What is trust in digital government?

Trust – level of confidence of citizens and businesses that digital government services are reliable, secure, transparent and fair.

Transparency – ensuring people know how their data is used, who has access, and how decisions are made.

Why are people afraid to use digital government services?

- Fear of Mistakes

- Low Trust in Security and Data Privacy

- Complex Systems

- Bad Past Experiences

- Digital Divide
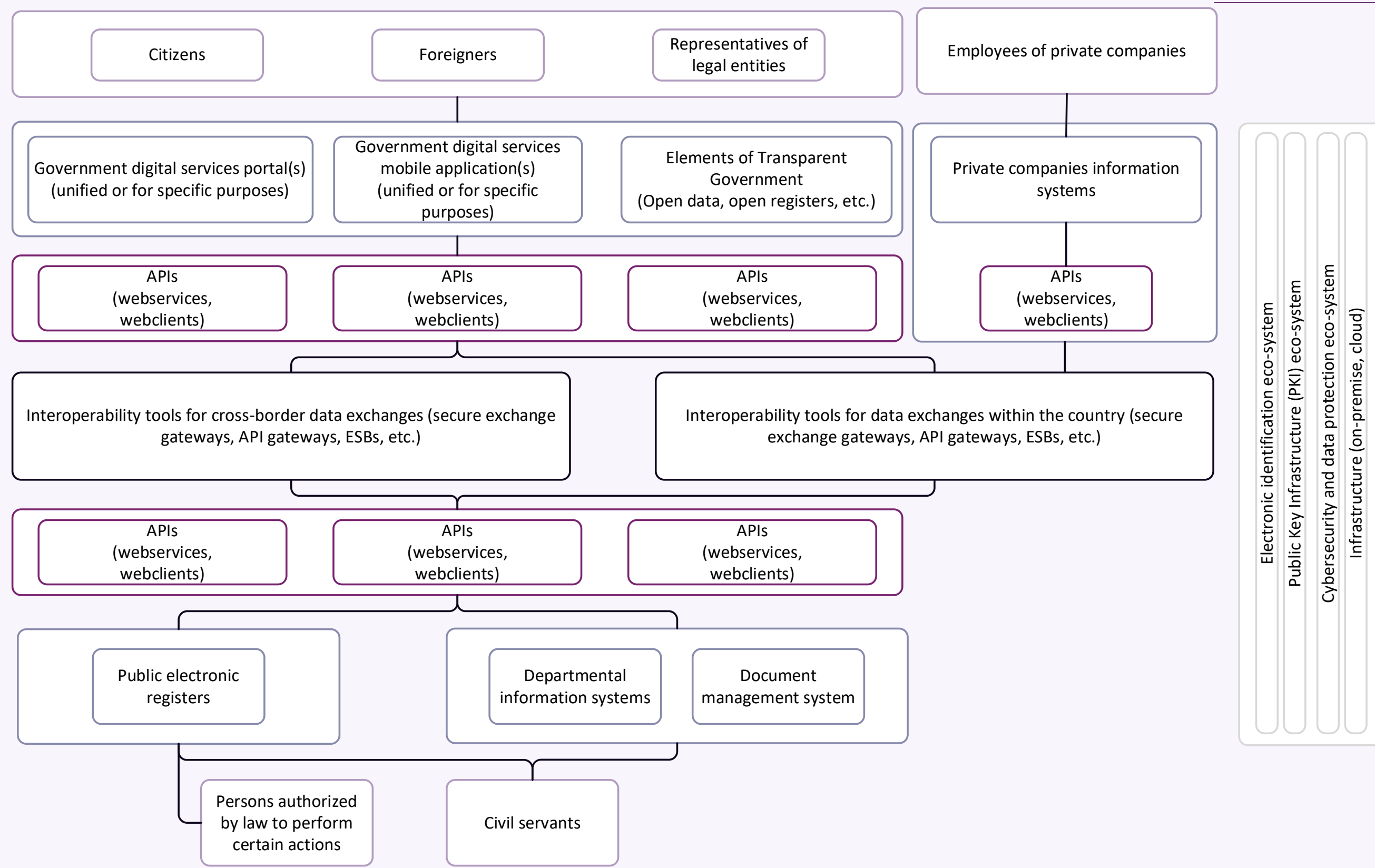
- Fear of No Support

- Language & Accessibility Barriers

e-Governance Conference Tallinn. Estonia

Personal data processing principles

* Regulation (EU) 2016/679, General Data Protection Regulation, Article 5

Digital government architecture

| Citizens | Foreigners | Representatives of legal entities | Employees of private companies |

| Government digital services portal(s) (unified or for specific purposes) | Government digital services mobile application(s) (unified or for specific purposes) | Elements of Transparent Government (Open data, open registers, etc.) | Private companies information systems |

| APIs (webservices, webclients) | APIs (webservices, webclients) | APIs (webservices, webclients) | APIs (webservices, webclients) |

