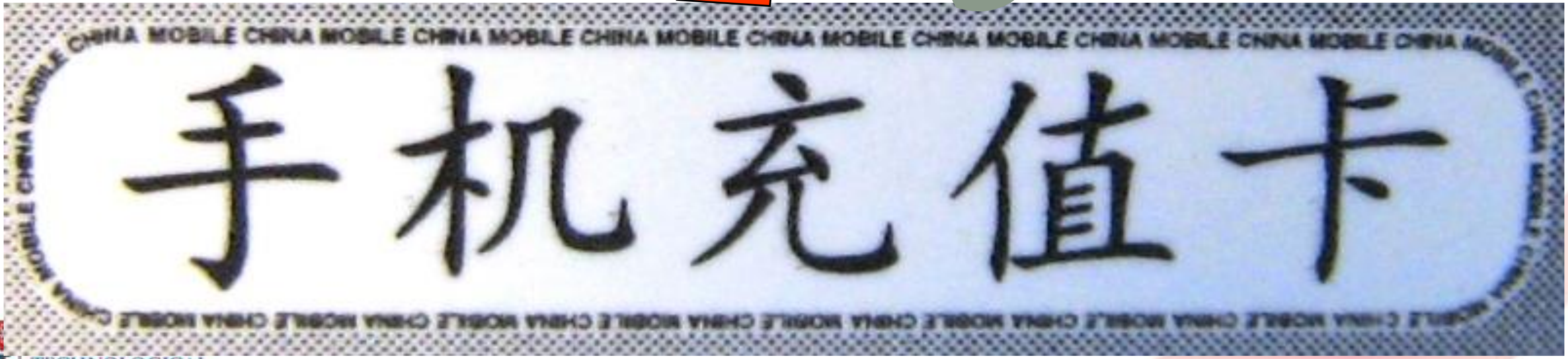
<u>More about hologram</u>

Setup charge for molding may cost US $2,000!

