TATA CONSULTANCY SERVICES

TATA

Internet of Things - A Standardization Perspective

Jaydip Sen

Agenda

- Internet of Things (IoT) – Introduction
- Technological trends
- IoT- Enablers, Barriers and Applications
- IoT Architectural Trends
- IoT- Current Standardization Efforts
  - CASAGARAS
  - W3C
  - ANEC, BUEC
- IoT-Standardization Issues
  - Interoperability
  - Security and Privacy
  - Device and Systems Management- Self-configuration, Device Discovery
  - Device/Object Identity
  - Application Deployment
  - Regulations
- Proposals for Delivery

Internet of Things

- Internet → The world-wise network of interconnected computer networks, based on a standard communication protocol (TCP/IP).
- Thing → An object not precisely identifiable.
- Internet of Things → A world-wide network of interconnected objects uniquely addressable, based on standard communication protocol.
- While current Internet is a collection of rather uniform devices, IoT will exhibit much higher level of heterogeneity, as objects of totally different functionality, technology and application fields will belong to the same communication environment.

Technological Trends

- It is possible to identify five distinct macro-trends that will shape the future of IT, together with the explosion of ubiquitous devices that constitute the future of IoT:
  - **Data deluge** : explosion of the amount of data collected and exchanged. Forecasts indicate that in the year 2015 more than 220 Exabytes of data will be stored. Novel mechanisms to find, fetch, and transmit data will be needed.
  - **Decrease in energy required to operate intelligent devices**: the search will be for a zero level of entropy where the device or system will have to harvest its own energy.
  - **Miniaturization of devices**: the devices will become increasingly smaller.
  - **Autonomic management:** the devices/systems will have self-management, self-healing, and self-configuration capabilities.
  - **IPv6 as an integration layer**:

Internet of Things Enablers

- **Energy:** issues such as energy harvesting and low-power chipsets are central to the development of IoT.
- **Intelligence:** devices should have capabilities such as context-awareness and inter-machine communication etc.
- **Communication:** new, smart multi-frequency band antennas, integrated on-chip and made of new materials are the communication means that will enable the devices to communicate.
- **Integration:** integration of smart devices into packaging, or better, into the products themselves will allow a significant cost saving and increase the eco-friendliness of the products.
- **Interoperability:** protocols for interoperability have to be standardized.
- **Standards:** open standards will be the key enablers for the success of the IoT. Sustainable. Fully global, energy-efficient communication standards that are security and privacy centered and use compatible or identical protocols ate different frequencies are needed.

Internet of Things Barriers

- **Governance:** without an authority, it will be impossible to have a truly global IoT.
  - No universal numbering system currently exists. EPC Global and Ubiquitous ID are two different, non-compatible ways of identifying objects.
  - There is a need of keeping governance as generic as possible. One authority per field will certainly lead to overlap, confusion and competition between standards. Example: EPC Global architecture has a “single point of failure and control” where Verisign has the records of all the numbers, and can track where any object is.
  - What would be the governance of the IoT is an open question. Will it be a state-led agency, or a group under the supervision of the UN, or an industrial consortium?
- **Privacy and Security:**
  - Public acceptance of IoT will happen only when strong security solutions are in place.
  - The standards must define different security features to provide confidentiality, integrity, or availability of services.
  - The issues related to identity of people must be dealt with in politics and legislations.

Internet of Things Applications

- **Manufacturing, logistics and retail sectors** → product authentication and anti-counterfeiting, next-generation industrial automation and supply chain management, inventory management, track & trace, remote maintenance, service and support.

- **Energy and utilities sectors** → smart electricity and water transmission grids, real-time monitoring of sewage systems, efficient energy and water consumption at homes enabled by connected devices to the grid.

- **Intelligent transportation systems** → support for vehicular ecosystems, use of in-vehicle sensor networks, telematics, GPS and wireless networks for developing smart vehicles, vehicle-to-vehicle and vehicle to roadside communication for collaborative road safety and efficiency, vehicle tracking, traffic data collection for traffic management etc.