Interoperability tools for cross-border data exchanges (secure exchange gateways, API gateways, ESBs, etc.)

Interoperability tools for data exchanges within the country (secure exchange gateways, API gateways, ESBs, etc.)

| APIs (webservices, webclients) | APIs (webservices, webclients) | APIs (webservices, webclients) |

| Public electronic registers | Departmental information systems | Document management system |

| Persons authorized by law to perform certain actions | Civil servants |

- Electronic identification eco-system
- Public Key Infrastructure (PKI) eco-system
- Cybersecurity and data protection eco-system
- Infrastructure (on-premise, cloud)

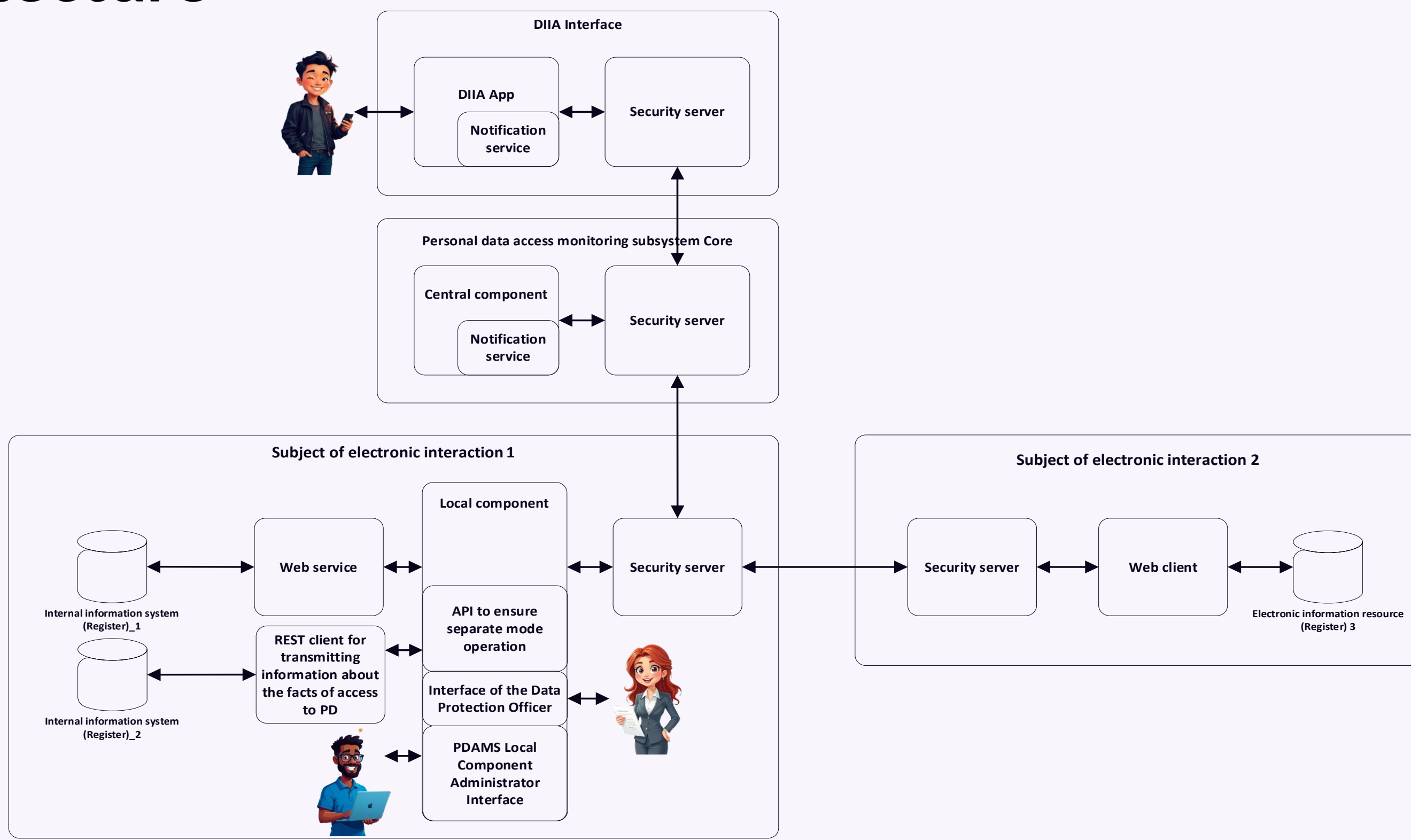# How is personal data access monitoring organized in Ukraine?

