

# Building Verifiable Trust in DFFT through PETs

- Introducing Use Cases Utilizing Trusted Execution Environments -

**Takao Takenouchi**

VP of Public Affairs, Acompany Co., Ltd. /

Executive Director, Privacy Tech Association, Japan

# Contents

## **Part 1: What is trust**

- Verifiable trust would be desirable
- PETs provide verifiability

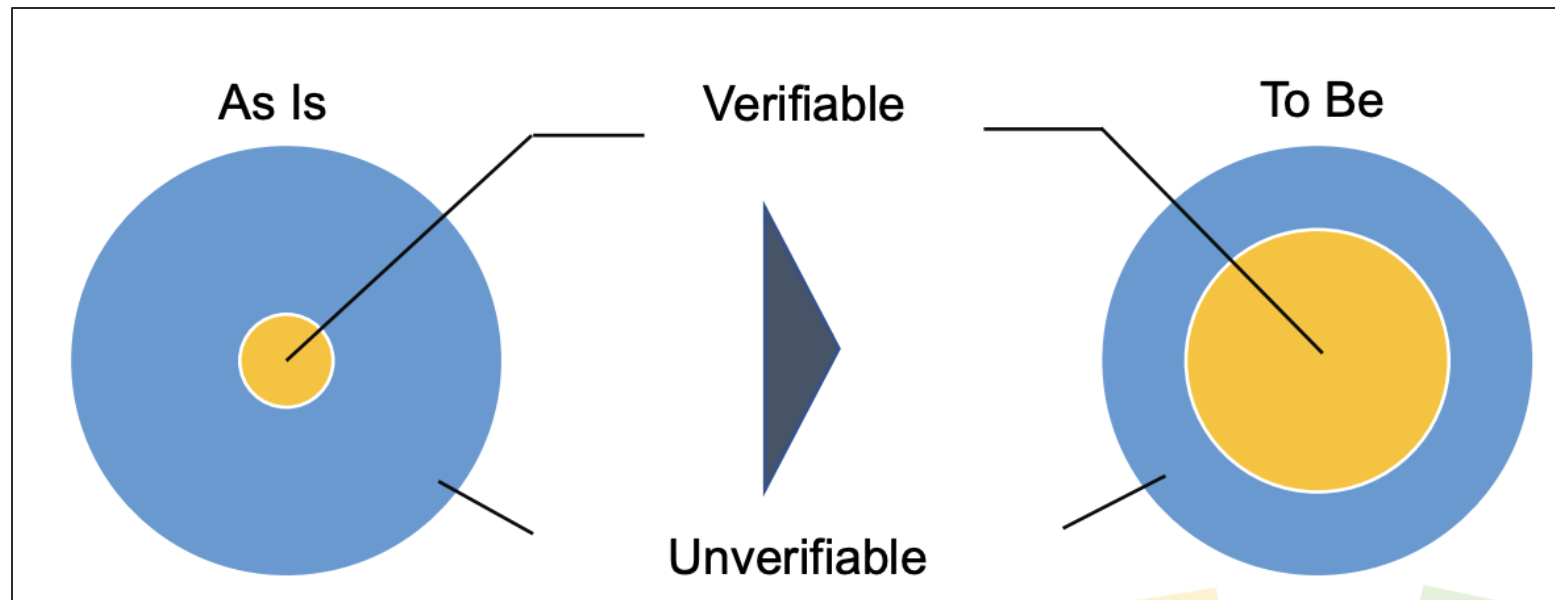
## **Part 2: Use cases using TEE** (TEE: Trusted Execution Environment)

# **Part 1: What is trust**

# What is Trust : Trust needs Verifiability

- From a technical perspective, trust can be divided into two types:
  - **Implicit trust** : Trust established without taking any special action
  - **Explicit trust** : Trust that **can be verified** when necessary <sup>\*1</sup>
- PETs enable technically **verifiable trust** and efficient security.