- **Environment monitoring systems** → wireless sensor nodes to monitor weather, environment, civil structures, soil conditions etc.

- **Home management and monitoring** → use of sensor nodes, smart applications, wireless networks, home gateways for applications such as home security, elderly care, smart energy control etc.

Internet of Things - Architectural Trends

- The following issues are important for IoT standardization

  - **Designing Web Services** as a common platform to publish service definitions and exchange configuration information between various hosts.
  - **Designing Messaging Services Layers** providing a basic web-services messaging framework between hosts which abstracts lower layers.
  - **Designing Common Data Exchange Formats** for sharing of structural data across different systems.
  - **Using Internet Protocol Layers or an IP proxy layer**, for connecting network nodes across multiple types of networking technologies, RF waveforms, and radio platforms.

- The architectural framework needs to incorporate all the desired aspects such as scalability, flexibility, adaptability etc.

- The components, and interfaces for various building blocks such as device interfaces, data formats, networking standards and protocols, service platforms and application interfaces are to be defined in IoT standards.

Current Standardization Efforts on Internet of Things

IoT Standardization Efforts in CASAGARAS

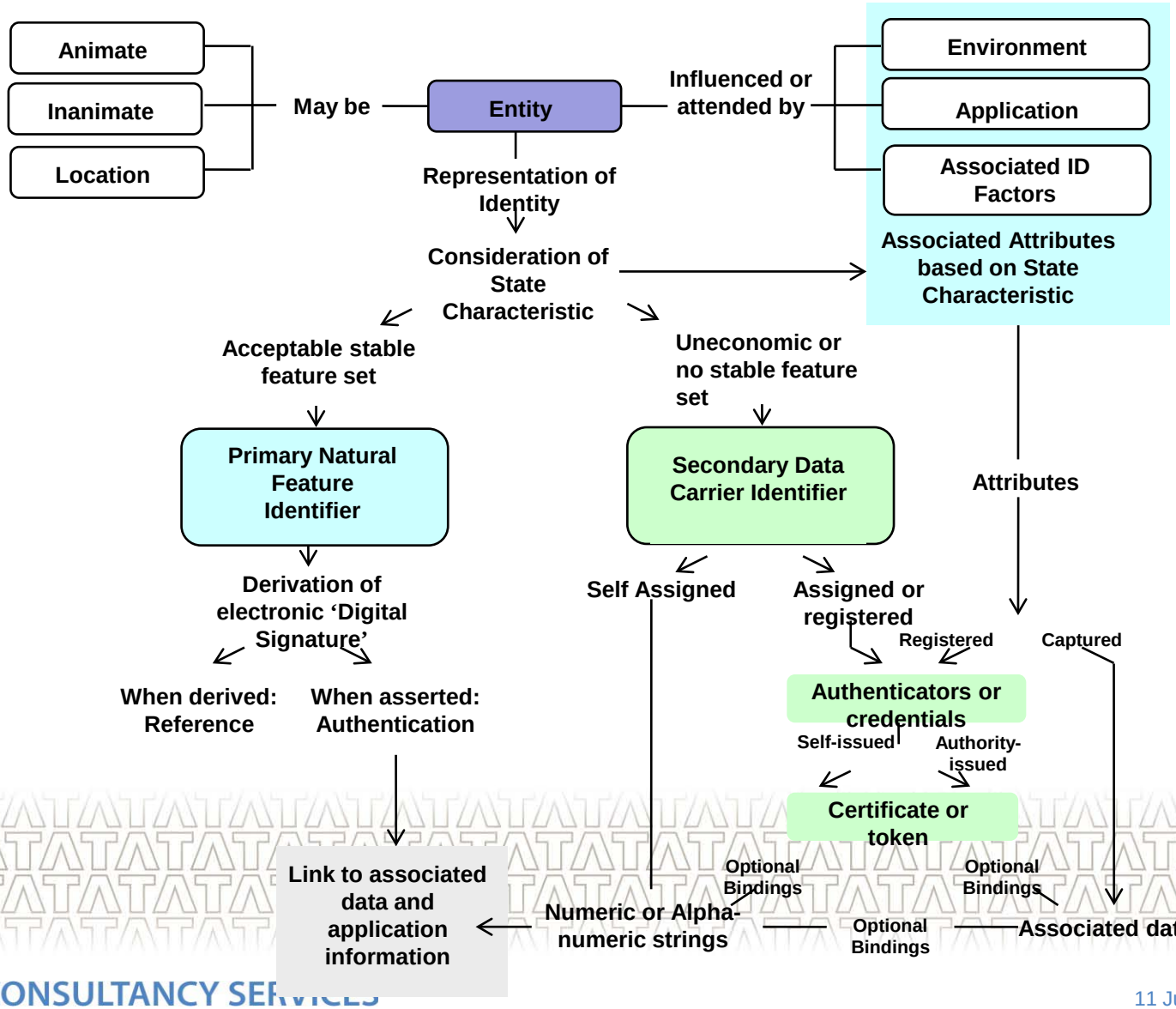
- The aim of CASAGARAS (Coordination And Support Action for Global RFID-related Activities and Standardization) is:
  - To provide an incisive framework of foundation studies that can assist in influencing and accommodating international issues and developments concerning radio frequency identification (RFID) and the emerging Internet of Things, particularly with respect to standards and regulations.

