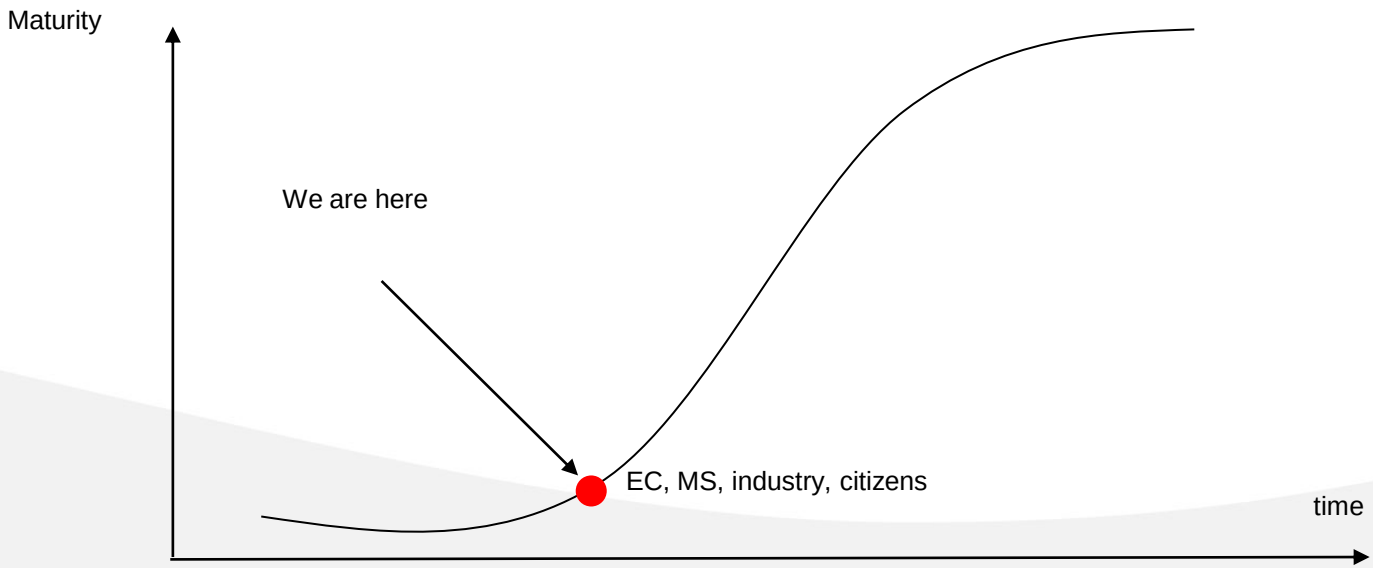
Building a Trust Framework for Future Internet Services and Infrastructures

