From Trust Antecedents to Trust Frameworks: Co-Creating Multi-Actor Agreements for Data Sharing

Louise van der Peet [a*], *Nitesh* Bharosa[a], *Marijn* Janssen[a]

[a]Faculty of Technology, Policy, and Management, Delft University of Technology, Delft, the Netherlands, l.vanderpeet@tudelft.nl, 0009-0008-5022-4279.

Submitted: 31 January 2025, Revised: 26 March 2025, Accepted: 21 April 2025, Published: 23 May 2025

Abstract. Companies and public agencies who are looking to improve their services can benefit from more data sharing. However, due to regulations and security concerns, data sharing between individuals, businesses and public agencies is complicated. There are many variables to consider in a multi-actor environment where actors with various roles and incentives look for legal and technical certainty. Public and private organizations increasingly acknowledge the need for multi-organizational agreements on data sharing standards. This results in the rise of trust frameworks to guide efforts towards trustworthy data sharing in an interorganizational setting. However, academic literature on trust frameworks is scarce, and we lack a systematic understanding of the factors that constitute trust in a multi-actor data sharing environment. The objective of this paper is to provide a systematic understanding of the antecedents of trust playing a role in trust frameworks. A two-stage approach is followed, starting with a systematic review of antecedents, followed by an empirical inquiry as verification. Our findings indicate a wide range of antecedents -including technological and organizational antecedents - can be considered.

Keywords. Trust frameworks, Multi-actor data sharing, GovTech, Digital infrastructures, Trust antecedents, Data sharing collaboration, Transformative innovations
Research paper, DOI: https://doi.org/10.59490/dgo.2025.1029

1. Introduction

Organizations increasingly recognize the value of sharing data across organizations and sectors to unlock new insights, optimize operations, and create public value (Dawes, 1996). When it comes to public service delivery and private service delivery, organizations seek to provide more personalized and proactive services, requiring more up front data from citizens or clients (Scholta et al., 2019). However, multi-actor data sharing is complex due to increased regulations on data, privacy requirements, heightened security risks, and diverse stakeholder interests. For instance, the General Data Protection Regulation (GDPR) poses strict requirements for personal data collection and processing in Europe. The revised eIDAS regulation (for "electronic IDentification, Authentication and trust Services") adds strict rules for identification, authentication, authorization, data exchange and archiving. And the NIS2 directive requires European organizations to enhance their cybersecurity capabilities, while introducing risk management measures and reporting requirements to entities from more sectors and setting up rules for cooperation, information sharing, supervision, and enforcement of cybersecurity measures. Accumulated, getting data from persons and organizations in a manner that is compliant to such regulations is not easy. There are even more complexities in multi-actor environments, where diverse stakeholders—ranging from individual citizens and private companies to governmental agencies—must balance various roles, cost structures, installed base, incentives, and legal obligations in data sharing decisions. In a sector or networked setting without a hierarchically dominant standard setter, actors looking to avoid costly 1-1 solutions or proprietary standards, must collaborate and agree on open standards that are compliant and scalable.

Trust frameworks seem to be an emerging solution for arranging information-sharing in multi-actor ecosystems. While much has been done on trust and trustworthiness, there is little academic grounding for the construct of trust frameworks in the context of multi-actor data sharing. "Trust" is frequently mentioned as foundational for successful data sharing: trust in responsible data handling, trust in regulatory compliance, and trust in the broader ecosystem of partners, etc. Trust can be both the input for collaboration, as well as the outcome of collaboration. Trust signals certainty, for instance regarding technology investment decisions by public and private organizations. Lack of trust can impede innovation and digital transformations that rely on multi-actor data sharing (Bharosa, 2022). Yet which factors determine trust are not known.

This paper seeks to address this gap by defining and categorizing the antecedents of trust in trust frameworks. The main research question is: *what are the antecedents of trust in multi-actor data sharing?*

We should distinguish between trust and trustworthiness. Although the two are used interchangeably, they have different meanings (Greenwood and Van Buren III, 2010). Trust is situational and exists on the trustor's side when they assess trustworthiness of the trustee (Sekhon et al., 2014). Trustworthiness is based on the characteristics of the trustee that lead the trustor to believe that the trustee will act in their best interest (Greenwood and Van Buren III, 2010). The articles included in the literature review often mean trustworthiness when they mention trust. However, it can be argued that antecedents for trust - factors leading to trust from the trustor - are the same as trustworthiness factors from the trustee. Therefore, and because previous literature refers to trust antecedents, we use trust rather than trustworthiness.

This paper proceeds as follows. Section 2 outlines the research approach. Section 3 presents the results of the systematic review of the literature: a long list of antecedents of trust. Section 4 outlines the empirical verification of the antecedents found in literature. Section 5 provides a discussion of the findings, comparing the literature with practice. Finally, Section 6 concludes this paper and provides recommendations for research and policy-making.

2. Research approach

The paper aims to provide a systematic understanding of the antecedents of trust in trust frameworks. A two-stage approach is followed, starting with a systematic review, followed by an empirical inquiry on antecedents. We found a large number of antecedents in the literature; therefore, explorative empirical research was needed to verify the list of antecedents. The central unit of analysis are the antecedents of trust, organized into categories.

First, we performed a systematic literature review to identify a long-list of trust antecedents from related topics of trust frameworks. We used the PRISMA method (Page et al., 2021) for systematic review of the literature to exclude papers from the search. The search query is discussed in section 3. The resulting long-list presented in Appendix A can be used as a starting point and refined in subsequent research. The goal of this paper is to find antecedents of trust for trust frameworks, but there is a limited amount of research that is about trust frameworks (van der Peet et al., 2024), therefore we investigated trust antecedents for related topics like interorganizational data sharing, information systems, and standardization.

