# Understanding Public-Private Collaboration Configurations for International Information Infrastructures

Klievink, Bram

**DOI**
10.1007/978-3-319-22479-4_13

**Publication date**
2015

**Document Version**
Accepted author manuscript

**Published in**
Proceedings of IFIP eGOV and ePART 2016

**Citation (APA)**
Klievink, B. (2015). Understanding Public-Private Collaboration Configurations for International Information Infrastructures. In *Proceedings of IFIP eGOV and ePART 2016* (pp. 1-13). (Lecture Notes in Computer Science; Vol. 9248). https://doi.org/10.1007/978-3-319-22479-4_13

# Understanding public-private collaboration configurations for international information infrastructures

Bram Klievink

Delft University of Technology, Delft, the Netherlands
a.j.klievink@tudelft.nl

**Abstract.** Collaboration between the public and the private sector is seen as an instrument to make governance smarter, more effective, and more efficient. However, whereas there is literature on public-private collaboration, very little of it addresses how these collaborations can be shaped to make use of the huge potential that technological innovations in ICT may offer. To address this gap, this paper addresses public-private collaborative development of digital information infrastructures (IIs). Drawing on a combination of literature on public-private partnerships and on digital information systems or infrastructures, this paper studies an initiative for exchanging information among international trade supply chain partners and between the businesses and government (e.g. for declarations, compliance, border control). Specifically, it explores what would be the Dutch end of such an II, to understand the interplay between the technological innovation and partnerships that form the social context thereof.

**Keywords.** information infrastructure · e-government · public-private collaboration · international trade · public-private information infrastructures · collaborative governance

## 1 Introduction

To address the complexity of today's problems in networked societies, governance needs to be organised in a smarter way. In literature on innovation and improvement of the public sector, one of the proposed answers is that governments should strengthen the collaboration with societal actors, and include private partners in the strategy to realise public goals [1–4]. Smarter government can leverage information and communication technologies (ICTs) to enable governments to do more with less [5]. However, the role that ICTs can play in public-private collaboration to facilitate smarter, collaborative governance, is rarely studied. Studies focusing on the role of public-private collaboration, and on the public sector in general, tend to not really accommodate technological change [6]. Hence, to understand how public-private collaborations can take shape in an information infrastructure (II), insights from these studies will need to be combined with knowledge on how information infrastructures are shaped.

This is the author's version of this paper. The final publication is published in volume 9248 of the series Lecture Notes in Computer Science (pp. 170-180) and is available at Springer via http://dx.doi.org/10.1007/978-3-319-22479-4_13

In this paper, we combine a number of insights from literature on public-private partnerships with insights from literature on information systems or infrastructures. Using this analytical background, a case is described in which a public-private information infrastructure is developed for the domain of international trade. This case is interesting to study as a complex governance challenge as due to the international setting, there is no principal actor to realise IIs in this domain.

In international trade lanes, the system through which information is shared between stakeholders is deficient. For commercial reasons (e.g. to not disclose commercially sensitive information), supply chain actors do not always fully inform the next actor in the chain about who the original shipper is, and what precisely is in a container. Hence, the data found in transport documents and (based thereon) also in official declarations, are often not from the originator; i.e. not from the actor that really knows the specific goods being shipped [7]. Key parties such as buyers, customs and other authorities, have to manage and supervise the supply chain with second-hand information that is frequently inaccurate [7].

The original and correct information is present in the information systems of the various actors involved in international trade. ICT innovations enable electronic connections and information exchange between these systems and thereby access and re-use of these original trade data by other actors in the supply chain [8]. These developments can be considered a re-arrangement of the information infrastructures in international trade. Adapting the information infrastructures in international trade concerns the evolution and dynamics of existing information systems of supply chain actors, existing processes and procedures, and all the diversity in systems and relationships present therein [9–12]. Over the past few years, multiple initiatives have been undertaken to connect systems from all over the globe to each other in a standardized way, to capture data from their original source and to facilitate the exchange of data.

