The FutureTPM project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 779391.

FutureTPM H2020 PROJECT:

WP6 - Activity Tracking Demonstrator

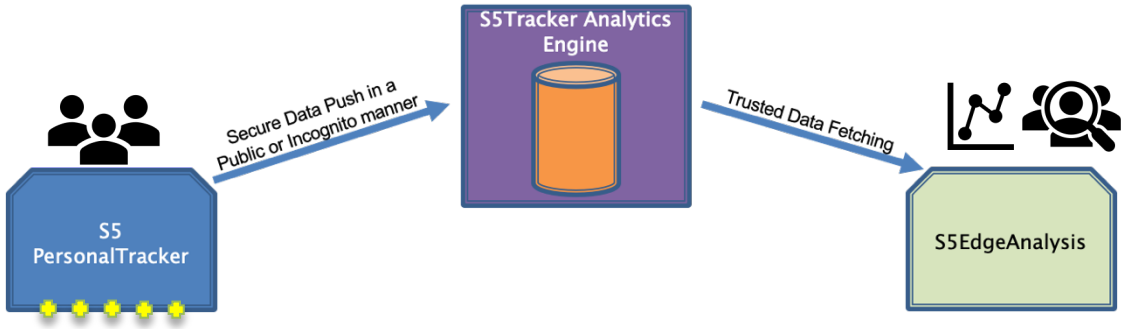
Dr. Sotiris Koussouris

Suite5 Data Intelligence Solutions Ltd
sotiris@suite5.eu

Final Review Meeting

Activity Tracker Overview

A Personal Data Analytics Engine that is handling personal data streams related to activities performed by individuals which are shared to business users.



- Upload to a trusted platform users' personal activity data
- Provide guarantees on the veracity of the data
- Share personal data with trusted parties
- Contribute anonymously for creating aggregate user profiles (Personas)

Information sources:
Wearables (FitBit, Garming, etc.), Smartphone Hubs (e.g. Google Fit, Apple Devices) and IoT devices (Smart Home sensors, etc.), Web2.0 social platforms (such as Facebook, Twitter, Google+, Instagram), as well as other smart devices that offer accessible APIs.

Why there is the need for (Future)TPM

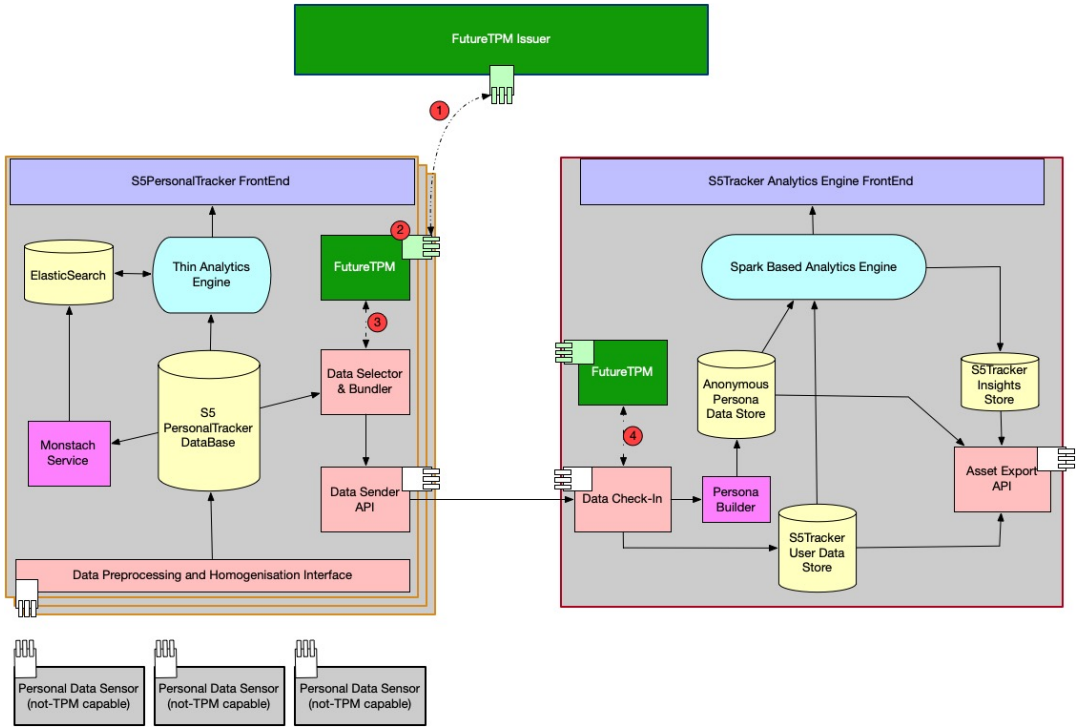
The S5Tracker Cloud Analytics resides in a cloud provider operating as a centralized infrastructure. Current approach is based on a simple central authentication scheme.