The Personal Data Access Monitoring Subsystem (PDAMS)

is a component designed to record and store information about the facts of personal data transfers by data exchange subjects within the "Trembita" system. It accumulates this data and ensures that personal data subjects are informed about each transfer.
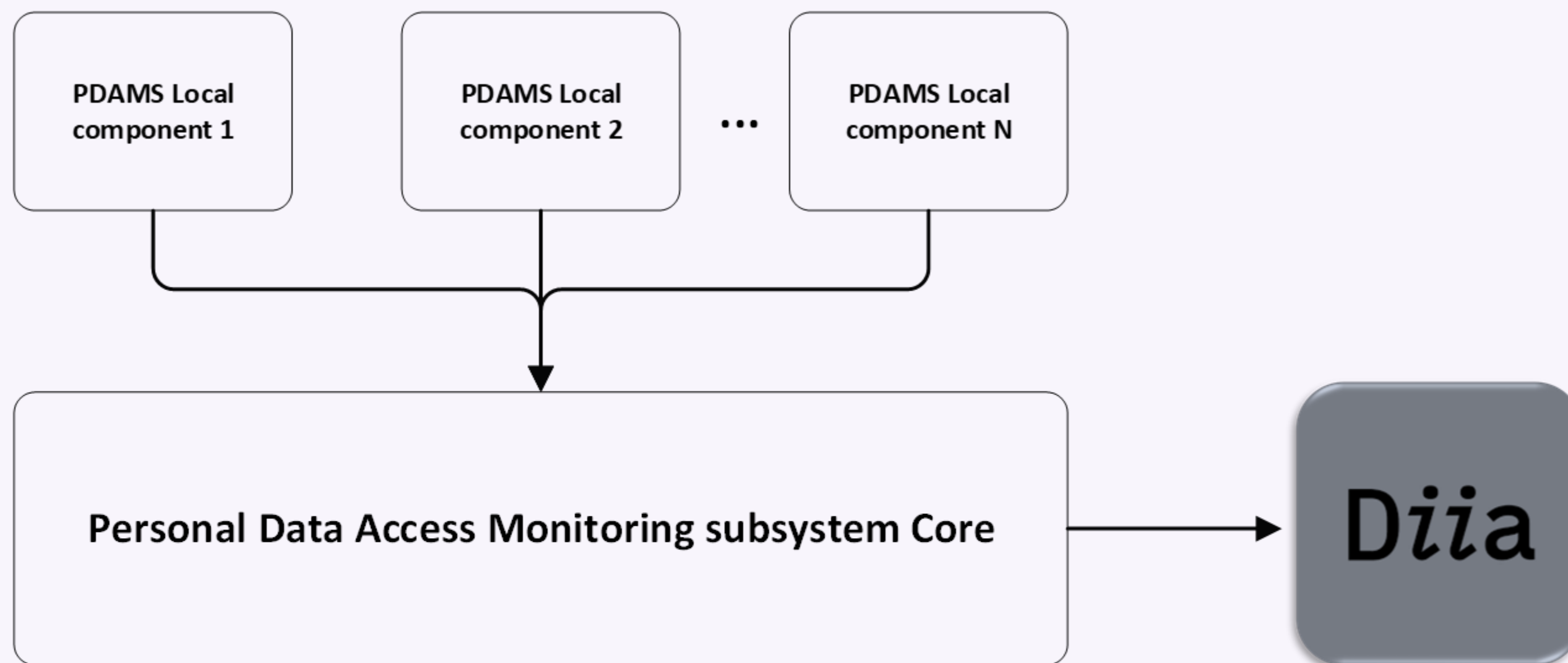
PDAMS is the part of the Ukrainian interoperability system "Trembita".