Information infrastructures (II) concern heterogeneous sociotechnical systems [10], which are systems that involve both complex (physical) technical systems and networks of interdependent actors [13]. Within such a sociotechnical system, questions arise on the technological system and standards used, but also on aspects such as responsibilities and ownership. Balancing the need that the infrastructure works for commercial parties and simultaneously for the community and the government is challenging. These questions have to be addressed collaboratively by the key stakeholders that are to build, finance, operate, use and facilitate the II. Hence, setting up such II goes beyond the technical challenges (e.g. interconnecting diverse information systems) and yields questions that have to be addressed by looking at the *socio* side of these developments (e.g. the partnerships that have to make this work). It is a collaborative setting in which autonomous actors control their own information systems, information sources and links with the II. It is a federated system that is largely built and operated by businesses. To avoid monopolization by single business actors and to

This is the author's version of this paper. The final publication is published in volume 9248 of the series Lecture Notes in Computer Science (pp. 170-180) and is available at Springer via http://dx.doi.org/10.1007/978-3-319-22479-4_13

ensure that public values are realised, governments must actively participate in the stakeholder community working on these innovations.

In public management literature, more is known tools of governance for public-private collaborations. There is much literature on public sector reform and innovation that in various ways argue for collaboration between the public and the private sector, also as a way to realise public goals [4, 14–16]. Partnership and collaboration are presented as new forms of governance, giving new legitimacy to government by combining the efficiency of the private sector with an involvement of society and other stakeholders [17]. The idea behind partnership is the notion of collaborative advantage [18].

Probably neither the public sector field nor the information systems field has the complete picture when it comes to understanding how public-private information infrastructures are or could be developed. Even when public-private collaborations live up to their promise of mutuality, a key question remains how government actions can accommodate the requirement of accountability when using infrastructural components, original business data, and shared functionality in an II. This paper focuses on challenges of partnership for II; the idea of bringing together public and private nodes in a form of partnership to play a role in something that is (partially) a public service or asset.

In this paper, we first discuss the background of two main challenges of partnership, which also serves as the main contribution of the paper. For illustration, in section four we look at how these challenges play out in a specific initiative for creating the Dutch end of an II for international trade, in the form of a Port Community System.

## 2 Background

This paper focuses on public-private collaboration; these partnerships do not conform to one organisational type, but could include combinations of involving private parties in the design, building, owning and operation of public sector assets or services by the private sector, or to transfer public sector assets to the private sector altogether [19]. In partnership terms, the II of study could be considered a 'Build-Own-Operate' type, in which the private sector finances, builds and operates the information infrastructure. An open question is to what extent and which parts of the information infrastructure can indeed be seen as a public sector asset. Strictly speaking, it is a partnership that concerns the integration of various private sector assets and public sector assets, in a way that needs to fulfil the public goals and has to make business-sense.

This is the author's version of this paper. The final publication is published in volume 9248 of the series Lecture Notes in Computer Science (pp. 170-180) and is available at Springer via http://dx.doi.org/10.1007/978-3-319-22479-4_13

The insights from studies on public-private partnerships (PPPs) seem relevant to this set-up, and PPPs are one of the most studied forms of public-private collaboration, and include empirical studies. However, a lot of emphasis in PPP literature is on the contracts, the process of setting up PPPs (e.g. finding contractors), payment, performance monitoring, etc. That is not entirely the same as trying to build an II in which (new and existing) private sector IT assets will largely be the main building blocks.