Second, we wanted to explore the antecedents of trust in practice. Therefore, we organized an expert workshop to identify trust antecedents and ultimately verify those discovered in the literature. This workshop took place at a government practitioner's conference in October 2024 in the Netherlands. The workshop was around 45 minutes long. In total, 88 unique respondents participated in the workshop. 88% of the participants had direct experience working with one or more trust frameworks in practice. The first part of the workshop contained introductory questions on the concept of trust frameworks and the second part questioned the antecedents of trust, which were discussed in a large group setting. The antecedents were collected on Slido, an online platform for data collection. The participants contributed by adding trust antecedents in free form.

We used the results from the workshop to verify the long-list of antecedents derived from the literature. This is done by verifying subcategories that emerge from the literature, and adding antecedents mentioned in the workshop that were not found in literature. In this manner, we verify the subcategories for trust antecedents of trust frameworks, and extend the long-list.

2.1. Complexity of trust in multi-actor data sharing

In a multi-actor setting, data sharing becomes inherently more complex due to the involvement of multiple organizations, each with its own objectives, processes, standards, installed base and requirements for data processing and sharing. In such ecosystems, data sharing components (e.g. data specifications, definitions, APIs, exchange patterns, security policies, processing requirements etc) are never in sync. There is a continuous need for further development, harmonization and standardization due to changing regulations, business models, values chains, partners and security requirements. Moreover, as new technologies such as digital identities, cloud systems, wallets, distributed ledgers, sensors, IOT and artificial intelligence mature and enter the board room, new data sharing requirements and architectures emerge. That is why data sharing infrastructures are dynamic and always in transition to a new state. The varying interests and starting points complicate harmonization and standardization efforts. Some standards may cost some actors more than others, and at the same time benefit some actors more than others. The potential cost and benefits of standardization for data sharing is unevenly distributed in the ecosystem (e.g. Bharosa et al., 2015). Consequently, getting actors to collaborate requires a majority to trust that the future data sharing infrastructure is in their best interest and will benefit all of them on the long run, even though it will cost time, money and collective action on the short run. In a multi-actor ecosystem, it is very difficult to know, let alone trust each individual in the ecosystem. This means we have to move from trusting the human, to trusting the infrastructure, creating trustworthy systems. For this, data sharing collaborators can make agreements to ensure the trustworthiness of the system. In practice, these types of agreements are often described within a trust framework. A trust framework, as described by ARF, is "a legally enforceable set of operational and technical rules and agreements that govern a multi-party system designed for conducting specific types of transactions among a community of participants and bound by a common set of requirements." (eIDAS Expert Group, 2023).

The complexity of making these agreements highlights the need to understand trust antecedents for creating trustworthy multi-actor data sharing systems. Identifying and addressing these antecedents helps build confidence among participants, reduces uncertainty, and ensures collaboration in a diverse, multi-actor setting. By designing a framework around these factors of trust, a trustworthy system for multi-actor data sharing can emerge.

3. Literature review on trust antecedents

Although there is limited research about trust related to trust frameworks, there is a large amount of literature on trust antecedents in various settings. To find those applicable in trust frameworks, we performed a literature review that searches for trust in both organizational and technological contexts, specifically: trust in data sharing, interorganizational and cross-domain trust, trust in information systems and technology, trust in standardization, legal trust, operational trust, trust in governance and trust in collaboration. Consumer-centric terms like "social media" and "commerce" were excluded to maintain focus on trust frameworks. A Scopus 'title-keyword-abstract' search for these keywords, excluding social media, commerce, human-robot interaction, the sharing economy related papers, results to the following:

> TITLE-ABS-KEY (("antecedent of*" W/1 trust) OR "trust antecedent" OR "trust factor" OR "trust variable" OR (("antecedent of*" W/1 trustworthiness) OR "trustworthiness antecedent" OR "trustworthiness factor" OR "trustworthiness variable") AND TITLE-ABS-KEY ("data sharing" OR "interorganizational" OR "cross-domain" OR "information systems" OR "technology" OR "standardization" OR "legal" OR "operational" OR "governance" OR "collaboration") AND NOT TITLE-ABS-KEY ("social media" OR "social networking" OR "social network" OR "human-" OR "consumer" OR "customer" OR "commerce" OR "buyer" OR "technology acceptance model" OR "sharing economy")

The query was run in December 2024 and reveals 266 academic papers.

We used the PRISMA method (Page et al., 2021) for systematic literature reviews to exclude papers from the search. After excluding papers that do not identify trust antecedents, or that are not specific to the scope there are 45 papers left. A large amount of noise in the results came from the term trust factor, which is often used to describe a the result of a calculation to determine the trustworthiness of an actor or technical component in a digital environment (e.g. Chen et al., 2023, Wang et al., 2023, Al Shahrani et al., 2024). We systematically reviewed each included paper and extracted all reported trust antecedents, enabling comparison and

Subcategory	Description	Examples of Trust Antecedents
Organizational trustworthiness	Factors used to judge if an organization is credible, competent, and reliable	Reputation, Certifications, Demonstrated reliability, Partner's competence, Perceived similarity
Calculative trust	Rational assessment of costs, benefits, and feasibility in a partnership	Perceived feasibility, Benefit, Adoption by partners, Successful precedents
Transparency	Openness and clarity of communication, processes, and information sharing	Operational and procedural transparency, Open communication, Timely exchange of information, Pricing transparency
Institution-based trust	Formal rules, structures, and legal frameworks	Regulations, Contracts, Structural assurance, Procedural fairness, Consensus mechanisms
Relational trust	Trust arising from interpersonal bonds, goodwill, and shared values over time	Shared values, Commitment/loyalty, Benevolence, Predictability/consistency, Honesty/integrity
Mutuality	Equal distribution of roles, responsibilities, and influence	Equality in decision-making, Collaborative problem-solving, Balance of control, Mutual dependence
Intra-organizational competence	Internal capacity and support	Quality of governance, Organizational/technical support, Stable organizational structure, Power relations
Trust initiator	Roles or actions within the organization that spark or promote trust	Leadership engagement, Organizational encouragement, Recommendation
Data governance	Policies and processes ensuring data security, privacy, and reliability	Security, Regulatory compliance, Confidentiality, Data integrity, Data auditability
Knowledge (Tech)	Stakeholder skill, familiarity, and acceptance of technology	Satisfaction with existing system, Experience with the tech, Perceived usefulness, Positive user skill perception
Ability (Tech)	Technical system's performance, reliability, and user-friendliness	Availability, Usability, Network reliability, Privacy, Simplicity, Speed
Technical components	Specific tools or features that facilitate trust in technology	Smart contracts, Electronic documents, Audit and verification mechanisms