## Trusted Web in Japan: Trust requires verifiability



In Japan, the concept of a “**Trusted Web**” has been discussed since around 2020. Through these discussions, it was concluded that **verifiability is essential** in order to establish trust

Source: “Trusted Web White Paper ver. 3.0 Overview”, <https://trustedweb.go.jp/en/documents/>

\*1 Ref: Mike Bursell, “Zero trust and Confidential Computing”, Alice, Eve and Bob – a security blog, <https://aliceevebob.com/2023/06/20/zero-trust-and-confidential-computing/>

## Target of Trust

- Each PET focuses on a different aspect of verifiability
  - Combining PETs is desirable for more secure trust

Trust Targets and Supporting PETs

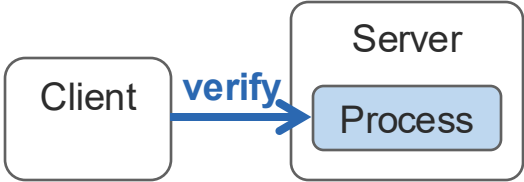
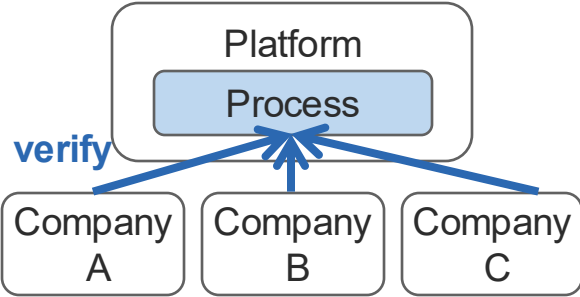
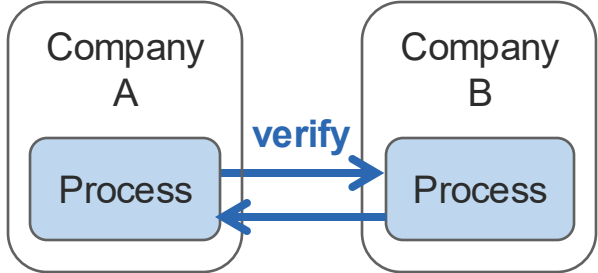
Trust Target	Supporting Technologies / PETs
Processing Environment	TEE (Trusted Execution Environment) ,...
Data Integrity / Authenticity	Verifiable Credentials, Digital Signatures,...
Data Confidentiality	MPC (Multi-Party Computation), Homomorphic Encryption,...
Counterparty	PKI, Trust Frameworks,...
...	...

 **Focus**

Processing Environment  
is important in AI workloads.

# Trust Models for AI processing

- In AI processing, there are three typical patterns of trust models.

Trust Model	Delegated Processing Model	Centralized-Collaboration Model	Decentralized-Collaboration Model
Purpose	To offload heavy AI processing to the cloud	To improve AI performance by integrating data	
Detail	<ul style="list-style-type: none"><li>• Client delegates processing to the cloud.</li><li>• Client verifies the cloud.</li></ul> 	<ul style="list-style-type: none"><li>• Companies A, B, and C send data to the platform.</li><li>• Each company verifies the platform.</li></ul> 	<ul style="list-style-type: none"><li>• Company A and B verify each other.</li></ul> 