- CASAGARAS work package includes the following:
  - Standards and procedures for international standardizations in relation to RFID, including applications and conformance standards.
  - Regulatory issues with respect to RFID standards.
  - Global coding systems (GCS) in relation to RFID systems.
  - RFID in relation to ubiquitous computing and networks.
  - Functional including sensory, developments in RFID and associated standards.
  - Areas of applications, existing and future, and associated standards.
  - Socio-economic components of RFID usage.

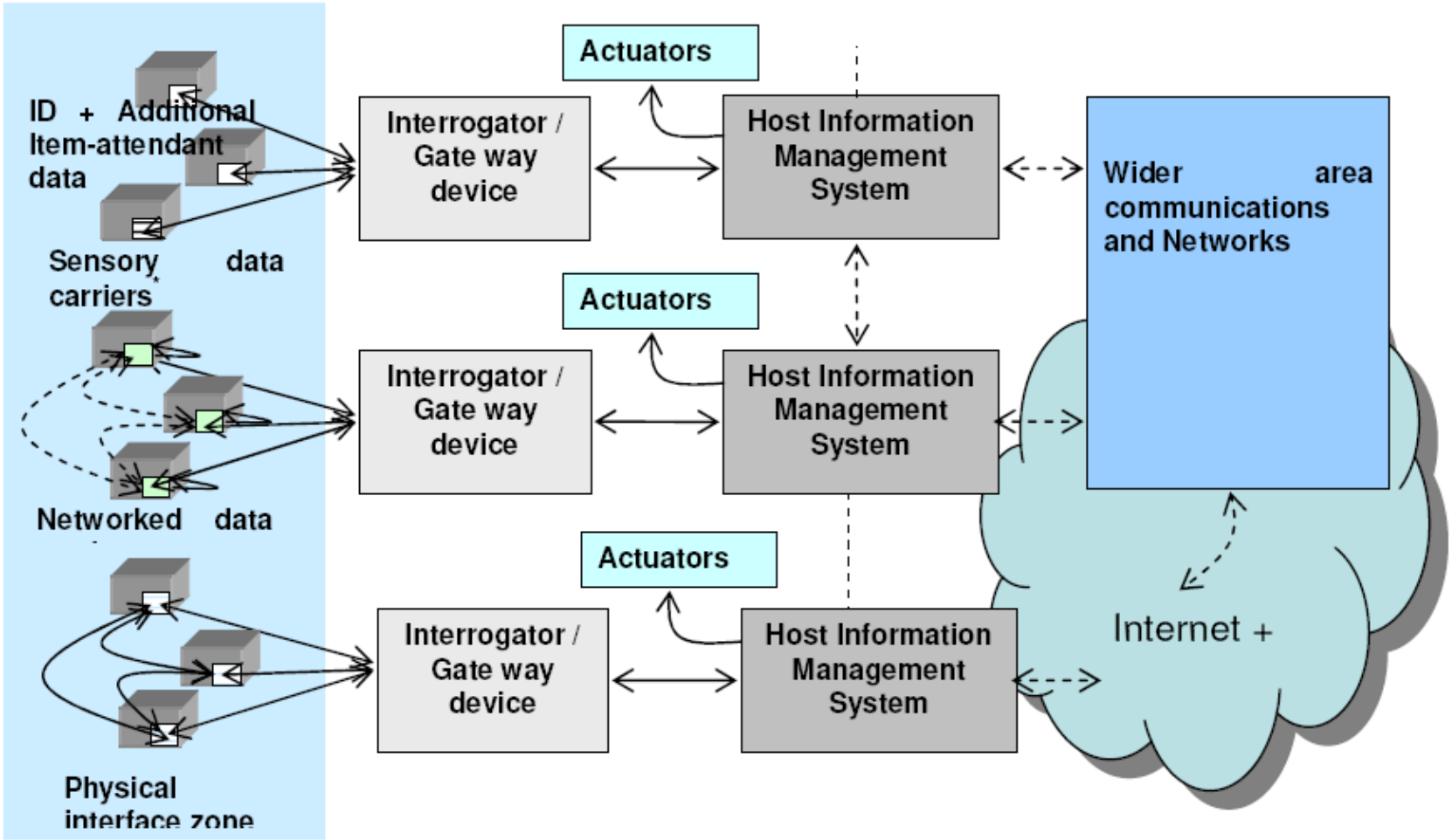
CASAGARAS Model of Internet of Things

- CASAGARAS has adopted a fully inclusive model for Internet of Things:
  - Embracing a fully inclusive range of ‘edge’ technologies, including RFID for interfacing with the physical world.
  - Exploiting the evolving object-connected data capture technologies and networking capabilities – sensory, location, local communication and security.
  - Exploiting existing and evolving communications and mobility structures.
  - Integration with the evolving Internet.

CASAGARAS – Ontology for Identification



IoT- Architectural Components (CASAGARAS)



IoT Standardization Efforts in W3C

- W3C is involved in the following standardization efforts on IoT:
  - Mix of rapidly evolving networking technologies
    - Ethernet over twisted pair or coax
    - DSL over copper phone lines
    - Ethernet over building power wiring
    - WiFi and WiMAX
    - Bluetooth
    - ZigBee Sensor networks
    - Cellular packet radio
  - Challenges related to different addressing schemes in a P2P network
  - Security and privacy issues in communication
    - Prevention of Phishing attacks, DoS attacks
    - Protection of Vulnerabilities of the Sandbox model of the browsers
    - Designing trust management solutions
  - Device coordination → for binding devices and services as part of distributed applications.
  - Event transportation mechanisms → how to transport events to devices
    - Tunneling through NAT
    - Public and Private agents
    - Remote user interfaces
  - Dynamic adaptation to user preferences, device capabilities and environmental conditions→ server side and client-side adaptations based on policies

IoT Standardization Efforts in ANEC and BEUC

- European consumer voice in standardization in IoT
- Standardization efforts are towards making standards that are open and have the following features:
  - Interoperable
  - Neutral
  - Trustworthy
  - Transparent in governance
  - Protects privacy and fundamental rights of users
  - Security
  - Liability and accountability → chains of responsibility should be clearly established and remedies must be available.
  - New sections on health, safety, and environmental aspects of IoT are added.