Secure Printing – *more examples*

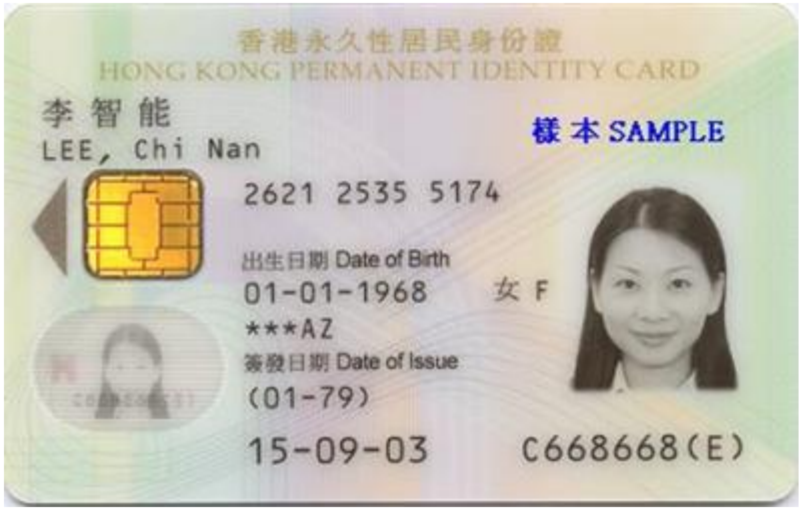


Microtext


手机充值卡
CHINA MOBILE CHINA MOBILE CHINA MOBILE CHINA MOBILE CHINA MOBILE CHINA MOBILE CHINA MOBILE CHINA MOBILE CHINA

Secure Printing – *more examples*

UV Printing



香港永久性居民身份證
HONG KONG PERMANENT IDENTITY CARD

李智能
LEE, Chi Nan

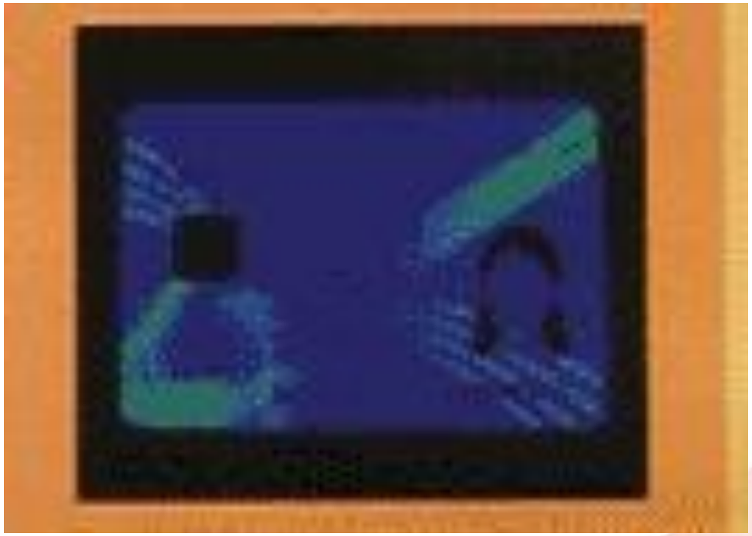
樣本 SAMPLE

2621 2535 5174

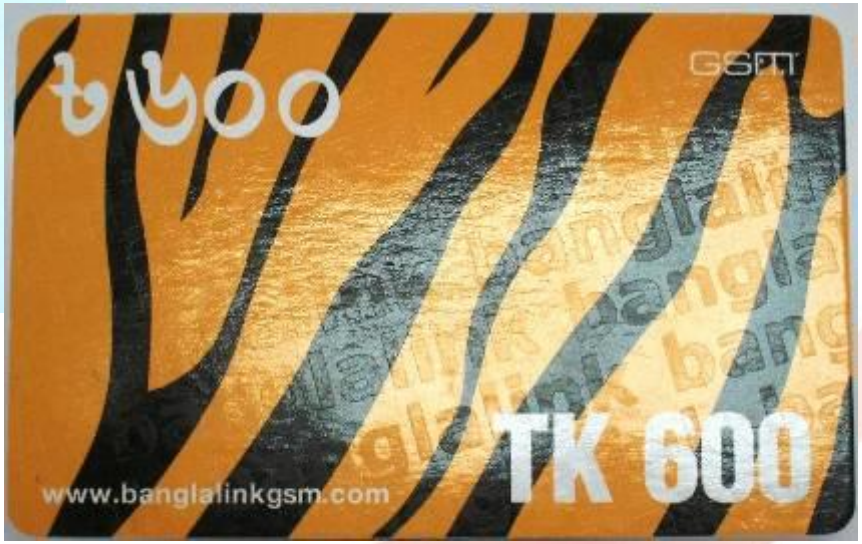
出生日期 Date of Birth
01-01-1968　女 F
***AZ

簽發日期 Date of Issue
(01-79)
15-09-03　C668668(E)

UV light



Secure Printing – *more examples*



Watermark

Glossary (for Secure Printing)

Guilloche: printed security lines, where the layout of intersections and geometry are unique.

Hologram: Is a unique form of photographic printing that is flat optical image to the naked eyes and provides a three-dimensional effect on a flat surface.

Microtext: This involves extremely small text which is small enough to be indiscernible to the naked eye.

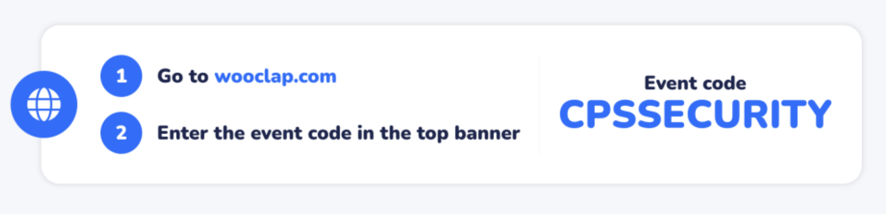
Multiple Laser Image (MLI): Multiple laser image can be viewed at different angels.

Optical Variable Ink (OVI): a high security feature showing different colors as the angle of view changes.

