SPE and TRE terminology for sensitive data processing

Heikki Lehväslaiho, CSC, FI
Last modified 2025-06-10

Introduction

This white paper summarises the finding of the first version of the EOSC-ENTRUST Architecture Blueprint[1] about terminology used to describe computing environments for sensitive data processing. They are commonly used interchangeably, but in professional context they can have different scope and need to be used correctly.

Secure Processing Environment

Secure Processing Environment (SPE) was added to European Union legislation in the Data Governance Act (EU 2022/868) to address the data privacy and security needs expressed in the General Data Protection Regulation (GDPR, 2016/679). SPE is a computing environment that uses heightened technical and operational measures to fully isolate sensitive data processing by permitted users. SPEs can be used in multiple use cases, domains of knowledge, and governance structures; the latest being European Health Data Space[2] which requires the using of an SPE for health data research.

Trusted Research Environment

The Trusted Research Environment (TRE) concept was developed in the United Kingdom over the past decade as a safer computing environment to protect the identity of human genomic sequences and then expanded to cover health and social data. It is now seen as the preferred national approach to ensure the safety of processing of any sensitive data.

[1] https://zenodo.org/records/14362388
[2] European Health Data Space (EHDS) regulation https://www.europarl.europa.eu/meetdocs/2024_2029/plmrep/COMMITTEES/ENVI/DV/2024/12-04/2022_0140COR01_EN.pdf

The TRE concept is based on the Five principles[3], has a set of community-defined requirements and a derived high-level architecture[4], but not one agreed definition. It has been called by many alternative names like Secure Data Environment (SDE by the England National Health Service) or Data Safe Heaven (Scotland), and the TRE specification allows it to be organised in many ways.

The recent DARE UK Federated TRE Blueprint v2.2[5] clarifies the concept by specifying three functional zones that any TRE may contain in any combination:

- Research Analytics Zone (RAZ) to contain project-specific data processing by users
- Secure Data Zone (SDZ) for active data management roles of data governance
- Query Management Zone (QMZ) to provide secure remote data access services

In an extreme case, a TRE can be composed only of RAZ making it impossible to draw any functional conclusions from the name. Any practical discussion about TRE functionalities should therefore indicate the zones included.

Equivalence

Both TRE-RAZ and SPE are based on securing sensitive data privacy within a secure computing environment for the exclusive use by data users (Figure 1). Both isolate users by project and demand clearly defined, limited, and secure interfaces out of them (Figure 2).

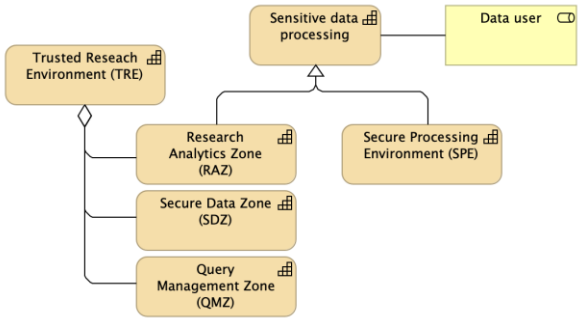

Figure 1. Equivalence of SPE and TRE-RAZ.

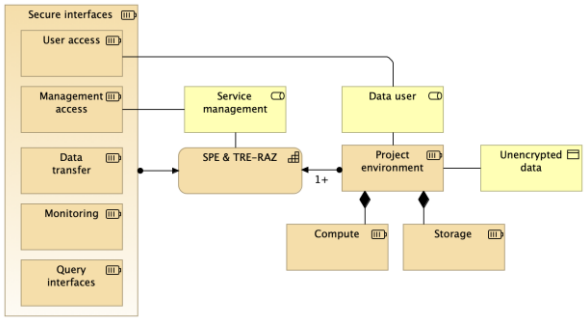

Figure 2. SPE and TRE-RAZ may contain multiple isolated project environments that have only secure and limited access to the outside.

[3] See Five Safes Principles: https://www.dundee.ac.uk/stories/data-safe-havens-keeping-data-secure-using-five-safes-framework

[4] Standard Architecture for Trusted Research Environments (SATRE) https://satre-specification.readthedocs.io/

[5] DARE UK (Data and Analytics Research Environments UK). (2024). DARE UK Federated Architecture Blueprint (2.2). Zenodo. https://doi.org/10.5281/zenodo.14192786

Future challenges

There is now a need to extend the processing of sensitive data beyond a single, isolated environment that can offer only limited capabilities and capacities. Individual SPEs will be expected to function together in several federations with varying legal, data management, and governance structures. Data will be accessed, transferred and processed in remote locations in multiple different ways. This will create an increasingly complex challenges to maintain data privacy, data security, interoperability and accountability among widely diverse use cases. Clear and unequivocal terminology is the first requirement for tackling these.