Understanding trust frameworks: goals and components identified through a case study

Louise van der Peet[1][0009−0008−5022−4279], Nitesh Bharosa[1][0000−0002−3919−6413], Sander Dijkhuis[2], and Marijn Janssen[1][0000−0001−6211−8790]

[1] Delft University of Technology, Delft Netherlands
[2] Cleverbase, The Hague Netherlands

Abstract. Amidst increasing online data sharing among organisations, there is a growing need for interoperability and trust in the digital space. When there is no infrastructure provider for sharing information (e.g. by Big Tech players and / or government-owned infrastructures), public and private actors must figure out how to reach agreements about the technical specifications and data infrastructure components to facilitate inter-organizational collaboration. This paper zooms in on the empirical phenomenon of trust frameworks emerging in practice. The main research question is twofold: (1) what are the goals actors strive for with trust frameworks and (2) which components are developed for achieving these goals? Drawing on previous literature and a case study approach, interoperability, certainty, efficiency, and security emerge as goals of trust frameworks. As for the second question, we draft an exhaustive diagram of components from both the literature and our case study. This explorative research lays the foundation for future research into trust frameworks as a major change in traditional approaches to cross-sector data exchange.

Keywords: Trust frameworks · Digital governance · Data interoperability

1 Introduction

Globally, digital data sharing has reached unprecedented heights, organisations and individuals (unintendedly) share massive amounts of data. There is an ongoing steep data growth going on, with only 2 zettabytes in 2010, and in 2025 it is projected to be 181 zettabytes [23]. As shared data volume and sensitivity continue to grow, so does the need for robust mechanisms to ensure secure, efficient and trustworthy data sharing across various sectors and organisations. This is especially true for situations where sharing incorrect data can have legal consequences. Examples include applying for public services, filing corporate reports and buying a house [7]. In such cases, all actors seek legal certainty, for instance about the identity of the supplier and receiver of data, as well as the confidentiality, integrity and availability of digital infrastructure components. When there is no infrastructure provider (e.g. by Big Tech players and / or government-owned

infrastructures), organisations must themselves make to agreements about various specifications and data infrastructure components needed for interoperability and trust for inter-organizational data sharing. In other words, they are developing trust frameworks which guide information sharing among public and private organisations. The need for interoperability across organisations and sectors is recognized on a broader scale, as shown by the interoperability initiative in the European Union, the European Interoperability Act. This legislation aims to promote a more open and secure digital space, encouraging cooperation across borders and sectors [20].

Against this background, this paper zooms in on the empirical phenomenon of trust frameworks. Trust frameworks are capturing how actors seek to build cross-organisational and cross-sectoral interoperability and trust.

An example of such a framework in action is MedMij [13], a Dutch initiative aimed at establishing a secure and reliable ecosystem for health data exchange. MedMij serves as a set of standards and agreements designed to ensure that personal health data can be shared securely between healthcare providers' and patients' personal health environments. Prior to MedMij, the healthcare sector faced significant challenges due to the disparate methods of data sharing among various healthcare providers. These inconsistencies can lead to fragmented patient information, inefficiencies, and increased risks to patient privacy [11]. MedMij addresses these problems by providing a unified framework that standardizes data exchange processes. This framework enables patients to gain control over their health data, merging information from various sources into one single location. Medmij was developed through collaboration between healthcare providers, app developers, patient representatives and personal health environment providers. These efforts have resulted in a secure, interoperable framework that empowers patients to manage their health data while promoting efficiency and privacy.

While organizations are increasingly incorporating trust frameworks, such as the MedMij framework, there is little scientific literature providing a conceptualization of trust frameworks, and in the literature that exists, there is no complete consensus on the term (section 3 provides more details).

This explorative paper aims to introduce a clearer understanding of trust frameworks. Our goal is to comprehensively conceptualize trust frameworks, including components and goals. Accordingly, the main research question is twofold: (1) what are the goals actors strive for with trust frameworks and (2) which components are developed for achieving these goals? By offering a conceptualization informed by literature and empirical evidence, this research aims to contribute to theory building on trust frameworks, advancing academic scholarship and practical applications. This paper proceeds as follows. Section two presents the research approach followed and section three provides a conceptu-

alization of trust frameworks. Section four reveals the findings of the empirical case study. Section five concludes this paper and presents directions for future research.

