Mechanisms of Power Inscription into IT Governance

Lessons from Two National Digital Identity Systems

Medaglia, Rony; Eaton, Ben; Hedman, Jonas; Whitley, Edgar A.

Document Version
Accepted author manuscript

Published in:
Information Systems Journal

DOI:
10.1111/isj.12325

Publication date:
2022

License
Unspecified

Citation for published version (APA):
Medaglia, R., Eaton, B., Hedman, J., & Whitley, E. A. (2022). Mechanisms of Power Inscription into IT Governance: Lessons from Two National Digital Identity Systems. *Information Systems Journal*, *32*(2), 242-277. https://doi.org/10.1111/isj.12325

Mechanisms of Power Inscription into IT Governance: Lessons from Two National Digital Identity Systems

ABSTRACT

Establishing IT governance arrangements is a deeply political process, where relationships of power play a crucial role. While the importance of power relationships is widely acknowledged in IS literature, specific mechanisms whereby the consequences of power relationships affect IT governance arrangements are still under-researched. This study investigates the way power relationships are inscribed in the governance of digital identity systems in Denmark and the United Kingdom, where public and private actors are involved. Drawing on the theoretical lens of circuits of power, we contribute to research on the role of power in IT governance by identifying two distinct mechanisms of power inscription into IT governance: power cultivation and power limitation.

Keywords: Power; IT Governance; Digital Identity; Denmark; United Kingdom

1 Introduction

A key factor influencing the success of strategic opportunities arising from information technology (IT) is IT governance (De Haes & Van Grembergen, 2004; Gregory et al., 2018; Keen, 1981; Kling & Iacono, 1984; Saunders, 1981; Tiwana & Kim, 2015). IT governance is concerned with how a company allocates its IT decision rights and accountabilities (Weill & Ross, 2005), and is a key activity that aligns IT investment with business objectives.

IT governance questions around contentious elements of traditional IT projects, for example around prioritization and investment decisions (Weill & Ross, 2005), often unfold through a series of political processes (Sabherwal & Grover, 2010), resulting in further, political counter-counter-implementation strategies (Keen, 1981). New organizational forms can also change the power relationships between users, developers and organizations, and therefore transform how decision rights and accountabilities are managed. These include IT consumerization (Gregory et al., 2018), and the growing number of rapid, large scale IT projects in cross-sectoral collaboration between public and private actors (Klievink et al., 2016; Pouloudi et al., 2016), where many diverse stakeholders are involved.

However, while the importance of power has been widely acknowledged in IS literature (Jasperson et al., 2002; Keen, 1981; Marabelli & Galliers, 2017), the ways in which power relationships affect IT governance are less well understood (Bazarhanova et al., 2020; Magnusson et al., 2020). For example, the studies that touch upon the role of power and IT governance (Leclercq-Vandelannoitte & Bertin, 2018; Tallon et al., 2013; Williams & Karahanna, 2013) tend to "black-box" the way power relationships affect governance, seeing power as simply an obstacle or something negative in the establishment of IT governance. Moreover, power in this literature is frequently conceptualized simply as 'power over' that allows governance to be force-fitted upon the organization. In this way power is often seen as something that is reified, owned and instantiated as a restraining force linked to control, coercion and authority (Hislop et al., 2018). Consequently, researchers do not look at how power relationships affect the emergence of flexibility in the decision rights and accountability of IT governance (Wareham et al., 2014, p. 1196) or the transformation of IT governance (Gregory et al., 2018). Therefore, our aim is to understand how power relationships affect the governance of information systems and is driven by the following research question:

What are the mechanisms through which power relationships are inscribed into the governance of information systems?

In order to answer this research question, we investigate the development and delivery of two, large scale, shared and public information systems, namely the national digital identity systems of Denmark and the United Kingdom. Increasingly, governments turn to collaboration with private actors to solve challenges of system complexity, given their limited skill sets (Cordella & Willcocks, 2010; Klievink et al., 2016; Klievink & Janssen, 2014). In these public-private partnerships, power

relationships play a central rule, due to the nature of the dependencies between public and private actors (Eaton et al., 2018; Medaglia et al., 2017). Yet, the actors involved are expected to adopt governance practices that can inscribe these evolving and dynamic power relationships (Bekkers, 2009; Ojo & Mellouli, 2018) to be able to form a coherent service delivery system (Bertot et al., 2016; Scupola & Zanfei, 2016). National digital identity systems are therefore a case in point to investigate how power is inscribed in IT governance.

