



EOSC and Trusted Research Environments

Supporting the “Five Safes”

Mark Dietrich

EGI Senior Advisor

Dissemination level: label

21/09/2023

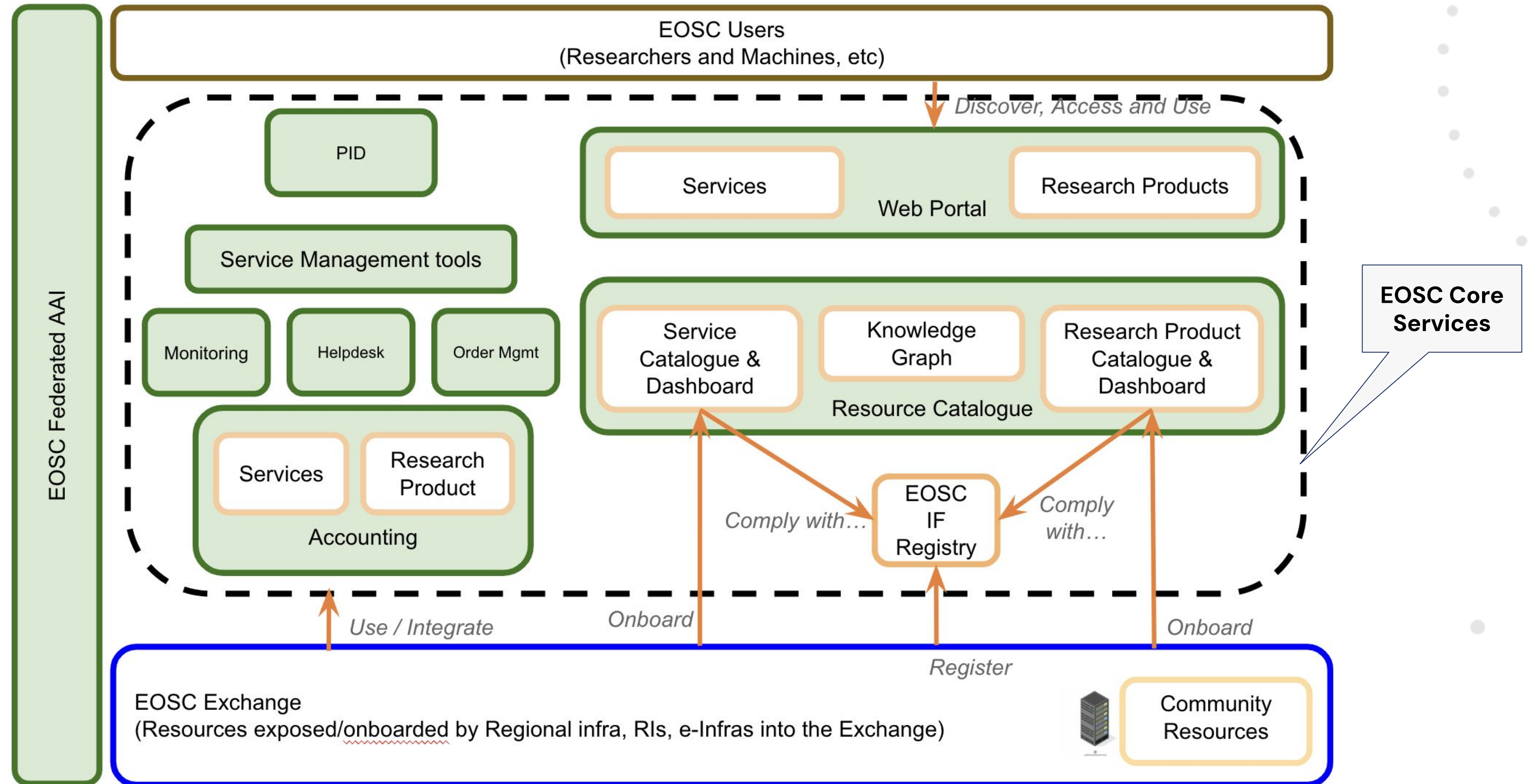
EOSC Symposium 2023

EOSC Today (thanks to EOSC Future)