UV (Ultraviolet) Printing: is invisible under regular illumination. By viewing the text/graphic under UV light, they become visible in yellow color.

Contents

- CPS/IoT: Again
- *Smart Cards*
  - Chip Security
  - Plastic Card Security
  - Communication Security
- Discussion



1 Go to wooclap.com

2 Enter the event code in the top banner

Event code

CPSSECURITY

NANYANG
TECHNOLOGICAL
UNIVERSITY

RF ID

LF

Low Frequency

- 125-134 KHz
- Small memory (few tens byte)
- No need for inter-operability
- Low security
- Animal tagging

HF

High Frequency

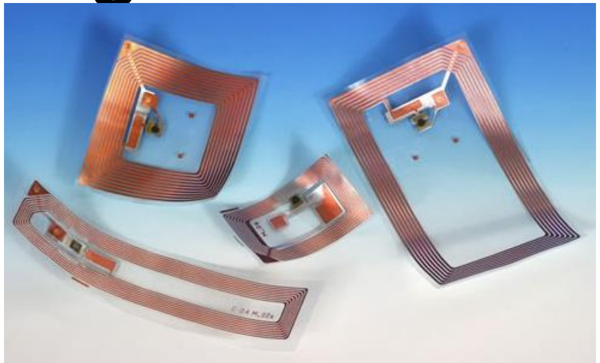
- 13.56 MHz
- ISO14443, ISO15693, NFC
- Various memory size from few tens bytes to several tens Kbytes
- Low, Medium, High Security
- NFC tags
- E-purse, EMV, Passport, Organization / National ID card

UHF

Ultra High Frequency

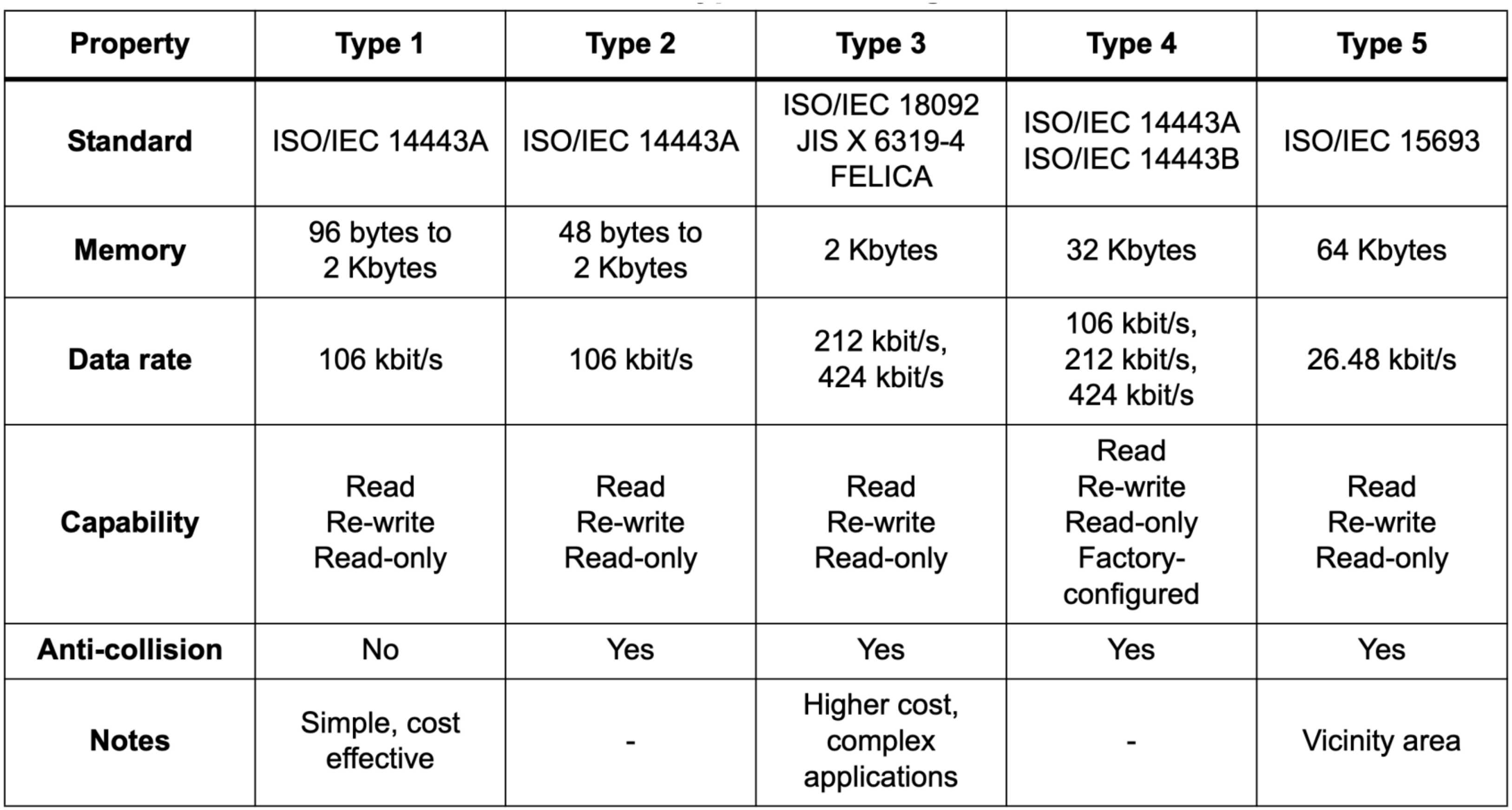
- 856-960 MHz
- ISO 18000-6C
- Detection distance of up to 10+ m
- Small memory
- inter-operability
- Low, medium security
- Logistics, retailer, road toll, airport luggage tracking

