Managing the Risks of IoT in Cities and Communities Through Standards

Abdulhadi AbouAlmal
Q6/20 Rapporteur, ITU-T Study Group 20

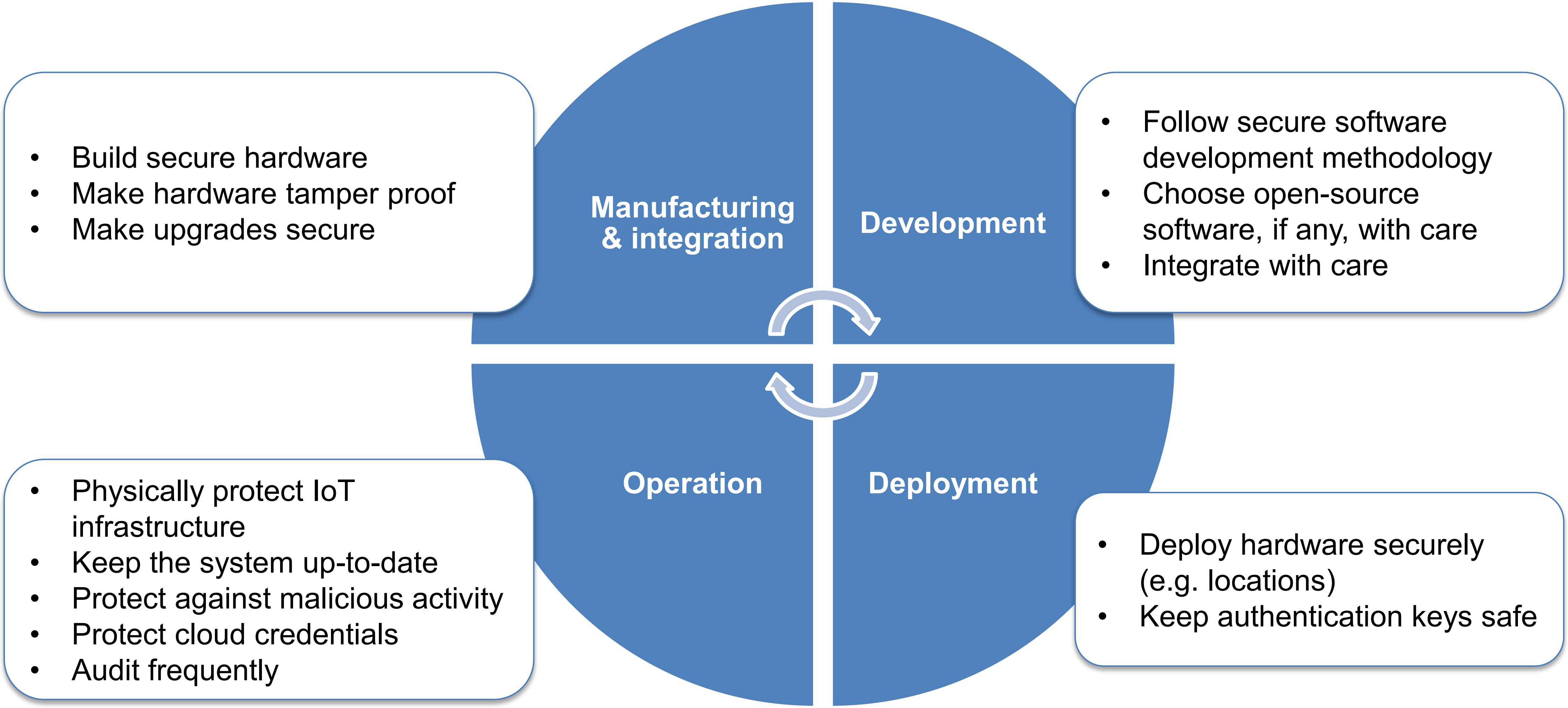
Growing Challenges in IoT & SCC Domains …

- Network exposure in IoT & SCC Domains could lead to a greater attack surface
- Compromised IoT devices may expose data, cause disruption of services, damage of systems, or attack infrastructure and devices (e.g. DDoS, MitM, Malware …etc.)
- International standards are developed to secure IoT devices and networks against malicious actions based on in-depth strategies, architectures, processes and solutions.

Security Risks and Challenges Faced by Cities

Security Impacts	Privacy Impacts
Disruption of essential services	Personal information
Loss of trust	Financial/banking information
Disruption of operations	Health records
Economic impacts	Domotics
Damaging equipment	Wearable Device
Public safety	Metadata

Possible Security Layers for IoT Solutions



Manufacturing & integration

- Build secure hardware
- Make hardware tamper proof
- Make upgrades secure

Development

- Follow secure software development methodology
- Choose open-source software, if any, with care
- Integrate with care

Operation

- Physically protect IoT infrastructure
- Keep the system up-to-date
- Protect against malicious activity
- Protect cloud credentials
- Audit frequently