Need for improving data privacy (confidentiality) and trust!

FutureTPM provides a solution by:

- Reassuring users of the level of data privacy during data sharing — Privacy Guarantees
- Permitting only trusted stakeholders to exchange data — Increase level of Trust

Demonstrator Architecture



- S5.IU.1 - As an Individual User I want to provide authenticated data to the S5Tracker Analytics Engine, so that I can be served with user-specific services such as notifications send by the analysts
- S5.IU.2 - As an Individual User I want to provide anonymous and privacy-preserving data to the S5 Analytics Engine, so that data analysts can have a rich repository of activity data for exploration

V1 V2

LDAA
Lattice Based Direct Anonymous Attestation

1st Evalution Cycle (till M24)

- Refactoring of architecture for enabling QR-TPM methods
- Integration of the FutureTPM LDAA-v1 algorithm mechanisms in the overall architecture
- Testing and evaluation based on KPIs on a round of tests using different payload sizes
  - At Application Level
  - At TSS Level

Very high memory usage – necessity to truncate payload to be signed, to avoid halts

Necessity to use weaker security parameteres to refrain from system timeouts

LDAA Process sucessfull in allowing only trusted devices to provide data

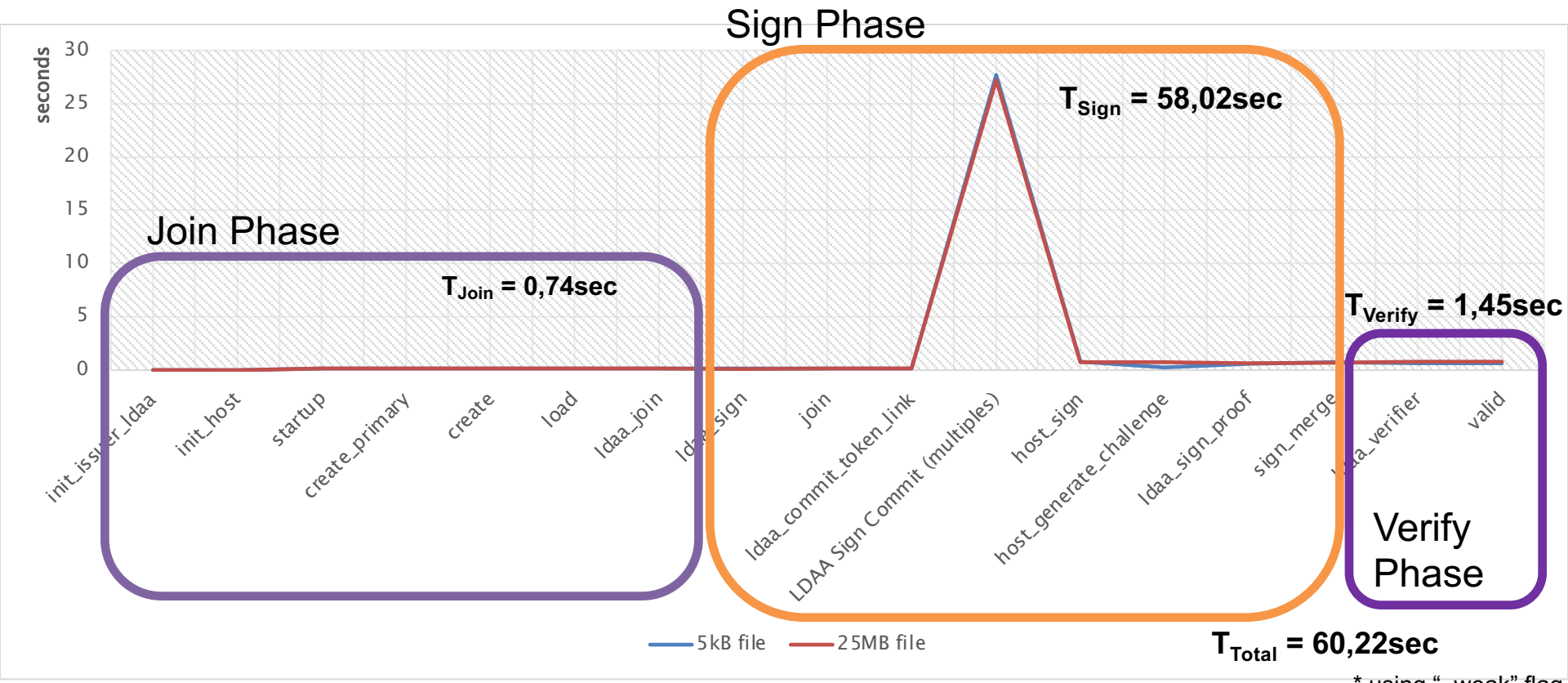
Join () and Verify () command evaluation produced **acceptable timing** results