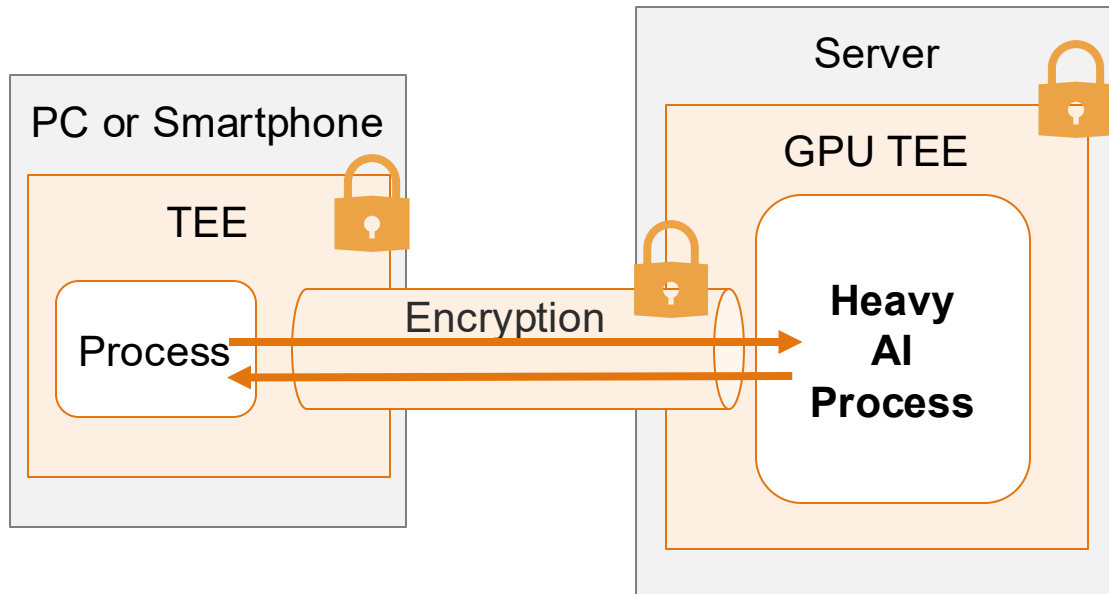
## Requirements for Trust in the Processing Environment

- To verify processing environments, it is desirable to have the following:
  - **Data Confidentiality**: No data leakage at the processing destination
  - **Code Integrity**: No unauthorized modifications (e.g., no backdoors)
- Trusted Execution Environment (TEE) support both and **AI workload**.
  - TEE can also be combined with other PETs (e.g., MPC) for stronger guarantees.

# What is TEE

- TEE is a **hardware-based** technology that ensures data confidentiality.
- TEE provides **remote attestation** to verify code integrity externally.
- Some GPUs include TEE functionality, enabling secure AI processing.

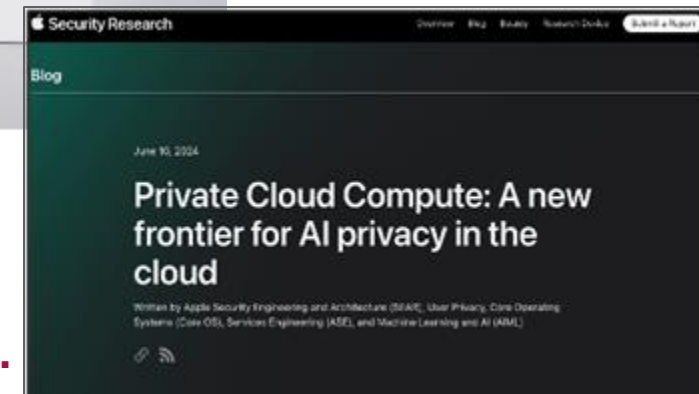
## Example of TEE use in cloud-based processing