One of the viewpoints offered by literature on PPP that seems relevant in assessing II is the distinction between the various analytical contexts and the way they are reflected in the governance of the partnership. For example, Johnston and Gudergan [19] distinguish between the technical-rational context, the social context and risk as an overarching governance consideration. They find that the rational-technical context and processes assume logical and linear decision-making and are typically reflected in legal contracts that define a partnership. This becomes the 'de facto' primary governance system [19]. However, contracts are based on limited, biased or otherwise imperfect knowledge and expectations that were prevalent at the time of drafting the contract, but not at the time of actual implementation or operation. As these contracts are therefore likely to be incomplete (and rationally bounded) and can or do not take into account contingencies, this is unlikely to be an effective governance instrument for a partnership [19]. Even if the technical-rational context works well for the contract, there is often an implicit social contract and problems related to that may threaten a 'rational' approach, especially at later points in the partnership. In other words: even if one could manage the technical complexity completely, the actor-related complexity has its own dynamics. Here, a project approach to managing a partnership would be insufficient, and process management seems required as social and political risks are far more difficult to control than project risks [20]. Johnston and Gudergan [19] argue that a risk assessment method is needed that looks at social risks in the partnership as much as at the defined technical-rational risks. A "strong dysfunction in the social organisation dimension of governance [cannot] be contained by the rational logics of contract" [19] (p580).

When assessing literature on public-private collaboration and literature on II (or its conceptual predecessor; IOS) from the perspective of these contexts, two insights on the challenges of partnership come up that seem relevant to understand the public-private collaboration for the international trade II.

### 2.1 Conflicting and converging goals: parties 'hidden' agenda's in the collaboration

The ideal for partnership is that partners agree on a common and agreed upon set of aims [18]. Also Hailey [21] thinks that a clear and shared vision on the purpose and

This is the author's version of this paper. The final publication is published in volume 9248 of the series Lecture Notes in Computer Science (pp. 170-180) and is available at Springer via http://dx.doi.org/10.1007/978-3-319-22479-4_13

objectives of partnership is necessary to drive a partnership based on a clear purpose. However, just agreeing on the goals of the partnership is only part of the story; partnerships are usually set-up because the partners are different, have different resources and have different purpose [22]. The idea of collaborative advantage is that bringing them together would be a source for advantage. Partners can agree to such advantage at a generic level, but they have different reasons for getting involving in the partnership (e.g. trading partner pressure). Agendas (both organisational and individual) might be hidden at the initiation of the partnership, but when the partnership gets specific, there is the danger that "irreconcilable differences will be unearthed", that weren't obvious yet when the aims were "vague enough that none of the parties involved can disagree with it" [22] (p296).

Partnerships take place in context and not in isolation, further adding to the complexity [18]. Because in an II for international trade a host of private parties are involved that also have dealings with each other beyond the collaboration, they may (officially) seek *collaborative advantage* in the partnership, but traditionally, ICTs are often used to gain a *competitive advantage* [23][24]. Once common goals are translated to actual implementations, the status quo and legacy (both organisational and technical) may mean that the strategies that partners would like to follow for realising the shared goals differ greatly for different partners [25]. In the context of an II, we expect to see that parties try to maximise their control over the II [26] and wish to minimise the degree of vulnerability the II and the collaboration may bring [27].

The strategy will look different for different parties; IT solution providers and existing information brokers could aim to become a leader in the information infrastructure and seek input control (i.e. control what functionality may be offered via the infrastructure) in an attempt to maximise control and minimise dependency on others. To those parties, the II function is their core resource, which they would not want to govern collaboratively, but want to keep within their control [28]. Such a strategy is incompatible with the II as a collaborative endeavour [10] and will divvy up the business community, as parties that are involved from the physical handling of goods in international trade will seek benefits from an open II and fear getting locked-in by the IT solution providers [29]. For them, they seek to minimise potential homing and switching costs. Homing costs are the costs of being involved with a certain II and include costs of adoption, operation and opportunity costs [26]. If these costs are high, parties are less inclined to link with an II, especially if there are multiple II solutions they have to connect to (which lead to multi-homing costs, see [30]Eisenmann, Parker, & Alstyne, 2006). These costs that parties have to make to connect to a system of II increased their dependence and vulnerability on IT solution providers [31]. They have invested in a connection and might face switching costs or additional investments if different II providers do not adhere to the same (open) standards. That is a major barrier to collaboration between logistical parties and IT solution providers. In general, a lack of standards hampers adoption because parties might not be able to

This is the author's version of this paper. The final publication is published in volume 9248 of the series Lecture Notes in Computer Science (pp. 170-180) and is available at Springer via http://dx.doi.org/10.1007/978-3-319-22479-4_13

make use of their investments made in connecting with one to re-use in connections with others [32]. This is also the rationale for open standards (also to avoid lock-in and to facilitate re-use).