2 Research Approach

The objective of this explorative paper is to gain a better understanding of trust frameworks, particularly the definition, components and goals. We follow a three-step approach in order to achieve the objective. First, we conduct a systematic literature review on the concept of trust frameworks, allowing for the development of a lens for investigating the case study. The main goals of this literature research is to find components of trust frameworks in the literature, and a robust definition for the term. We employed thematic analysis to identify and cluster key components into broader categories, ensuring a systematic and rigorous understanding of trust frameworks. Section 3 provides an overview of the findings of the literature review.

Second, we conduct an empirical case study that zooms in on the ongoing development of a trust framework called Trusted Information Partners (TIP) [25]. TIP is a public-private system of agreements for the exchange of digital data, primarily with significant financial or legal impact. Yin [27] proposes that case studies contribute to the examination of contemporary phenomena within their natural context, especially in new phenomena where existing theory might be limited; and that a single use case study is well-suited for exploratory research aimed at theory development. The TIP case study was chosen due to its widely collaborative nature, involvement in the public sector, and because it is used for the purpose of data sharing, making the case relevant for the research goals. The qualitative data was collected through semi-structured interviews, with representatives from different organisations.

We interviewed a total of eight experts involved in the case study. The interviewees were gathered through the network of the researchers, the criteria for the interviewees being that they are actively involved in the development of TIP; and have expertise on some aspect of digital data sharing. The respondent description can be found in table 3. Each interview lasted around 60 minutes. Three main goals were pursued in the interviews: (1) find a common definition for trust frameworks, (2) gather the essential components for trust frameworks, and (3) find the goals that are pursued using trust frameworks. The resulting interviews were recorded, transcribed, validated by the respondents, and analysed by comparing common themes. This analysis involved thematic coding, where each interview transcript was examined line-by-line to identify and categorize mentioned goals and components, allowing for the systematic identification of recurring themes.

Lastly, the findings from the literature review are compared with the findings from the interview. The main findings of this comparison are captured in figure 1. This leads to a greater understanding of the components and definition of trust frameworks.

3 Conceptualizing Trust Frameworks

We searched the literature for examples of trust frameworks, in order to establish a definition and conceptualization. A Scopus 'title-keyword-abstract' search for the keywords *'trust framework'* and *'governance'* in November 2023 reveals 37 papers.

Alternative terms such as *'trust model'*, *'trust scheme'*, and *'trust protocol'* were considered but ultimately excluded from the primary search. The reasons for this exclusion are twofold: (1) these terms are often related to quantifying trust for better decision making, rather than creating a practical framework that can be used without trust among the participants; and (2) including these terms leads to more irrelevant results in the systematic review. For instance, the term *trust model'* refers to "methods on how to model and quantify trust with sufficient detail and context-based adequateness" [5]. 'Trust schemes' help automate trust decisions by leveraging technical standards, legal regulations, and infrastructure, highlighted by More [15]. Lastly, 'trust protocol' refers to a method for modeling indirect trust [21]. Including these terms would thus dilute the focus of our review and lead to less relevant literature being considered.

In the set of papers, only one contains a definition for the term trust framework. Brewer et al. [3] take a definition from the white paper of the National Institute of Standards and Technology (NIST) [24] where trust frameworks are defined as following:

> "a generic term used to describe a legally enforceable set of specifications, rules, and agreements that govern a multi-party system established for a common purpose, designed for conducting specific types of transactions among a community of participants, and bound by a common set of requirements".

All other papers in the review use the term one or multiple times throughout the paper, but never refer to its definition. This confirms our starting point, that there is no universal definition for trust frameworks. Furthermore, the term is also used to describe a framework for conceptualizing trust, rather than the sort of practical framework that builds cross-organisational and cross-sectoral interoperability and trust that we aim to discuss. [6] [9] [14] [18]. In this analysis we will mostly focus on the practical perspectives on trust frameworks.