Ineternet of Things

Current Issues in Standardization

Specific Issues in IoT Standardization

- Interoperability
  - Radio access level
  - Protocol level
  - Semantic level (unified data exchange format within a specific domain
  - Semantic and Context level (between different industry domain)

Radio Access Level Issues

- Dynamic Spectrum Access (DSA) techniques are becoming a key issue for heterogeneous communication environment characterized by the sharing of the spectrum and the coexistence among various radio access nodes. This becomes more important in IoT, where multitude of devices communicate and rearrange their network configuration in an autonomous way.

- Finding new spectral resources or developing new techniques to assure a more flexible and efficient utilization of communication channel is a key issue.

- Frequency band allocations are not harmonized across all regions of the globe.

- Standards regarding spectrum allocation, radiation power levels and communication protocols will ensure that IoT co-operates with other users of the radio spectrum including mobile telephony, broadcasting, emergency services etc.

Semantic Interoperability Issues

- In Internet of Things framework, it becomes imperative for the providers and requestors to communicate meaningfully with each other despite the heterogeneous nature of the underlying information structures. This is termed as semantic interoperability.

- Semantic interoperability can be achieved in a multitude of ways:
  - **Development of a comprehensive shared information models** can facilitate semantic interoperability among the participant applications and businesses.
  - It can also be achieved by **providing appropriate semantic mediators (translators)** at each participant's end, to facilitate the conversion of the information format which the participant understands.
  - Most often systems use a **combination of context independent shared information models**, coupled with **context specific information specialization** approaches to achieve the semantic interoperability.
  - By use of semantic mediators

Semantic Interoperability- Standardization Efforts

- Initiatives such as **International Standard for Metadata Registries (ISO/ IEC 11179)** and implementation of it, such as the **Universal Data Element Framework (UDEF)** from OpenGroup aim to support semantic interoperability between structured data.
- Semantic web based standards from W3C such as **DAML (Darpa Agent Markup Language)**, **RDF (Resource Description Framework)** and **OWL (Ontology Working Language)** are useful in providing semantic foundations for dynamic situations involving dynamic discovery of services.
- The standardization effort towards achieving semantic interoperability should involve development of standardized semantic data models and ontologies, common interfaces and protocols, initially defined at an abstract level, then with example bindings to specific cross-platform, cross-language, technologies, such as XML, ASN.1, web services etc.
- Standards are required for bi-directional communication and information exchange among things, their environment, their digital counterparts in the virtual clouds and entities that have an interest in monitoring, controlling, or assisting the things.

Interoperability in Medical Devices

- CIMIT (Center for Integration of Medicine and Innovative Technology) initiated a program in 2004 to lead the development of open standards for medical device interoperability.

- It supports:
  - Clinical decision support systems
  - Smart medical alarms
  - Medical device safety interlocks
  - Closed-loop control of medication delivery
  - Remote healthcare delivery (home, battlefield, e-ICU etc.)
  - Complete, accurate electronic medical records
  - Hospital emergency preparedness
  - Increase quality and completeness of research databases

Security and Privacy Issues

- **Security and Privacy** → security technology that will make trust lifecycle management intuitive and hidden from the user.

  - **Communication security (end-to-end)**
    - Resilience to attack
    - Data authentication
    - Access control

  - **Privacy of communication and user data**: A number of technologies have been developed to achieve information privacy goals. Some privacy enhancing technologies (PET) are:
    - Integrating policy-based release of data
    - Virtual Private Networks (VPNs): impractical beyond the borders of the extranets.
    - Transport Layer Security (TLS): as each ONS delegation step requires a new TLS connection, the search performance will be affected by introduction of additional layers.
    - DNS Security Extensions (DNSSEC):
    - Onion Routing
    - Private Information Retrieval (PIR)