Based on this, we would expect to see two blocks in the private sector involved in the II: the parties with a big role in logistics, and parties with a big role in the II. That will mean that governments (as a third block) will have play a role in building trust and dealing with problems related to the social context, making the government a third party in the mix. Hence, even if they don't want to [33], government will sooner or later find itself in a position where they have to ensure the collaborative aspect, because the idea of having a partnership is that the II has an open architecture, which (given the dependencies this might bring to parties) requires a form of bidirectional control and possibly shared ownership [26].

### 2.2 Trust and vulnerability: technological convergence and dynamics in the playing field

Trust among partners is an important ingredient for making partnerships work [18]. When trust and reciprocity exist, it is much easier to "negotiate issues, resolve problems and work towards a common purpose" [21]. Trust facilitates communication, and sharing of sensitive information, but there are many obstacles to getting there. These obstacles include the existing power relationships, the involvement of parties for the reason that government wants them to be involved, parties with necessary resources that threaten to leave a partnership, parties with limited power, but with resources essential to the partnership (e.g. access to communities, markets, data) [18]. As not all aspects to a partnership can be covered in a contract [19], parties perceive the risk that any future partner (or change in direction or leadership of a company) may not "honour the many unwritten aspects of the initial agreement" [18]. Trust is needed, but the social context [19] might result in a situation (e.g. a lack of history between partners) that is ill equipped for forming trust.

Developing trust in the collaborative development of II is potentially even more difficult, as the interdependencies that such an II will bring, are a source of (perceived) vulnerability for the parties involved [27]. Especially developments like technological convergence threaten parties playing a role in existing II's, especially those that offer parts of the II (e.g. infrastructure components, databases, functionality). Whereas the role of parties in the physical logistics process is not as easily threatened, each information function that parties have and the power they derive from that, is threatened by the fact that technical components increasingly become integrated and providers of technological solutions increasingly have the opportunity to expand into this domain. This may tilt the power balance in favour of parties without a primarily information function, as they have an (be it implicit or explicit) threat of moving away

This is the author's version of this paper. The final publication is published in volume 9248 of the series Lecture Notes in Computer Science (pp. 170-180) and is available at Springer via http://dx.doi.org/10.1007/978-3-319-22479-4_13

from the II if the others (especially the IT solution providers) do not do more to meet their interests and demands. Following both public-private collaboration and information system literature, explicitly using such power would have negative consequences on the collaboration as this hampers the development of trust [18, 19, 27]. However, technical-rational instruments like contracts and project management cannot control this. Mitigating such a situation is hard, as there are power differences, but no actor with hierarchical authority to enforce action [18]. Without an approach to initiate a 'trust-building loop' [18], the result might be that the private sector is unable to collaboratively develop the II, calling for a bigger role of government, either as mediator [19] or in an active role in setting-up and governing the II. Pressure from the environment (both trading partners and government) and trust (also in the regulatory regime) are considered important antecedents to the adoption of an information system [31].

## 3 Research approach

The empirical part of the paper is based on a study of a Dutch initiative to support innovations in logistics (Topsector Logistics). Part of this initiative is the development of an II called the Neutral Logistics Information Platform (NLIP, see www.nlip.org). This II is still under development and aims to support information exchange in international supply chains. The starting point in the NLIP are the Port Community Systems (PCSs) in mainports in the Netherlands, and build from there. As a case study we picked a specific PCS which is one of the building blocks of the national II. As part of the case, we made a detailed mapping of the process and data flows in various services that could become part of the NLIP, to enable the identification of issues in the current situation. These mappings and descriptions are based on interviews with the PCS, a branch organisation representing a large group of shippers/consignees, a carrier, a terminal operator, and Dutch Customs. Furthermore, documentation on services, processes and pricing also were used in the analysis. To ensure that our understanding of the current situation was correct, we discussed our descriptions with our interviewees or sent them for checking.