PDAMS was created based on the UXP Access Tracker product.

Personal data access monitoring subsystem architecture

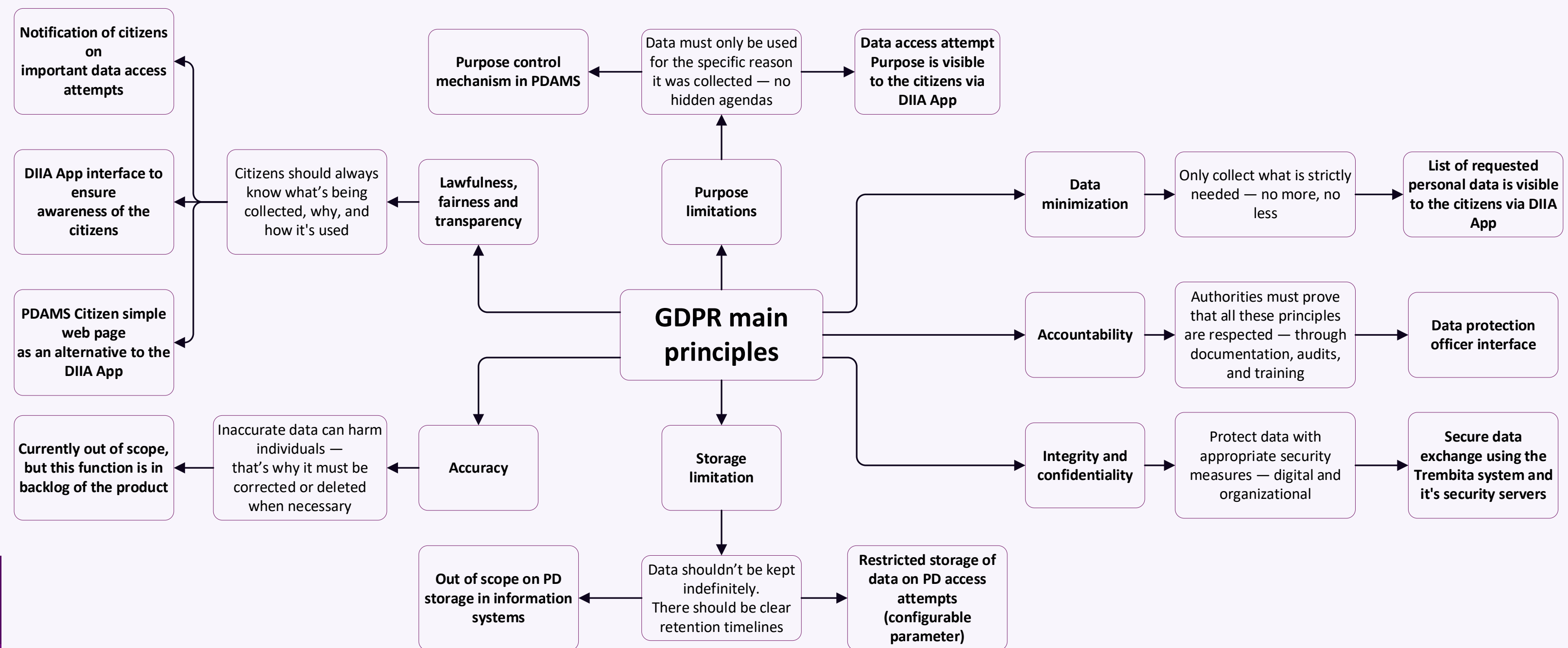e-Governance Conference / Tallinn / 28–29 May 2025 / #egov2025

Simplified Personal data access monitoring subsystem architecture

Direction of transfer of facts of access
to personal data

Personal data access monitoring subsystem GDPR principles coverage

Notification of citizens on important data access attempts

DIIA App interface to ensure awareness of the citizens

PDAMS Citizen simple web page as an alternative to the DIIA App

Citizens should always know what's being collected, why, and how it's used

Lawfulness, fairness and transparency

Purpose control mechanism in PDAMS

Data must only be used for the specific reason it was collected — no hidden agendas

Data access attempt Purpose is visible to the citizens via DIIA App

Purpose limitations

Data minimization

Only collect what is strictly needed — no more, no less

List of requested personal data is visible to the citizens via DIIA App

GDPR main principles

Accountability

Authorities must prove that all these principles are respected — through documentation, audits, and training

Data protection officer interface

Accuracy

Inaccurate data can harm individuals — that's why it must be corrected or deleted when necessary

Currently out of scope, but this function is in backlog of the product

Storage limitation

Integrity and confidentiality

Protect data with appropriate security measures — digital and organizational

Secure data exchange using the Trembita system and it's security servers

Out of scope on PD storage in information systems

Data shouldn't be kept indefinitely. There should be clear retention timelines

Restricted storage of data on PD access attempts (configurable parameter)

What information about the facts of access to personal data is recorded?