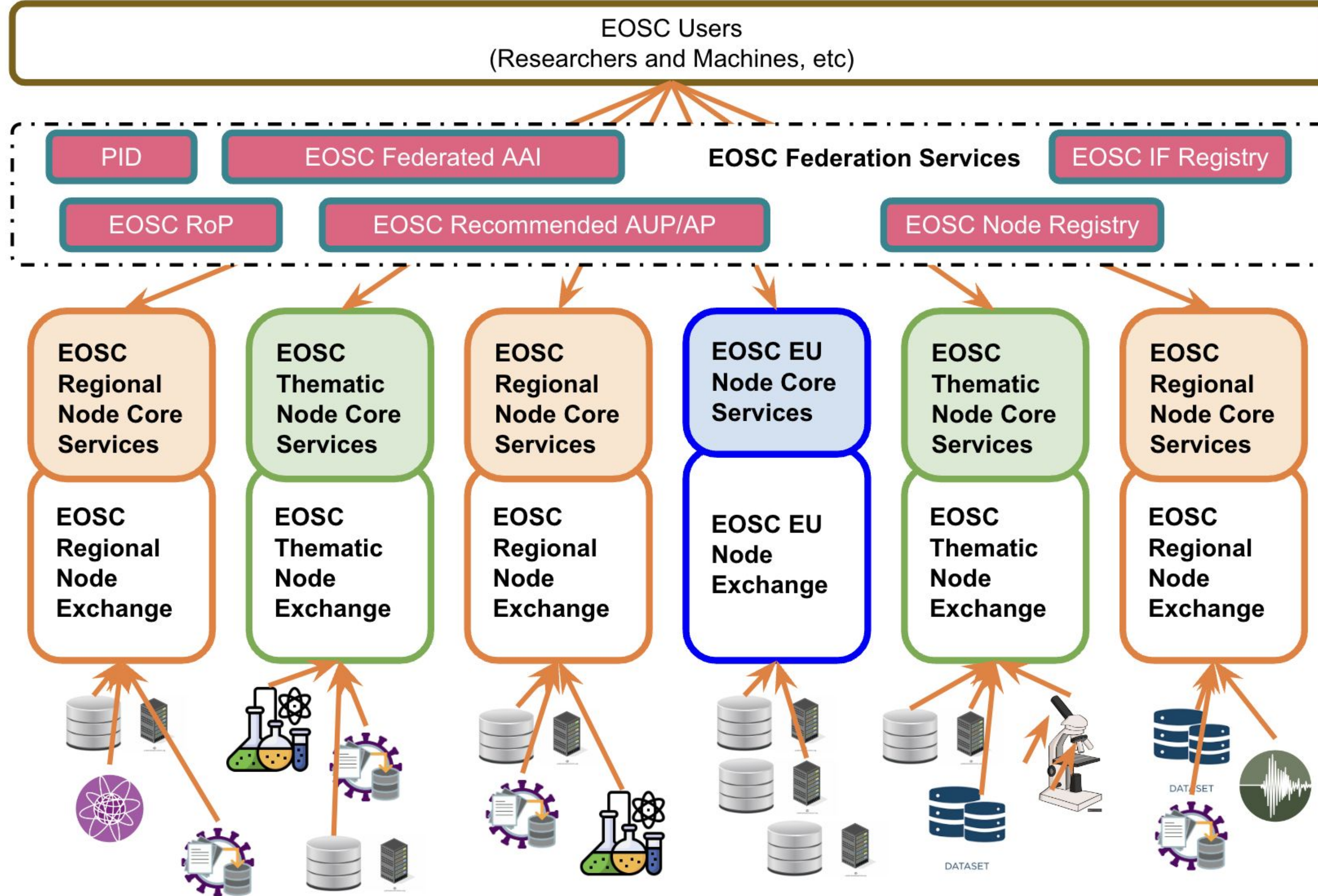
Core vs. Exchange

Actual Resources come from RIs, communities, etc.