  - **Trust and Reputation framework**
    - TPM
    - TCG

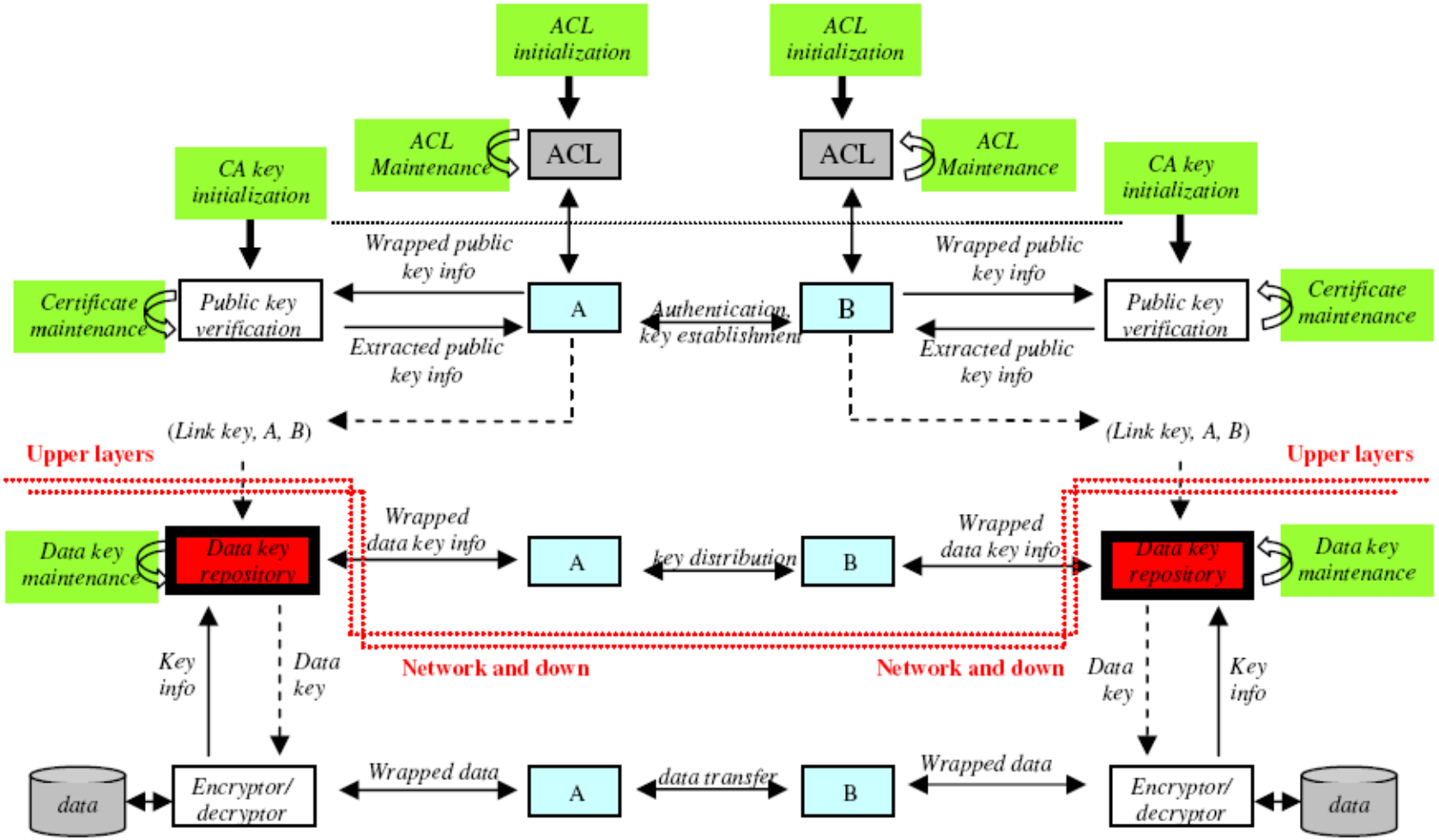
Deployment Scenario vs. Security Design

- Diverse deployment scenario:
  - Home automation:
  - Building automation:
  - Urban settings:
  - Industrial controls:
  - ZigBee, Internet of Things, Smart Grids etc.