Sign() command processes were introducing **significant/non acceptable delays**

Implementation Path

Results and Challenges Faced

LDAA-v1 Timings*



* using "–weak" flag

2nd Evalution Cycle (till M35)

- Refining Data management framework of the system to facilitate larger payload packages
- Refactoring of architecture for enabling the LDAA-v2 QR-TPM methods
- Testing and evaluation based on KPIs on a round of tests using different payload sizes
  - At Application Level
  - At TSS Level

Lower Memory Consumption – Payload does not need to be truncated

Application of strongest security parameteres possible

Join () command evaluation produced acceptable timing results yet longer than LDAA-v1

Sign() command processes (extrapolated) were highly satisfactory

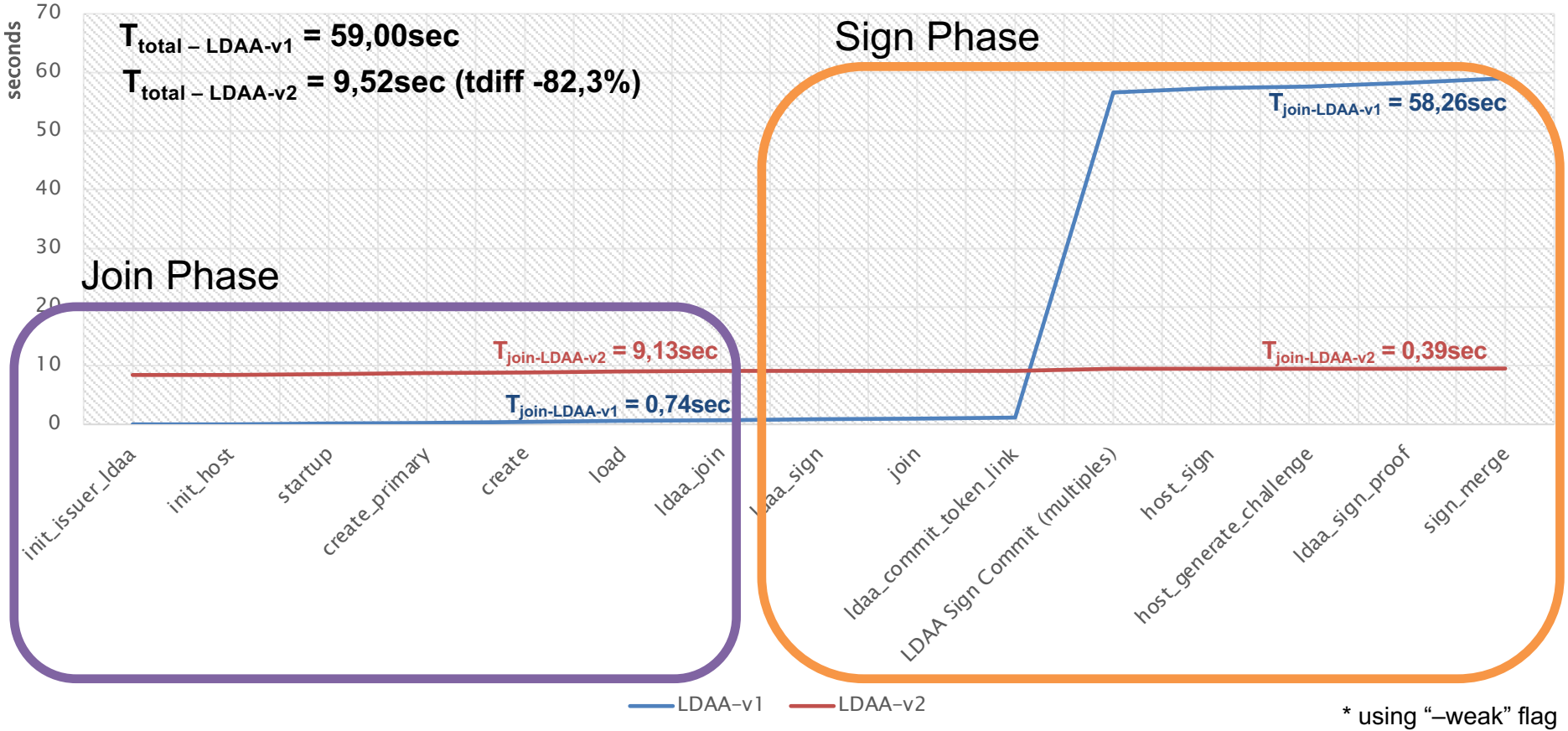
LDAA Process end-to-end not integrated (but was in standalone version developed by INESC-ID)