- “Home” communities remain responsible – and accountable – for their assets and services.
- EOSC Core Services work to enable findability, accessibility, and interoperability.
- The Interoperability Framework (IF) plays an important role in this.

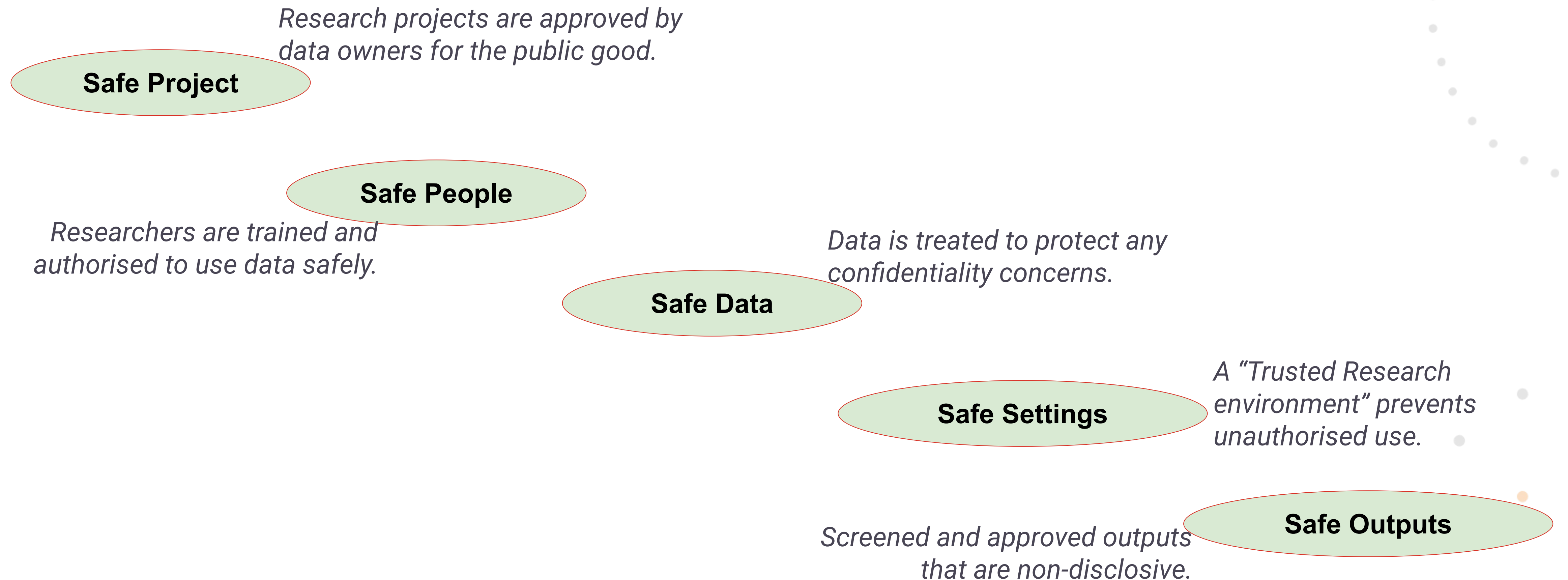


EOSC Tomorrow (possible Node-based architecture)