In the literature that describes practical frameworks, we identify several common components of trust frameworks that recur across the literature as outlined

Study	Technical specifications	Governance specification	Operational requirements	Legal requirements
[1]	✓	✓		
[2]	✓	✓	✓	✓
[3]	✓	✓	✓	✓
[4]	✓			
[8]		✓		
[10]	✓		✓	
[12]	✓		✓	✓
[16]		✓	✓	✓
[19]	✓	✓	✓	✓
[22]	✓	✓		

Table 1. Categories of trust framework components in the literature

in table 4. In this context, the term 'components' is defined as something needed in order to facilitate information sharing or the governance of information sharing. We extracted all components from the literature, and group these into categories: similar components were clustered together based on their purpose and through this grouping patterns emerge, allowing the discerning of categories. Four categories emerge from this analysis: operational requirements, legal requirements, governance, and technical implementation.

- **Operational Requirements**: These are the procedural and protocol-driven aspects critical for the daily functionalities and security measures of the trust framework, including data operations and technical specifications.
- **Legal Requirements**: This category represents the compliance and regulatory framework, ensuring alignment with legal standards and practices through e.g. audit schemes and terms of service.
- **Governance**: Governance components outline the organizational structure and the distribution of roles within the framework, detailing the mechanisms for auditing, validation, and collaboration among stakeholders.
- **Technical Implementation**: Most of the literature relies on technical specifications to model a trust framework. This occurs in various forms, from the implementation of user dashboards [19] to the application of blockchain methods [22].

Furthermore, in the literature we found a diverse application of trust frameworks across several sectors. For example improving data exchange in the food and agriculture sector [3] [19], and improving trust among users of virtual environments [4] [12] . The wide range of sectors applying trust frameworks underscores the universal relevance of trust frameworks in fostering trust and security across various industries.

We further identify the goals of the trust frameworks. These can be summarized into five categories:

- **Security and privacy**: nine out of ten of the relevant papers mention security and privacy as a goal of the trust framework. More specifically, privacy of personal data [3] [8] [10] [12] [16], and the security principles of the CIA triad (confidentiality [16], intergrity [10] [1], availability [12] [16] [22]) are common goals in the literature.
- **Certainty and compliance**: Increasing certainty and compliance is another goal. Certainty in the form of accountability [2] [16] [19], and in the form of reliable information [4] [10] [22] were most common in the literature. Compliance to privacy regulations [3] [16] and legal certainty [2] could be important, with frameworks designed to align with existing laws and standards to facilitate adoption and integration into current systems.
- **Societal impact:** Trust frameworks in different sectors have different goals in terms of societal benefits. From the improvement of food safety and quality [3], to maintaining free movement during the COVID-19 pandemic [8]. More common goals in this category are: users' control over their personal data [9] [10] [19] [22]; establishing ethics and shared values [2] [12] [22]; and increasing transparency [19] [22].
- **Interoperability and scalability:** Interoperability is a goal that emphasizes the need for systems and technologies to work together seamlessly, it is specifically mentioned as a goal in two previous works [8] [16]. Scalability [22] and multi-lateral data exchange [3] are found as goals as well.
- **Efficiency:** Efficiency is mentioned only by one study as a goal [3]. This trust framework promotes efficiency by means of supply-chain efficiency, and by unlocking the full potential of already-existing technologies.

An overview of which relevant work contains which categories of goals can be found in table 2.

	Security & privacy	Certainty & compliance	Societal impact	Interoperability & scalability	Efficiency
[1]	✓				
[2]	✓	✓	✓		
[3]	✓	✓	✓	✓	✓
[4]		✓	✓		
[8]	✓		✓	✓	
[10]	✓	✓	✓		
[12]	✓		✓		
[16]	✓	✓		✓	
[19]	✓	✓	✓		
[22]	✓	✓	✓	✓	

Table 2. Categories of trust frameworks' goals in the literature

A unified understanding of trust frameworks is still missing, underscoring the need for a more cohesive conceptualization.

4 Case study: Trusted Information Partners

4.1 Background

Trusted Information Partners (TIP) is an initiative consisting of public and private parties in the Netherlands, where the goal is to increase ease and trustworthiness of online interactions for citizens, businesses and government. The collaborating partners share a vision that once citizens and entrepreneurs have access to a high level of assurance; electronic identities; functions for personal data management; and exchange within relevant legal frameworks, eSociety would function without paperwork. The resulting product of this collaboration is a cross-domain public-private trust framework. For this, components are specified and governed regarding the following topics:

- Identities at a high level of assurance (conform eIDAS)
- Qualified trust services (conform eIDAS)
- Methodology for legal representation with a high level of assurance
- Methodology for funding of collective functionalities and (maintenance of) the trust framework
- Shared digital infrastructure for information exchange
- Trusted registration and publication of service and chain specifications
- Discovery of shared information services
- Payment system for services delivered within the ecosystem.