Tab. 1 – Subcategories of trust antecedents for trust frameworks, verified subcategories in italics

categorization of the extracted concepts. All extracted trust antecedents were categorized by grouping into thematically related categories and subcategories. The antecedents can be divided into two main categories: organizational trust and trust in technology. For both of these categories, the defined subcategories and trust antecedents can be found respectively in Appendix A. In total we find 118 trust antecedents, divided into 12 subcategories. The subcategories are defined in Table 1.

Collecting and classifying the trust antecedents mentioned in the literature gave us a starting point for understanding how trust is formed and maintained in multi-actor data-sharing settings like trust frameworks. Our classification into categories and subcategories shows that existing research covers a wide range of areas—such as technology, interorganizational relationships, and internal organizational factors—but does not directly address the context of trust frameworks. This gap highlights the need to study how these trust antecedents apply, or may need to be adapted, for trust frameworks specifically.

3.1. Examples of antecedents in practice

To illustrate the practical use of the identified antecedents, we investigate the paper 'Steering the adoption of Standard Business Reporting for cross domain information exchange' by Bharosa et al., 2018, which outlines adoption of the SBR trust framework.

Standard Business Reporting (SBR) is a government-led initiative that aims to standardize the way businesses

Trust category	Trust antecedent	Implementation in SBR
Transparency	Operational and procedural transparency	Open governance, clearly defined procedures
	Timely exchange of relevant information	Expert working group where knowledge is shared as much as possible
Institutional	Regulations	Mandate by public organizations
	Contract	Covenant to adopt SBR
	Consensus mechanism	Decision-making bodies
	Support structure	Direct feedback when parties encounter problems
Mutuality	Clarity of roles and responsibilities	Governance with Board, Platform and Expert groups
	Equality in decision-making and resource sharing	All parties have a say
Data governance	Data accuracy / authenticity	Standardized data formats, business rules
Technical ability	interoperability	Generic and shared exchange infrastructure
	Simplicity	Technically simple syntax and interface
	Compatibility	Reuse technical components as much as possible

Tab. 2 – Examples of how trust antecedents are implemented in Standard Business Reporting based on Bharosa et al., 2018

report information to public agencies. It was designed to reduce administrative burdens on businesses by enabling Qualified Information Exchange (QIE), achieved through a set of standards and a shared technical infrastructure.

The study highlights how various steering instruments were used to positively influence adoption. These strategies map well to the trust antecedents discussed in our framework. For example, transparency is reinforced through open governance structures and expert working groups that facilitate knowledge sharing; institutional trust is built through formal agreements; mutuality is reflected in the inclusive governance model, where all stakeholders, public agencies, businesses, intermediaries, and software providers, have a voice; data governance is strengthened through the use of business rules that ensure accuracy and authenticity; and technical trust is fostered through interoperability and simplicity. More examples of the antecedents in SBR can be found in table 2.

As highlighted in prior work the SBR case, where standardization was advanced through a deliberate combination of engineering and learning approaches (Bharosa et al., 2011), trust similarly emerges not from a single mechanism but from the intentional design, iterative learning, and adaptation of technical, institutional, and relational practices. This case serves as a practical demonstration of how trust antecedents can be implemented in a complex, multi-stakeholder setting.

4. Empirical verification: five additional antecedents

As the literature review focused on concepts related to trust, rather than trust frameworks specifically, we conducted a workshop with practitioners experienced in government-related trust frameworks. This allows us to verify the applicability and completeness of the literature-derived antecedents in a real-world setting. The participants were asked to come up with antecedents for trust in collaborative trust frameworks in free-form. In Table 1, the subcategories in italics were verified during the workshop. Furthermore, there were five antecedents mentioned in the workshop that did not appear in the literature, namely the following:

1. Oversight: Supervision, inspection and enforcement to ensure compliance, accountability, and alignment with agreed-upon standards or goals. This transparency reduces uncertainty and risk of hidden opportunistic behavior, reassuring parties that if something goes wrong, it will be detected and corrected.

2. Shared responsibility: The partners collectively bear the obligations, decision-making authority, and consequences of an initiative or process. Shared responsibility aligns incentives among partners, reducing suspicion of opportunism and creating trust.
3. Inclusion: The practice of actively involving diverse stakeholders—regardless of background, status, or perspective—in decision-making, processes, or benefits. The more people believe their voices influence outcomes and that processes are fair to all, the stronger the foundation for trust.
4. Trust services: An electronic service normally provided for remuneration that ensure the reliability, security, and legal validity of electronic transactions, as mentioned in eIDAS article 3 (European Parliament and the Council of the European Union, n.d.). This technical and legal assurance removes much of the guesswork and fear of fraud, making parties feel safer to interact or do business online.
5. Design: The purposeful planning and creation of processes, or systems optimize experiences, and align with overarching objectives. A well designed system makes expectations clear, minimizes errors, and prioritizes user needs, creating more confidence in the system or organization.

Given that the participants are all related to government agencies, the emphasis on oversight and shared responsibility may reflect public-sector norms of accountability and transparency, which might not be as pronounced in purely private-sector collaborations. Similarly, some of the trust frameworks that participants were involved in are related to digital identity, explaining why trust services related to eIDAS and digital identity were mentioned.

