Customer Case:
Secure distributed processing for Smart Cities & Intelligent Transport Systems with RTI DDS and ObjectSecurity OpenPMF 4.0

Today, most smart cities and intelligent transport systems are implemented in a very centralized way: Sensors send their data to a central control center, where all data is processed at in the same place and control signals, for example for traffic signs are generated. This very centralized approach is not efficient and does not scale well. In a city wide parking management system, the central server does not need to know which individual parking slots are available – all it needs to know is the occupancy of a parking site as a whole.

Secure distributed system design.
Therefore, a secure distributed system processing local data locally and only sending preprocessed data to a central control center is much more appropriate. It also much better reflects the hierarchical structure of transport systems from a local level over a city municipal and regional level to a national level.

Build it and protect it.
But despite all these advantages, the development of such highly distributed, large scale and geographically dispersed systems raises two main challenges: firstly, how to build such a demanding system at all; secondly – but equally importantly – how to protect the now highly distributed and geographically dispersed systems with many nodes at different places.

Stringent data protection standards: OpenPMF™ 4.0

For the protection of the ICSI intelligent transport system and for meeting Europe's high stringent data protection standards, the innovative **OpenPMF 4.0 Security Policy Automation Platform** of project partner ObjectSecurity was used.

OpenPMF allows the i**ntuitive authoring of rich, but human-understandable policies** driven by operational and regulatory security and data protection requirements.

From these policies, OpenPMF automatically **generates the matching technical security enforcement** for "defense in depth" across many systems and technology layers.

"Using RTI Connext DDS and ObjectSecurity OpenPMF, you can build secure and complex distributed applications much more easily. You can concentrate on your business, the development of the application itself, and do not need to think about all the little technical details. So we were able to build two innovative systems in a short time frame."

- Elena Cordiviola, Intecs, ICSI coordinator

"Using OpenPMF 4.0, we were able to enforce rich and adaptive access control policies across ICSI's distributed IoT landscape. OpenPMF 4.0 lets ICSI users author intuitive IoT policies such as 'non-government organizations assigned to an accident site can only view live CCTV feeds from that accident site'. OpenPMF 4.0 automatically turns such policies into the matching technical enforcement across all affected systems."

- Ulrich Lang, CEO, ObjectSecurity

More information:

objectsecurity.com
@objectsecurity
info@objectsecurity.com