In this paper, given the various ways of framing understandings of power that exist in the literature, we draw on Clegg's Circuits of Power (1989). This framework is explicitly intended to go beyond the most apparent and visible forms of 'power over', to also highlight rules of meaning and membership that affect social relations and alliances, as well as the role of power to produce and achieve collective goals. We borrow the concept of *inscription* from Latour and Woolgar (1986) as an analytical lens to understand the connection between power relationships and IT governance.

By doing so, we make three distinct contributions to research on power and IT governance. First, we make a core theoretical contribution concerning the articulation of *power cultivation* and *power limitation* as two distinct mechanisms through which this inscription takes place. Second, we provide a methodological contribution, by developing the notion of inscription to conceptualize how power relationships affect IT governance patterns. Finally, we offer a perspectival contribution: we complement the dominant view in IS research of power as 'power over' as we present a detailed analysis of the circuits of power (Clegg, 1989) between the actors involved, to show how power relationships can be a relational and productive force that can be inscribed in effective IT governance arrangements.

In the remainder of the paper, we begin by first reviewing the literature about power in IS, where we introduce Clegg's Circuits of Power. We also consider the literature concerning power in IT governance and IT governance patterns in particular, and we reflect on literature that helps us conceptualise the notion of power inscription. Next, we present the research methods adopted in the study. This is followed by a case analysis of the digital identity systems in Denmark and the UK. This analysis presents the findings that include two distinct mechanisms (power cultivation and power limitation) that inscribe power relationships into IT governance. We end with a discussion of implications of this analysis for research on power and IS and on IT governance.

2 Conceptualizing power inscription into IT governance

2.1 Power and IS

The relationship between power and information technology has long been discussed in the IS field (Introna, 1997; Jasperson et al., 2002; Keen, 1981; Kling & Iacono, 1984; Saunders, 1981). Many of these studies sought to adopt conceptualizations of power from related fields of study and apply them to information systems. Key amongst

these approaches are the work of Emerson (1962), Foucault (1980a, 1980b), Clegg's circuits of power (1989) and Lukes (1974). Other, complementary, reflections on power include Star (1991), Latour (1986, 2005) and Lessig (1999).

Early studies showed how information systems development is an "intensely political" process (Keen, 1981) with the resulting development trajectory being "the outcome of a political process" (Kling & Iacono, 1984). Other studies involved political considerations to address notions of centralization and decentralization (King, 1983; Leavitt & Whisler, 1958), power as a social process unaffected by IT (Fleming & Spicer, 2014), reinforced by IT (Leavitt & Whisler, 1958), or mutually emerging with IT (Jasperson et al., 2002).

One of the seminal studies on power and information systems is by Markus (1983), who draws the connection between "political" actions that might be used to resist particular forms of change arising from computer-based information systems, and the effects on "the balance of power" (1983, p. 431) that can arise. Building on this, there are several studies that seek to understand the effects of power on systems development activities, including IT governance. For example, there have been studies that have looked at power in terms of decision making, resource control, authority and influence (Webster, 1995), knowledge sharing (Simeonova, 2018), organizational change (Allen et al., 2013), and workarounds (Malaurent & Avison, 2016) in relation to the development, use and impact of information technology.

Two main strands of research on power and IS can be identified. One strand views power as structural (Astley & Sachdeva, 1984; Eaton et al., 2015; Karhu et al., 2018; Levina & Arriaga, 2014; Tiwana et al., 2010). The other strand takes a critical perspective that acknowledges the relationship between power and IT from a broader societal perspective (Avgerou & McGrath, 2007; Introna, 1997; Leclercq-Vandelannoitte & Bertin, 2018; Myers & Young, 1997). The predominant focus adopted in both strands of studies on power and IS remains the perspective of 'power over', that is as a restraining force linked to control, coercion, and authority (Clegg et al., 2006; Hislop et al., 2018) where there is a power dependence between one actor and another (Emerson, 1962). Indeed, Clegg (1989) notes that this is "the most apparent, the most easily accessible and most visible" form of power (Clegg, 1989, p. 211).