The trust framework is an implementation of the European eIDAS regulation (EU) 910/2014 [26], establishing trust frameworks for electronic identification and trust services in the internal market. As stated in the eIDAS recitals, there is a need for online trust and legal certainty.

> "(1) Building trust in the online environment is key to economic and societal development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services."

> "(2) This Regulation seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union."

Whereas eIDAS establishes minimum legal and technical requirements and standards to enable electronic transactions, the regulation does not replace member state laws and agreements. The way electronic identification and trust services are applied differs per member state. The partners in TIP aim to leverage the legal and technical standards of eIDAS in a public-private collaboration to design, govern and contribute to the adoption of qualified information exchange on a shared infrastructure in a common trust framework.

4.2 Interview results

We have interviewed eight experts who are all currently part of the TIP collaboration. Table 3 provides an overview of interview respondents. These respondents were selected based on their expertise in developing components. Seven out of the eight respondents have been involved in the implementation of at least one other trust framework. In this section we will discuss how respondents define trust frameworks and what they see as the goals for trust frameworks.

Respondent	Role	Expertise
1	Product owner data exchange at public organisation	maintenance and standardisation of trust frameworks, governance
2	Customer journey expert at private organisation	finance, digital innovation
3	Advisor for digital society at public organisation	governance, standardised information exchange development of trust frameworks
4	Policy officer at public organisation	control over data, data sharing, government transparency, data governance, policy frameworks
5	Product owner and security officer at private association	tech, finance, efficiency, security and privacy, enterprise architecture, requirements
6	Business architect at private organisation	compliance, process design, management, data sharing, cyber security
7	CTO at private organisation	taxonomies, technical strategies and operations, standard reporting
8	Project manager innovation at private organisation and ecosystem developer via foundation	ecosystem development, control over data, communication, strategy, standardisation

Table 3. Overview of interview respondents

Definition When discussing definitions of trust frameworks, respondent 1 described the need for an independent regulatory organisation (possibly the government), respondent 3 mentioned the introduction of processes or technology in a standardised way, and reliable communication, while respondent 6 mentioned multiple parties in a chain working together to introduce agreements. It is important to note that these definitions offer valuable perspectives on trust frameworks, focusing on agreements, standards, and regulatory conditions. However, no definition given is exhaustive. Five out of eight respondents did not give a concise definition of the term.

Components All of the respondents named components from all four previously identified categories: legal, governance, operational and technical. The following new components were identified, and were found important by multiple interviewees:

- Future-proof technology (respondent 2 and 3)
- Financial liability (respondent 1, 2, 4, 5, 6, 7 and 8)
- Code of conduct (respondent 1, 2, 5, 7 and 8)
- Trust services (respondent 1, 3 and 7)

The following was mentioned by only one respondent:

- Data stewardship (respondent 7)

We add these components to the components found in the literature in figure 1 to create a comprehensive overview.

Another interesting finding from the interviews is that two respondents (2,5) stressed that a trust framework should contain technical guidelines, but no implementations. This is significantly different from what the literature regards as trust frameworks, where the majority of the papers focused on the technical implementation as the core of the trust framework.