## Apple adopts TEE for generative AI



**Apple provides a verification environment for security researchers.**

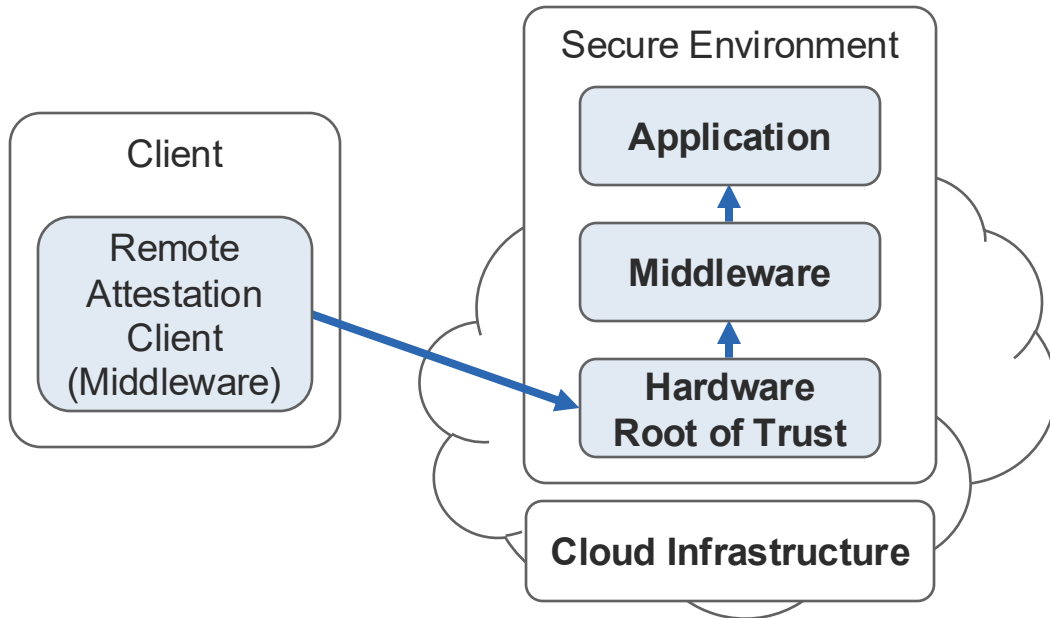




# Detail of Remote Attestation

- In TEE Remote Attestation, **hardware is the root of trust**.
- **Middleware** helps make TEE application development **easier**, and it must be secure.

## Conceptual Illustration of Remote Attestation



Starting from the Root of Trust, a chain of trust is built through verified hardware and software layers. <sup>\*3</sup>

## TEE Hardware and software vendors

TEE Stack	Example Vendors <sup>*2</sup>
Middleware <sup>*1</sup>	Fortanix, Anjuna, Opaque Systems, Decentriq, BeeKeeperAI, Edgeless Systems, Acompany,...
Hardware Chip	Intel, AMD, NVIDIA,...
Cloud Infrastructure	Google, Amazon, Microsoft, Sakura Internet, NTT Data...

Because middleware requires less investment than hardware, several vendors offer their own implementations.

<sup>\*1</sup> In this presentation, “middleware” includes both libraries inside the TEE that are part of the TCB(Trusted Computing Base), and external applications that handle remote attestation on behalf of the client.

<sup>\*2</sup> The list of vendors was created by the author, referring to sources such as the Azure Partner list. <https://learn.microsoft.com/en-us/azure/confidential-computing/partner-pages/partner-pages-index>

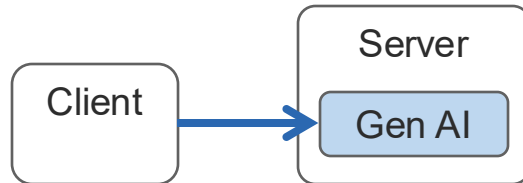
<sup>\*3</sup> Confidential Computing Consortium focuses on hardware-based roots of trust, [https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC\\_outreach\\_whitepaper\\_updated\\_November\\_2022.pdf](https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC_outreach_whitepaper_updated_November_2022.pdf)

## **Part 2: Use cases using TEE**

# Use Cases by Trust Model Patterns

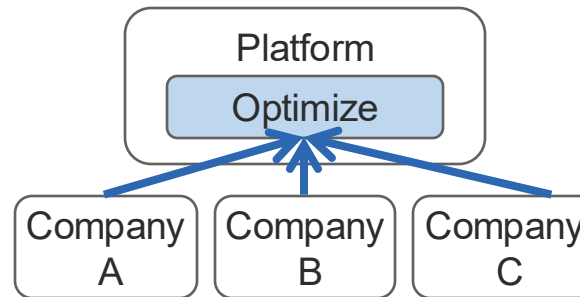
## Generative AI for smartphones

Since generative AI is too heavy for smartphones, processing is offloaded to servers with data confidentiality preserved. (e.g. Apple Intelligence)