While early studies saw information systems as simply crystallizing balances of power (Webster, 1995), the bulk of existing research in IS approaches power relationships mostly as challenges to be coped with in IS implementation. Such coping strategies include, for example, aligning stakeholders' power (Dhillon et al., 2011), institutionalizing power in policies (Deng et al., 2016), mediating power imbalances through knowledge exchange (Pozzebon & Pinsonneault, 2005, 2012), or resorting to unilateral governance schemes (Xiao et al., 2013). Other studies consider IS implementation as an arena of continuous power contention without eventual resolution (Azad & Faraj, 2011; Doolin, 2004).

There are examples of IS studies taking a structural view that have begun to approach power as a productive force that can be 'translated' into IS solutions

(Marabelli & Galliers, 2017). Inspired by the later writings of Foucault, Willcocks (2006) highlights the key role of technologies of power and indicates that "modern subjects can and do subvert the conditions of their own subjectivity" (2006, p. 276). Whitley & Hosein (2008) also draw upon Foucault's concept of technologies of power which guides our attention to the symbolic power and the role of knowledge and knowledge conventions, including what is considered to be a fact in technical discourses. Another approach to applying Foucault's work is found in Beresford (2003) which employs it to highlight the network of relationships between the governing and the governed.

Based on the need to look beyond conceptualising power as just 'power over' (Marabelli & Galliers, 2017), we choose to employ a theoretical framework that draws its explanatory capability from its emphasis on the relational nature of power, and on its ability to integrate different conceptions of power, that is Clegg's circuit of power framework (Clegg, 1989). This framework allows us to better investigate how power relationships affect IT governance.

2.2 Circuits of power

The theoretical framework proposed by Clegg (1989) uses the metaphor of electric circuits to represent power relationships. Power manifests itself as a set of norms, procedures, and techniques of discipline that act as forces, similar to electricity in a circuit, that shape the scope of action of individuals in organizations. The framework has proven a powerful lens in several IS studies (Backhouse et al., 2006; Fragos et al., 2007; Lapke & Dhillon, 2008; Silva, 2007; Silva & Backhouse, 2003; Silva & Fulk, 2012; Smith et al., 2010).

Clegg argues that "a theory of power must examine how the field of force in which power is arranged has been fixed, coupled and constituted in such a way that, intentionally or not, certain 'nodal points' of practice are privileged in this unstable and shifting terrain" (1989, p. 17). Thus, his framework focuses on "the strategies and practices whereby, for instance, agents are recruited to views of their interests which align with the discursive field of force that the enrolling agency is able to construct" (1989, p. 17). As a result, power is better regarded "as a process which may pass through distinct circuits of power and resistance" (1989, p. 18). The metaphor of the circuit emphasizes the relational rather than reified nature of power, i.e. that it is not something to be owned (Backhouse et al., 2006) or belonging to one party.

Clegg's framework distinguishes between three "circuits of power": episodic, social, and systemic. The first circuit, the *episodic circuit of power,* refers to relationships of 'power over' between actors, and is characterized by domination and self-interest (Clegg et al., 2006). This circuit reflects Dahl's definition of power where "A has power over B to the extent that he can get B to do something that B would not otherwise do" (Dahl, 1957, pp. 202–203). The type of power manifested in this circuit is *causal*: for episodic circuits of power to be made manifest, there must be evidence that B really is being coerced, implying that in so doing B's resistance should be apparent.

Research in IS using Clegg's lens has shown how episodic circuits of power occur, for example, in relationships between actors engaged in IS policy implementation, or in complying with regulation. Lapke and Dhillon (2008) identify evidence of an episodic circuit of power in the resistance enacted by middle managers and employees of a bank that was mandated by national regulation to establish an IS security policy. In this example, the episodic circuit exists in relation to the causal power of policy-makers (A) over the bank managers and employees (B) who have to accept the policy.

The second circuit, the *circuit of social integration,* refers to rules of meaning and membership that affect social relations and alliances. Such rules represent the conditions that need to be in place for A to be able to exercise power over B. The type of power manifested in this circuit is *dispositional*: it is power as legitimized by status, position or access to resources that allow to exercise power.

