



# Safe Human Robot Interaction in Automated Assembly Lines

**Reyan Korel Erben, Karthik Shenoy Panambur**

BIBA – Bremer Institut für Produktion und Logistik GmbH - Germany

**Review meeting**

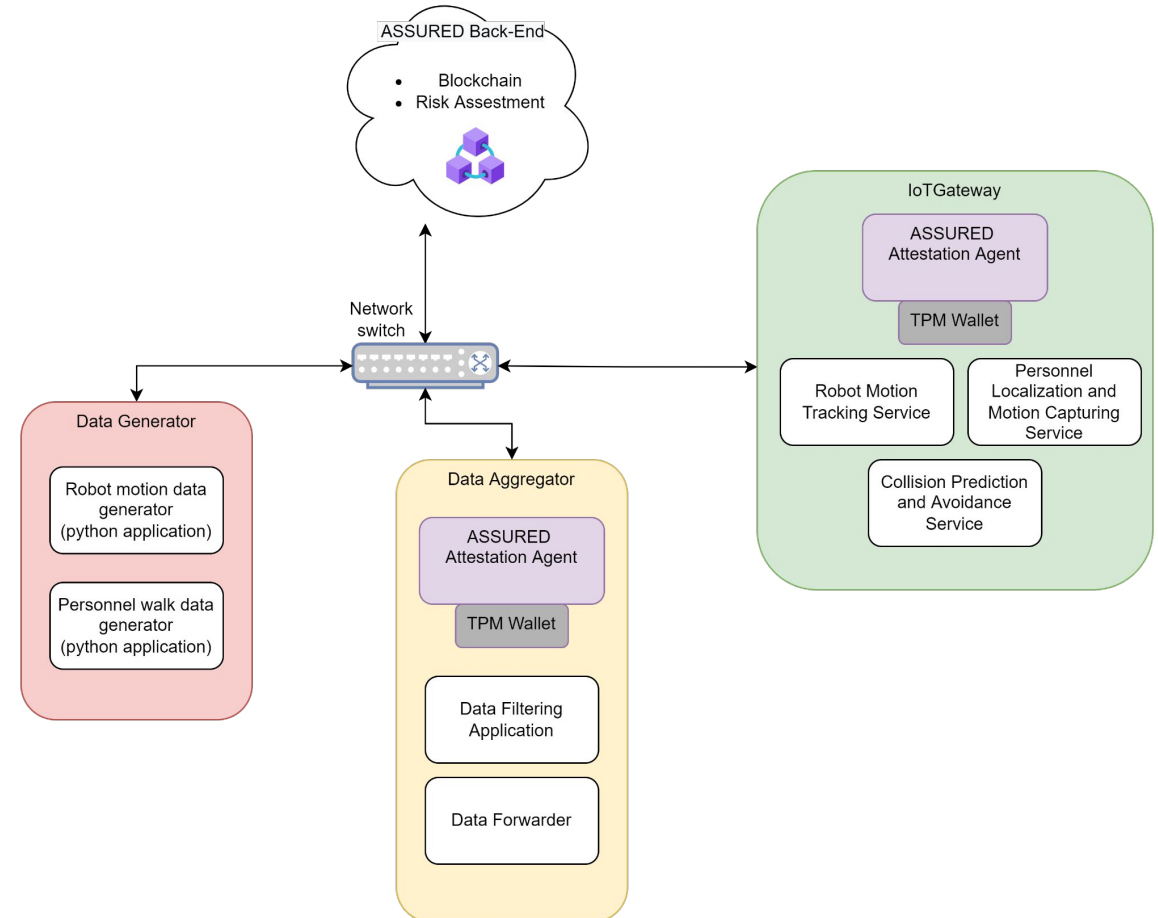
*Online | 27 April 2022*

[www.project-assured.eu](http://www.project-assured.eu)

# Demonstrator Overview

- Two components:
  - Data aggregation and forwarding.
  - Processing of the collected data.
- Data Aggregator:
  - Collects the generated data, apply filtering and forwards to the IoTGateway.
- IoTGateway:
  - Processing of the motion and location data.