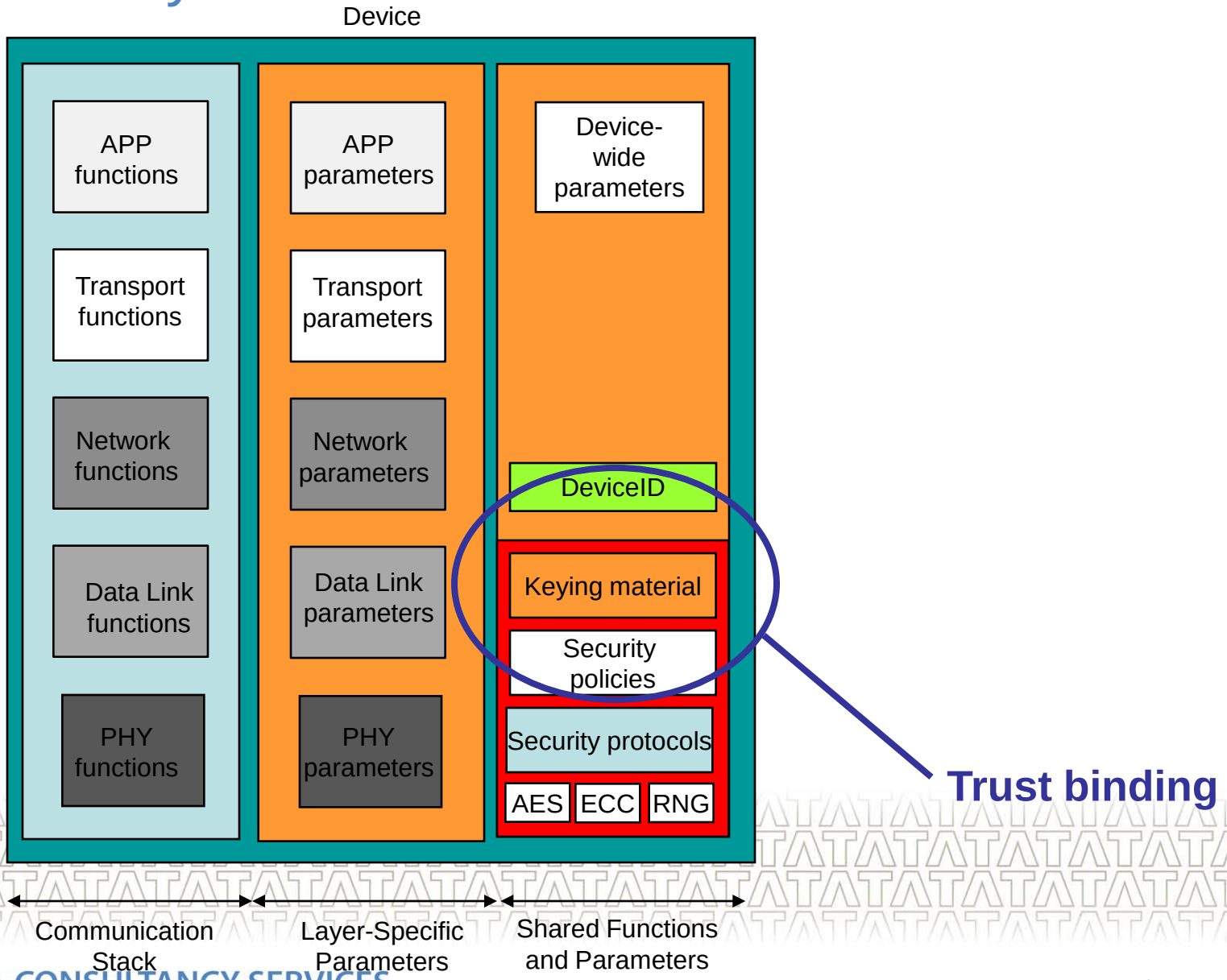
- The security design should fit into these diverse deployment scenarios:
  - Concise set of cryptographic and security mechanisms.
  - Single security policy framework
  - Configuration parameters policy-dependent.