Amardeo Sarma, NEC Laboratories Europe

TDL | Trust in Digital Life

TDL | Trust in Digital Life

Current state of things



We are still in the early stages of the digital society

Trustworthy ICT will be a key enabler

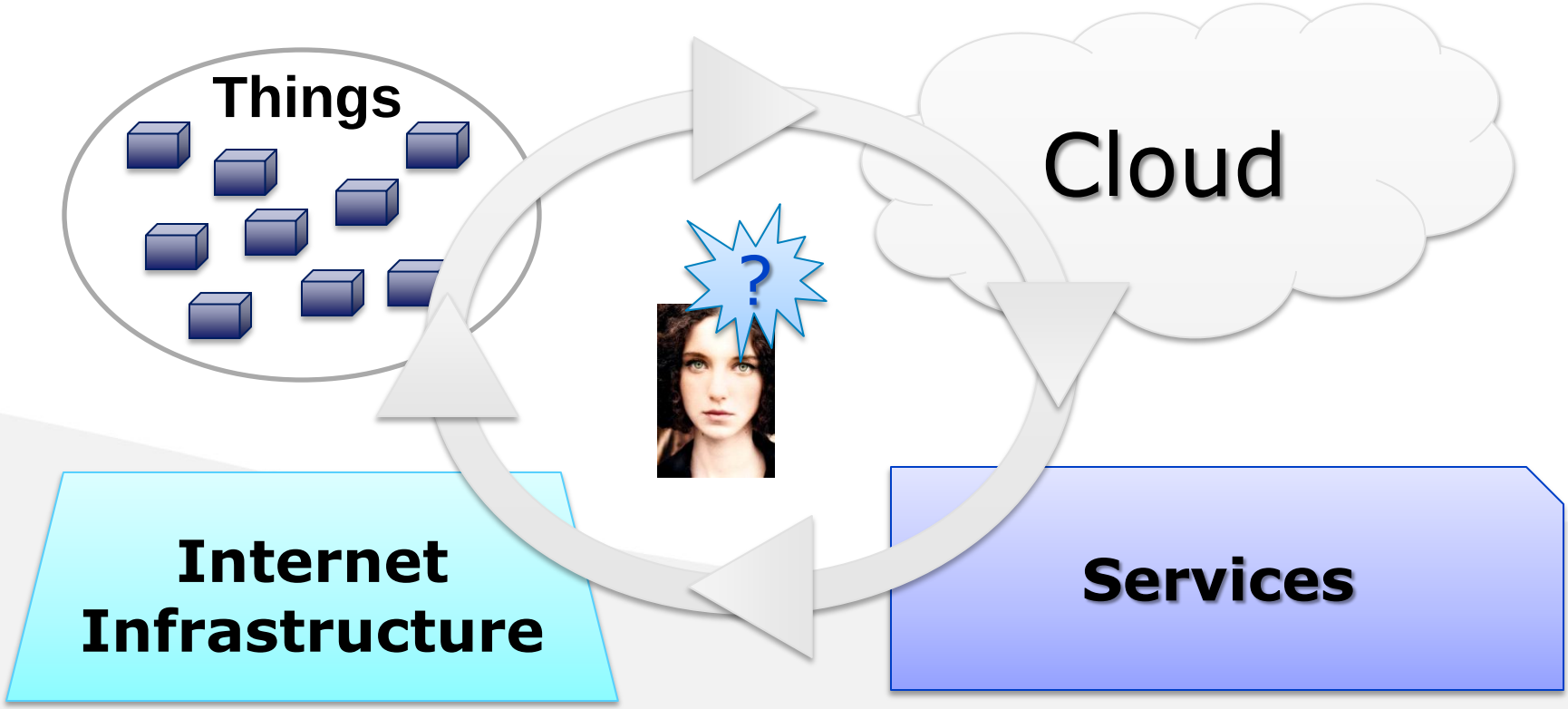
TDL | Trust in Digital Life

Understanding Trust

- Reliance on the character, ability, strength, or truth of someone or something (Webster)
- Elements of trust according to Wikipedia
  - the willingness of one party (trustor) to be vulnerable to the actions of another party (trustee);
  - reasonable expectation (confidence) of the trustor that the trustee will behave in a way beneficial to the trustor;
  - risk of harm to the trustor if the trustee will not behave accordingly; and
  - the absence of trustor's enforcement or control over actions performed by the trustee.
- A fundamental societal challenge, understanding that
  - We need a combination of **policy, technology, legislation** to protect the tangible and intangible assets of citizens and enterprises

TDL | Trust in Digital Life

Trust in Digital Life



TDL | Trust in Digital Life

Some key issues

- We need to ensure end-to-end trust across applications, services, systems or devices
  - Crosses usage areas, services, systems and infrastructures.
  - Involves technology and solution operators, service providers and software developers.
- Trust frameworks need to go beyond trusted systems and include those that use, operate, or access it.
- Need to deal publication, discovery, composition and management of trustworthiness enabling multiple Levels of Assurance (LoA) for different end-to-end environments and application scenarios towards a **continuum and total trust management**

TDL | Trust in Digital Life

Dimensions of Trust

- **Network-centric trust**, dealing with autonomic networks and their behavioral models, in terms of compliance/conformance to operator and service strategies.
- **Component-centric trust**, dealing with software components, services and their respective security aspects.
- **User-centric trust**, dealing with authentications, identity management, operational issues, socio-economic and psychological factors, vendors, end-user, etc. assuming a growing number of stakeholders

TDL | Trust in Digital Life

Questions

- Question 1 – Which is the failure/threat/attack model that should be considered in designing an autonomous infrastructure, system or service targeting "trust erosion"? What needs to be protected?
- Question 2 – What is the end-to-end trust model? How is "transitive" or "modular" trust modeled, designed and which trust mechanisms are applied in your domain? (To address/solve Q1) – Are there agreed or useful metrics or characteristic information on the current reliability and assurance level of a specified service and infrastructure component? Are these different for critical and non-critical environments?
- Question 3 – How to describe/communicate/discover/translate trust framework elements or what to communicate to enable end-to-end trust interworking and interoperability (e.g. across user/application/service/network)?
- Question 4– Is trust and trustworthiness an element to consider only at the design-time or run-time?
- Question 5 – What actions should be taken towards certification, standardization or regulation, which research directions or seeds should be fostered?
- Question 6 – What is new, unsolved, changed by the introduction of software and autonomic systems (less human in the loop) in telecommunication infrastructures and processes? Which introduction/migration/transition path(s), and technical/business incentives should be considered and developed?

www.trustindigitallife.eu

TDL | Trust in Digital Life