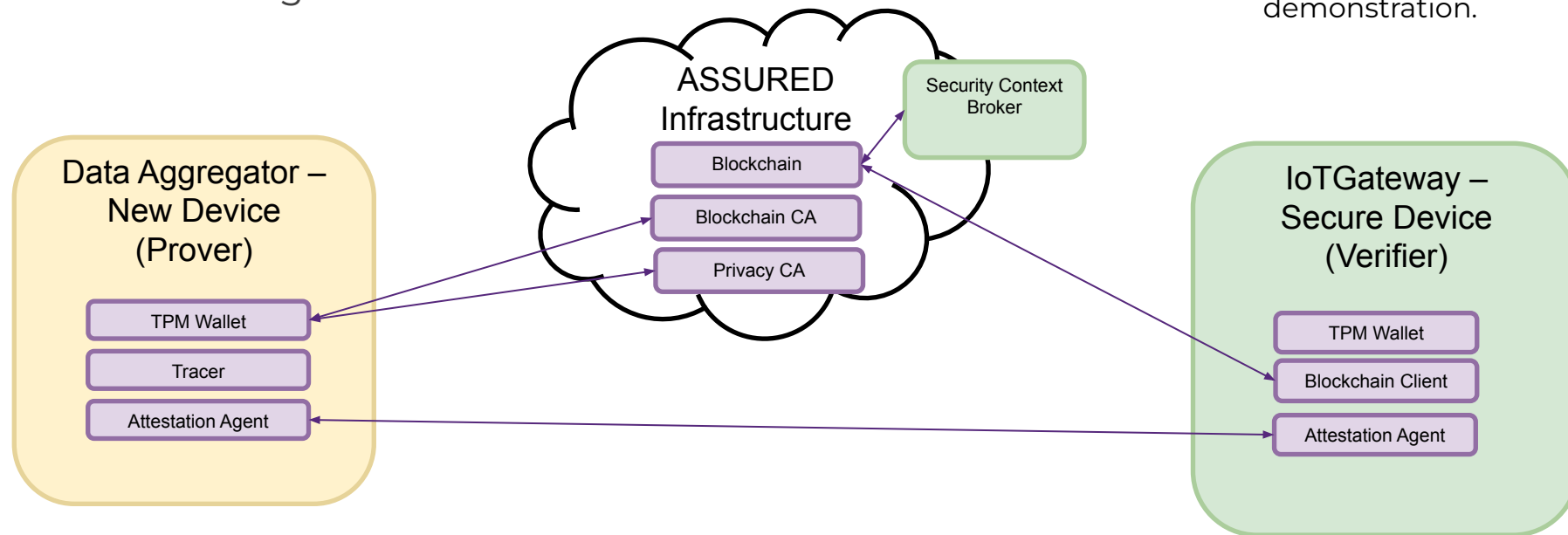
Both components must be secured by ASSURED framework to enable safe HRI.



# Demonstrator Overview

- Breach of the security of the devices can result in harm to collaborating humans.
- Goal: Achieve security by only allowing trusted devices to be used in the application, through ASSURED Secure Enrollment.
- Demonstration: Enrolling a new trusted device.


Note: Security Context Broker is showcased at the IoTGateway for this demonstration.



- Verifier queries the **Blockchain** and receives the **Device Enrollment Policy** and the **challenge nonce** that will be used for secure enrollment of the new device.
- **Verifiers attestation agent** sends a request to initiate secure device enrollment with the **challenge nonce**, that is signed with **verifiers attestation key**, to the **provers attestation agent**.
- Prover will successfully enroll by:
  - **Creating DAA Attestation Key (AK)**
  - **Register with Privacy CA**
    - For certifying the correctness of the underlying TPM and also for activating the AK
  - **Retrieve Authorized Policy from Blockchain CA**
    - Retrieve the “digest list” with all of the hashes representing the correct configuration of the binaries that are expected to be installed on the new device (RabbitMQ and REDIS DB) so as to create the appropriate key protection usage policies
  - **Handle and Respond to Challenge Credential from the Privacy CA**
    - Verification that the AK was binded to correct authorization policies - policyPCR (link to a specific device state) and policySigned (AK to be used only for signing traces originating from the authentic Tracer)
  - **Successfully Respond to Challenge to obtain Credential**
    - Receive back a token verifying the correct creation of the AK and validation of all system attributes
  - **Successfully Obtain Blockchain Keys**
    - Forward token to the Blockchain CA for securely retrieving the Public-Private Key pair for later on-chain interactions
    - Also register ASSURED TPM-based Wallet to the Blockchain CA for issuing Verifiable Credentials (second release)
  - **Use Attestation Key to sign Verifiers Nonce**
  - **Respond to verifier with details of the successful enrollment**
    - DAA Signature + anonymized credential to be verified - If verification succeeds, proof that the registration was done correctly since all keys were created under the correct policies
- **Verifier notifies blockchain about successful enrollment**
  - Records the result on the ledger

# Demonstration

ASSURE



**SMART  
MANUFACTURING**

SAFE HUMAN-ROBOT  
COLLABORATION IN  
AUTOMATED ASSEMBLY LINES

**USE CASES: DISCOVER MORE »**





# Meet the consortium

ASSURE 





# THANKS



PROJECT-ASSURED.EU



@Project\_Assured



ASSURED project is funded by the EU's Horizon2020 programme under Grant Agreement number 952697