Implementation Path

Results and Challenges Faced

LDAA-v1 vs LDAA-v2 Join and Sign Phase - Total Execution Time*

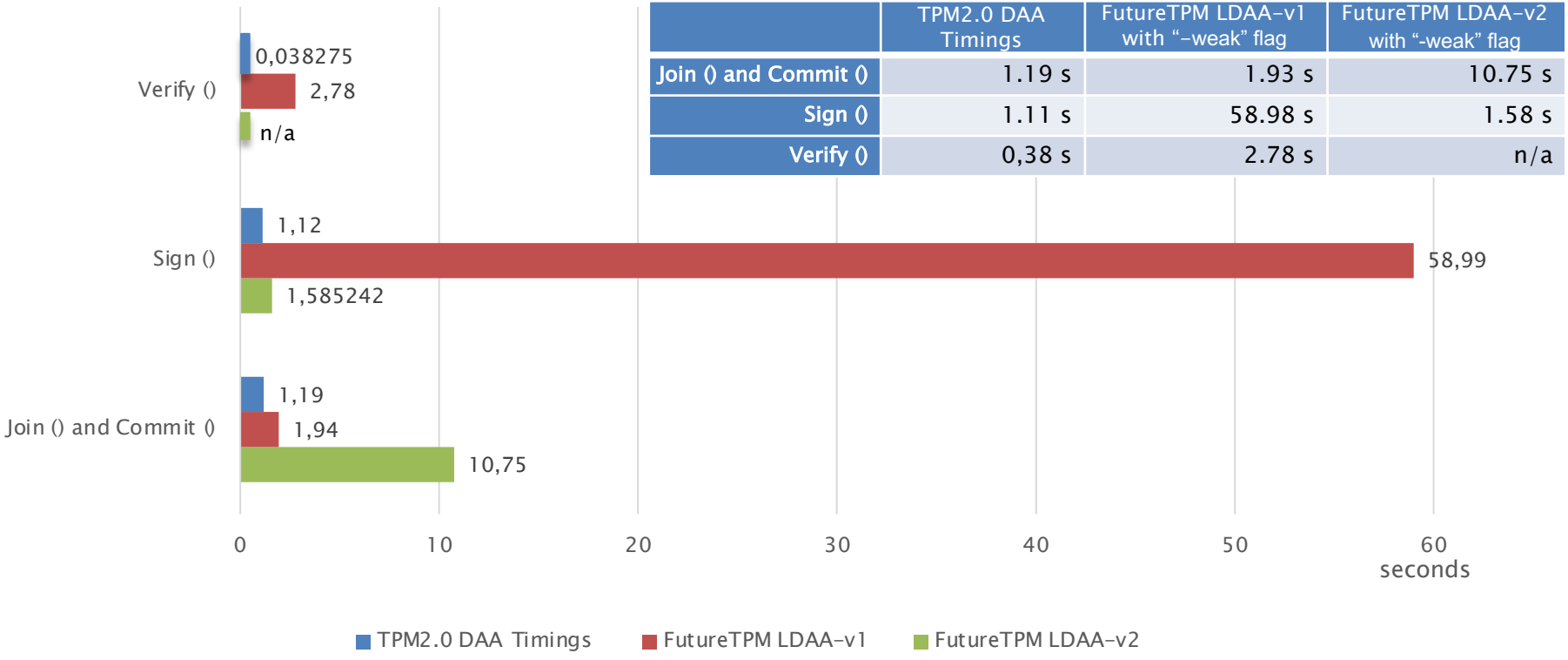
FutureTPM



* using "–weak" flag

Application Level Comparisons of Timings

	TPM2.0 DAA Timings	FutureTPM LDAA-v1 with "-weak" flag	FutureTPM LDAA-v2 with "-weak" flag
Join () and Commit ()	1.19 s	1.93 s	10.75 s
Sign ()	1.11 s	58.98 s	1.58 s
Verify ()	0,38 s	2.78 s	n/a



LDAA-v2 – Experimentation as Standalone Version

QR FutureTPM Public Key, Private Key and Signature Sizes LDAA*		
	TPM Memory – LDAA v1	TPM Memory – LDAA v2
Public Key	25	32,8
Private Key	24	65,7
Signature	624.000	1.300

QR FutureTPM Memory Consumption LDAA*			
	TPM Memory – LDAA v1		TPM Memory – LDAA v2
Persistent Memory	35.000	Join()	1.600
Versatile Memory	512.000	Sign	1.300
TCP I/O buffers	128.000	Sign	1.600

QR FutureTPM Timings LDAA		
	TPM Timings – LDAA v1	TPM Timings – LDAA v2
Join()	374 ms	3.538 ms
Sign ()	$7{,}2 \times 10^6$ ms	48.055 ms

X150 faster

*All sizes are kBs

Quantitative KPIs

Id	Metric	Target Value	Acceptance criteria	Measured by M24	Comments
1	Allowing only for trusted S5 PersonalTracker interfaces to interact with the S5Tracker Analytics Engine	100%	100%	With TPM2.0: 100% With FutureTPM (LDDA v1): 100% With FutureTPM (LDDA v2): 100%	Target **Achieved**. Packets that have not be signed, are automatically dropped
2	Performance evaluation of process of sending for analyses an average set of 5kB of daily collected personal data at application level	+35%	+45%	With TPM2.0: 1,5 seconds With FutureTPM (LDDA v1): 61,40 s With FutureTPM (LDDA v2): 10,07 s	Target not achieved, however using the LDAA-v2 the timings can be **accepted** from a business point of view, when transport Is performed on a schedule manner