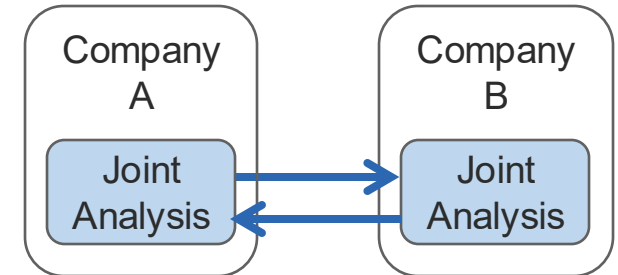
## Global Supply Chain Optimization

Sharing manufacturing data confidentially across borders, while optimizing the overall process.



## Cross-analysis of location and other data

A company holding location data and another company perform joint analysis while keeping their data confidential.



I will explain these use cases

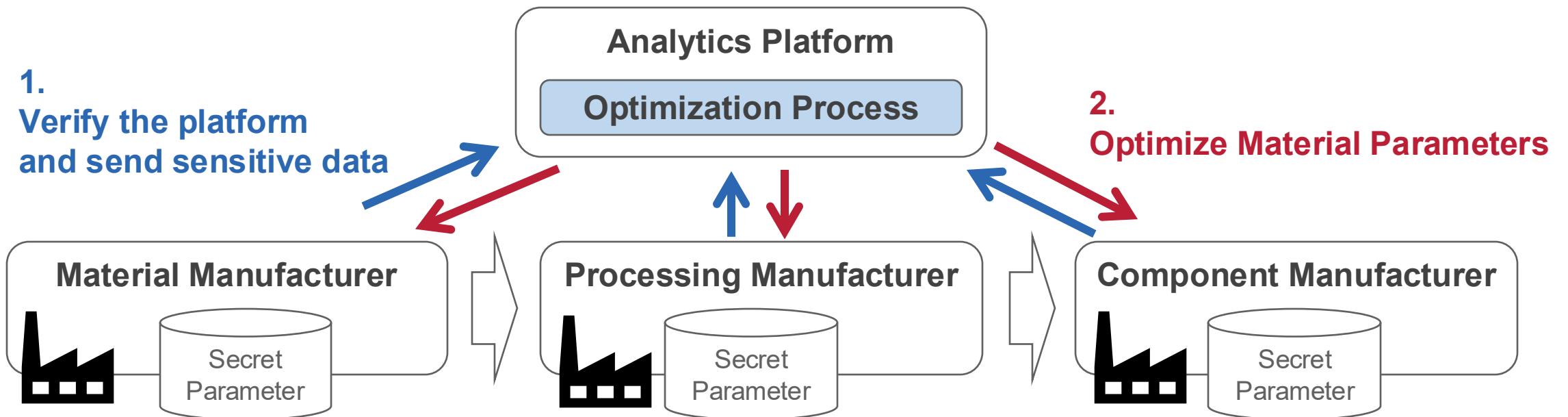
## Use case : Global Supply Chain

### ■ Challenge:

- In manufacturing industry, **raw material data is sensitive** and hard to share across borders.
- However, **optimizing** the full manufacturing process requires data sharing between companies.

