Case Statement:
Trusted Research Environments for Sensitive or Confidential Data:
FAIRness for Controlled Data and Processes

1. Background

The conflicting goals of protecting and maintaining control over sensitive data, confidential data or data protected by intellectual property rights, while striving to give third parties access to the data, pose a significant challenge. Trusted Research Environments (TREs), also referred to as Secure Research Environments (SREs), have been established in the last decade that, when properly set-up and operated, help ease this problem by providing high security guarantees of a highly controlled and monitored environment.

The Working Group on **T**rusted **R**esearch **E**nvironments for **S**ensitive **D**ata (WG-TRESD) seeks to produce a better understanding of the elements making up TREs (and their different extensions, flavors, etc.) and the processes running in and supported by them, bridging terminology boundaries to ease the set-up and operations of, and the co-operation and interoperability between, such infrastructures, enabling FAIR access and use of data in such restricted settings.

Following the TRE Green Paper [10] requirements we consider systems where users are presented with a remote desktop where they can run analysis on confidential data (applying algorithms to datasets exploratively). With this working definition, we do not consider job-submission systems like Blind SANE[1] who apply (approved) algorithms to sensitive/confidential data a full TRE, while such components may form part of the tooling environment for specific types of interaction. We found that many SREs/TREs are similar in architecture design and technical implementation. There is, however, a lack of openly available guidelines and explanations on design decisions for setting up and running a SRE/TRE, including technical implementation of roles and their permissions, ingesting data, processing data, exporting data, provision of virtual machines/compute units, isolation, privacy-preserving techniques, etc. This deficiency comes to light especially when planning towards federation across SREs/TREs to connect infrastructure providers with shared interfaces, bilateral trust and shared resources or data, due to the lack of standards.

In this working group we will identify common concepts that SREs/TREs implement in different flavors, suggest common interfaces between those concepts and communicate them to the public.

[1] https://www.surf.nl/files/2022-02/saneproposal.pdf, accessed 2023-12-12

2. Charter

This charter will provide a concise articulation of what issues the WG will address within a 18-month time frame and what its “deliverables” or outcomes will be.

Data holders struggle to make sensitive data available to researchers due to concerns of losing control over it. As a result, the data is often completely sealed off in a safe room that needs to be visited physically.

Taking utility into consideration, modern SREs/TREs usually operate on a data-visiting (rather than data sharing) principle [9], where a researcher visits the sensitive data virtually. Data owners may want to make their sensitive data available to researchers but do not know how to start with the SRE/TRE methodology, how to reveal non-sensitive metadata to make it findable, provide a transparent sensitive data access procedure, or make it interoperable and reusable. In this WG, we want to harmonize the understanding of concepts that TREs incorporate, which are either not currently public or are implemented in different flavors, but which, in the end, share core methodology and concepts.

2.1. Problems

P1. *Blueprints*. The technical implementations and processes behind data visiting have existed for a decade, yet there are no community-agreed technical blueprints that provide building blocks and adaptable infrastructure components as well as community best-practice processes. This increases the complexity for anyone wanting to set-up such an SRE/TRE, renders the infrastructures less comparable, hinders easier communication and may lead to suboptimal design decisions when everybody has to go through the conceptual design process again and again.

P2. *Interoperability*. In the context of data visiting, interoperability between SREs/TREs is crucial as no data will leave an SRE/TRE. Instead a user federation (not in the sense of identity federation) is needed for users to work across several SREs/TREs, i.e. have code move from one to another, work with the data locally such as in federated learning in machine learning settings. Currently, SREs/TREs lack such interoperability, making cooperation, mutual trust etc. difficult to establish.

P3. *Risks*. Balancing risks of data disclosure and utility of the environment for researchers is an ongoing problem for SREs/TREs. For informed decision making, a risk catalog would be helpful, with mechanisms specified to lower the exposure to a specific risk. Currently, there is no shared catalog of risks and security allowing infrastructure providers to understand and accept or reject a specific risk or implement mitigation mechanisms.

