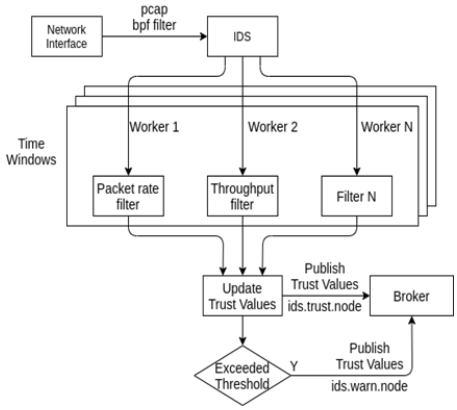
IntellIoT component available for OC #2 integration – Details

Name	IDS
Responsible partner(s)	Telecommunication Systems Institute (TSI)
Brief description	The **Trust-based Intrusion Detection System (Trust IDS)** is a decentralized application that monitors network traffic. Each instance creates a trust value for each node that it communicates with, based on the observed network activity and how this is classified (as acceptable/normal or potentially harmful). When the trust value for a node drops below a threshold, it generates a warning. These warnings are propagated to security components responsible to determine if an action is needed and which mitigation process should be triggered.



Interfacing (I/O)	The Trust IDS instances use the RabbitMQ message broker to publish their local trust values for the nodes they are communicating with along with warnings for offending nodes. These values are accessible for the SAP/MTD to consume.
Main interactions	The Trust IDS publishes events through the RabbitMQ message broker. Transmission of trust values directly to: MTDs, SAP. Deliverable D2.6, subsection 2.2.3, provides more details regarding main component interactions involving Trust-based IDS.
Deployment	It is deployed as Docker container for both x86-64 and AArch64 targets. It requires elevated access privileges for network interface packet sniffing.
Licensing	Proprietary
Deliverable references	Please refer to deliverable **D2.6 – "High level architecture (final version)", subsections 2.1.3, 2.2.3, 2.3.3 & 2.4.3**, for more details regarding interfacing & integration of Trust-based IDS and other trust components & deliverable **D4.4 – "Trust mechanisms (first version)", section 2**, for more details on the design and development of the component.

ICT-56-2020 "Next Generation Internet of Things" Grant
Agreement number: 957218