Five Safes

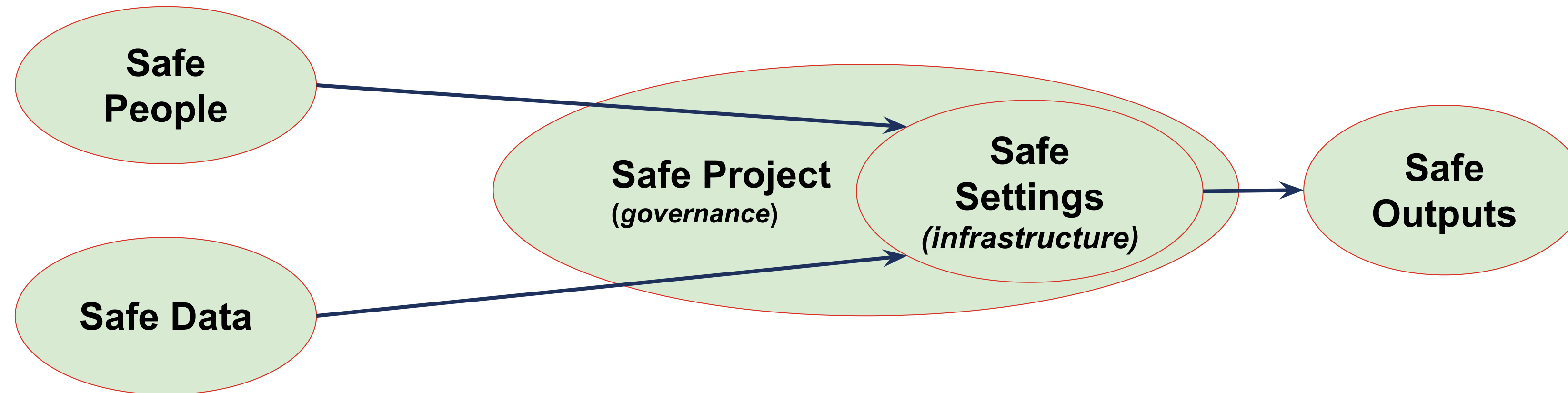
Originally proposed (2017) for safe handling of national statistical data, e.g. from censuses. Extended to health data by UK HDR and others.



Building Trusted Research Environments
Principles and Best Practices; towards TRE ecosystems
DOI: <https://doi.org/10.5281/zenodo.5767586>

Five Safes

Architectural concept



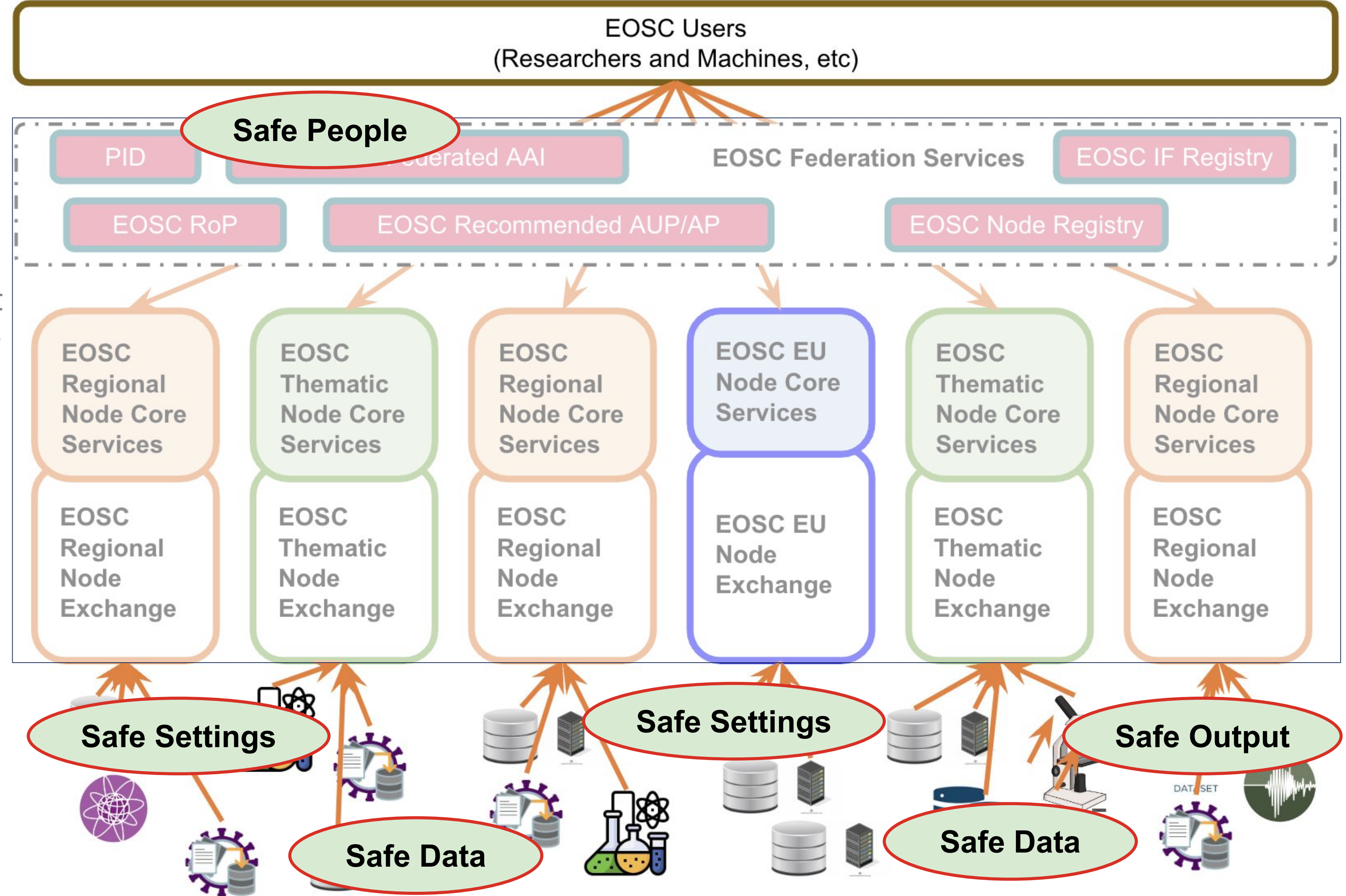
4 Enhancements to Support 4 "Safes"