These findings underscore the importance of situational factors—like regulatory oversight and digital identity requirements—in shaping trust frameworks. Overall, the workshop validated most of our literature-derived subcategories and revealed additional considerations unique to governmental and regulated environments.

5. Discussion

The findings from our literature review and workshop show that there are many different trust antecedents potentially relevant to designing a trust framework. While this variety captures the complexity of trust, it also creates what we call 'trust design overload.' Practitioners aiming to design trust frameworks can quickly become overwhelmed by the extensive list of potential factors to consider.

This overload is further complicated by the fact that some trust antecedents are context-dependent. For instance, public-sector environments tend to emphasize formal oversight and regulated trust services, whereas private-sector collaborations may focus more on financial incentives or calculative trust. Similarly, small or medium-sized organizations might weigh resource availability and ease of implementation more heavily than larger entities with more capacity.

One way to address trust design overload is through prioritization. Practitioners can evaluate which trust antecedents are most relevant, deciding how to balance the need for different forms of trust. Nonetheless, prioritization demands overview of trust antecedents and insights in various design options and consequences. A potential solution for prioritization is tooling that can help practitioners navigate these choices.

This raises the question of whether a trust framework can be deliberately designed or whether it must grow organically through collaboration and trial and error—a question largely shaped by one's epistemological outlook. In this study, we adopt a positivistic stance by identifying and verifying antecedents for trust. Rather than viewing trust solely as an organic outcome, we treat it as a construct that can be systematically measured and deliberately shaped through specific interventions. However, the degree to which each antecedent is "designable" varies: for example, perceived similarity is contextual and not easily engineered, whereas certifications can be straightforwardly designed and implemented.

6. Conclusion and recommendations

6.1. Conclusion

The main goal of this paper is to contribute to an understanding of trust frameworks, specifically to provide a systematic understanding of antecedents of trust in trust frameworks. By systematically reviewing the literature and validating our findings with expert practitioners, we fill a gap in existing research on trust frameworks. The defined set of trust antecedents specifically addresses multi-actor data-sharing contexts.

In section 3, we create a long-list of antecedents of trust in trust frameworks through a systematic literature review. This results in 118 antecedents, which can be divided in 12 subcategories, and 2 categories. The practical relevance of these antecedents is illustrated through the case of Standard Business Reporting (SBR), highlighting that trust does not emerge only from implementing predefined mechanisms, but from the deliberate design combined with learning and continuous adaptation of technical, institutional, and relational practices.

We verified these antecedents with 88 trust framework practitioners in a workshop. Of the twelve subcategories in our original framework, nine were discussed in detail: 1. Organizational trustworthiness (e.g., reputation, certifications), 2. Calculative trust (e.g., perceived feasibility, successful precedents), 3. Transparency (e.g., open communication, timely exchange of information), 4. Institution-based trust (e.g., regulations, contracts), 5. Relational trust (e.g., shared values, benevolence), 6. Mutuality (e.g., equality in decision making, mutual dependence), 7. Data Governance (e.g., security, regulatory compliance), 8. Knowledge of technology (e.g., experience, perceived usefulness), and 9. Ability in technology (e.g., availability, usability). Practitioners also identified five additional antecedents not found in the literature: Oversight, Shared Responsibility, Inclusion, Trust Services, and Design.

By summing these antecedents and clarifying their relevance to multi actor collaborations, our study fills a research gap in the field of trust frameworks. Specifically, it provides an empirically validated set of trust antecedents that practitioners and researchers can use to develop, refine, and implement trust frameworks in diverse data sharing scenarios.

6.2. Limitations and Recommendations

We acknowledge several limitations. First, due to the scarcity of academic research on trust frameworks, our literature review focused on related areas. While this approach enabled the generation of a broad list of antecedents, it may have overlooked unique factors specific to trust frameworks. Second, the focus on Dutch public sector might limit the generalizability of the findings to private sector collaborations or other national contexts. Third, the use of free-text input through an online platform allowed for an open exploration of ideas, yet it may have resulted in less structured and consistent data, potentially missing subtle or implicit antecedents.

Public private organizations seeking to share data in a trustworthy way can use the insights from this study to inform collaborative data sharing agreements. By systematically incorporating the trust antecedents identified here, data sharing initiatives can better address legal and technical uncertainties, leading to more secure and trustworthy multi actor collaborations. However, implementing too many trust measures at once risks creating 'trust design overload,' emphasizing the need for further research on how to prioritize and balance these antecedents.

From a theoretical standpoint, we recommend three directions of research. First, tools or decision support systems are needed to simplify the design and implementation of trust frameworks, guiding organizations in selecting the most relevant antecedents without overcomplicating their agreements. Second, a further foundation for advancing or refining trust theory in multi-actor data sharing contexts can be developed. Third, research should expand the scope by examining diverse countries, industries, and settings to validate and deepen our understanding of trust antecedents in multi actor collaborations.

References

Abbas, R. M., Carroll, N., Richardson, I., & Beecham, S. (2018). Trust factors in healthcare technology: A healthcare professional perspective.

Adjei, J. K. (2015). Explaining the role of trust in cloud computing services. *info*, *17*(1), 54–67.

Al Shahrani, A. M., Rizwan, A., Sánchez-Chero, M., Cornejo, L. L. C., & Shabaz, M. (2024). Blockchain-enabled federated learning for prevention of power terminals threats in iot environment using edge zero-trust model. *The Journal of Supercomputing*, *80*(6), 7849–7875.

Alzahrani, A. S., Tsai, Y.-S., Aljohani, N., Whitelock-Wainwright, E., & Gasevic, D. (2023). Do teaching staff trust stakeholders and tools in learning analytics? a mixed methods study. *Educational technology research and development*, *71*(4), 1471–1501.

