Cataldo Basile, Diego R. Lopez
Politecnico di Torino, Telefónica

I2NSF meeting,
Berlin,
July 21st, 2016
Introduction: the context

- policy enforcement
  - example 1: what policy can I enforce with the NSFs in the network, given their topological arrangement?
  - example 2: what NSFs should I use and with what topological arrangement if I need to enforce these security requirements?
- the question: what a NSF can do for policy enforcement?
- capability: the policies a NSFs can enforce
  - regardless of the customer and provider interfaces
    - abstract but with clear semantics, not only flexibility
    - vendor-independent core, not only custom controls
- Capability Model based on an abstract model of policies

The proposed Capability Model

- **actions**
  - what a NSF does on packets/traffic/PDU (e.g., deny, encrypt)
    + related actions (e.g., logging)

- **conditions**
  - how the NSF determines on what actions will be applied
  - fields in packets/PDU, stateful info acquired by the NSF
  - what operations available to verify condition truth (matching)

- **other parameters to complete the policy specification**
  - resolution strategy, e.g., First Matching Rule + external data
to take decisions + default action, if fixed or configurable

- **templates and algebra of capabilities**

- **events supported as native element or types of conditions**
Relations with other capability models

- complementarity with Xia’s capability model
  - draft-xia-i2nsf-capability-interface-im-06
- will be merged in a single draft