Deployment

- Deploy hardware securely (e.g. locations)
- Keep authentication keys safe

Importance of International Standards

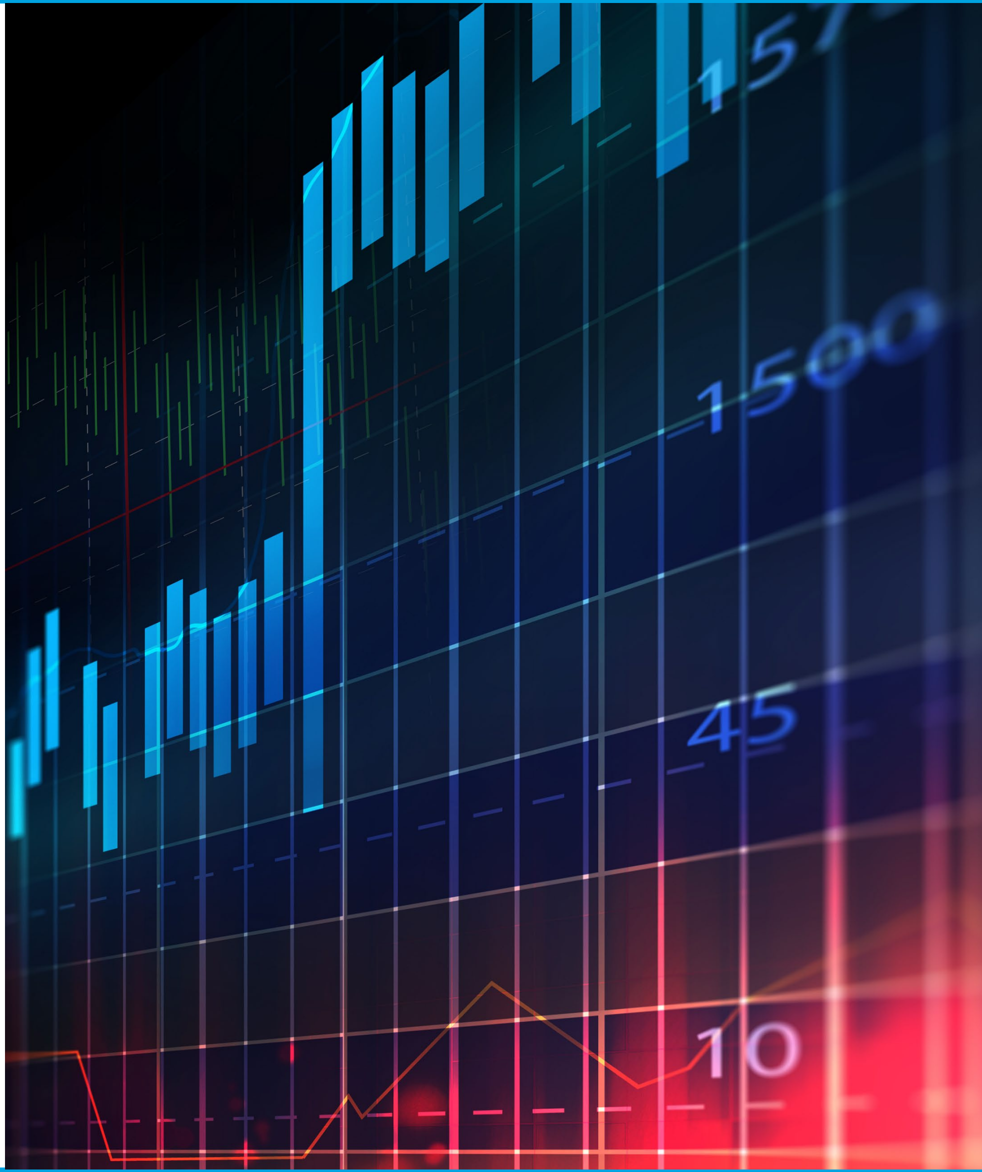
Overarching frameworks

Define objectives and priorities

Best practices

Provide specific guidelines

Measure and improve performance



ITU-T Study Group 20:
IoT and Smart Cities and Communities

ITU-T Study Group 20:
Internet of Things and
Smart Cities and Communities

Lead Study Group on

- Internet of Things and its applications
- Smart cities and communities
- IoT Identification

Q1/20 Interoperability and interworking of IoT and SC&C applications and services

Q2/20 Requirements, capabilities and architectural frameworks across verticals enhanced by emerging digital technologies

Q3/20 IoT and SC&C architectures, protocols and QoS/QoE

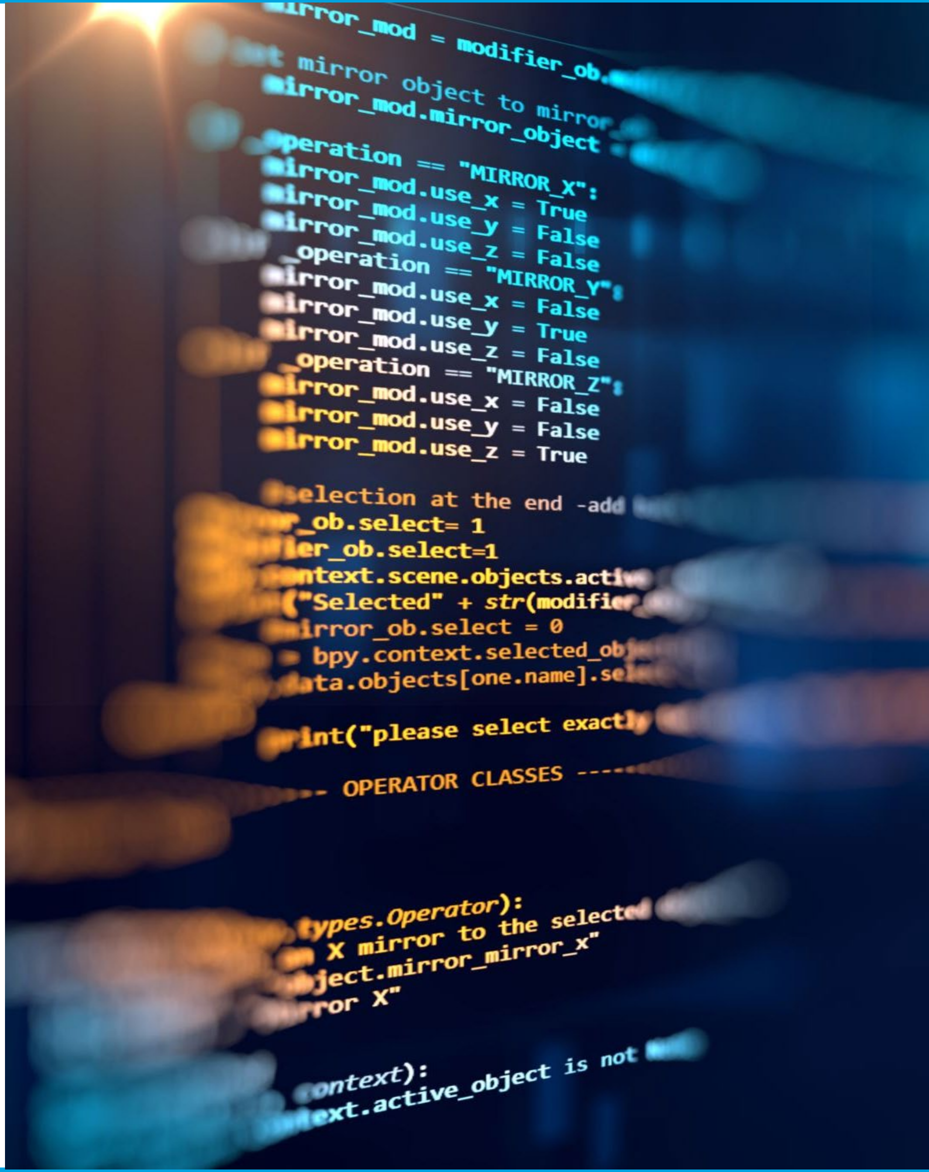
Q4/20 Data analytics, sharing, processing and management, including big data aspects, of IoT and SC&C