Different Forms Of RF ID Tags



NANYANG
TECHNOLOGICAL
UNIVERSITY

What is NFC Tag

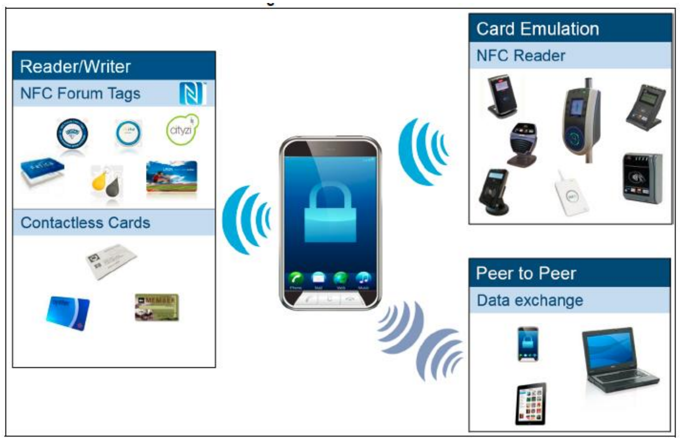


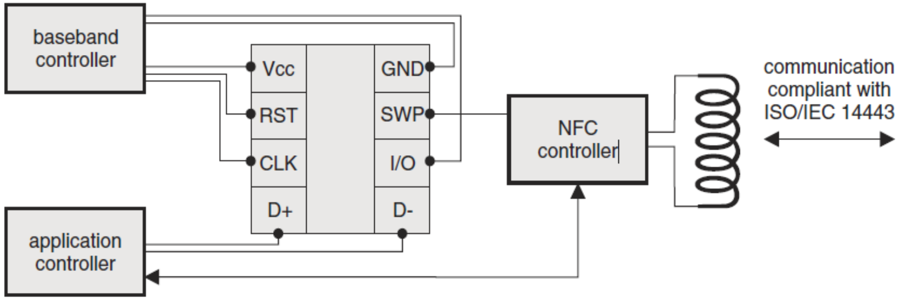
Property	Type 1	Type 2	Type 3	Type 4	Type 5
Standard	ISO/IEC 14443A	ISO/IEC 14443A	ISO/IEC 18092 JIS X 6319-4 FELICA	ISO/IEC 14443A ISO/IEC 14443B	ISO/IEC 15693
Memory	96 bytes to 2 Kbytes	48 bytes to 2 Kbytes	2 Kbytes	32 Kbytes	64 Kbytes
Data rate	106 kbit/s	106 kbit/s	212 kbit/s, 424 kbit/s	106 kbit/s, 212 kbit/s, 424 kbit/s	26.48 kbit/s
Capability	Read Re-write Read-only	Read Re-write Read-only	Read Re-write Read-only	Read Re-write Read-only Factory-configured	Read Re-write Read-only
Anti-collision	No	Yes	Yes	Yes	Yes
Notes	Simple, cost effective	-	Higher cost, complex applications	-	Vicinity area