2.2. Specific Outcomes

We expect outcomes to be the result of the activities addressing the list of problems and subsequently being shaped into deliverables. Taking the problems from Sec. 2.1 as input, the following outcomes are proposed:

- **A shared understanding of the functional components, processes, identifiers, and roles in a SRE/TRE setting** and its mapping to the various instantiations of such infrastructures around the world.
    - Problem: P1 Blueprints
    - Comprises of:
        - Working definition of what components need to be present to consider a secure data infrastructure a TRE (e.g. trusting the infrastructure via handover of confidential data, potentially allowing linking with other confidential datasets).
        - Architectural blueprint: components, functionalities and a mapping to their implementation in different TREs, vocabularies, terminology mappings[2]
        - Identification and definition of typical processes for data acquisition, access requests, analysis and the associated risks, vocabularies, terminology mappings,
        - Definitions of roles, responsibilities, and mechanisms for establishing trust levels and associated consequences, mutual exclusiveness of roles, extent of role interaction with each component.
        - Blueprint what constitutes trust in the dimensions of infrastructure technology, -software and -processes to be trustworthy for certain expected activities (i.e. analysis, infrastructure federation)
    - Deliverable: D1 TRE Blueprint
    - Coordinator: Martin Weise

- **A shared understanding** of the **context of user federation** and **interfaces across TREs**:
    - Problem: P2 Interoperability
    - Comprises of:
        - Documentation of social architecture for roles, interfaces between people, e.g. data trustees as human secure enclaves [8]
        - Identification of common machine-actionable and readable interfaces between TREs for processes: authorization, data import, data export, legal processes e.g. data access agreements, federated analysis, payment
        - A collection of best practices and identified issues in the context of interoperability (e.g. design flaws when placing the artifacts in the export folder allowing symbolic links to non-authorized artifacts)
        - Identification of issues related to legal interoperability considering data protection laws (GDPR, HIPAA) preventing some data from being opened to the public and/or linking of data.

    - Deliverable: D2 TRE Interoperability Recommendations
    - Coordinator: Rob Baxter

---

[2] V 1.0.0 of the SATRE specification is a good place to start: https://satre-specification.readthedocs.io/en/v1.0.0/index.html

- **Catalog of bad-actor threat models** associated with data access and **mechanisms to lower them** or **accept them**.
    - Problem: P3 Risks
    - Compromises of:
        - Catalog of bad-actor threat models and black-hat scenarios at infrastructure level (as technical risks get platform-dependent quickly, especially on public cloud providers, this is a challenge).
        - Collection of security levels applied in TREs, associated tools to assess issues/weaknesses/threats, e.g. DRAT data risk assessment tool [7], identifying structured mistrust issues between countries in traditional/non-traditional research communities and potential users and data owners
        - Commonly accepted practices for lowering the risks of sensitive data, such as the Five Safes Framework[3] and an ISO 27001 certification
        - Collecting worst-case scenarios (data loss, data breach), consider cultural aspects (e.g. in Sweden, personal income data is not considered sensitive since it is public knowledge)
        - Identify “standardized” set of data sharing conditions, that encompasses the data sharing policy.
        - Finding the balance between enforcing policies and letting the researchers do their work (usability) so they don’t bypass the policies (security).
    - Deliverable: D3 TRE Risk Catalogue
    - Coordinator: Ville Tenhunen

3. Value Proposition

This group will bring together:

- infrastructure providers who enable data visiting (with technical-, organizational- and legal measures);
- data stewards who curate the metadata; data owners who want to provide access to the sensitive data, and;
- researchers who find metadata, request access to the sensitive data and, ultimately, conduct data owner-approved research on the data with known research questions in a secure environment that prevents data from leaving.

If the WG is successful it will be easier for institutions to set up data infrastructures that allow researchers to gain access to sensitive data (irrespective of whether that sensitivity stems from privacy/GDPR reasons or is due to the commercial/IPR sensitivity of the data). It will also demonstrate that such data, in spite of not being freely share-able, can still be FAIR and made available for research.

It will also demonstrate how results obtained on such closed data can still be made reproducible and transparent to the degree permitted by data sensitivity, establishing a clear

[3] http://www.fivesafes.org/, accessed 2023-08-25

public metadata record on the research performed as well as supporting findability of the data, linked to clear access request/permission processes and public verification of access by specific trusted parties. For example, the public / other researchers will be able to verify, whether a specific researcher had actually access to the data underlying a specific publication, and will allow them to determine the rules applying for requesting access to perform reproducibility studies or comparative evaluations, thus increasing trust in results obtained on otherwise inaccessible (and thus largely non-transparent) data.