Q5/20 Study of emerging digital technologies, terminology and definitions

Q6/20 Security, privacy, trust and identification for IoT and SC&C

Q7/20 Evaluation and assessment of Smart Sustainable Cities and Communities

Q6/20:
Security, Privacy, Trust and Identification for IoT and SC&C



More info:
https://www.itu.int/en/ITU-T/studygroups/2017-2020/20/Pages/q6.aspx

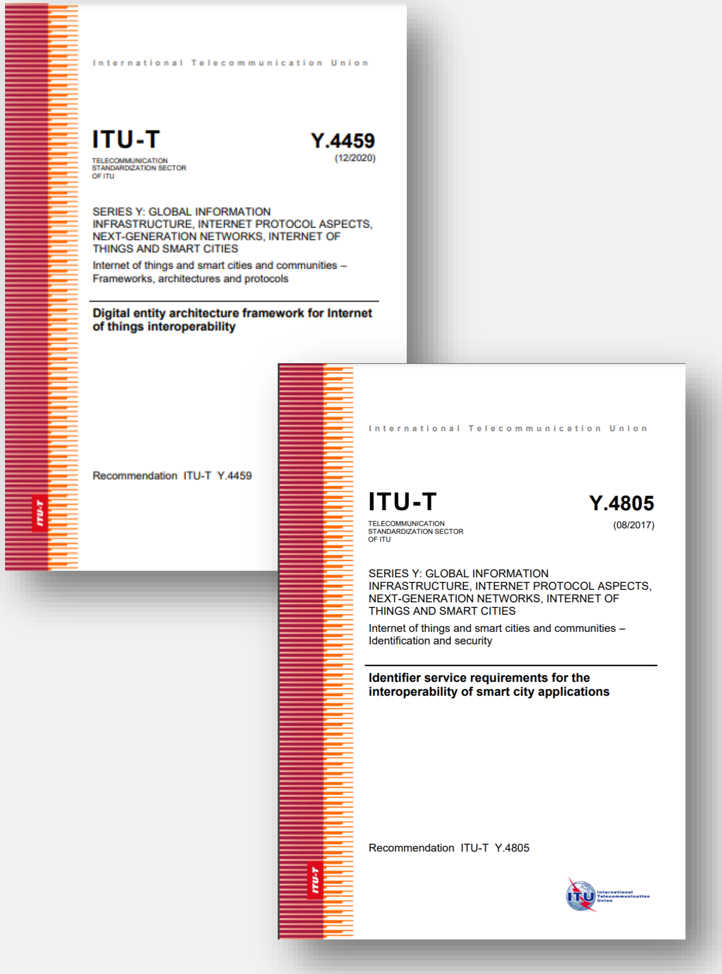
Recommendations ITU-T Y.4459 and ITU-T Y.4805

ITU-T Y.4459

- Digital entity architecture framework for Internet of things interoperability

ITU-T Y.4805

- Identifier service requirements for the interoperability of smart city applications



International Telecommunication Union

ITU-T

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

Y.4459 (12/2020)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet of things and smart cities and communities – Frameworks, architectures and protocols

Digital entity architecture framework for Internet of things interoperability

Recommendation ITU-T Y.4459

International Telecommunication Union

ITU-T

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

Y.4805 (08/2017)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet of things and smart cities and communities – Identification and security

Identifier service requirements for the interoperability of smart city applications