e.g. Topaz *e.g. My-D, NTag* *e.g. Felica* *e.g. ST25TA, ST25TB* *e.g. ST25TV*

Source: ST Microelectronics NFC Guide
https://www.st.com/content/ccc/resource/technical/document/technical_note/f9/a8/5a/0f/61/bf/42/29/DM00190233.pdf/files/DM00190233.pdf/jcr:content/translations/en.DM00190233.pdf

Near Field Communication (NFC)





- Inspired by RF ID to be used in mobile phone in 2002.
- In 2004 NXP, Sony and Nokia founded the NFC Forum.
- An **NFC phone** works in 3 modes:
  - Card Emulation Mode
  - Reader/Writer Mode
  - Peer-To-Peer Mode

- Driven by an application (applet) installed in Secured Element (SE), as part of SIM (operator) or as part of eSE (mobile device)

Trusted Service Manager (TSM)

- Trusted Service Manager (TSM) is a unifying service provider that enables various modes for the NFC application operator
- NFC application operator needs a card emulation applet inside a Secured Element (SE) (NFC SIM, eSE)
  - **NFC SIM**: Need to work with different telecom operators (some may want exclusivity)
  - **eSE**: Need to work with different mobile manufacturers
- Need to qualify different phone models as performance can differ
  - To qualify the card emulation application working with mobile
  - To be securely loaded into the SE

EZ-Link and SimplyGo

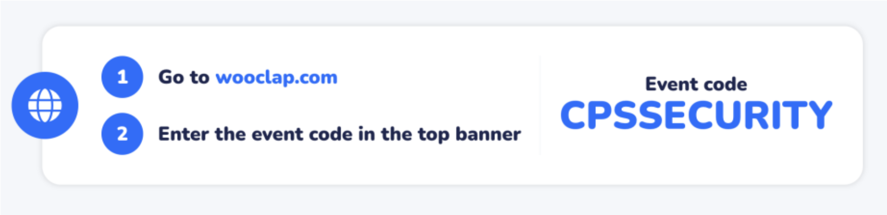
- EZ-link started in 2001, with a card-based wallet requiring top-ups. This is now upgraded to *account-linked system* in 2021.
- SimplyGo started in 2019, with *account-linked* (e.g. Mastercard) payment.
- Follows Specification for Contactless e-Purse Application (CEPAS).
- Account-linked payment systems in smartphone, it utilizes *Trusted Service Manager (TSM)* to maintain the wallet.

- EZ-link used Triple DES[1], which is deprecated by NIST since a major vulnerability was discovered[2]. Other smartcards (e.g. Mifare) using Triple DES has been shown to be vulnerable[3]. Privacy leaks of EZ-link has been studied earlier with side-channel attack setting in 2014[4].