### ■ Solution:

- TEE enables verified, confidential sharing of data for cross-step optimization.
- The **middleware** performs remote attestation, and it should be **secure and vendor-neutral**.



e.g. type and amounts of ingredients,  
how they mixed

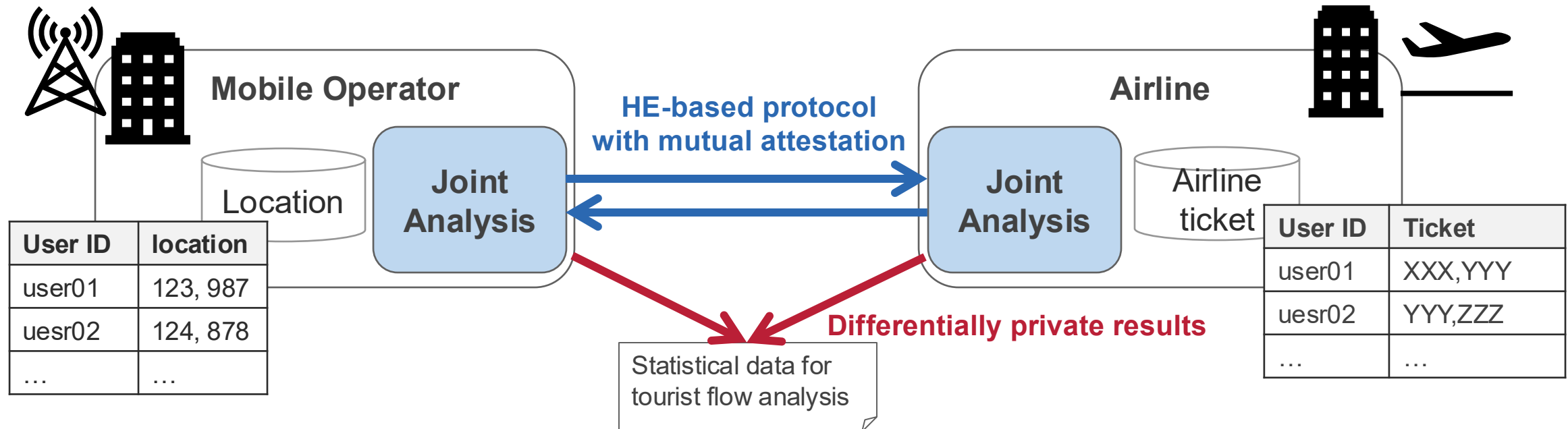
# Use case : Cross-analysis of location and other data

## ■ Challenge

- **Location data is sensitive**, yet extremely valuable.
- Because it qualifies as personal data, user consent is required.

## ■ Solution

- A combination of PETs, including TEEs, provides robust protection against privacy breaches.
- Mutual attestation of TEEs is leveraged to prevent parties from acting maliciously.



\*1 For details, please refer to [https://www.docomo.ne.jp/english/corporate/technology/rd/technical\\_journal/bn/vol25\\_1/](https://www.docomo.ne.jp/english/corporate/technology/rd/technical_journal/bn/vol25_1/)

\*2 There are several cases of secure data matching and analysis like this. <https://en.acompany.tech/news/acompany-joint-KDDI-DCR>

## Legal Treatment in Japan for This Use Case

- In this use case, various PETs are used in combination, including TEE, homomorphic encryption, differential privacy, and others. <sup>\*1</sup>
- In Japan, this is generally **not regarded as personal data processing** under the law.
- However, when exporting such technologies, **legal compatibility must be checked in each country.**
  - This process involves significant time and cost.

<sup>\*1</sup> Details of the PETs combination

- Homomorphic encryption-based protocol enables parties to cross-analyze data without disclosing personal information to each other
- Differential privacy protects the privacy of the output
- Mutual attestation of TEEs ensures the soundness of the system

# Summary and Recommendations

## ■ Summary

- It would be beneficial if trust in DFFT could be verified.
- PETs contribute to verifiable trust — Remote Attestation with TEE is a strong example.

## ■ Recommendations

1. Include **TEE Remote Attestation in use case repository**.
  - Middleware must also be verifiably included — full-stack trust is essential.
2. In the context of global cooperation, **clarify the legal treatment** of PETs and personal data.
3. **Promote investment** and international participation in PETs development.
  - This helps prevent over-reliance on any single provider.