- Request identifier

- Date and time of personal data request

- Identifier of an individual whose personal data was accessed

- Information on Information system (register) and it's owner

- Information on organization that requested related personal data

- List of requested personal data

- Purpose and reasons of personal data access

Who has access to the information captured by the PDAMS?

Citizens using **Diia**

Data Protection Officer using PDAMS Local component interface

The interface of the Data Protection Officer

e·Governance Conference
Tallinn. Estonia

Organizational things for personal data protection in Trembita system

In order to formalize the data volume involved in the exchange in the Trembita system and to ensure compliance with the data minimization principle, an information exchange agreement is concluded.

This agreement includes information on:
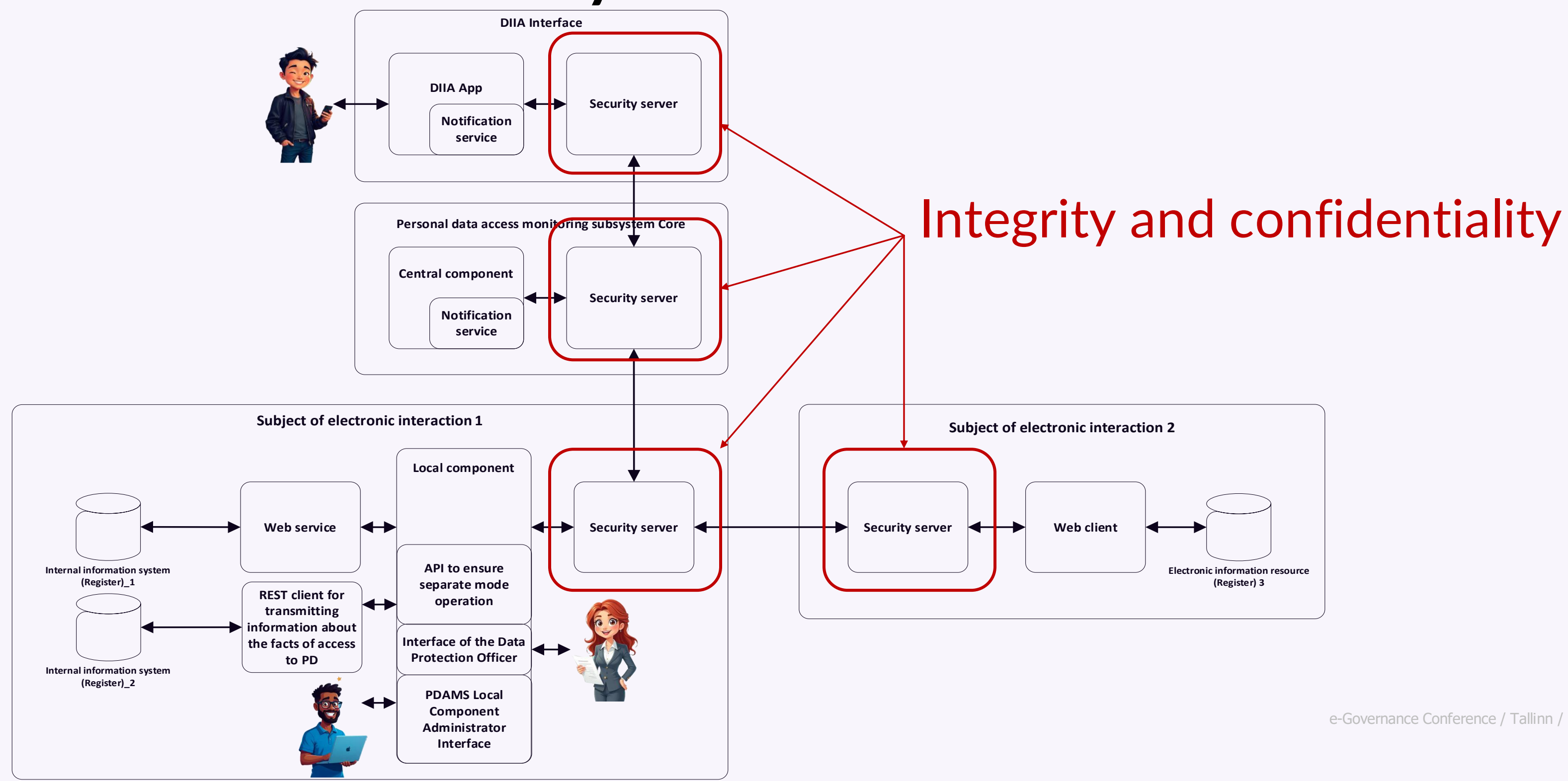
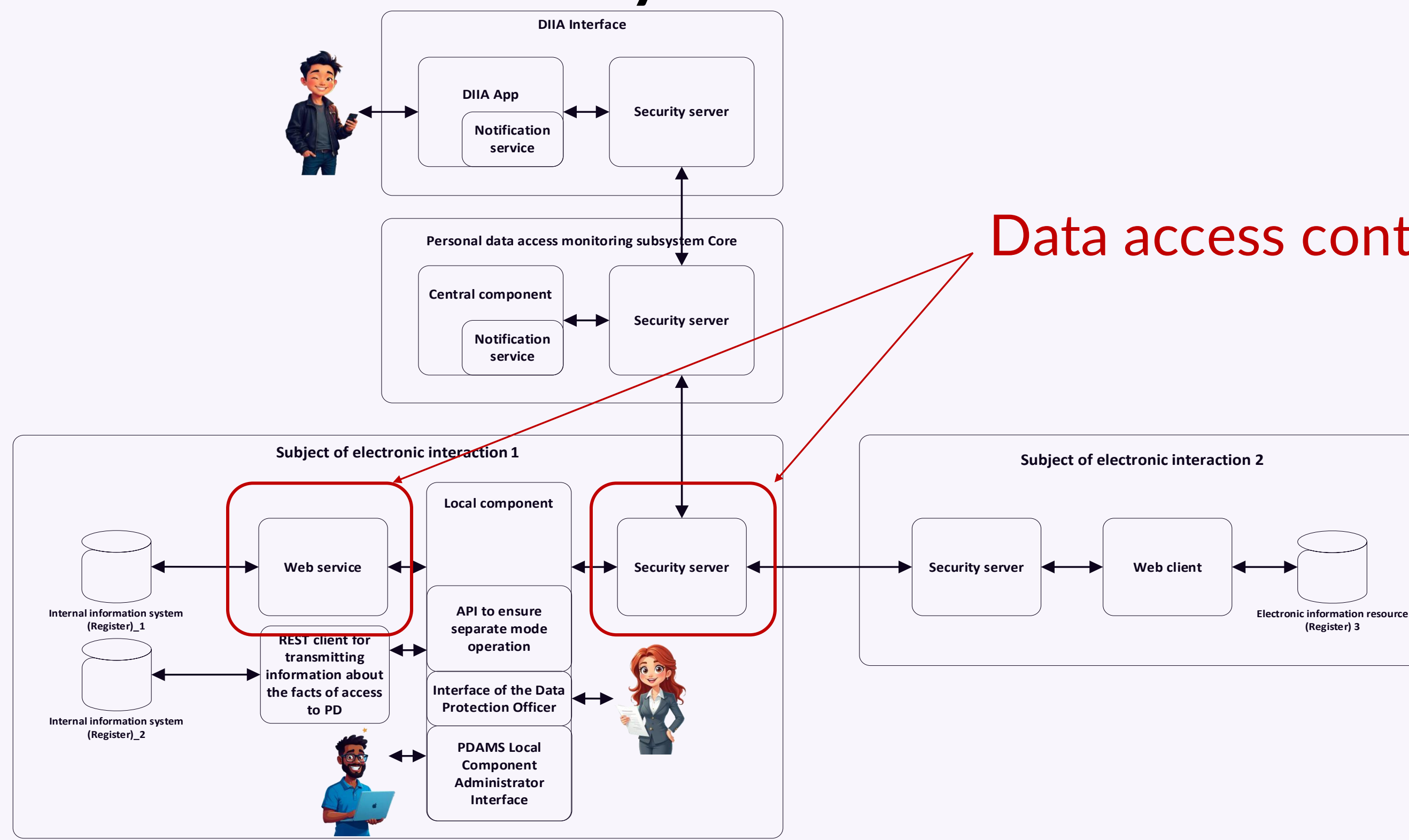| Legal entities involved to data exchange	Legal grounds of data exchange	Electronic information resources	APIs (with a scope)	Personal data access purpose (s)