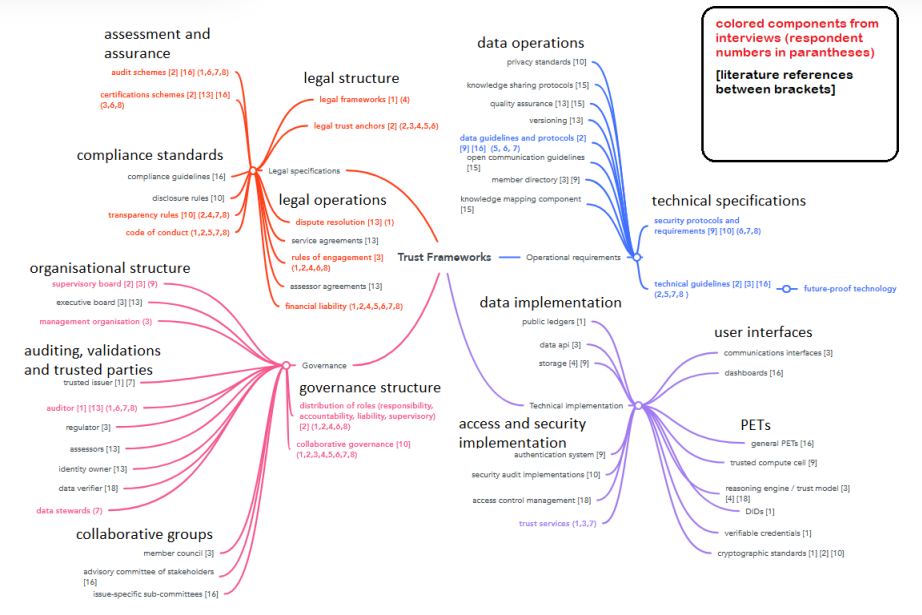

Fig. 1. Components of trust frameworks in the literature and from interviews

Taking these results into account: often the respondents do not necessarily agree with the literature, and some components of trust frameworks are only mentioned in one paper or by one respondent. We can therefore consider the components described in figure 1 as exhaustive but not exclusive to the components of trust frameworks. Table 4 describes the subcategories that these components are divided in.

Goals The goal of trust frameworks came forward more strongly in the interviews, and can be summarized into six main categories: efficiency, interoperability, certainty, security, economic viability, societal impact.

Efficiency

All respondents mentioned efficiency as a goal of trust frameworks in one way or another. Respondent 3 mentioned that the standards created by trust frameworks are necessary for large-scale innovation:

> "Trust frameworks are essential, and generally digitalization consists of trust frameworks. (...) If we do not make agreements on how video works, then my camera would not work with both Zoom and WebEx. So if you want to work on innovation and create large-scale innovation in a chain, forms of standards will emerge."

Efficiency also extends to regulatory compliance, where trust frameworks could streamline this process and reduce complexities of compliance. By adhering to standardized protocols, organizations can navigate regulatory requirements more effectively, saving time and resources while ensuring adherence to legal obligations. Respondent 5 mentioned that trust frameworks generally require fewer resources to create a solution for everyone, after which it is widely implementable. This type of widely implementable standard will most likely emerge from Europe or the US and Big Tech according to one respondent, but it is not useful to wait until this happens:

> "The Netherlands does not decide the world standard, not even Europe. We could wait for an American or Big Tech standard, but there is no use to that. [So right now] we are looking at how we can make it better in the Netherlands."

Four respondents (1, 4, 5, 8) mentioned that there currently are enough technical solutions to make this large-scale innovation work, but they are not used on a large scale as of now. Trust frameworks could use these techniques for increased quality and efficiency of information chains.

Interoperability

Interoperability, or more specifically syntactic interoperability, is the application-level interoperability that allows multiple software components to cooperate even

though their implementation languages, interfaces, and execution platforms are different [17]. Respondent 8 exemplifies how oftentimes when we use terms to describe data we are not exactly talking about the same concept:

> "[It is important] to use the same language. For example, if you would like to know someone's income, what do you mean? Is that the fiscal income? There are a lot of definitions for the term. That could lead to difficult situations, because something might have been meant differently then it is interpreted, and this results in poor information exchange."

This interoperability could be achieved through the adaptive standardisation that a trust framework provides. Two respondents (6,7) also mentioned that this interoperability could reduce vendor lock-in within domains. Trust frameworks describe the requirement for services and the communication between them. Several parties can join and more suppliers could emerge around the same service. The trust framework would assure that these communicate in the same manner, making the barrier for switching between vendors minimal.

Certainty

Certainty of data and documents, as well as legal certainty have operational and societal implications. All respondents mentioned that the quality of data, the certainty of data transfers or the legal certainty of documents would improve when standards are in place to make set conditions for this data. Respondent 6 exemplifies improved legal certainty:

> "It is mostly about the certainty that [for example] an accountant would have: 'This [document] was actually sent by the municipality or the tax authorisation, so I can use this in the process with certainty'"

Moreover, respondent 7 mentions that in an increasingly digitalized world where face-to-face interactions are limited, trust frameworks can play a role in enabling certainty and trust without physical contact, mitigating risks associated with digitalized or remote engagements.