Ando, N., & Kee Rhee, D. (2009). Antecedents of interorganizational trust: Joint decision-making, cultural adaptation, and bargaining power. *Journal of Asia Business Studies*, *3*(2), 16–28.

Aulakh, P. S., Kotabe, M., & Sahay, A. (1996). Trust and performance in cross-border marketing partnerships: A behavioral approach. *Journal of international business studies*, *27*, 1005–1032.

Ayong, K., & Naidoo, R. (2020). An institutional trust perspective of cloud adoption among smes in south africa. *Information and Cyber Security: 18th International Conference, ISSA 2019, Johannesburg, South Africa, August 15, 2019, Proceedings 18*, 145–157.

Barroso-Méndez, M. J., Galera-Casquet, C., Valero-Amaro, V., & Nevado-Gil, M. T. (2019). Antecedents of relationship learning in business-non-profit organization collaboration agreements. *Sustainability*, *12*(1), 269.

Bharosa, N. (2022). The rise of govtech: Trojan horse or blessing in disguise? a research agenda. *Government Information Quarterly*, *39*(3), 101692.

Bharosa, N., Hietbrink, F., Mosterd, L., & Van Oosterhout, R. (2018). Steering the adoption of standard business reporting for cross domain information exchange. *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, 1–10.

Bharosa, N., van Der Voort, H., Hulstijn, J., Janssen, M., De Winne, N., & Van Wijk, R. (2011). Impose with leeway: Combining an engineering and learning approach in the management of public-private collaboration. *Electronic Government: 10th IFIP WG 8.5 International Conference, EGOV 2011, Delft, The Netherlands, August 28–September 2, 2011. Proceedings 10*, 392–403.

Bharosa, N., van Wijk, R., & de Winne, N. (2015). *Challenging the chain: Governing the automated exchange and processing of business information*. Ios Press.

Chen, J., Wang, X., & Shen, X. (2023). Rte: Rapid and reliable trust evaluation for collaborator selection and time-sensitive task handling in internet of vehicles. *IEEE Internet of Things Journal*, *11*(7), 12278–12291.

Cheng, X., Fu, S., & de Vreede, G.-J. (2021). Determinants of trust in computer-mediated offshore software-outsourcing collaboration. *International Journal of Information Management*, *57*, 102301.

Cheng, X., Fu, S., & Druckenmiller, D. (2016). Trust development in globally distributed collaboration: A case of us and chinese mixed teams. *Journal of Management Information Systems*, *33*(4), 978–1007.

Cheng, X., Liu, J., Druckenmiller, D., & Fu, S. (2016). Trust development in globally distributed collaboration: A case study in china. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 480–489.

Cheng, X., Liu, J., Huang, J., Yan, X., & Han, Y. (2016). Investigating trust factors in global virtual collaboration: A case study of a manufacturing company in china. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 697–706.

Cheng, X., & Macaulay, L. (2014). Exploring individual trust factors in computer mediated group collaboration: A case study approach. *Group Decision and Negotiation*, *23*, 533–560.

Cheng, X., Macaulay, L., & Zarifis, A. (2009). A case study of individual trust development in computer mediated collaboration teams. *2009 International Conference on Computational Science and Engineering*, *3*, 277–282.

Curcuruto, M., Mariani, M. G., & Lippert, S. K. (2009). La fiducia nei sistemi informatici. contributo alla validazione italiana di un modello. *Psicologia sociale, Social Psychology Theory Research*, (2/2009), 255–276. DOI: https://doi.org/10.1482/30126.

Dawes, S. S. (1996). Interagency information sharing: Expected benefits, manageable risks. *Journal of policy analysis and management*, *15*(3), 377–394.

De Jong, G., & Woolthuis, R. K. (2008). The institutional arrangements of innovation: Antecedents and performance effects of trust in high-tech alliances. *Industry and Innovation*, *15*(1), 45–67.

eIDAS Expert Group. (2023). EUDI Wallet Architecture and reference framework [Accessed: 2025-02-06]. https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.1.0/arf/

Emaminejad, N., & Akhavian, R. (n.d.). Trust in construction ai-powered collaborative robots: A qualitative empirical analysis. In *Computing in civil engineering 2023* (pp. 513–521). DOI: https://doi.org/10.1061/9780784485224.062.

Ennen, N. L., Stark, E., & Lassiter, A. (2015). The importance of trust for satisfaction, motivation, and academic performance in student learning groups. *Social Psychology of education*, *18*, 615–633.

European Parliament and the Council of the European Union. (n.d.). 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 (Article 3) [Accessed: 2025-01-20]. https://eur-lex.europa.eu/eli/reg/2014/910/oj

Fischer, T. A., Hirschheim, R., & George, B. (2012). Governance in outsourcing relationships–the role of information technologies.

Ford, J. K., Riley, S. J., Lauricella, T. K., & Van Fossen, J. A. (2020). Factors affecting trust among natural resources stakeholders, partners, and strategic alliance members: A meta-analytic investigation. *Frontiers in Communication*, *5*, 9.

Gil-Garcia, J. R., Guler, A., Pardo, T. A., & Burke, G. B. (2010). Trust in government cross-boundary information sharing initiatives: Identifying the determinants. *2010 43rd hawaii international conference on system sciences*, 1–10.

Greenwood, M., & Van Buren III, H. J. (2010). Trust and stakeholder theory: Trustworthiness in the organisation–stakeholder relationship. *Journal of business ethics*, *95*, 425–438.

Hasche, N., Linton, G., & Öberg, C. (2017). Trust in open innovation–the case of a med-tech start-up. *European Journal of Innovation Management*, *20*(1), 31–49.

Hsu, M.-H., & Chang, C.-M. (2014). Examining interpersonal trust as a facilitator and uncertainty as an inhibitor of intra-organisational knowledge sharing. *Information Systems Journal*, *24*(2), 119–142.