1. *https://en.wikipedia.org/wiki/EZ-Link*
2. *https://nvd.nist.gov/vuln/detail/CVE-2016-2183*
3. *https://www.iacr.org/archive/ches2011/69170208/69170208.pdf*
4. *A. Zankl, "Security and Privacy in an RFID-based Electronic Payment System", Masters Thesis, TU Graz Austria.*

Contents

- CPS/IoT: Again
- Smart Cards
- *Discussion*



1 Go to wooclap.com

2 Enter the event code in the top banner

Event code

CPSSECURITY

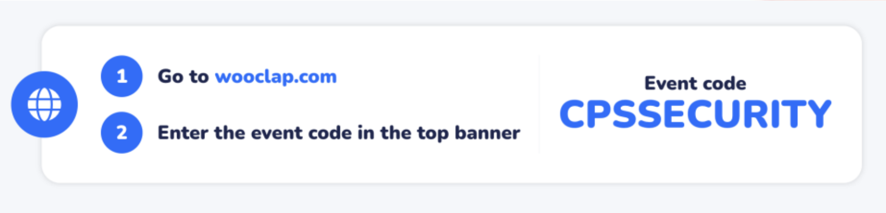
NANYANG TECHNOLOGICAL UNIVERSITY

What did we learn?

- **What are various CPS/IoT ?**
  - Few Examples
  - Attack Classification Example → highlight smart automotive
  - Communication Protocols → heterogeneity

- **Smart cards?**
  - Chip security
  - Secure printing (card protection)
  - NFC/RFID (communication protection)
  - Trusted Service Manager (implementation)