Security

All respondents mentioned security as a goal of trust frameworks in one way or another. Online security could increase for businesses as well as individuals. Respondent 6 mentioned that trust frameworks could help create an official digital address making sensitive interaction far more safe:

> "Currently there is no [all-purpose] digital address for individuals. Email addresses are not official digital addresses. (...) If I would like to work digitally, I need a digital address where the tax authorisation, government, private organisations, etc can reach me in a trusted and secure manner."

The increase of digital business will also increase fraud opportunities in online networks. When state-of-the-art technical standards are widely used, and implemented in a standardised way, the risk for fraud could decrease. Personal data will in turn also be shared and kept more securely. Fraud in digital environments happens in numerous ways, respondent 2 illustrates this with how we currently sign digitally:

> "You give someone something very personal, namely your signature. This might not be perceived as very personal, but it is. In that organisation [which you send your autograph to], you have no idea what people could do with it. Someone could save it, everyone can see it"

Respondent 7 speaks of creating a comfort zone where parties can trust each other through security measures and agreements, and data can be shared safely:

> "What might be the most important part of trust frameworks (...) is the creation of a certain comfort zone where people can share data. (...) It is often about data that can be very sensitive, or where decisions are being made with a societal impact. The comfort zone is the security: will we not lose the data? What is the source? Is there a risk for a man-in-the-middle attack? Using security, you earn trust."

Overall trust frameworks would model trust and security more similarly to how it is modelled in the physical world, where trust is created through agreements and laws. As illustrated by respondent 8:

> "When you get into a public bus, you probably do not think 'I should check the brakes of this bus.'. Sometimes it is logical that we do not think about this anymore. In our digital world [this is different]: when you install an app or use a service, there is often be an entire book's worth of policy on how your data will be processed, and you have to find out legally what is written and what is actually meant. [You could compare this] with finding out by yourself whether the brakes work before using the app or service. Many people will therefore click 'accept' because few people will have the time, willingness or knowledge to [micromanage their trust]."

Economic viability

Six respondents (1,2,3,5,6,7) mention some form of economic gain in the use of trust frameworks. If many parties use one system, the costs will go down. Furthermore, the increased digitalization of data could reduce administrative costs, according to respondent 1:

> "A lot of documents [in healthcare] are being retyped. The standards and the way of work in TIP could be a blessing for hospitals to reduce their costs and solve the problem [of re-entering information]."

Respondent 7 names the reductions of administrative costs that results from the decrease of paperwork. Moreover, respondent 2 names that the increased ease of doing online business could also give a boost to the internet and online business.

Three respondents (1,2,7) mention that mutual relationships and the creation of new business relations is another goal for trust frameworks. The enhanced trust fosters stronger partnerships and collaborations, leading to more efficient and productive business interactions. The frameworks also lower the barriers of entry for businesses seeking to enter new markets or engage with new partners. Through interoperable standards and protocols, businesses can connect with a broader network of suppliers, customers, and stakeholders. These relationships and the network creates opportunities for knowledge sharing. By promoting open collaboration and information exchange, trust frameworks facilitate the sharing of insights, expertise, and resources across domains. Through collaborative platforms, businesses can learn from each other's experiences, leverage emerging technologies, and drive continuous improvement and innovation.

Societal impact

All respondents agreed that societal causes could benefit from the implementation of trust frameworks. The following examples were named that could be partially alleviated by trust frameworks:

- irrefutability of documents and identities is not sufficiently guaranteed (2,6,7)
- leaking or losing of important information with societal impact (7)
- unfair distribution of costs and benefits in business (4, 7)
- lack of certainty for citizens due to processing times of public organisations (7)
- closed business format and lack of inclusivity (7, 8)
- high administrative load on healthcare workers (1)
- lack of open, honest and transparent processes (2, 4, 7, 8)
- citizens being excluded to means e.g. people who do not have access to financial means (2)

However, respondent 5 argues that societal causes will never be the main goal for trust frameworks, as the incentive will always come through some operational or financial goal.

5 Conclusions and future research

This explorative paper provides a comprehensive conceptualisation of trust frameworks, including components and goals. Drawing on literature and the case study, we can answer the three research questions as follows.