Recommendation ITU-T Y.4805

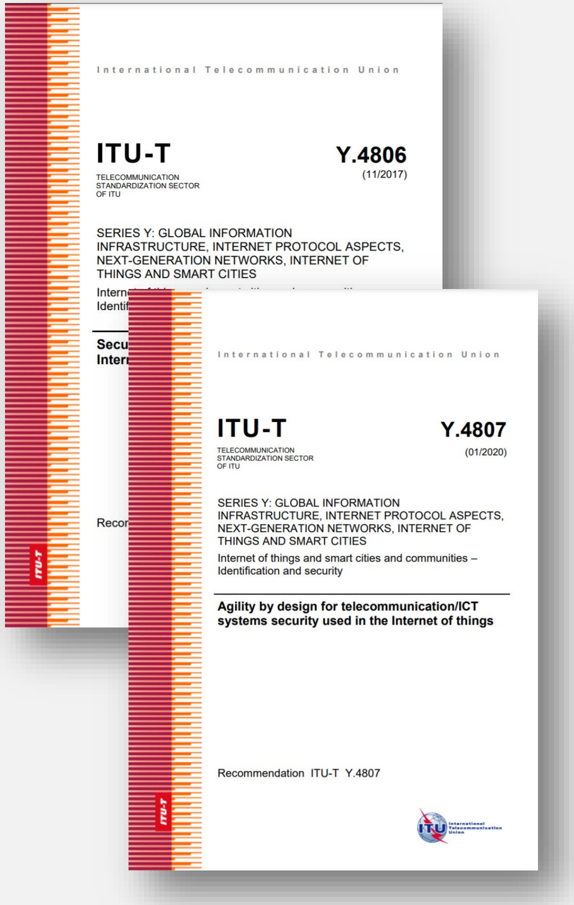
Recommendation ITU-T Y.4806 and ITU-T Y.4807

ITU-T Y.4806

- Security capabilities supporting safety of the Internet of things

ITU-T Y.4807

- Agility by design for telecommunication/ICT systems security used in the Internet of things



International Telecommunication Union

ITU-T
TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4806
(11/2017)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Intern
Identif

Secu
Inter

Recor

International Telecommunication Union

ITU-T
TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4807
(01/2020)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet of things and smart cities and communities – Identification and security

Agility by design for telecommunication/ICT systems security used in the Internet of things

Recommendation ITU-T Y.4807

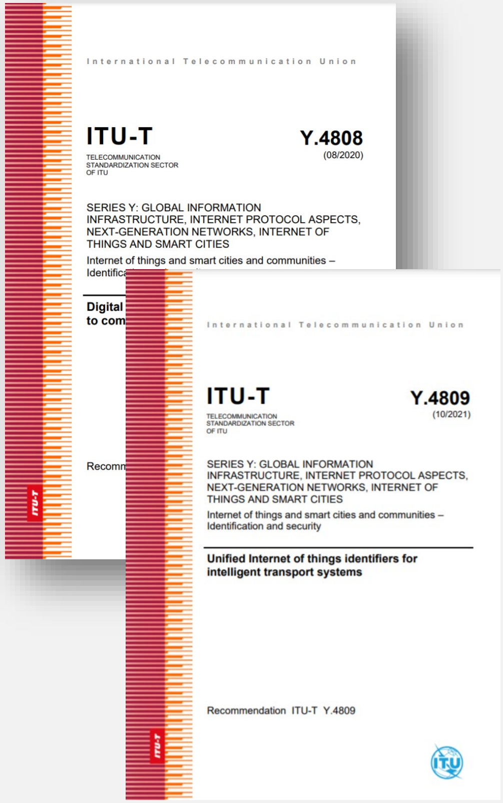
Recommendations ITU-T Y.4808 and ITU-T Y.4809

ITU-T Y.4808

- Digital entity architecture framework to combat counterfeiting in Internet of things

ITU-T Y.4809

- Unified IoT Identifiers for intelligent transport systems



International Telecommunication Union

ITU-T
TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4808
(08/2020)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet of things and smart cities and communities –
Identifica

Digital
to com

Recomm

International Telecommunication Union

ITU-T
TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4809
(10/2021)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet of things and smart cities and communities –
Identification and security

