Context & associated issues:

The emerging Internet of Things (IoT) is expected to host billions of devices that regularly report sensor readings by using long or short-range radio channels. Generated content items and also collateral metadata are not well protected today because (i) channel encryption is commonly intercepted at gateways, (ii) identifiers reveal communication partners and contexts, and (iii) cryptographic protection embedded in the low-end transmission infrastructure remains too weak to resist attacks.

Challenges & Technological Barriers:
Most research in IoT focuses on ensuring Channel Security i.e. securing the communication path between two entities at the transport layer. In most cases in IoT, the communication is not end-to-end secured and the channel encryption is intercepted by a gateway to transition between the end-device (i.e. sensors) and the endpoints (i.e. the Cloud infrastructure). Hence, the data associated with the communication which is not encrypted, such as the identifier, the context and additional metadata are revealed during this transition process. The **first challenge** is that this associated metadata should not be exposed and that we want to minimize the information (personal data or other) that can be inferred from it.

It is very difficult to deploy classical cryptographic algorithms to secure channel as well as to object security in IoT due to its constrained nature. The **second challenge** is to scale down algorithms and protocols that could function in components operating at few MHz, Kbytes and packets per hour.

To ensure security and privacy, there exists Pre-Shared Key symmetric cryptography. But, in order to operate in a dynamic manner, and use asymmetric keys, a trust anchor is required. How to have a decentralised trust anchor that resembles the Certificate authority model on the Internet for IoT is the **third challenge**?

Cryptographic Keys are always associated with an identity. On the Internet, the identifiers are either IP addresses or domain names which are governed by a well defined and structured mechanism. In the IoT, there are different identifiers and governance mechanisms. The **fourth challenge** is to design a global and scalable multi-stakeholder namespace management.

Approaches to solve the technological challenges:

PIVOT will advance open protocol standards used on the Internet to enable an integrated content object security model for IoT communication. For this goal, we will leverage IoT specific standards such as CoAP/OSCORE. We will also explore content-centric clean-slate approaches that are part of the Future Internet Initiative.

PIVOT will analyse interdependencies between different stakeholders in the DNS and PKI ecosystem to derive a minimal set of trust anchors. Following these insights, we will be able to model trust chains, identifying multiple trust anchors and cross-certified trust anchors.

Host-based networks operate on a well-defined namespace such as domain names, which are provisioned and resolved based on the Domain Name System (DNS) infrastructure. PIVOT will require a naming system for content objects, which remain decoupled from individual hosts.
With experience in namespace management gained by the consortium members from the DNS ecosystem, we plan to transform the existing structures and overcome the technical and organisational challenges in content-based networking. We also plan to study NDN (Named Data Networking) based on DNSSEC (Domain Name System Security), with the ambition of joint deployment in the current Internet.

To analyse the operational feasibility of the proposed design and protocols, we will build a crypto toolbox and integrate it in the RIOT OS. A demonstrator based on RIOT will verify our solutions in ultra-constrained IoT networks such as LoRaWAN.