Overview of the personal data protection mechanisms in Trembita system

Overview of the personal data protection mechanisms in Trembita system
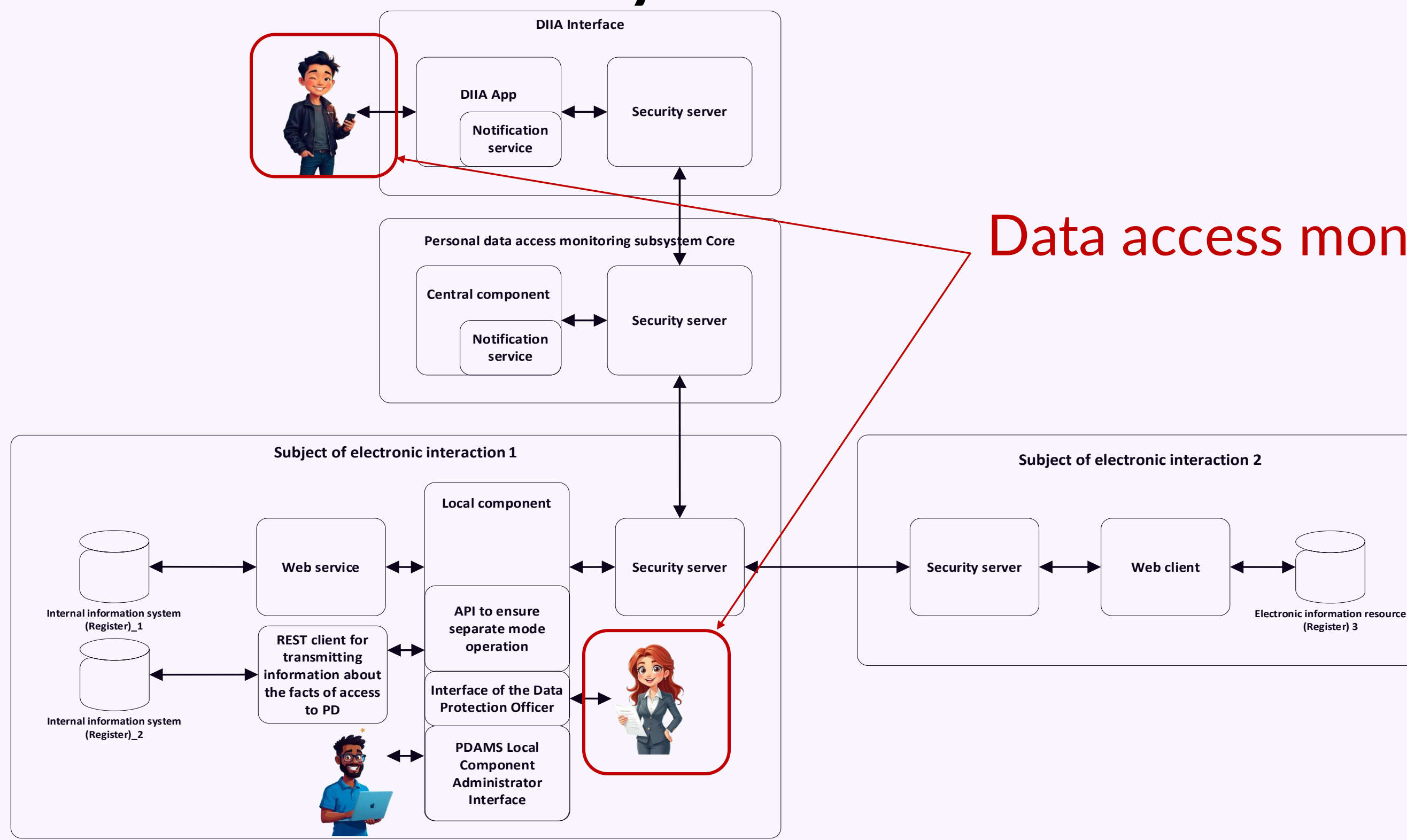