Kett, H., Kasper, H., Falkner, J., & Weisbecker, A. (2012). Trust factors for the usage of cloud computing in small and medium sized craft enterprises. *Economics of Grids, Clouds, Systems, and Services: 9th International Conference, GECON 2012, Berlin, Germany, November 27-28, 2012. Proceedings 9*, 169–181.

Khorassani, J. M., Al-Karaghouli, W., & Ayios, A. (2011). Antecedents of trust in international joint ventures'(ijvs) performance in developing countries: A review of empirical evidence.

Kim, C.-S., Dinwoodie, J., & Seo, Y.-J. (2018). Inter-firm cooperation and collaboration in shipper—shipping company relationships for enhancing sustainability. *Sustainability*, *10*(10), 3714.

Kivijärvi, H., Leppänen, A., & Hallikainen, P. (2013). Technology trust: From antecedents to perceived performance effects. *2013 46th Hawaii International Conference on System Sciences*, 4586–4595.

Lai, I. K., & Tong, V. W. (2013). The impact of company, subject, and system characteristics on the trust factors affecting the adoption of internet-based interorganizational systems. *Information systems management*, *30*(4), 280–292.

Lai, I. K., Tong, V. W., & Lai, D. C. (2011). Trust factors influencing the adoption of internet-based interorganizational systems. *Electronic Commerce Research and Applications*, *10*(1), 85–93.

Lee, H.-W., Robertson, P. J., Lewis, L., Sloane, D., Galloway-Gilliam, L., & Nomachi, J. (2012). Trust in a cross-sectoral interorganizational network: An empirical investigation of antecedents. *Nonprofit and Voluntary Sector Quarterly*, *41*(4), 609–631.

Lippert, S. K., & Forman, H. (2006). A supply chain study of technology trust and antecedents to technology internalization consequences. *International Journal of Physical Distribution & Logistics Management*, *36*(4), 271–288.

Martins, J. T., & Baptista Nunes, M. (2016). Academics'e-learning adoption in higher education institutions: A matter of trust. *The Learning Organization*, *23*(5), 299–331.

Moon, S., Jung, S., & Jung, S. (2018). A study on trust factors in a multimedia service environment. *2018 International Conference on Information Networking (ICOIN)*, 67–69.

Mukherjee, D., Renn, R. W., Kedia, B. L., & Mukherjee, D. (2012). Development of interorganizational trust in virtual organizations: An integrative framework. *European Business Review*, *24*(3), 255–271.

Nilsson, M., & Mattes, J. (2015). The spatiality of trust: Factors influencing the creation of trust and the role of face-to-face contacts. *European Management Journal*, *33*(4), 230–244.

Oba, B., & Semercioöz, F. (2005). Antecedents of trust in industrial districts: An empirical analysis of inter-firm relations in a turkish industrial district. *Entrepreneurship & Regional Development*, *17*(3), 163–182.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The prisma 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, *372*, n71. DOI: https://doi.org/10.1136/bmj.n71.

Pinem, A. A., Immanuella, I. M., Hidayanto, A. N., & Phusavat, K. (2018). Trust and its impact towards continuance of use in government-to-business online service. *Transforming Government: People, Process and Policy*, *12*(3/4), 265–285.

Putz, B., & Pernul, G. (2019). Trust factors and insider threats in permissioned distributed ledgers: An analytical study and evaluation of popular dlt frameworks. *Transactions on Large-Scale Data-and Knowledge-Centered Systems XLII*, 25–50.

Rashid, F., & Edmondson, A. C. (2011). Risky trust.

Rusman, E., Van Bruggen, J., Sloep, P., & Koper, R. (2010). Fostering trust in virtual project teams: Towards a design framework grounded in a trustworthiness antecedents (twan) schema. *International journal of human-computer studies*, *68*(11), 834–850.

Rychkova, I., & Ghriba, M. (2023). Trustworthiness requirements in information systems design: Lessons learned from the blockchain community. *Complex Systems Informatics and Modeling Quarterly*, (35), 67–91.

Salampasis, D., Mention, A.-L., & Torkkeli, M. (2014). Open innovation and collaboration in the financial services sector: Exploring the role of trust. *International Journal of Business Innovation and Research*, *8*(5), 466–484.

Scholta, H., Mertens, W., Kowalkiewicz, M., & Becker, J. (2019). From one-stop shop to no-stop shop: An e-government stage model. *Government Information Quarterly*, *36*(1), 11–26.

Sekhon, H., Ennew, C., Kharouf, H., & Devlin, J. (2014). Trustworthiness and trust: Influences and implications. *Journal of marketing management*, *30*(3-4), 409–430.

St. John, M. F., & Dustin Young, M. (2021). A decision support tool for assessing trust in an enterprise data sharing partner. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *65*(1), 1015–1019.

van den Heuvel, R., van de Wetering, R., Kruidhof, O., Bos, R., & Trienekens, J. (2021). How distributed ledger technology can influence trust improving data sharing in collaborative networks. *Exploring Innovation in a Digital World: Cultural and Organizational Challenges*, 62–76.

van der Peet, L., Bharosa, N., Dijkhuis, S., & Janssen, M. (2024). Understanding trust frameworks: Goals and components identified through a case study. *International Conference on Electronic Participation*, 223–238.

Wang, S., Zheng, X., Yang, S., & Wang, X. (2023). Towards efficient blockchain-based cross-domain trust reputation management for ls-hetnet. *GLOBECOM 2023-2023 IEEE Global Communications Conference*, 5129–5134.

Zhang, Y., Tavalaei, M. M., & Parry, G. C. (2024). Trustless is not trust free: How to build trust for organisations adoption of blockchain technology. *IET Conference Proceedings CP881*, *2024*(7), 163–168.

Zuppa, D., Olbina, S., & Issa, R. (2016). Perceptions of trust in the us construction industry. *Engineering, Construction and Architectural Management*, *23*(2), 211–236.