The value per role is expected as follows:

- As a *researcher*, better understanding of similarities and differences between TREs is expected, knowledge how TREs are set-up and operated, thus understanding better whom to entrust with their data, how to get access to sensitive data, and how to perform research in such TREs.
- As a *data steward*, a list of TREs and their contact information, processes and definitions for data management, involved roles (especially mutual exclusiveness), legal interoperability [2], achieve maximum FAIRness for sensitive data, confidential data or data related to intellectual property.
- As an *infrastructure provider*, the manner in which data is used (mostly interactive, explorative) is expected to be better understood, the threat model of the infrastructure, along with the importance of exposing non-sensitive metadata in public repositories to enable findability, the collaboration capabilities between TREs better understood, identify best practices and open issues, approaches that did not work mappings of terminology, roles, processes, functional components/blueprint, and architecture
- As a *data holder/provider*, better understanding of how to make data accessible and usable without giving up control of the data; security & privacy risks and requirements for SREs/TREs, being able to understand to which extent a TRE may satisfy his or her requirements.

It will also increase interoperability between such environments on a technical, legal and organizational level, hopefully enabling easier set-up of ad-hoc joint SREs/TREs in settings where specific data sources need to be joined but may not be passed on to a third party for hosting. It may further make it easier to set-up data visiting platforms where trusted code can be executed, with monitoring and result inspection processes clearing results for return to a researcher so that, in some cases, even a completely shielded interaction with sensitive data may be possible. The goal is to establish best practices for balancing these differing requirements for access limitations and flexibility of interaction / analysis, understanding associated risks, with the goal of making data accessible and usable to research that otherwise would not be possible.

4. Engagement with existing work

4.1. Activities outside RDA

Many organizations worldwide already operate their own SRE/TRE, while academic and government bodies (e.g. statistical offices) are predominant. We provide a non-exhaustive landscape of SREs/TREs identified in Table 1.

Name	Region
SURE	Australia
SeRP Australia	Australia
Australian Research Environment	Australia
DEXHELPP	Austria
OSSDIP	Austria
Wellfort	Austria
AMDC	Austria
Statistics Belgium	Belgium
Population Data British Columbia	Canada
Croatian Bureau of Statistics	Croatia
Scientific Data Center of CAS	China
National Genomics Data Center	China
National Bureau of Statistics China	China
Statistics Denmark Remote Desktop	Denmark
EHDEN	Europe
EJP RD Virtual Platform	Europe
European Genome-phenome Archive	Europe
GAIA-X DataLoft	Europe
Federated EGA	Europe
GAIA-X DataLoft	Europe
HONEUR	Europe
LETHE project infrastructure	Europe
PANCAIM project infra	Europe
CSC ePouta	Finland
CSC SD Services	Finland
Statistics Finland FIONA	Finland
SPESiOR	Finland
de.NBI Cloud	Germany
Research Data Centre (FDZ) JoSuA	Germany
UseGalaxy.eu	Germany

L3S	Germany
Medical Informatics Initiative (MII)	Germany
RemoteNEPS	Germany
Pedianet Database	Italy
EPIC Cloud	Italy
RDC Bank of Italy	Italy
Eurostat	Luxembourg
ODISSEI Secure Supercomputer	Netherlands
SANE	Netherlands
Statistics Netherlands Remote Access	Netherlands
anDREa	Netherlands
Personal Health Train / Vantage6	Netherlands
HUNT Cloud	Norway
TSD	Norway
Statistics Norway	Norway
National Statistics Office	Norway
Federal State Statistics Service	Russia
Statistical Office of the Republic of Slovenia	Slovenia
nCloud	Spain
Statistics Sweden – MONA	Sweden
National Academic Infrastructure for Supercomputing in Sweden(NAISS) - BIANCA	Sweden
Scilife Lab- AIDA Data Hub	Sweden
BioMedIt	Switzerland
eDRIS	Great Britain
SHAIP	Great Britain
EMBL-EBI Embassy Cloud	Great Britain
NHS England National TRE	Great Britain
Data Access Environment	Great Britain
Secure Research Service	Great Britain
SAIL Databank (Wales)	Great Britain
National Safe Haven	Great Britain
SeRP (TRE platform)	Great Britain
Clinical Practice Research Datalink	Great Britain
QResearch	Great Britain
FSRDC (currently 33 separate, merged)	USA
SRE	USA

SRE UCI	USA
SRDE New York University	USA
SCRE UC Santa Barbara	USA

Table 1: List of Trusted Research Environments across the world, extended from [6].