Considering the first research question (what are the goals actors strive for with trust frameworks?), we found that the literature broadly outlines goals within six categories: security and privacy, certainty and compliance, societal impact, interoperability, efficiency, and trust. The goals emerging from the case study can be categorized into six categories: efficiency, interoperability, certainty, economic viability and societal impact. Out of these goals, all respondents agreed on four of them: interoperability, certainty, efficiency and security. All four of these goals also emerge from the literature. While the other goals were not agreed upon to be a universal goal of trust frameworks.

Considering the second research question and (which components are developed for achieving these goals?), we found four categories of components: technical specifications, governance, operational requirements, and legal requirements. However, even though technical specifications are widely used as a component in the literature, not all respondents agree that this should be a part of trust frameworks. Similarly, even though the categories of components can be mostly agreed upon, a fair amount of the components that we found are only mentioned in one article or by one respondent, indicating even more that there is no consensus on the essential components of trust frameworks. Therefore, no minimal set of components for trust frameworks has been found.

The research, while explorative, lays the foundation for future research into trust frameworks. Trust frameworks represent a major change in traditional approaches to cross-sector data exchange and could use further research and development. By investigating trust frameworks across diverse use cases, exploring their transformative potential, and drawing upon insights from analogous concepts, we can progress the academic literature and provide real-world solutions for complex problems. Future research should expand to multiple use cases, to explore trust frameworks in various sectors and contexts for a more complete view. Additionally, drawing parallels with analogous concepts from related fields may offer novel perspectives and methodologies that can help in the development of trust frameworks.

category name	description	example
Legal specifications		
assessment and assurance	Processes and schemes focused on ensuring compliance and standards through audits and certifications.	Audit schemes, certification schemes.
compliance standards	Guidelines, rules, and codes established to ensure legal compliance within the organizational framework.	Compliance guidelines, transparency rules.
legal structure	Frameworks and anchors that define the legal basis and requirements for operations.	Legal frameworks, legal trust anchors.
legal operations	Operational aspects related to legal matters	Dispute resolution, service agreements.
Governance		
organisational structure	The structure and roles within the organization, including various boards and management entities.	Supervisory board, executive board.
auditing, validations and trusted parties	Responsibilities and roles of entities involved in auditing, validation, and secure issuing.	Trusted issuer, auditor, regulator.
collaborative groups	Groups established for collaborative purposes within governance	Member council, advisory committee.
governance structure	Structure for governance, focusing on the distribution of roles.	Distribution of roles, collaborative governance.
Operational requirements		
data operations	Operations related to managing data.	Privacy standards, knowledge sharing protocols.
technical specifications	Specifications detailing the technical requirements, protocols, and guidelines for systems.	Security protocols, technical guidelines.
Technical implementations		
data implementation	Implementation aspects concerning technical data management.	Public ledgers, data APIs.
access and security implementation	Implementation aspects related to access control, security measures, and trust services.	Authentication systems, security audit implementations.
user interfaces	Interfaces designed for user interaction with systems.	Communications interfaces, dashboards.
PETs	Technologies aimed at enhancing privacy, including models, standards, and trusted environments.	General PETs, trusted compute cell.