Appendix A

Tab. 3 – Inter-organizational trust antecedents

Subcategory	Trust Antecedent	References	Trust antecedent	references
Organizational trustworthiness	Reputation	Zhang et al., 2024 Cheng et al., 2021 Ford et al., 2020 Moon et al., 2018 Nilsson and Mattes, 2015 Cheng and Macaulay, 2014 Kett et al., 2012 Lee et al., 2012 Oba and Semercioöz, 2005	Relational history, previous experience	Zhang et al., 2024 Alzahrani et al., 2023 Ford et al., 2020 Kett et al., 2012 Mukherjee et al., 2012 Khorassani et al., 2011 De Jong and Woolthuis, 2008
	Partner's environment	Moon et al., 2018 Cheng, Fu, and Druckenmiller, 2016 Cheng, Liu, Huang, et al., 2016 Khorassani et al., 2011	Perceived similarity	Ennen et al., 2015 Nilsson and Mattes, 2015 Khorassani et al., 2011 Rusman et al., 2010
	Trusting stance	Nilsson and Mattes, 2015 Kivijärvi et al., 2013 Lee et al., 2012	Certifications	Kett et al., 2012
	Knowledge of partners	Gil-Garcia et al., 2010	Project as main business focus	Alzahrani et al., 2023
	Demonstrated reliability	Cheng et al., 2021 van den Heuvel et al., 2021 Cheng, Fu, and Druckenmiller, 2016 Zuppa et al., 2016 Alzahrani et al., 2023 Cheng and Macaulay, 2014 Moon et al., 2018 Rusman et al., 2010 Cheng et al., 2009	Partner's competence	St. John and Dustin Young, 2021 van den Heuvel et al., 2021 Moon et al., 2018 Hasche et al., 2017 Zuppa et al., 2016 Mukherjee et al., 2012 Rusman et al., 2010 Oba and Semercioöz, 2005 Lee et al., 2012
	Shared sectoral affiliation	Lee et al., 2012		
Calculative trust	Perceived feasibility	Zhang et al., 2024	Adoption by partners and competitors	Ayong and Naidoo, 2020
	Benefit	Cheng, Liu, Druckenmiller, and Fu, 2016 Cheng, Liu, Huang, et al., 2016 Cheng and Macaulay, 2014 Cheng et al., 2009 Cheng et al., 2021	Successful precedents	Zhang et al., 2024
Transparency	Operational and procedural transparency	Putz and Pernul, 2019 van den Heuvel et al., 2021 Alzahrani et al., 2023 Rashid and Edmondson, 2011	Open communication	Ford et al., 2020 Kim et al., 2018 Cheng, Fu, and Druckenmiller, 2016 Mukherjee et al., 2012 Khorassani et al., 2011 De Jong and Woolthuis, 2008
	Timely exchange of relevant information	Kim et al., 2018 De Jong and Woolthuis, 2008 Oba and Semercioöz, 2005 Aulakh et al., 1996	Pricing and cost transparency	Kett et al., 2012
	Transparency facilitated by IT	Fischer et al., 2012		
Institution-based trust	Structural assurance	Cheng et al., 2021 Nilsson and Mattes, 2015	Adaptability of agreements	van den Heuvel et al., 2021

	Procedural fairness	Ford et al., 2020 Rusman et al., 2010 Ando and Kee Rhee, 2009 Rashid and Edmondson, 2011	Regulations	Ayong and Naidoo, 2020 Kim et al., 2018 Salampasis et al., 2014
	Contracts	Ayong and Naidoo, 2020 Hasche et al., 2017 De Jong and Woolthuis, 2008	Standards	Ayong and Naidoo, 2020
	Consensus mechanisms	Putz and Pernul, 2019	Rewards and recognition	Martins and Baptista Nunes, 2016
	Support structure	Martins and Baptista Nunes, 2016	Consistency in policy and guidelines	Martins and Baptista Nunes, 2016
	Informal institutional arrangements	Oba and Semerciöz, 2005		
Relational trust	Shared values	van den Heuvel et al., 2021 Ford et al., 2020 Barroso-Méndez et al., 2019 Ayong and Naidoo, 2020 Kivijärvi et al., 2013 Mukherjee et al., 2012 Rusman et al., 2010	Commitment / loyalty	van den Heuvel et al., 2021 Khorassani et al., 2011 Rusman et al., 2010
	Benevolence / supportiveness	van den Heuvel et al., 2021 St. John and Dustin Young, 2021 Ford et al., 2020 Hasche et al., 2017 Adjei, 2015 Mukherjee et al., 2012 Rusman et al., 2010	Predictability / consistency	van den Heuvel et al., 2021 Moon et al., 2018 Rusman et al., 2010
	Friendliness	van den Heuvel et al., 2021 Cheng and Macaulay, 2014 Rusman et al., 2010	Spirit of cooperation	van den Heuvel et al., 2021 Cheng, Liu, Huang, et al., 2016 Salampasis et al., 2014 Cheng and Macaulay, 2014
	Honesty / integrity	van den Heuvel et al., 2021 Moon et al., 2018 St. John and Dustin Young, 2021 Adjei, 2015 Mukherjee et al., 2012 Rusman et al., 2010	Equitable treatment of partners	Kim et al., 2018
	Positive attitude	Moon et al., 2018	Effective collaboration	Zuppa et al., 2016
	Face-to-face communication	Zuppa et al., 2016	Engagement and motivation	Cheng, Liu, Druckenmiller, and Fu, 2016 Cheng, Liu, Huang, et al., 2016 Cheng and Macaulay, 2014 Rusman et al., 2010
	Direct social exchange	Nilsson and Mattes, 2015	Social interaction ties	Hsu and Chang, 2014
	Shared knowledge-sharing vision	Hsu and Chang, 2014	Shared goals	Lee et al., 2012 Mukherjee et al., 2012 Rusman et al., 2010
	Relationship multiplexity	Lee et al., 2012	Boundary spanner trust	Mukherjee et al., 2012
	Strategic bond	Khorassani et al., 2011	Flexibility	Khorassani et al., 2011 Aulakh et al., 1996
	Shared language	Rusman et al., 2010	Availability	Rusman et al., 2010