Unified Internet of things identifiers for intelligent transport systems

Recommendation ITU-T Y.4809

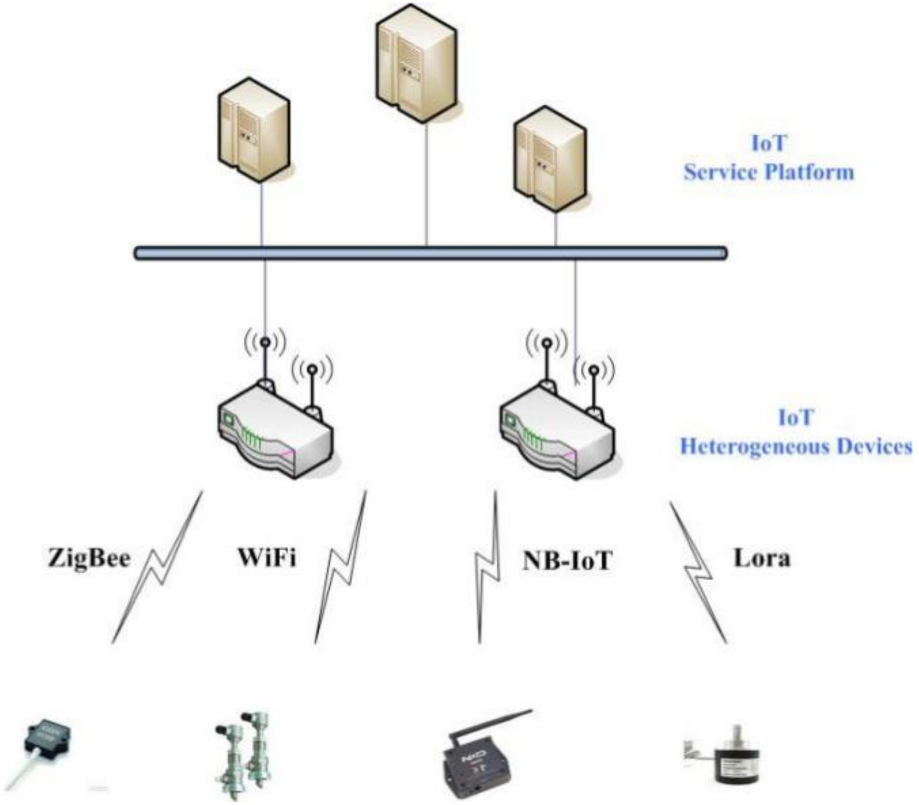
Q6/20 Ongoing Work Items

Work items	Subject / Title
Y.4810 (ex Y.Data.Sec.IoT-Dev)	Requirements of data security for the heterogeneous IoT devices
Y.4811 (ex Y.IoT-CSIADE-fw)	Reference framework of converged service for identification and authentication for IoT devices in decentralized environment
Y.FW.IC.MDSC	Framework of identification and connectivity of moving devices in smart city
Y.IoT-Ath-SC	Framework of IoT-devices authentication in smart city
Y.IoT-IoD-PT	Identity of IoT devices based on secure procedures to enhance trust of IoT systems
Y.IoT-Smartcity-Risk	Reference framework of cybersecurity risk management of IoT ecosystems on smart cities
Y.oneM2M.SEC.SOL	oneM2M Security Solutions
YSTR.Feas-DID-IoT	Feasibility of Decentralised Identifiers (DIDs) in IoT
YSTR-IADIoT	Intelligent Anomaly Detection System for IoT

Data-Security

- **Challenges:** IoT devices are exposed to a variety of data security threats that could impact Confidentiality, Integrity, and Availability (e.g. MitM attacks, DDoS attacks, etc.)

- **Standard-based solution:**
    - Recommendation ITU-T Y.4810 specifies Requirements of data security for the heterogeneous IoT devices including:
        - Modeling scenarios of data security for IoT devices
        - Defining data security threats & requirements for IoT devices under specific scenarios

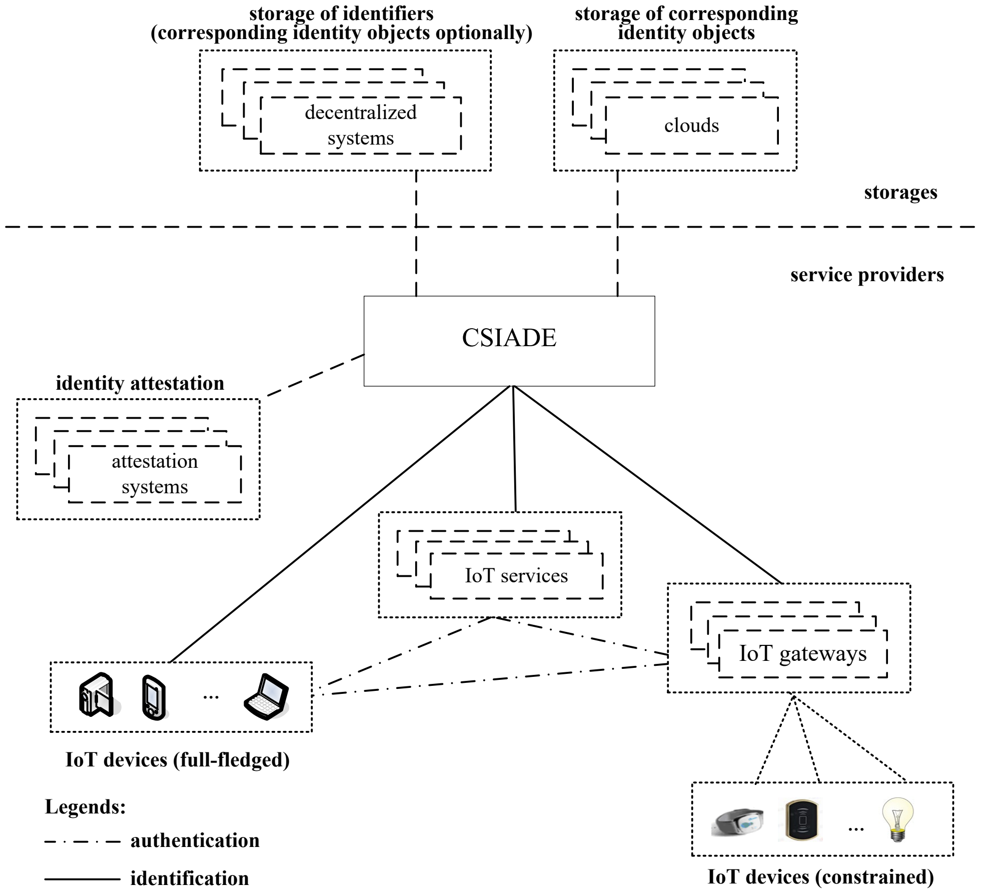


Identification & Authentication in Decentralized Environments

- **Challenges:** Identification & authentication of IoT devices across different IoT systems can be complicated.

- **Standards-based solution:**

  - Recommendation ITU-T Y.4811 provides reference framework of converged service for identification and authentication for IoT devices in decentralized environment
  - Leverages IoT services and devices to access capabilities of identification & authentication.
  - Supports interactions between large numbers of IoT devices and services which use different decentralized IoT systems.