## 4 Case description

One of the main challenges for international trade information infrastructures is how the diverse and (also geographically) dispersed business community can be joined-up to support visibility solutions that cross many international trade lanes, but to do this without a single lead actor with the power or jurisdiction to decide on a solution. A potential answer to this challenge found in a European project is that the business communities that make up a trade lane select a solution provider to which they open-up their data. As part of this, also parties with low levels of IT maturity and

This is the author's version of this paper. The final publication is published in volume 9248 of the series Lecture Notes in Computer Science (pp. 170-180) and is available at Springer via http://dx.doi.org/10.1007/978-3-319-22479-4_13

parties with legacy information systems, are connected to the system by the solution provider.

However, as the 'last leg' of the information infrastructure - connecting to a wide variety of businesses and local and national government agencies - is so difficult, the current role of PCSs come into view. A PCS (port community system) is an information hub, through which the business community in the port can exchange information that they need as part of their logistical processes. Through this function, a PCS has custody of much information that is relevant in the port environment. A PCS also plays a role in much of the data exchange between businesses and government, although companies can exchange information with government directly. The electronic exchange of data reduces the administrative burden, and saves operational costs (e.g. on personnel and couriers).

Apart from exchanging information among business actors, PCSs are often the linking pin between the business community, the port authority and government inspection agencies such as customs. In fact, many PCSs have originally been set-up or at least initiated by a government organization [34]. This is because much of the reporting towards government contains data of multiple actors. For example, in the clearance process at export, data need to be combined from (amongst others) the exporter (the export declaration), from the terminal (on which vessel goods were loaded), and the port authority (confirmation of vessel departure). By combining these data through a PCS, customs knows that goods have been exported and a confirmation of exit can be provided to the business.

This PCS role is a specific one, also in the context of international IIs, as in a (geographically limited) port community, a specific situation exists, with smaller and local companies, high interdependence and specific rules and regulations. This results in many 'thick' links between parties, which makes it hard to apply an open architecture. In some countries, such as the Netherlands, the idea is that because PCSs have these 'thick' connections with many parties – public and private – these PCSs are the existing systems that are well equipped to form the basis for bigger-scale information platforms at a national or supranational level.

However, a PCS is primarily a clearing house [35], which can and must rely on contracts with all kinds of actors, and agreeing on individual services and uses of data and is therein supported by having a specific role and data structure. As a result, the PCS relies on data contributors and does not have a clear incentive to move to an open architecture or to help the global IT solution providers in supporting their II, as that would threaten their 'monopoly' on acting as a clearing house for a specific geographically confined trade hub. At the same time, this makes data contributors (e.g. carriers, terminal operators) vulnerable, as their data are handed over to a party under financial pressure that can only be resolved by re-using that data for more commercial

This is the author's version of this paper. The final publication is published in volume 9248 of the series Lecture Notes in Computer Science (pp. 170-180) and is available at Springer via http://dx.doi.org/10.1007/978-3-319-22479-4_13

functionalities. Furthermore, as most international companies have dealings with multiple ports, every port having its own proprietary solution increases multi-homing costs.

The current design of the PCS is that of a public-private collaboration. In that design, data are handed over to the PCS but are still owned by the individual actors submitting the data. This enables government to access the data, and enables the PCS to optimize port operations by enabling companies operating in the port to share data without losing control of it. The PCS's revenue currently comes from subscriptions and a fee-per-message method. The core community services are funded through general funds of the shareholders, which are public or semi-public organisations.

