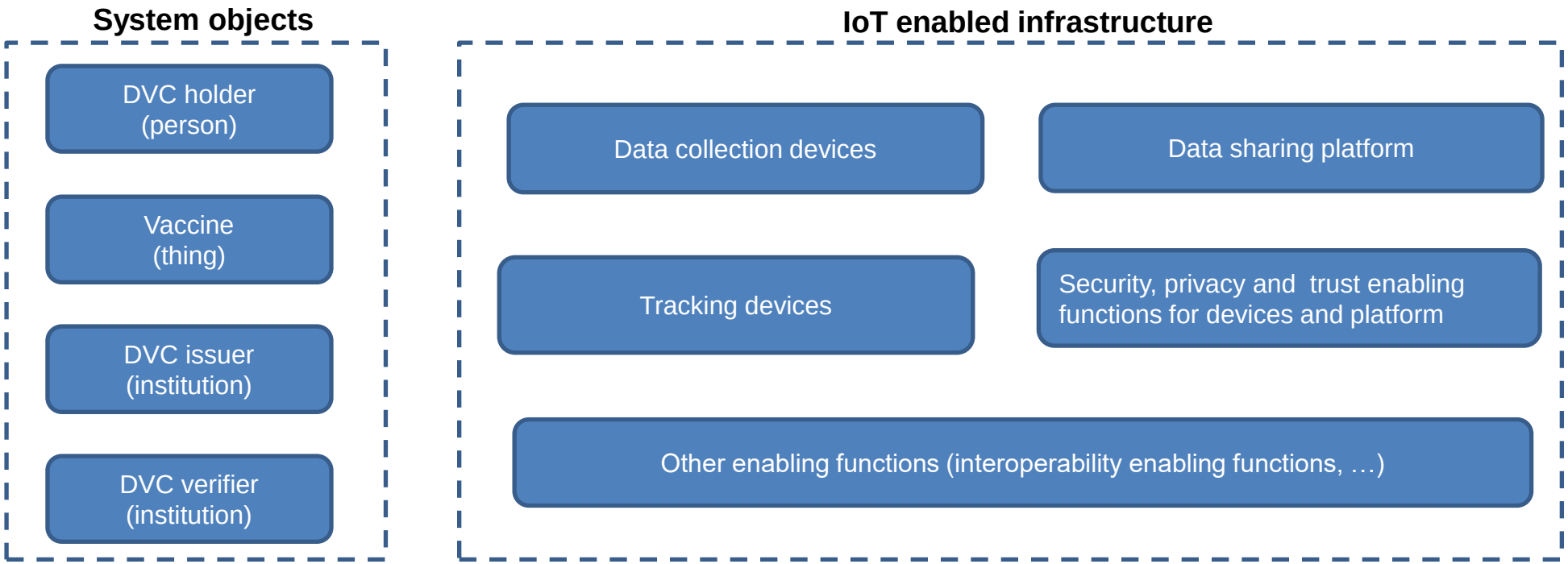
Standardization related considerations on digital vaccination certificate from an Internet of Things perspective - ITU-T SG20 input

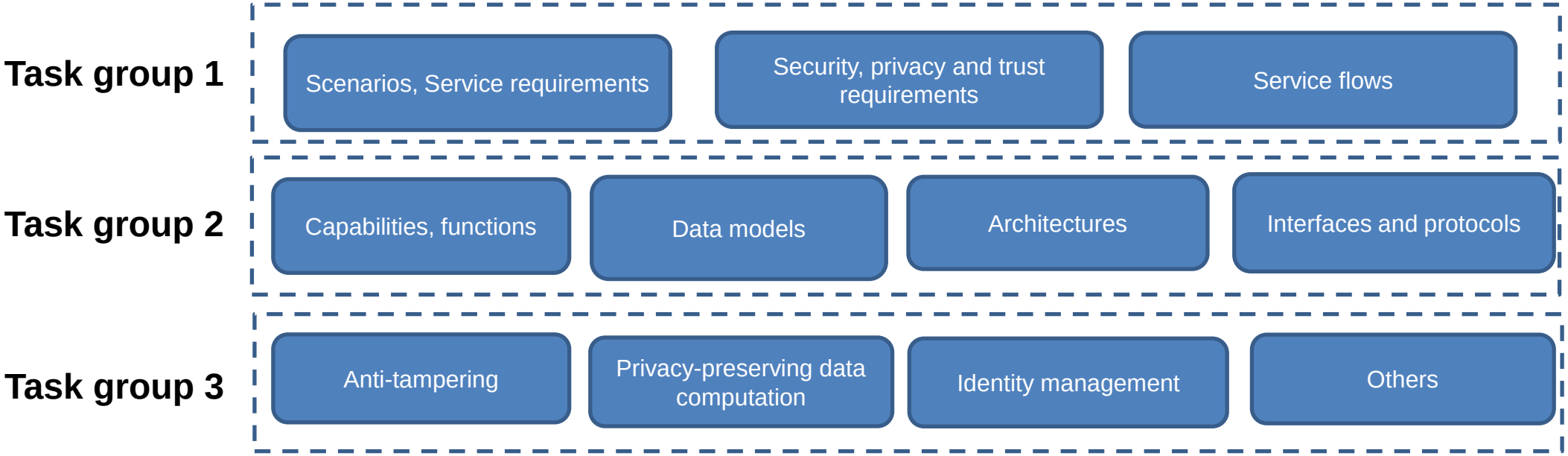
A digital vaccination certificate supporting system from an Internet of Things (IoT) perspective

Key elements of a DVC supporting system



DVC: digital vaccination certificate

Standardization related tasks - ITU-T SG20 considerations as starting point for discussion



Standardization task group 1: scenarios, service requirements and service flows

- To identify scenarios, service requirements and service flows related to DVC holder, DVC issuer, DVC verifier and Vaccine
  - Scenarios and service requirements may include but are not limited to
    - Description of the different system objects and their service relationships
    - Service requirements for the system objects
    - Existing scenarios of devices and system infrastructures used by the system objects (it is recommended to describe mobility aspects, data flows, data sources, data sizes, data transmission frequencies, volume of involved devices, other)
  - Service flows may include but are not limited to
    - Service flows among the system objects
    - Devices, platforms and other facilities which may be used to support the foresaid service flows
- Key: to identify the security, privacy and trust requirements
- Key: to identify the different challenges (technical, other)
  - Faced by scenarios
  - Faced by devices, platforms and other facilities

NOTE: it is expected that at least Administrations and DVC service providers be involved in this task group.

Standardization task group 2: IoT enabled infrastructure

- To identify IoT enabled capabilities and functions for support of DVC
- To specify IoT enabled data models for support of DVC
- To specify IoT enabled architectures for support of DVC
- To specify IoT enabled interfaces and protocols for support of DVC

NOTE: it is expected that ITU-T SG20 (but not limited to) be involved in the IoT enabled infrastructure standardization activities

Standardization task group 3: security, privacy, trust and other enabling functions

- To specify security and privacy enabling functions
  - Privacy-preserving data computation
- To specify trust enabling functions
  - Anti-tampering
- To specify other enabling functions
  - Identify management (for interoperability)

NOTE: these tasks are appropriate for (at least) the Standardization Expert Groups on Security.

For information: ITU-T SG20 ongoing activities

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

Thank you!

Email

tsbsg20@itu.int

Website

www.itu.int/go/sg20