Safe People: Stronger assurance levels for authentication, plus certifications (as attributes)

Safe Settings: More complete declaration/transparency about security, jurisdictions, SW stack, etc

Safe Data: More complete declaration of "data types" and "data characteristics", as well as support for access/use control for each piece of data.

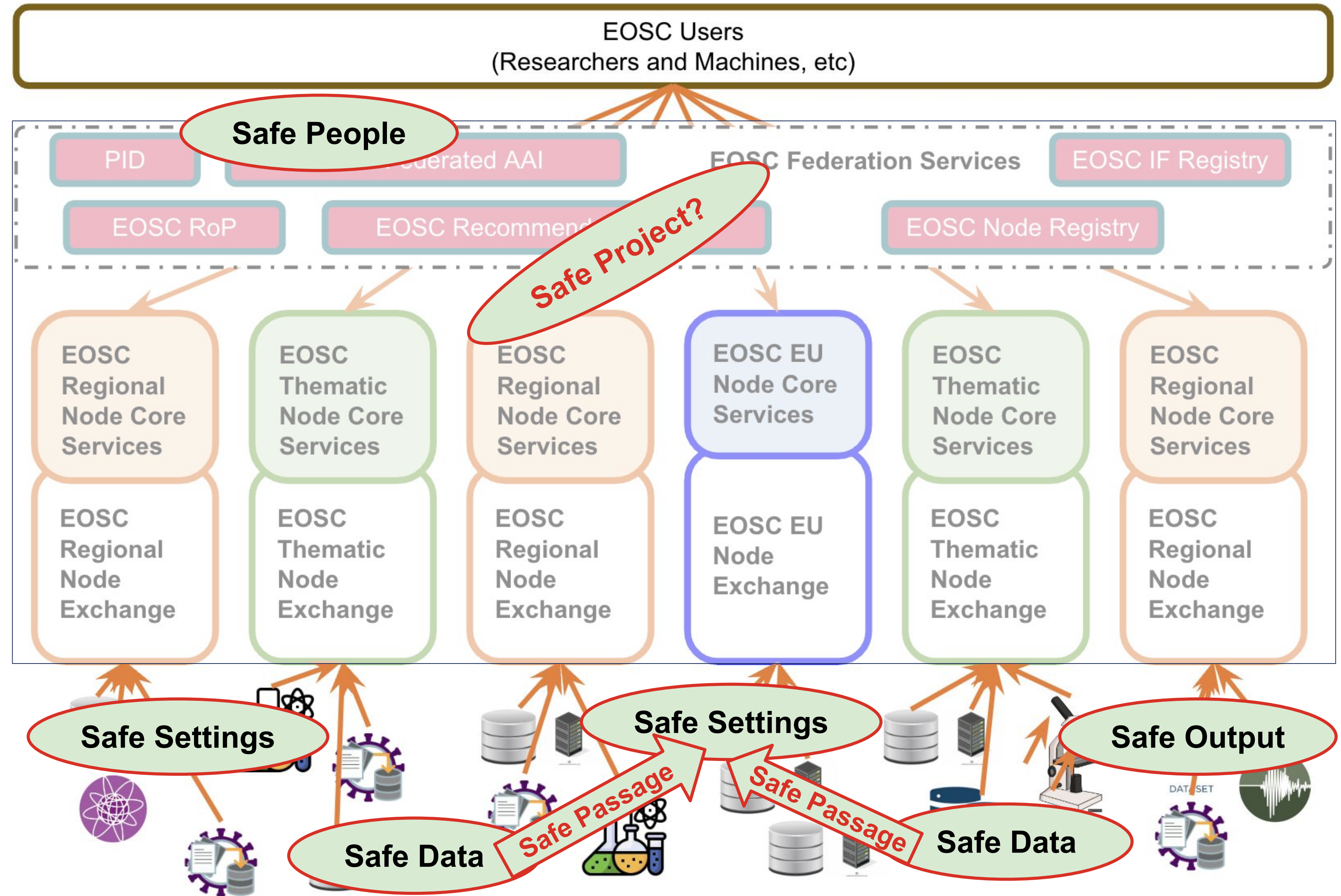
Safe Output: Like Safe Data, more complete declaration of "data types" and "data characteristics", as well as support for access/use control for each piece of data.