IS studies using Clegg's lens have identified circuits of social integration in the analysis of the differences of meanings attributed to IS initiatives. For example, Fragos et al. (2007), studying the management of IS security in a public sector organization, analyse the power relationships in a situation where managers see a security policy as a means for protecting an information system, while employees see it as a constraining overhead. Public managers (A) draw on rules of meaning and membership – such as status, authority, social relations and alliances in the formal and informal structure of the organization – to tell employees who see the policy as a constraint (B) what to do (Fragos et al., 2007).

The third circuit, the *circuit of systemic integration,* refers to relationships of power understood in terms of their ability to produce and achieve collective goals. The type of power manifested in this circuit is *facilitative*: it comprises the means for controlling the physical and social environment in organizations, which Clegg refers to as "techniques of production and discipline" (Clegg, 1989), echoing Foucault (1977). The focus of power here is on achieving individuals' compliance to specific goals; in doing so it employs techniques to ensure and monitor compliance and instil discipline.

IS studies using Clegg's lens have identified circuits of systemic integration, for example, in investigating how IS security standards set by national and international bodies (A) are used as techniques of production and discipline that influence the working practices of the organizations that have to follow them (B) (Backhouse et al., 2006).

Table 1 Summary and illustration of Clegg's circuits of power provides a summary and an illustration of Clegg's three circuits of power drawing on prior IS literature (see also Clegg, 1989, fig. 8.1). The first column indicates the circuit of power, the second the type of power, and the third provides examples of the circuit of power applied in an IS setting.

Table 1 Summary and illustration of Clegg's circuits of power

Circuit of power	Type of power	Examples of application of the circuit in information systems research
Episodic circuit	Causal Power: When A makes B do something which B would not otherwise do. This emphasizes A's 'power over' B.	The episodic circuit that exists in relation to the causal power of policy-makers (A) over the bank managers and employees (B) who resist and eventually accept an IS security policy (Lapke & Dhillon, 2008).
Circuit of social integration	Dispositional Power: The conditions (resources and organizational rules and norms) that need to be in place for A to be able to exercise power over B. This is rooted in rules of meaning and membership of the organization and the power dynamics that give them their form.	Managers (A) of a public sector organization adopting an IS security policy draw on rules of meaning and membership – such as status, authority, social relations and alliances – in interacting with employees (B) who see the policy as a constraining overhead (Fragos et al., 2007).
Circuit of systemic integration	Facilitative Power: The techniques employed by A to ensure and monitor B's compliance. This is defined by the techniques of production and discipline of the organization, and is successful when it brings about desired changes in routines and ongoing work practices. This power is therefore productive in the sense that causes the organization to generate outcomes.	IS security standards set by national and international bodies (A) are used as techniques of production and discipline that influence the working practices of the organizations that have to follow them (B) (Backhouse et al., 2006).

2.3 Power and IT governance patterns

IT governance is defined as the decision rights and accountability framework (Olson & Chervany, 1980) used to ensure the alignment of IT-related activities with the organization's strategy and objectives (Sambamurthy & Zmud, 1999; Tiwana & Kim, 2015; Wu et al., 2015). Assuming its prominence in IS research from the second half of the 1990s (Sambamurthy & Zmud, 1999), research on IT governance over time has reflected the increasing complexity of IT, the expanded range of actors involved, and the increased diversity of emerging organizational forms.

The classic foci of IT governance research highlighted tensions between centralization and decentralization (George & King, 1991; King, 1983), and investigated how governing the IT function can affect synergies and economies of scale (Tiwana & Kim, 2015; Wu et al., 2015; Xue et al., 2008), the degree of social alignment between business and IT units (Schlosser et al., 2015) and ambidexterity (Magnusson et al., 2020). More recently, the focus of IT governance research has begun to span organizational boundaries, following developments such as new forms of IT service delivery (Winkler & Brown, 2013), the evolution of digital infrastructures (Tilson et al., 2010), and of platform-based business models (Huber et al., 2017; Tiwana et al., 2010; Wareham et al., 2014).

Broadly speaking, extant research on IT governance addresses three questions: *what* is governed, *who* is governed, and *how* it is governed (Tiwana et al., 2013).

Recently, Gregory et al. (2018) projected these questions onto three key dimensions: the *focus* of IT governance (what to govern), the *scope* of IT governance (who to govern), and the *patterns* of IT governance (how to govern).