Looking at it from a technical-rational perspective, a PCS adds value to the community as a whole, and specifically in the interactions with government. However, an open II for global trade would be open to many powerful parties, also those with a strong information function. To survive in that setting, a PCS will have to offer more, in the sense of more services, bigger scale, more parties, smarter combinations, etc. The ties to specific localised communities may not be enough for globally acting players to continue to prefer a PCS over business solutions. In the public-private structure of the PCS, the public component makes it difficult for a PCS to focus on commercial services and compete with business solutions. National governments do not have the jurisdiction or capacity and the business community is too fragmented to make the decisions, the long-term commitments and the ICT investments. Hence, an II can only be realised if the parties collaborate. Governments will have to facilitate (e.g. incentivise) and support (e.g. develop a Single Window, provide digital government building blocks, and ensure a level playing field) and businesses need to find sustainable businesses models and build the II.

## 5 Discussion and conclusion

In a public-private partnership approach to an II based on PCSs, the public component makes it difficult for a PCS to focus on commercial services and compete with business solutions. Much of the data that would be the basis for those commercial services, are gotten because of the community role. When discussing re-use of the data that is needed for this core functionality in order to provide additional services, this community or public role gets obscured and parties object to a growing role of the PCS. However, now that due to austerity the general funds of the PCS are decreasing, some kind of additional sources of income for the PCS are needed. Increasing the fees for their services is one of the few instruments they have, next to developing new (business) services based on the data they have. If businesses consider this to be misuse of data provided for compliance purposes they could move to building direct links between various actors (e.g. send electronic messages to customs systems directly),

This is the author's version of this paper. The final publication is published in volume 9248 of the series Lecture Notes in Computer Science (pp. 170-180) and is available at Springer via http://dx.doi.org/10.1007/978-3-319-22479-4_13

and if government agencies argue that a PCS is optional because direct data provisioning to e.g. customs is also possible, all of them risk that the core flow of data that the PCS bases its services on dries out. The consequence may be that cascading inefficiencies in operations due to suboptimal data exchange, lead to depriving the entire port community of the benefits, which might make the port less interesting for globally operating players. The total set of core functionalities is without a very clear beneficiary community (other than the government), but our study shows that they are needed to offer the services that makes the port community as a whole more efficient and attractive to trade. When developing an NLIP in which the government aims for a role in the background, the question is if such a platform would ultimately provide the core functionality, for which a business model is so hard to find.

This creates a tension that is not easily resolved. Ungoverned use of community functionality and the data that follows from that for business services may lead to a slippery slope; the barrier between community and commercial functionality and assets becomes vague and the fear is that community data will be used to make more than just enough money to cover all costs of the system. However, when depriving a PCS of the option to use their infrastructure and the data that they have in custody to offer value-added services, which is one of their few ways to make money, the PCS as one of the main building blocks (at least in the short to intermediate term) of NLIP may run into difficulty sustaining itself. Either way, whether because the source of data dries out (if a few key providers of data do not wish to contribute to the PCSs business services) or whether the source of funding dries out (if no new sources of revenue are found), without a solution to this tension, it will be very difficult to find a sustainable model for creating NLIP as a platform of existing community systems.

Hence, in line with the theoretical background of the paper, the technical-rational approach that the actors followed resulted in tensions that block the enactment of the II. The role of the 'social' complexity proved to be large and measures were taken to address this type of complexity, primarily in the form of establishing a committee dealing with governance of the platform. The existing first steps towards a governance model for NLIP primarily concern governance as a process. In other words; it focuses on facilitating that the right people decide on how decisions are going to be made about combinations of public and private data. However, in this way many of those parties optimise for their own part of the operations, risking suboptimal decisions and configurations at the community (e.g. port community or supply chain) level. Small issues are easily resolved, but that does not solve that cascading issues lead to large costs for some parties, which, in line with the background, leads to a situation in which parties are reluctant to be actively involved. Simultaneously the perceived presence of hidden agenda's and additional vulnerabilities were not resolved by the governance model. Based on the theory, we suggest that to make NLIP work, it is vital that the community jointly decides that certain services and level of service should be considered community functionality and therefore also community

This is the author's version of this paper. The final publication is published in volume 9248 of the series Lecture Notes in Computer Science (pp. 170-180) and is available at Springer via http://dx.doi.org/10.1007/978-3-319-22479-4_13

funded. Our theoretical background suggests that this will involve a large government support, and even steering, whilst leaving some parts to the responsibility of the businesses. In any case, novel public-private governance models for decision-making on IIs should be further investigated.