Data access control

Overview of the personal data protection mechanisms in Trembita system
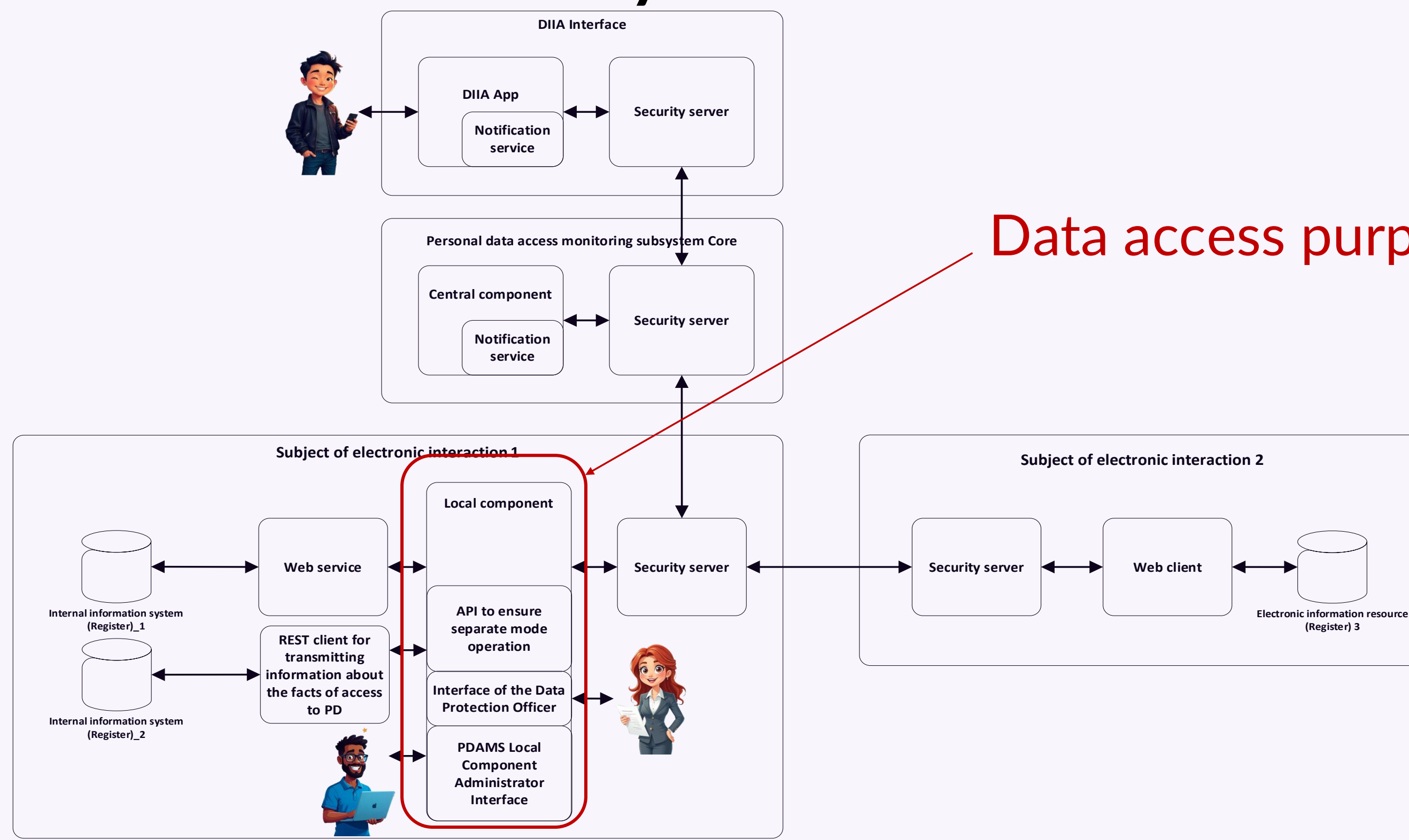
Data access purpose control

Overview of the personal data protection mechanisms in Trembita system

Data access monitoring

e·Governance Conference
Tallinn. Estonia

Thank you!

Organisers:

eGA

REPUBLIC OF ESTONIA
MINISTRY OF FOREIGN AFFAIRS

estdev
From the people of Estonia