The focus of IT governance refers to what IT-related activities and artefacts must be aligned with organizational strategy and objectives, roughly corresponding to the unit of analysis of a study. For example, for mainstream organizations focusing on governing their internal IT function, the focus of what is governed includes both the technological systems themselves and the business units that make use of them (Brown & Grant, 2005). The scope of IT governance refers to which actors and stakeholders are held accountable for ensuring IT contributes to the organization.

Finally, the *patterns* of IT governance refer to the governance arrangements that are put in place to pursue IT-related activities and outcomes. Examples of patterns of IT governance include formal processes (Tallon et al., 2013), budgets and contractual arrangements, such as service level agreements (Almeida et al., 2013), structures of distributed decision-making authorities (Constantinides & Barrett, 2014), arrangements for balancing between stability and change (Wareham et al., 2014), as well as values guiding co-creation (Huber et al., 2017). They cover functional structural arrangements and formal processes which are based "on the underlying assumption of achieving coordination among multiple internal stakeholders through complex organizing" (Gregory et al., 2018, p. 1232); but they also include platform standards, automated processes, and multi-layered architecture arrangements, which are based "on the underlying assumption of achieving automated coordination among internal and external stakeholders through platform design" (Gregory et al., 2018, p. 1241). Our study focuses on IT governance patterns (Almeida et al., 2013; Constantinides & Barrett, 2014; Huber et al., 2017; Tallon et al., 2013; Wareham et al., 2014).

Researchers have explored a number of possible factors that affect the effectiveness of IT governance, including IT and organizational properties (Tiwana et al., 2013), and the role of context (Brown & Grant, 2005). For example, in multi-firm situations, a key factor is the mix of formal contracts and rules to guide and coordinate e-business cooperative activities among firms and their partners, as opposed to more relational governance (Chi et al., 2017); while, in the context of technology ecosystems, tensions between complementary and contradictory logics of different actors (Wareham et al., 2014) and levels of transparency (Joshi et al., 2018) are found to affect governance patterns. Notably, in research focusing on any of the three dimensions of governance (what, who, and how), power is not mentioned among antecedents (Magnusson et al., 2020; Tiwana et al., 2013) or is subsumed under the concept of autonomy .

In line with this insight, we expect power relationships to play a significant role in the emergence of particular patterns of IT governance. In the few studies that mention power relationships in the IT governance literature, power is mostly conceptualized as a threat to governance (Leclercq-Vandelannoitte & Bertin, 2018; Tallon et al., 2013; Williams & Karahanna, 2013). While research considering systems with a scope

beyond a single organizational entity acknowledge the importance of power relationships (Gregory et al., 2018; Williams & Karahanna, 2013), the way by which power affects IT governance patterns remains under-investigated and is often black-boxed. Little consideration is given to the mechanisms by which power relationships affect IT governance patterns. To provide a conceptual foundation for the analysis of such mechanisms, we draw on the concept of inscription.

2.4 Power inscription

In seeking to better understand how power relationships affect patterns of IT governance, we borrow the notion of inscription, a key concept in actor-network theory. Our notion of inscription is based on the one introduced in Latour and Woolgar's original study of scientific practices (1986), where it is presented as "a method of transferring information as a material operation of creating order" (Latour & Woolgar, 1986, p. 245).

Examples of inscription include the making of maps based on observations by explorers (Latour, 1987); or converting, via the use of a pedocomparator and colour charts, soil samples from the edge of the savanna into the data for a scientific paper about vegetation dynamics and the differentiation of soils in the forest-savanna transition zone (Latour, 1999).

An account of a process of inscription includes the material *substance* that is transferred into an inscription device; the material *operation* of inscribing; and the *order* that is created through inscription (Latour & Woolgar, 1986).

In our study, we use the notion of inscription to identify how power relationships affect patterns of IT governance, where the material substance is the power relationships between actors involved in IT governance; the material operation is the negotiation and establishment of governance patterns that are compatible with such relationships; and the order that is created through inscription is the observed characteristics of IT governance patterns.