2 New Requirements?

Safe Passage: Like “Safe Settings” – how can Safe Data be moved to a new Safe Setting?

- Safe Projects:** New Governance Structure to control access to Data, TREs, etc.
- Variation on Groups & VOs?
 - Extension of “projects” already introduced in EOSC Marketplace (but more robust)
 - Something brand new?



- EOSC could potentially support the full “Five Safes” secure data management methodology
- Enhancements would be needed:
 - **Safe People:** Stronger assurance levels, plus certifications, in identity management
 - **Safe Data/Output:** Enriched metadata for declaration of existing sensitive data, plus mechanisms to manage access and use of that data
 - **Safe Settings:** Enriched metadata for declaration of security levels for TREs – certifications, security procedures, SW stack and allowed/supported analytics.
- New Capabilities
 - **Safe Passage:** allowing Safe Data to be moved “safely” from current location to agreed destination Safe Setting
 - **Safe Project:** a new governance structure, similar to, but stronger than, Groups and Virtual Organisations, to manage an entire Safe Project.

Note: Many of these requirements mirror requirements found in Data Spaces – so if EOSC wants to interoperate with Data Spaces, meeting similar requirements may be necessary.

Safe Project: Adopt/Implement Data Space solutions within EOSC – a closed environment, with clearly defined resources (data, services), participant management (credential based), as well as “export” controls.

- Links to “Research Activity” ID?
- Possible registry of Safe Projects – as subset of Data Spaces?

Safe People: W3C Verified Credentials/Verified Presentation, with “Five Safes” specific vocabulary of credentials/attributes. Includes stronger assurance identities (bound to legal or natural person, including eIDAS).

Safe Data: Attribute-based Encryption. Tokenized attribute/credential “vocabulary” (W3C VC/VP), used to encrypt data. Only users possessing the required credential types can decrypt.

- Although not required for Five Safes, “universal” data type vocabulary (aligned with legal requirements) might provide a useful higher-level framework for this approach.

Safe Passage: Trusted data transfer services, operating between well-identified Safe Settings (registry?)

Safe Settings: Trusted analytics services (includes transparent declaration of SW stack, location of infrastructure, legal owner, legal operator, security certificates, etc.)



Contact us

Join the Discussion!

Get in touch

mark.dietrich@egi.eu