In this case, all parties agree on the common goals, but have different underlying agenda's for the collaboration. What is clear is that due to the interdependence among the actors when it comes to data sharing, the fear for the agenda's of others, leads to actions to decrease additional vulnerabilities. As a result, solutions that should work well from a technical-rational perspective (e.g. an open infrastructure, separation between commercial and community functionality, a joint decision making structure), ultimately fail because of the social context in which the technical-rational solutions are perceived as potentially leading to new vulnerabilities (e.g. being locked-in, or being cut out of the information chain). Although the parties have long had dealings with each other as part of their role in the physical logistics flow, the existing relationships do not have sufficient trust basis to accommodate these vulnerabilities that follow from changes in the data position and role in the information infrastructure.

**Acknowledgements.**

This work is part of the research project "Governing public-private information infrastructures", which is financed by the Netherlands Organisation for Scientific Research (NWO) as Veni grant 451-13-020.

## References

1. Dunleavy, P., Margetts, H., Bastow, S., Tinkler, J.: New Public Management Is Dead - Long Live Digital-Era Governance. J. Public Adm. Res. Theory. 16, 467–494 (2006).
2. Milward, H.B., Provan, K.G., Fish, A., Isett, K.R., Huang, K.: Governance and Collaboration: An Evolutionary Study of Two Mental Health Networks. J. Public Adm. Res. Theory. 20, i125–i141 (2010).
3. Salamon, L.M.: The Tools of Government: A Guide to the New Governance, (2002).
4. Stoker, G.: Public Value Management: A New Narrative for Networked Governance? Am. Rev. Public Adm. 36, 41–57 (2006).
5. Scholl, H.J.: Five trends that matter: Challenges to 21st century electronic government. Innov. Public Sect. 20, 107–117 (2013).
6. Pollitt, C.: Mainstreaming technological change in the study of public management. Public Policy Adm. 26, 377–397 (2011).
7. Hesketh, D.: Weaknesses in the supply chain: who packed the box? World Cust. J. 4, 3–20 (2010).

This is the author's version of this paper. The final publication is published in volume 9248 of the series Lecture Notes in Computer Science (pp. 170-180) and is available at Springer via http://dx.doi.org/10.1007/978-3-319-22479-4_13

8. Tan, Y.-H., Bjørn-Andersen, N., Klein, S., Rukanova, B.: Accelerating Global Supply Chains with IT-Innovation. ITAIDE Tools and Methods, (2011).
9. Hanseth, O., Monteiro, E., Hatling, M.: Developing information infrastructure: The tension between standardization and flexibility. Sci. Technol. Human Values. 21, 407–426 (1996).
10. Hanseth, O., Lyytinen, K.: Design theory for dynamic complexity in information infrastructures: the case of building internet. J. Inf. Technol. 25, 1–19 (2010).
11. Henningsson, S., Henriksen, H.: Inscription of behaviour and flexible interpretation in Information Infrastructures: The case of European e-Customs. J. Strateg. Inf. Syst. 20, 355–372 (2011).
12. Tilson, D., Lyytinen, K., Sørensen, C.: Digital Infrastructures: The Missing IS Research Agenda. Inf. Syst. Res. 21, 748–759 (2010).
13. De Bruijn, J.A., Herder, P.M.: System and Actor Perspectives on Sociotechnical Systems. IEEE Trans. Syst. Man, Cybern. - Part A Syst. Humans. 39, 981–992 (2009).
14. Agranoff, R., McGuire, M.: Collaborative Public Management: New Strategies for Local Governments. Georgetown University Press, Washington, D.C. (2003).
15. Christensen, T., Lægreid, P.: The Whole-of-Government Approach to Public Sector Reform. Public Adm. Rev. 67, 1059–1066 (2007).
16. Goldsmith, S., Eggers, W.D.: Governing by Network - The New Shape of the Public Sector. Brookings Institution Press, Washington, D.C. (2004).
17. Teisman, G.R., Klijn, E.-H.: Partnership Arrangements: Governmental Rhetoric or Governance Scheme? Public Adm. Rev. 62, 197–205 (2002).
18. Huxham, C., Vangen, S.: What makes partnerships work? In: Osborne, S. (ed.) Public-Private Partnerships: theory and practice in international perspective. pp. 293–310. Routledge, London (2000).
19. Johnston, J., Gudergan, S.P.: Governance of public--private partnerships: lessons learnt from an Australian case? Int. Rev. Adm. Sci. 73, 569–582 (2007).
20. De Bruijn, J.A., Ten Heuvelhof, E.F., In 't Veld, R.J.: Process management: Why Project Management Fails in Complex Decision Making Processes. Springer, Berlin Heidelberg (2010).
21. Hailey, J.: NGO Partners - The Characteristics of Effective Development Partnerships. In: Osborne, S. (ed.) Public-Private Partnerships: theory and practice in international perspective. pp. 311–323. , London (2000).
22. Vangen, S., Huxham, C.: The Tangled Web: Unraveling the Principle of Common Goals in Collaborations. J. Public Adm. Res. Theory. 22, 731–760 (2011).
23. Johnston, H.R., Vitale, M.R.: Creating competitive advantage with interorganizational information systems. Mis Q. 12, 152–165 (1988).
24. Huxham, C., Vangen, S., Huxham, C., Eden, C.: The Challenge of Collaborative Governance. Public Manag. Rev. 2, 337–358 (2000).