There are two reasons for our use of this notion of inscription. First, many of the studies that use Clegg's circuits of power framework make reference to the "regulations and rules *inscribed* into an information system" (Silva & Backhouse, 2003, p. 322 emphasis added), echoing Orlikowski's (2000) insight that "technology is developed through a social-political process which results in structures (rules and resources) being embedded within the technology" (2000, p. 405). Second, Clegg himself draws heavily on actor-network theory and its "general methodological precepts" (Clegg, 1989, p. 205). It is to be noted, however, that Clegg's framework mostly draws on the concept of obligatory passage points (OPP), which is conceptually related, but different from the notion of inscription we draw on. An obligatory passage point is a situation defined by a focal actor that has to occur for all of the actors to be able to achieve their interests (Callon, 1984; Latour, 2005) and refers "to precisely what A wants B to do" (Backhouse et al., 2006, p. 415) and the institutionalisation of an OPP is an "outcome of power" (Backhouse et al., 2006, p. 416) rather than an input to analysis.

The concept of OPP rests on two assumptions: first, that there is a focal actor, typically chosen by the analyst, that has a prominent role and that "other actors need to be convinced to pass through the OPP (i.e., modify their alignments and behaviours such that they are consistent with the OPP)" (Sarker et al., 2006, p. 54); second, that an OPP is characterized by irreversibility, implying that "it is impossible to go back to a point where alternative possibilities exist" (Walsham & Sahay, 1999, p. 42). By drawing on the notion of inscription, instead, we consider IT governance as emerging from a power relationship interaction with no specific focal actor over time; and we consider IT governance patterns as potentially reversible, depending on the possible transformations in the power relationships between actors, thus opening up analytical consideration of all three circuits of power, not just the episodic circuit.

Using the notion of inscription helps us to make more generalizable claims about the processes whereby power relationships affect IT governance patterns. We label these generalizable claims as *mechanisms*, following the definition of mechanisms as "sets of social events or processes that, under certain circumstances, bring about changes in human social relations without necessarily being reducible to the actions of individuals" (Markus & Rowe, 2018, p. 1261). By using the concept of inscription, we move from individual instances of the various circuits of power, that affect specific IT governance patterns, into more abstract and generalizable mechanisms.

3 Methods

We carried out an interpretative study of two digital identity systems, namely the Danish MitID and the British GOV.UK Verify systems. We had the goal of understanding how power relationships between the various public and private sector actors involved in the two systems are inscribed into the IT governance patterns of each. Our unit of analysis was the public and private sector partners involved in implementing the specific national digital identity systems.

3.1 Case study approach and case selection

We chose a case study approach as it is viewed as a preferred method to explore in depth complex social issues related to information system development and use (Walsham, 1995). This approach also supports better comparison between different cases for theory building, testing, and generalization (Walsham, 1995, 2006). Digital identity systems typically support identity proofing, authentication, and authorization (Nyst et al., 2016, pp. 28–29) and are of relevance for our study for two reasons. First, they are moving away from their historical administrative dependency on the state, towards a greater involvement of the private sector (Gelb & Diofasi Metz, 2018; GSMA, 2016; Nyst et al., 2016). This change creates space for power relationships to arise due to the dependencies that emerge between public and private actors (Eaton et al., 2018; Medaglia et al., 2017). Second, the scope of digital identity system use is broadening, making governance issues even more important.

For example, in Europe, the European Union (EU) regulations concerning digital identity and digital signatures (eIDAS – electronic IDentification, Authentication and trust Services) (European Commission, 2016) include an interoperability requirement, which enables digital identification schemas to be usable across the EU, enabling citizens to benefit from the use of their digital identities more widely. Consequently, digital identity systems are becoming more complex as the range of public and private actors involved are required to adopt governance practices in order to form a coherent service delivery system. Digital identity within the EU provides an informative venue for understanding the consequences of power relationships for IT governance patterns. Based on this, we chose the Danish MitID and the British GOV.UK Verify systems as our empirical cases.

MitID is the third generation of digital identity system in Denmark (Digitaliseringsstyrelsen, 2020). Its history dates back to the early 2000s and draws on a well-established tradition of consensus-based collaboration between the public and the private sector (Hoff & Hoff, 2010). The main technology actors are the Danish Agency for Digitisation (*Digitaliseringsstyrelsen*), a consortium of Danish banks, represented by the Danish Bankers Association (*Finans Danmark*), and Nets – the developer.