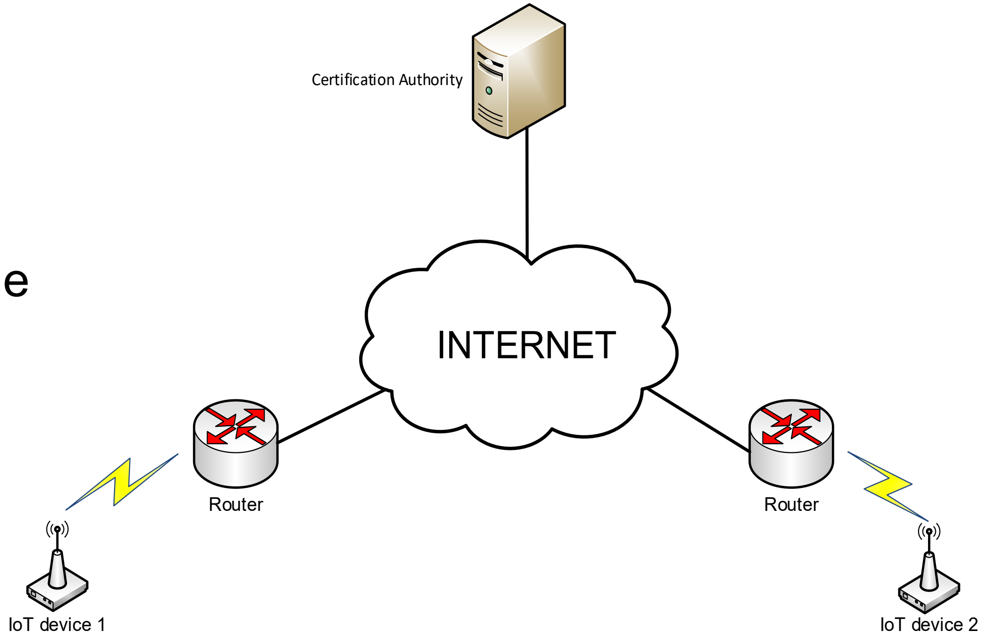
IoT Secure Identification Procedures

- **Challenges:** Security procedures to identify and certify IoT devices may be robust enough.

- **Standards-based solution:** WI Y.IoT-IoD-PT investigates methods for IoT device identification to ensure they are unique and robust:

  - Simple IoT devices – based on passive tags
    - e.g. utilize IP/MAC addresses.

  - Complex IoT devices – based on microcontrollers
    - e.g. utilize digital signatures and certificate authorities.

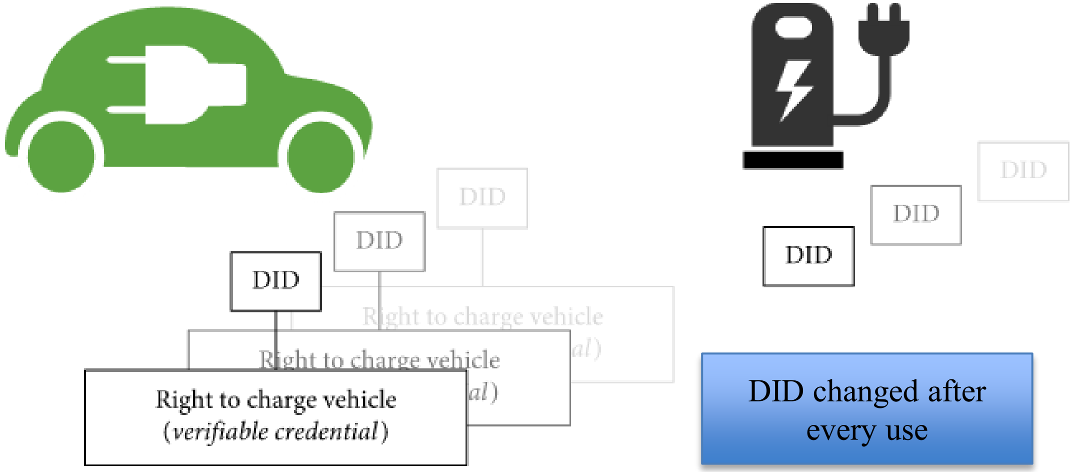


Decentralized Identifiers in IoT

- **Challenges:** Using persistent identifiers in IoT networks may pose a privacy risk (e.g. tracking and identifying users).

- **Standards-based solution:**
  - Decentralized Identifiers (DIDs) are independent of a central issuing identity provider that creates and controls the identifier.

  - WI YSTR.Feas-DID-IoT studies the feasibility of DIDs in IoT environments.

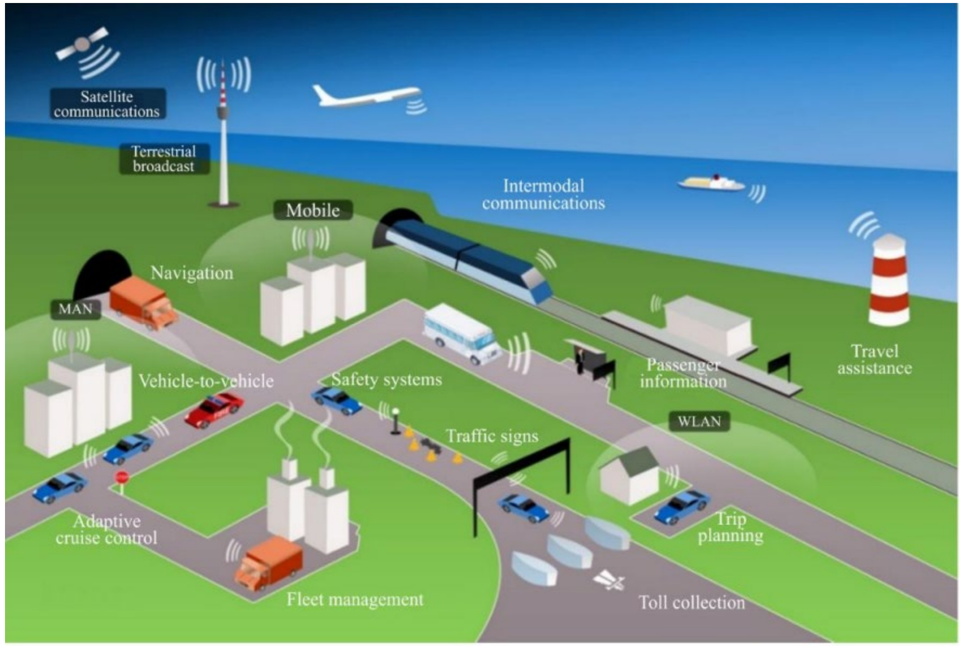


Unified IoT Identifiers for Intelligent Transport Systems (ITS)

- **Challenges:** Autonomous, unmanned and intelligent vehicles are becoming more common, with requirement to safely and efficiently transport goods and humans.

