# KER 6: Enforcement & Dynamic Config

## UNIQUE VALUE PROPOSITION

**Component architecture tailored to supply chains needs focussing especially to regulatory obligations (e.g., GDPR) and violations/compliance of service level agreements**

# KER 6: Enforcement & Dynamic Config

## SOLUTION BENEFITS

### SUPPORT FOR NEW SECURITY DEVICES

A capability model empowers the core of the EDC, allowing an administrator to add support for new types of security controls with ease. Adding new security devices is performed by describing what they offer (e.g., this device is a stateful firewall, supports traffic rate- limiting) without writing ad-hoc code logic

### QUICK & EASY NETWORK DESCRIPTION

The use of a high-level policy language grants the administrators the ability to quickly and easily describe what the network functionalities are in a way closer to the human language, without worrying about their actual implementation, which is demanded to the EDC itself

### PHYSICAL AND VIRTUALIZED SECURITY CONTROLS

The EDC seamlessly supports both physical and virtualized security controls and allows the administrators to configure mixed networks containing both types of devices

# KER 6: Enforcement & Dynamic Config

## INNOVATION SCOPE

### INNOVATION

Framework leveraging a capability model instead of the traditional refinement techniques based on logic rules, making use of a highly flexible security capability model and an inferential engine to smartly refine high-level policies into low-level configurations.

### PROBLEM

Correctly configuring network devices (particularly security controls) is a critical and, unfortunately, error-prone task, especially regarding the modern SDN-based infrastructures. An administrator must be aware of the entire network topology and the device configuration rules to avoid catastrophic mistakes, while the network size and heterogeneity keeps growing.

### SOLUTION

Technology allowing an administrator to effortlessly configure various security controls (e.g., a firewall or a VPN terminator) through high-level declarative policies that are automatically translated into a series of optimal low-level configurations.

### VALUE

Adding a new NSF type requires only describing its capabilities using a very simple model. Its innovative refinement process will consider the current network landscape topology and its configurations to avoid inconsistencies and issues in the deployed rules.

# KER 6: Enforcement & Dynamic Config

## EARLY ADOPTERS

### FARM 2 FORK

The EDC decides the banning of specific IPs and blockchain wallet IDs when these are issuing an attack (defined by a predefined rule set by the system operator through the IRO). Other similar policies may be defined based on the specifics of the IT solutions in place.

### SMART FACTORIES

This component implements security policies to mitigate risks, attacks or intrusions detected, applying security configurations when a non-compliance situation is detected.

### CONNECTED AUTOMOTIVE

This component is mainly used to apply security policies on the infrastructure to mitigate possible risks, attacks or intrusions detected, providing security configurations when any security policy is not complied with.