- This may require consideration of system perspectives, taking into account the entire system and device lifecycle, ease-of-use and ease-of-deployment.

A Security Architectural Framework



A Security Architectural Framework



Device and System Management Issues

- **Device and System Management**

  - **Self-configuration management framework**:
    - Intelligent embeddable processing and communication devices are needed to facilitate nodal functionality, including developments to support automated network management, self-configuration and self-repair.
    - Middleware and other software developments required including intelligent processing platforms to support IoT functionality and services design.

  - **Device discovery:**
    - IoT will consist of many distributed resources including sensors and actuators, as well as information sources and repositories. It will be necessary to develop technologies for searching and discovering such resources according to their capabilities (type of sensor/ services offered), their location and/or the information they can provide (e.g. indexed by the unique IDs of objects, transactions etc.).
    - Universal authentication mechanisms will be required together with granular access control mechanisms that allow owners of resources to restrict who can discover their resources.
    - For efficient search and discovery, metadata and semantic tagging of information will be very important. Large volume of data will pose a significant challenge.

Device/Object Identity-Related Issues

- Device/ Object Identity

  - Ubiquitous unique ID for Things (for addressing, ownership, information association and security):

  - Object Naming System (ONS): In EPC standards, the “things” carry RFID tags with a unique EPC. The infrastructure can offer and query EPC Information Services (EPCIS) both locally and remotely to subscribers. The information is not fully saved on an RFID tag, but a supply of the information by distributed servers on the Internet is made available through linking and cross-linking with the help of ONS. ONS is based on the well-known DNS.

Device/Object Identity-Related Issues

- In the vision of IoT, things have a digital identity (described by unique identifiers), identified with a digital name and the relationships among things can be specified in a digital domain.
- A unique identifier for an object can translate to a single permanent assigned name for the life of an object.
- However, there may be need to accommodate multiple identifiers per object, as well as changes to those identifiers. For example, many objects will have a unique identifier assigned by their manufactures. Some may have network addresses (IPv6), as well as temporary local identifiers within transient ad-hoc clusters of objects.
- Sensors and actuators attached to objects will be individually addressable; their identifiers may be constructed as extensions of the ID of the object or perhaps associated with the object's identifier via a lookup in a registry.
- Combinations of things will create "family of tree" identification schemes.
- It is important that identifiers are not constrained by current choices of technology for storing and communicating unique identifiers or their current limitations, since data carrier technology will evolve.
- Interoperability is required between applications using different identification schemes when those applications are operated in Future Internet.

Regulatory Issues

- Regulatory Issues
  - Spectrum usage
  - Mitigation of out-of-band interface
  - Power control

Application Deployment Issues

- Application Deployment Issues
  - Industry domain specific requirements
  - Generic framework/ Middleware for application and service deployment
  - Service oriented architectures for publishing, discovery and subscription of services

Different Industry Vertical Specific Use Cases

- Education
- Healthcare
- Home
- Supply chain
- Transportation
- Energy and Utilities
- Manufacturing and Process Industries
- .....

Proposals of Deliverables

- Identifying the technology gaps in IoT standardization and possible areas of contribution.
- Collection of requirements from Indian perspective of IoT
- Collection of requirements on handling intra- and inter-domain interoperability, security, privacy and trust management issues.
- Preparation of the initial proposals on IoT standardization on protocol and semantic interoperability, security, privacy and trust management issues.

Internet of Things: Team Organization

Chair : Debasis Bandyopadhyay

Vice-chair: Arpan Pal

Rapporteur of deliverables: To be confirmed

Related GISFI Groups

- Spectrum
- Security and Privacy SIG
- Green Energy

Related Standards

- ETSI
- IETF
- W3C
- CASAGARAS
- EPC Global

Environmental Aspects

- Internet-of-Electrical Things (an Internet connected home or workplace that interconnects all the energy appliances) can lead to significant energy savings in terms of energy visualization, appliance control and dynamic pricing.