NANYANG TECHNOLOGICAL UNIVERSITY



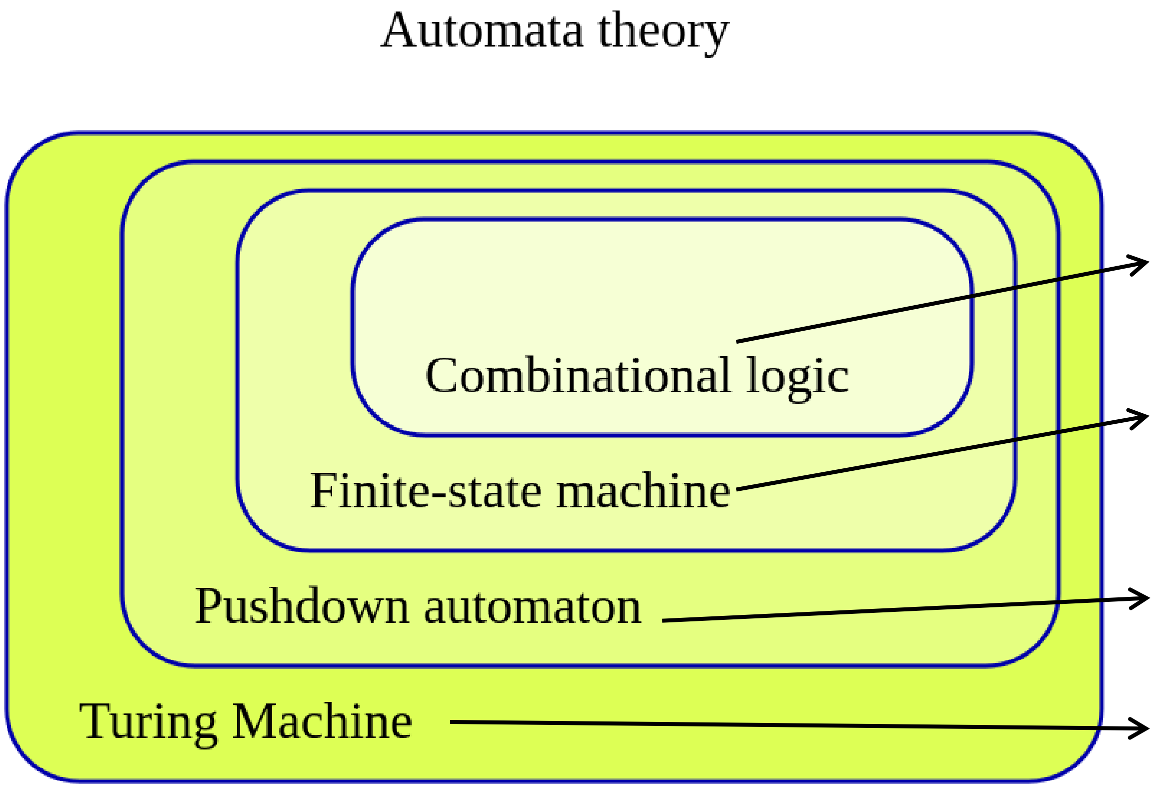
1 Go to wooclap.com

2 Enter the event code in the top banner

Event code
CPSSECURITY

Further Readings

Automata and *Examples*



Full-Adder

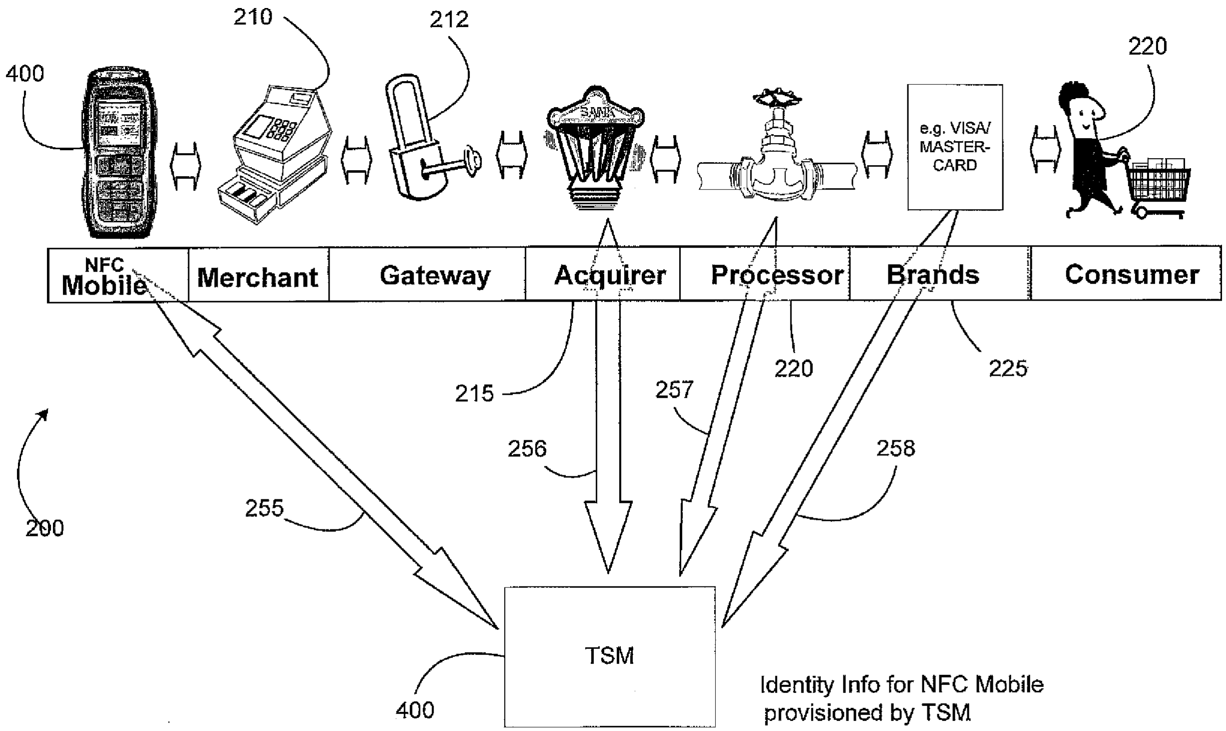
Regular Expression Matching

Expression w/ Parenthesis
e.g. evaluate {(6 + 2) – 4 }

Everything

Image source: wikipedia

Trusted Service Manager



Identity Info for NFC Mobile provisioned by TSM

FIG. 2

Image source: Paypal patent US8417643B2

Trusted Service Manager

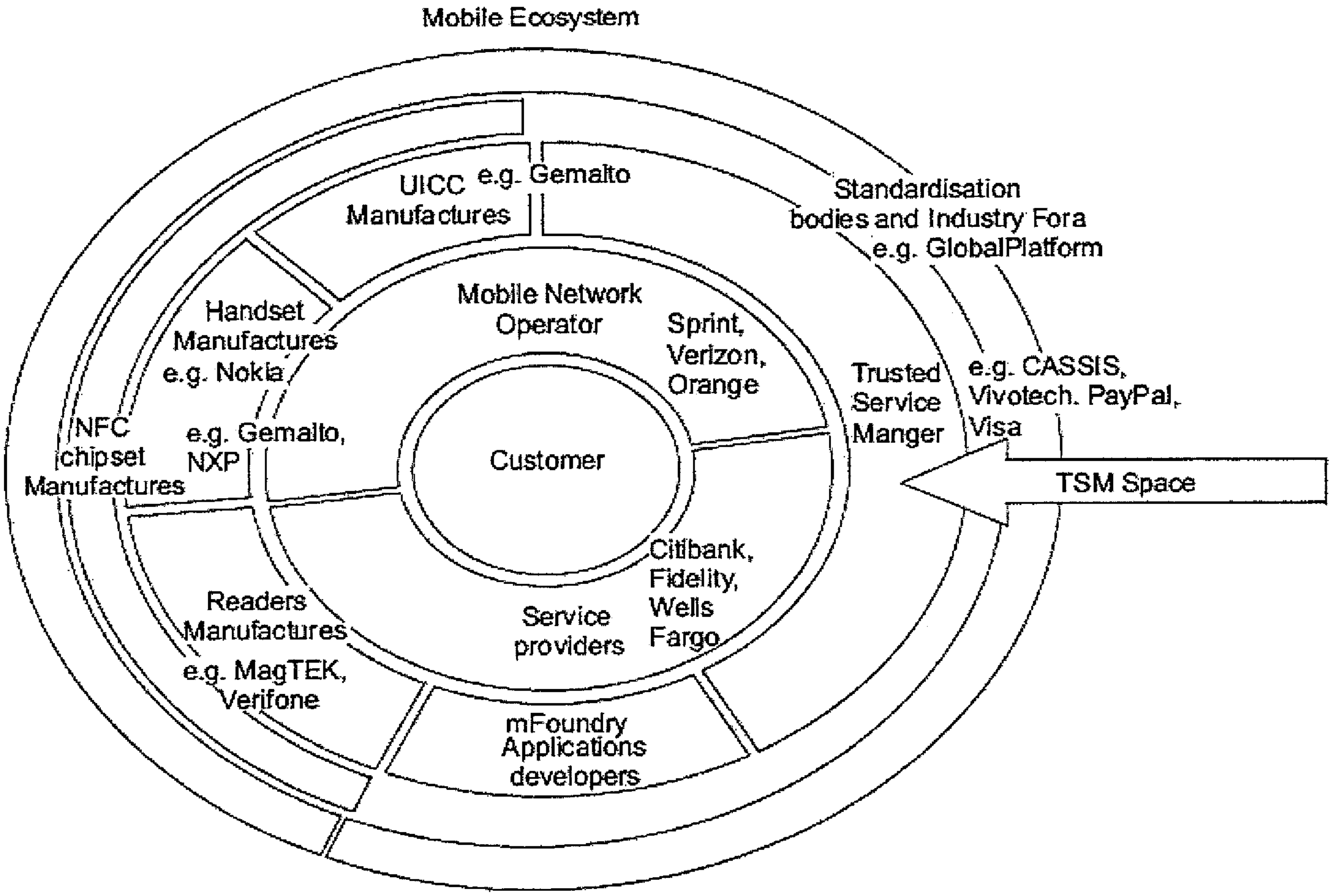


FIG. 1

Image source: Paypal patent US8417643B2

Trusted Service Manager: Tasks

- User registration: Corresponding to a bank
- Managing Digital Certificates: User identity
- Authentication and Verification: Transactions of the mobile wallet with a payment terminal

- The above services are delivered using the underlying platform, in particular
  - **SE**: Storage of keys, passwords, identity
  - **Secure Communication**: NFC
  - **TEE**: Secure Microprocessor for providing security services (e.g., encryption, authentication)

The End