- **Standard-based solution:**
  - Standards related to Intelligent transport systems (ITS) enable traffic and transportation services to users & connected vehicles, enabling them to perform more efficient decisions.

  - Recommendation ITU-T Y.4809 unifies the field formats for identifiers of road signs and signals and standardizes specific values of such identifiers for every signor signal.



Report M.2445-01

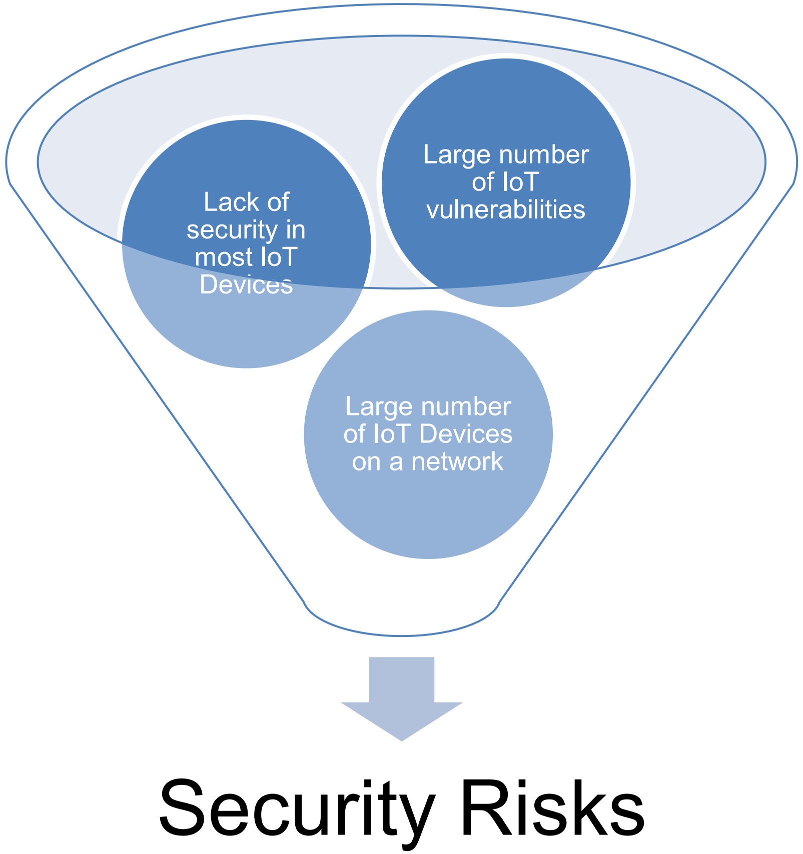
Smart City-Risk

- **Challenges:** Smart cities are exposed to many risks which must be identified for risk analysis.

- **Standards-based solution:** WI Y.IoT-Smartcity-Risk analyses cybersecurity risks presented by IoT ecosystems that affect Smart Cities, including:
  - Characteristics and high-level requirements of the risk management for IoT components;
  - Set of key risk indicators (KRI) for IoT ecosystems in the smart city domain.

Authentication in Smart Cities

- **Challenges:** Traditional authentication processes for IoT devices using WEP, WPA, WPA2 protocols could be vulnerable.
- Web based authentication could be more secure, but may not be practical for "simple" IoT devices (e.g. smart watches), which usually do not support HTTP.
- **Standards-based solution:** WI Y.IoT-Ath-SC is developing a secure methodology for authenticating IoT devices without using Web authentication.


Lack of security in most IoT Devices
Large number of IoT vulnerabilities
Large number of IoT Devices on a network
Security Risks

Moving Devices in Smart Cities

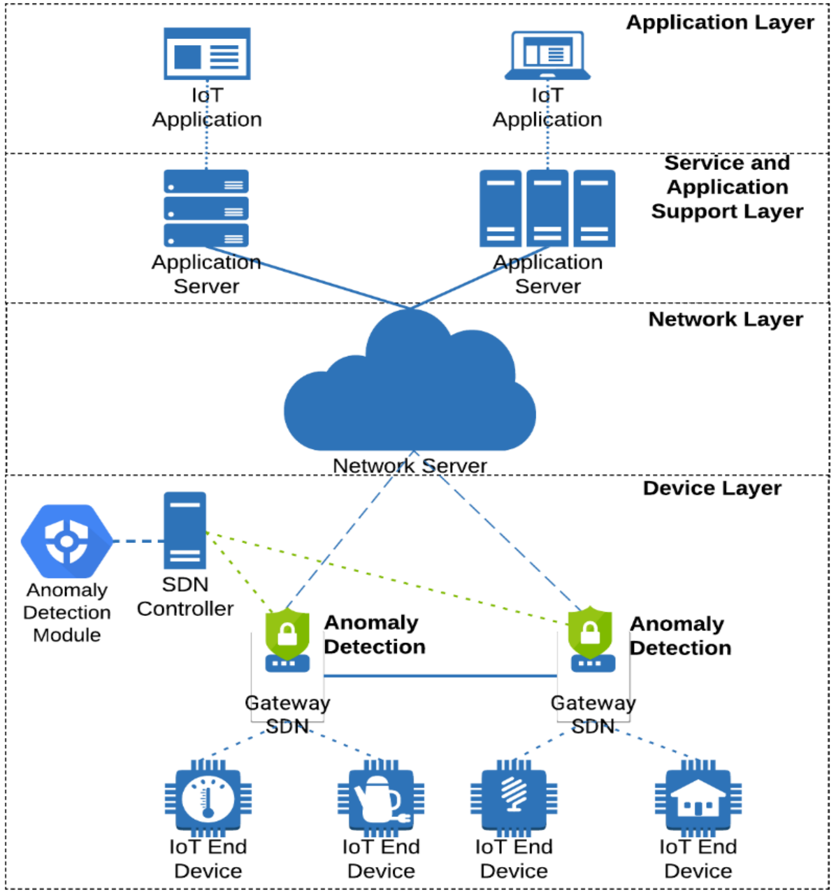
- **Challenges:** Existing methods of identifying and verifying MDSC & IoT systems are not sufficient for long distances.