The EGI also recently started a TRE Working Group. It focuses on technical and technological aspects, tools and architectures. In contrast, the idea of the RDA WG is to landscape this side of the TRE idea. Also, the EGI WG concentrates on European solutions and landscape (and takes into account also EDS and data spaces). Its chair is also part of this TRE Working Group. Although there may be some overlap, we are confident that they mostly complement each other.

4.2. Activities inside RDA

The WG-TRESD will engage with other RDA WGs whose interests overlap and ensure the alignment of our work with these groups. The WG-TRESD intends to engage with co-chairs of relevant working groups as well as members of the following groups; they are invited to regularly check our public updates via the mailing list archive.

- **TRUST Principles and Adoption WG**, to reuse the established concept of trustworthy digital repositories [4] in the context of TREs.
- **Artificial Intelligence and Data Visitation WG**, to address FAIRness in virtual research environments who are not covered by the FAIR principles for research software [5] paper.
- **Virtual Research Environments IG**, to have input on common policies and best practices, as well as specifications for underlying architectures and components and interfaces.
- **FAIR for Virtual Research Environments WG**, to address data steward requirements for human and machine-actionable interfaces to find, access, interoperate and reuse data stored in virtual research environments and output on making VREs themselves FAIR.
- **Sensitive Data IG**, to address sensitivity levels, re-identification challenges and informed consent for processing of this data. The activities can be aligned with and feed into the Virtual Research Environments IG who deals with the technical aspects of processing sensitive data. It will further have strong links to many other domain-specific WGs/IGs (e.g. health data), building on top of earlier WGs such as Working Group for Data Security and Trust (WGDST); It will also build upon numerous national initiatives and regional or domain-specific infrastructures. Though a classification of data sensitivity/confidentiality levels and access- or sharing conditions, grounding on work of e.g. DataTags[4] would be relevant, this is not feasible within the constraints (time, no dedicated funding) for this WG. We will contact the RDA Sensitive Data IG if this can be aligned within the IG.

[4] http://datatags.org/, accessed 2023-07-04

5. Work Plan

The WG-TRESD will investigate how SREs/TREs are operated and identify commonalities and compare them with best practices and standards and how SRE/TREs make sensitive data FAIR in regards to technical means. Guidance will then be developed for SRE/TRE developers on best practices / design decisions on making sensitive / closed data FAIR therein.

Not in scope of this working group is: i) developing a standard for how TREs should operate, ii) changing TRE operations, iii) training on SREs/TREs iv) implementation work v) issuing or conducting certifications.

5.1. Deliverables

The working group will refine its methods based on feedback from the review of this case statement and member input, but in general we anticipate taking these actions:

D1. *Blueprint.* Reference Model of TREs, comprising of:

- Architectural components and mapping to the actual implementation in different SREs/TREs along with the functional model (5-safes model)
- Processes
- Roles and responsibilities
- Indicators of trustworthiness as SRE/TRE provider
- Mapping of terminology (sensitivity levels, ….)

D2. *Interoperability Recommendations*. Concept, comprising of:

- Role social/technical interfaces
- Relations with existing identity federations and their architectures.
- Machine-actionable interfaces between SREs/TREs
- Legal compliance checklist for federating users across SREs/TREs
- Relevant success stories and lessons learned for interoperability
- Best practices to determine/freeze secure trusted research software suitable for federated computation
- Legal interoperability of data protection laws and SREs/TREs

D3. *Risk Catalog*. Compromising of:

- Catalog
- Recommended mechanisms to lower the risks
- Security level assessment
- Mapping mandatory + recommended tools per security level
- Collection worst-case scenarios

5.2. Timeline

- **Months 1-4:** information collection
- **Months 5-8**: consolidation/abstraction, mapping to the variety of current practices
- **Months 9-18**: consolidate and achieve community agreement on the outcomes / deliverables as a basis for subsequent adoption, deriving recommendations

5.3. Working Group Operations

The working group will have meetings online in the various sub-groups to facilitate information collection, using collaborative tools. Two calls in between the plenaries will ensure synchronization across the parallel activities to ensure outcomes and deliverables are in sync. Information will be shared via the mailing list, with a specific focus on bringing TREs/SREs across the world on-board to ensure representativeness of the insights gained. There will be in-person meetings at plenaries as well as individual sub-group meetings.