3	Performance evaluation of the infrastructure during the Join() phase at application level	800 ms	2.000 ms	With TPM2.0: 1,190250 seconds With FutureTPM (LDAA v1): 1,94 s With FutureTPM (LDAA v2): 10,33 s	Target not achieved but within the **acceptable** time space with LDAA-v2 as part of the total time considered
4	Improved perception of Individual Users' trust to S5PersonalTracker as a data hub	100%	60%	With TPM2.0: 100% With FutureTPM LDAA v1: 90% With FutureTPM LDAA v2: 95%	Target not achieved but highly **acceptable** 1 out of the 20 users gave a negative evaluation due to the delay experienced, which impacted negatively his perception of trust.

Demonstrator Discussion

- Performance issues (in terms of delays) have been noticed, as expected and are inherited by the nature and the overall architecture of the TPM and of course by the resources needed to work with QR algorithms.
- The integration of the QR-TPM methods in the infrastructure is in a position to provide acceptable results in an operational environment, even if the measured performance is not meeting the ideal targets set.
- LDAA-v1 was creating a burden and delays in the different peers, thus affecting the overall system of the S5 Activity Tracker, and eventually having a negative impact on its performance
- LDAA-v2 comes quite close to the targets set for the ATracker demonstrator. Still delays are there, but drastically FASTER than LDAA-v1, and can use HIGHEST security settings.
- If requirements of “close-to-real-time”, then LDAA-v2 is a good candidate!

FutureTPM Grant Agreement No. 779391

Thank You!