- **Standards-based solution:** WI Y.FW.IC.MDSC is defining a methodology for MDSC identification using wireless technologies, in particular mobile infrastructure supporting long distance MDSC connectivity and long battery life (e.g. NB-IoT and LTE-eMTC).

Intelligent Anomaly Detection

- **Challenges:** IoT devices exposed to the Web are vulnerable to global intrusion efforts considering impact on Resource-constrained (battery, processing, etc.).

- **Standards-based solution:** WI YSTR-IADIoT defines an Anomaly Detection System (ADS), which helps prevent and mitigate cybersecurity attacks in IoT devices and systems through the detection of abnormal activities.

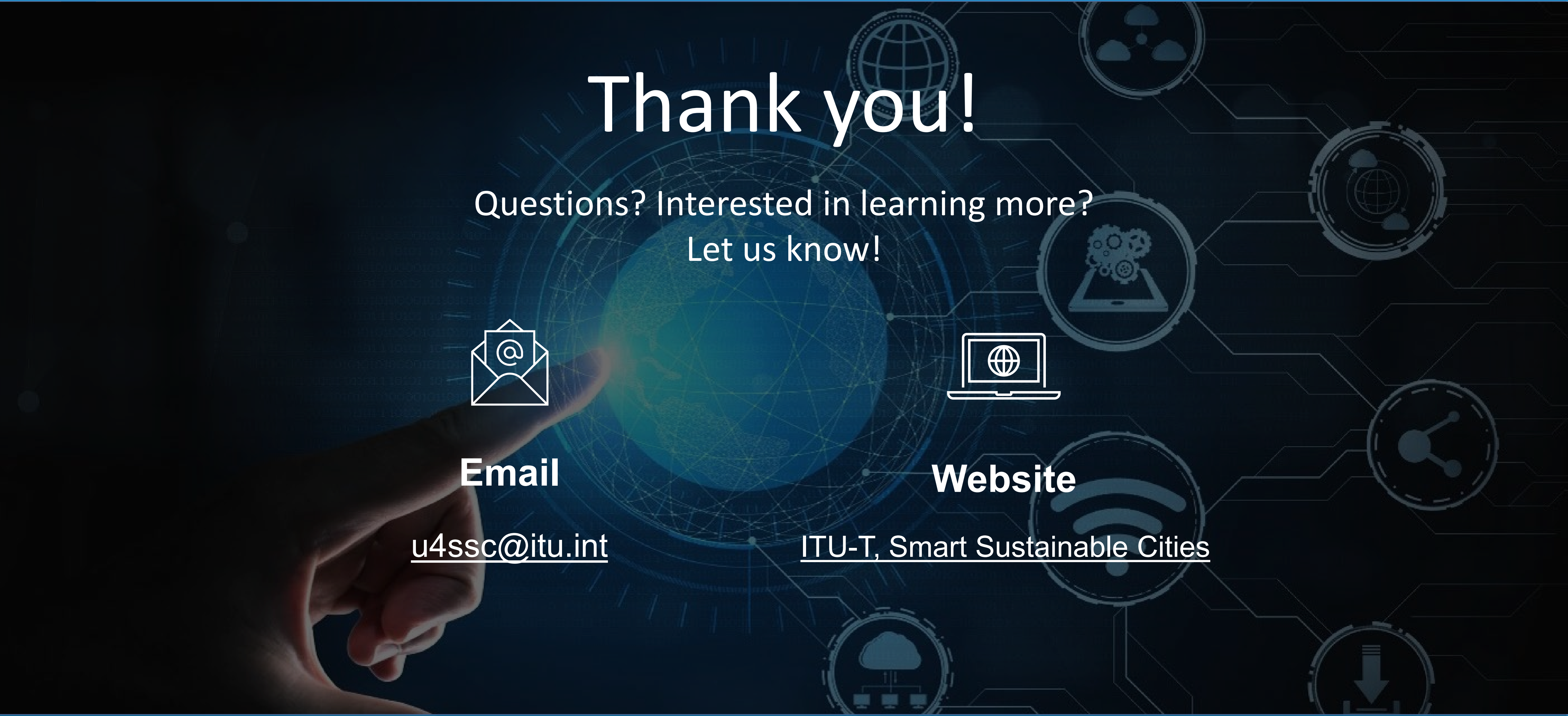


Conclusion

Accelerated digital transformation has led to increased risk of cyber security attacks.

City and Community leaders must be prepared to respond and prioritize security, privacy and trust.

Standards play a critical role in helping cities and communities enhance security capabilities.



Thank you!

Questions? Interested in learning more?
Let us know!

Email

u4ssc@itu.int

Website

ITU-T, Smart Sustainable Cities