Documents will be created as collaborative Google Doc files as well as using the RDA Wiki infrastructure for the information collected, to be disseminated via the RDA WG website.

5.4. Community Engagement

The WG-TRESD engages with the community:

- Co-chairs, they are responsible for leading the WG
- Working cohort, they are engaging and actively participating in the meetings to produce the deliverables and propose the focus of the work
- Advocate cohort, they endorse, implement and disseminate the results of the WG

All community members receive regular updates on the RDA email list. The list will facilitate collaborations through invitations to webinars, workshops, demonstrations, surveys, interviews and collaborative documents. The documentation, meeting minutes, etc. produced by the WG will be publicly available on the RDA WG website.

6. Adoption Plan

The work, outcomes, and recommendations developed by this working group will be presented at RDA Plenaries and via the network of infrastructure providers, specifically data and compute centers, that may serve as adopters. This will also include industry partners who may need to provide access to sensitive data.

7. Initial Membership

The initial membership of this group will be drawn from contacts who expressed interest at previous BOF meetings, which attracted between 60-100 participants. Communications around the formation of this WG will continue to promote membership to the wider

community. Active participation as a co-chair or working group member will be encouraged as the work plan is further refined.

Co-chairs (candidates):

- Andreas Rauber, TU Wien (Austria)
- Rob Baxter, DARE UK (UK)
- Lucas van der Meer, ODISSEI (The Netherlands)
- Ville Tenhunen, EGI Foundation (Finland)
- Martin Weise, TU Wien (Austria)
- (NN, to be confirmed) (US)
- (NN, to be confirmed) (Australia)

- *<further colleagues interested in co-chairing any of the three activities foreseen, please let us know>*

References

[1] Weise, M., Kovacevic, F., Popper, N. and Rauber, A. (2022). OSSDIP: Open Source Secure Data Infrastructure and Processes Supporting Data Visiting. *Data Science Journal*, 21(1), p.4. DOI: 10.5334/dsj-2022-004

[2] RDA-CODATA Legal Interoperability Interest Group (2016). Legal Interoperability of Research Data: Principles and Implementation Guidelines. DOI: 10.5281/zenodo.162241

[3] Sikorska, J., Bradley, S., Hodkiewicz, M., & Fraser, R. (2020). DRAT: Data Risk Assessment Tool for University-Industry Collaborations. *Data-Centric Engineering*, 1, 17 DOI: 10.1017/dce.2020.13

[4] Lin, D., Crabtree, J., Dillo, I. et al. (2020). The TRUST Principles for Digital Repositories. *Scientific Data* 7, 144. DOI: 10.1038/s41597-020-0486-7

[5] Barker, M., Chue Hong, N.P., Katz, D.S. et al. Introducing the FAIR Principles for Research Software. *Scientific Data* 9, 622 (2022). DOI: 10.1038/s41597-022-01710-x

[6] Van der Meer, Lucas et al. (2023). TruSSD: Trust in Sharing Sensitive Data. Project proposal. HORIZON-INFRA-2023-EOSC-01-06.

[7] Sikorska, J., Bradley, S., Hodkiewicz, M., & Fraser, R. (2020). DRAT: Data Risk Assessment Tool for university-industry collaborations. Data-Centric Engineering, 1, E17. DOI: 10.1017/dce.2020.13

[8] Specht-Riemenschneider, L., & Kerber, W. (2022). Designing Data Trustees - A Purpose-Based Approach. Berlin, Germany. Konrad-Adenauer-Stiftung e.V., ISBN 978-3-98574-044-4.

[9] Hanisch, R., Kaiser, D. L., Yuan, A., Medina-Smith, A., Carroll, B. C. & Campo, E. M. (2023). NIST Research Data Framework (RDaF). NIST Special Publication 1500-18r1, v1.5. DOI: 10.6028/nist.sp.1500-18r1

[10] Tim Hubbard, Gerry Reilly, Susheel Varma, & David Seymour. (2020). Trusted Research Environments Green Paper. Version 2. DOI: 10.5281/zenodo.4594703