	Discretion	Rusman et al., 2010	Cultural adaptation	Ando and Kee Rhee, 2009
	Continuity expectation	Aulakh et al., 1996	Shared interest	Nilsson and Mattes, 2015
	Interactional expertise	Rashid and Edmondson, 2011		
Mutuality	Equality in decision making and resource sharing	Kim et al., 2018 Khorassani et al., 2011 Rusman et al., 2010	Collaborative problem solving	Kim et al., 2018
	Monitoring mechanisms	Kim et al., 2018 Aulakh et al., 1996	Balance of influence / control	Cheng, Liu, Druckenmiller, and Fu, 2016 Cheng, Liu, Huang, et al., 2016 Cheng and Macaulay, 2014 Gil-Garcia et al., 2010
	Complementarity / compatibility	Khorassani et al., 2011	Clarity of roles and responsibilities	Gil-Garcia et al., 2010 Rusman et al., 2010 Emaminejad and Akhavian, n.d.
	Mutual dependence	De Jong and Woolthuis, 2008	Consequences for actions	Oba and Semerciöz, 2005
	Fair distribution of risks and profits	Kim et al., 2018 Khorassani et al., 2011		
Intra-organizational competence	Organizational and technical support and training	Alzahrani et al., 2023 Abbas et al., 2018 Emaminejad and Akhavian, n.d.	Quality of governance and leadership	Abbas et al., 2018 Adjei, 2015 Cheng, Fu, and Druckenmiller, 2016 Martins and Baptista Nunes, 2016
	Alignment with organizational culture	Martins and Baptista Nunes, 2016	Proprietary Legacy	Salampasis et al., 2014
	Societal orientation	Salampasis et al., 2014	Financial education	Salampasis et al., 2014
	Stable organizational structure	Kivijärvi et al., 2013	Power relations	Kivijärvi et al., 2013
	Understanding and education regarding tech	Emaminejad and Akhavian, n.d. Alzahrani et al., 2023		
Trust initiator	Leadership engagement	Zhang et al., 2024 Rashid and Edmondson, 2011 Cheng et al., 2009	Organizational encouragement	Kivijärvi et al., 2013 Emaminejad and Akhavian, n.d.
	Recommendation	Kett et al., 2012 Pinem et al., 2018	Authoritative endorsements	Zhang et al., 2024

Tab. 4 – Technical trust antecedents

Subcategory	Trust Antecedent	References	Trust antecedent	references
Data governance	Security	Zhang et al., 2024 Abbas et al., 2018 Lai and Tong, 2013 Kett et al., 2012 Lai et al., 2011	Regulatory compliance	Zhang et al., 2024 Abbas et al., 2018

	Access control / Authentication / Authorization	Alzahrani et al., 2023 Putz and Pernul, 2019 Rychkova and Ghriba, 2023	Data accuracy / Authenticity	Alzahrani et al., 2023 Putz and Pernul, 2019 Zhang et al., 2024
	Data understandability	Alzahrani et al., 2023	Confidentiality	Rychkova and Ghriba, 2023 van den Heuvel et al., 2021
	Accountability	Rychkova and Ghriba, 2023	Data integrity	Rychkova and Ghriba, 2023
	Data compliance	Rychkova and Ghriba, 2023	Data auditability	Rychkova and Ghriba, 2023
Knowledge	Satisfaction with existing system	Lippert and Forman, 2006	Experience with the tech	Lippert and Forman, 2006 Abbas et al., 2018 Pinem et al., 2018 Lippert and Forman, 2006
	Perceived usefulness / ease of use	Pinem et al., 2018	Positive perception of user skill	Kivijärvi et al., 2013
Ability	Competence of task	Rychkova and Ghriba, 2023 Abbas et al., 2018 Adjei, 2015 Cheng and Macaulay, 2014	Automation	Rychkova and Ghriba, 2023
	Decentralization	Rychkova and Ghriba, 2023	interoperability	Rychkova and Ghriba, 2023 Lai and Tong, 2013 Lai et al., 2011
	Performance / quality	Rychkova and Ghriba, 2023 Ford et al., 2020 Pinem et al., 2018 Kett et al., 2012	Resilience	Rychkova and Ghriba, 2023 Kett et al., 2012
	Availability	Rychkova and Ghriba, 2023 Putz and Pernul, 2019 Lai and Tong, 2013 Kett et al., 2012 Lai et al., 2011	Usability	Rychkova and Ghriba, 2023 Abbas et al., 2018 Lai and Tong, 2013 Kett et al., 2012 Lai et al., 2011 Cheng et al., 2009 Curcuruto et al., 2009 Lippert and Forman, 2006
	Non repudiation	Rychkova and Ghriba, 2023	Tech transparency	Rychkova and Ghriba, 2023
	Traceability	Rychkova and Ghriba, 2023	Privacy	Rychkova and Ghriba, 2023 Adjei, 2015
	Storage integrity	Putz and Pernul, 2019	Cryptographic reliability	Putz and Pernul, 2019
	Network reliability	Putz and Pernul, 2019	System reliability	Abbas et al., 2018 Lai and Tong, 2013 Lai et al., 2011 Curcuruto et al., 2009
	Compatibility	Abbas et al., 2018	Simplicity	Salampasis et al., 2014
	Speed	Kett et al., 2012	Predictability	Curcuruto et al., 2009
	Absence of problems	Curcuruto et al., 2009		
Technical components	Smart contracts	Putz and Pernul, 2019	Electronic documents	Zuppa et al., 2016
	Audit and verification mechanisms	Lai and Tong, 2013 Lai et al., 2011		