This is the author's version of this paper. The final publication is published in volume 9248 of the series Lecture Notes in Computer Science (pp. 170-180) and is available at Springer via http://dx.doi.org/10.1007/978-3-319-22479-4_13

25. Klievink, B.: Unravelling Interdependence: Coordinating Public-Private Service Networks. Delft University of Technology, Delft (2011).
26. Tiwana, A., Konsynski, B., Bush, A. a.: Research Commentary —Platform Evolution: Coevolution of Platform Architecture, Governance, and Environmental Dynamics. Inf. Syst. Res. 21, 675–687 (2010).
27. Hart, P., Saunders, C.: Power and trust: Critical factors in the adoption and use of electronic data interchange. Organ. Sci. 8, 23–42 (1997).
28. Klein, S.: The configuration of inter-organizational relations. Eur. J. Inf. Syst. 5, 92–102 (1996).
29. Wareham, J.D.: Information assets in interorganizational governance: Exploring the property rights perspective. IEEE Trans. Eng. Manag. 50, 337–351 (2003).
30. Eisenmann, T., Parker, G., Alstyne, M.W. Van: Strategies for Two- Sided Markets. Harv. Bus. Rev. 84, 12 (2006).
31. Robey, D., Im, G., Wareham, J.D.: Theoretical Foundations of Empirical Research on Interorganizational Systems: Assessing Past Contributions and Guiding Future Directions. J. Assoc. Inf. Syst. 9, 497–518 (2008).
32. Markus, M.L., Steinfield, C.W., Wigand, R.T., Minton, G.: Industry-Wide Information Systems Standardization as Collective Action: The Case of the U.S. Residential Mortgage Industry. MIS Q. 30, 439–465 (2006).
33. Klievink, B., Janssen, M., Tan, Y.-H.: A Stakeholder Analysis of Business-to-Government Information Sharing: the Governance of a Public-Private Platform. Int. J. Electron. Gov. Res. 8, 54 (2012).
34. Romochkina, I.: Cluster Perspective on Inter-Organizational Information Systems, (2011).
35. Kubicek, H., Cimander, R.: Three dimensions of organizational interoperability. Insights from recent studies for improving interoperability frame-works. Eur. J. ePractice. 1–12 (2009).

This is the author's version of this paper. The final publication is published in volume 9248 of the series Lecture Notes in Computer Science (pp. 170-180) and is available at Springer via http://dx.doi.org/10.1007/978-3-319-22479-4_13