Table 4. Components of trust frameworks

References

1. Abramson, W., Hall, A., Papadopoulos, P., Pitropakis, N., Buchanan, W.: A Distributed Trust Framework for Privacy-Preserving Machine Learning, vol. 12395 LNCS (2020). https://doi.org/10.1007/978-3-030-58986-8_14
2. Bharosa, N.: The rise of govtech: Trojan horse or blessing in disguise? a research agenda. Government Information Quarterly **39** (2022). https://doi.org/10.1016/j.giq.2022.101692
3. Brewer, S., Pearson, S., Maull, R., Godsiff, P., Frey, J., Zisman, A., Parr, G., McMillan, A., Cameron, S., Blackmore, H., Manning, L., Bidaut, L.: A trust framework for digital food systems. Nature Food **2**, 543–545 (2021). https://doi.org/10.1038/s43016-021-00346-1
4. Cardoso, R., Gomes, A.: Towards a trust framework for multi-user virtual environments, vol. 8579 LNCS (2014). https://doi.org/10.1007/978-3-319-09144-0_52
5. Cho, J.H., Chan, K., Adali, S.: A survey on trust modeling. ACM Computing Surveys (CSUR) **48**(2), 1–40 (2015)
6. Das, A.: Developing dynamic digital capabilities in micro-multinationals through platform ecosystems: Assessing the role of trust in algorithmic smart contracts. Journal of International Entrepreneurship **21**, 157–179 (2023). https://doi.org/10.1007/s10843-023-00332-7
7. Dijkhuis, S., Van Wijk, R., Dorhout, H., Bharosa, N.: When willeke can get rid of paperwork: a lean infrastructure for qualified information exchange based on trusted identities. In: Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age. pp. 1–10 (2018)
8. Gerybaite, A.: Digital governance: The case of proofs of vaccination. pp. 450–454 (2021). https://doi.org/10.1145/3494193.3494254
9. Getha-Taylor, H.: Cross-sector understanding and trust. Public Performance & Management Review **36**(2), 216–229 (2012)
10. Hardjono, T., Deegan, P., Clippinger, J.: Social use cases for the id3 open mustard seed platform. IEEE Technology and Society Magazine **33**, 48–54 (2014). https://doi.org/10.1109/MTS.2014.2345197
11. Iroju, O., Soriyan, A., Gambo, I., Olaleke, J., et al.: Interoperability in healthcare: benefits, challenges and resolutions. International Journal of Innovation and Applied Studies **3**(1), 262–270 (2013)
12. Kharvi, P.: Security risks, user privacy risks, and a trust framework for the metaverse space. pp. 119–123 (2023). https://doi.org/10.1109/MetaCom57706.2023.00033
13. Kusiak, L.: Baas over eigen zorgdata. Zorgvisie ICT **19**(4), 12–14 (2018)
14. Lu, B., Zhang, T., Wang, L., Keller, L.: Trust antecedents, trust and online microsourcing adoption: An empirical study from the resource perspective. Decision Support Systems **85**, 104–114 (2016). https://doi.org/10.1016/j.dss.2016.03.004
15. More, S.: Trust scheme interoperability: Connecting heterogeneous trust schemes. In: Proceedings of the 18th International Conference on Availability, Reliability and Security. pp. 1–9 (2023)
16. Mpofu, N., Staden, W.V.V.: A trust framework model for identity-management-as-a-service (idmaas). pp. 455–462 (2015)
17. Ram, S., Park, J., Lee, D.: Digital libraries for the next millennium: Challenges and research directions. Information Systems Frontiers **1**, 75–94 (1999)
18. Ramsheva, Y., Prosman, E., Wæhrens, B.: Dare to make investments in industrial symbiosis? a conceptual framework and research agenda for

developing trust. Journal of Cleaner Production **223**, 989–997 (2019). https://doi.org/10.1016/j.jclepro.2019.03.180
19. Raturi, A., Thompson, J., Ackroyd, V., Chase, C., Davis, B., Myers, R., Poncet, A., Ramos-Giraldo, P., Reberg-Horton, C., Rejesus, R., Seehaver-Eagen, S., Mirsky, S.: Cultivating trust in technology-mediated sustainable agricultural research. Agronomy Journal **114**, 2669–2680 (2022). https://doi.org/10.1002/agj2.20974
20. release, E.P.: New interoperable europe act to deliver more efficient public services through improved cooperation between national administrations on data exchanges and it solutions (November 2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6907, [Online; accessed 6-3-2024]
21. Resnick, P., Sami, R.: Sybilproof transitive trust protocols. In: Proceedings of the 10th ACM conference on Electronic Commerce. pp. 345–354 (2009)
22. Rouhani, S., Deters, R.: Data trust framework using blockchain technology and adaptive transaction validation. IEEE Access **9**, 90379–90391 (2021). https://doi.org/10.1109/ACCESS.2021.3091327
23. Statista: Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025 (June 2021), https://www-statista-com.tudelft.idm.oclc.org/statistics/871513/worldwide-data-created/, [Online; accessed 15-3-2024]
24. Temoshok, D., Temoshok, D., Abruzzi, C.: Developing trust frameworks to support identity federations. US Department of Commerce, National Institute of Standards and Technology (2018)
25. Trusted Information Partners: Eenvoudig en betrouwbaar online zakendoen (2024), https://www.trustedinformationpartners.nl/, accessed: 2024-03-19
26. Union, E.: Regulation (eu) no 910/2014 of the european parliament and of the council of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/ec (August 2014), https://eur-lex.europa.eu/eli/reg/2014/910/oj, [Online; accessed 12-3-2024]
27. Yin, R.K.: Case study research: Design and methods, vol. 5. sage (2009)