In contrast, GOV.UK Verify is effectively the first significant digital identity system in the UK, replacing the controversial national identity system that was scrapped by a coalition government in 2010. GOV.UK Verify was launched as a beta service in February 2014 and became a live service in May 2016. The main technology actors are the Government Digital Service (GDS), that oversees the scheme, and a series of private sector companies who act as identity providers. These operate alongside the providers of government services that consume assured digital identities (GOV.UK, 2020). In each case the relationship between citizens and government highlights further power issues that inform the analysis.

3.2 Data Collection and analysis

Given the focus of analysis on the power relationships among the actors involved in the digital identity systems and the IT governance patterns, we collected primary data through semi-structured interviews, and meetings (see appendix A). In line with the key informant approach (Kumar et al., 1993), we interviewed key stakeholders from government agencies and private organizations, including head of organizations involved in the establishment of the digital identity systems. We also participated in key meetings. The initial interviews were exploratory, aiming at understanding the background and context, whereas the later interviews were focused toward developing an understanding of existing power relationships, and they lasted on average for an hour. In the UK case, one of the authors also had direct access to key stakeholders in the GOV.UK Verify team and, as such, was able to obtain detailed clarification of key points and areas of ambiguity from the team. Many of these clarified points were then presented to the wider public as blog posts, thus providing official records of research data.

Additionally, throughout our study we collected secondary material, such as documents, online press releases, and material from key stakeholder web pages (see appendix A). This material was used both as background material, input to the narrative case writing, and triangulation points, contrasting the "researcher provoked data" with "naturally occurring data" (Sarker et al., 2018). The official documents (for instance Digitaliseringsstyrelsen (2016b) and GOV.UK (2012)) also provided a timestamp on events and gave an account of the relationship between actors that we used in the analysis.

In the MitID case, three of the authors began collecting data in 2014, whereas in the UK case one of the authors began his engagement with what became GOV.UK Verify in 2011. Table 2 Summary of approach to data collection provides a summary of the data collection, with more detail provided in appendix A.

Table 2 Summary of approach to data collection

Data sources	**Cases**	
	Denmark: MitID	UK: GOV.UK Verify
Primary data	Seven interviews with key informants	Participation in multiple key planning meetings and industry engagement events
Secondary data	Policy documents Legislation Tender proposals	Policy documents Legislation Business case documentation Technical documentation and service profiles Industry reports and white papers

The analysis of the collected data followed four phases, which are summarised in Table 3.

Table 3 Summary of approach to data analysis

Phase and Objective	**Researcher Activities**	**Focus of Coding**
Phase 1 Identifying events in the emergence of governance	Generating event-time series in the emergence of digital identity system governance	Events, decisions, actions and outcomes related to governance (open coding)
Phase 2 Identifying power relationships between actors for each case	Identifying circuits of power	Power relationships as circuits of power (a priori coding)
Phase 3 Identifying patterns of governance for each case	Identifying patterns of governance	Patterns of governance (open coding)
Phase 4 Identifying mechanisms of power inscription for each case	Identifying mechanisms of power inscription through which circuits of power affect patterns of governance	Inscription mechanisms (open coding)

In the first phase we focused on within-case analysis, where we applied an open coding of the data to capture an event-time series of the emergence of digital identity system governance (Pettigrew, 1985). Coding categories were developed around generic process codes including events, decisions, actions and outcomes. Thus, the category of "events" included exogenous factors that potentially affected the development and governance of the digital identity systems; "decisions and actions" included the responses taken by the central actors to determine the development of the digital identity systems; and "outcomes" were the emerging elements that resulted from the actions of the central actors. At this stage of the analysis there was no focus

on questions of power. The product of this phase was a timeline showing the key events in the public-private collaboration of the digital identity systems in Denmark and the UK that could then be used to help focus the remainder of our analysis. The MitID data was coded initially by three of the authors who discussed the within-case coding with each other to create a joint understanding of the MitID case data. The GOV.UK Verify data was initially coded by the fourth author and checked by the second author. Appendix B illustrates examples of this open coding of the events, actions and outcomes from phase 1.

In the second phase, we continued with our within-case analysis. Our objective in this phase was to identify and classify power relationships. To do this, we first analysed the output of phase one to identify instances and classify power relationships in a process of a priori coding based on the definitions of the circuits of power (Clegg, 1989) outlined in section 2.2 above. For example, the power relations of an episodic circuit are often revealed through the resistance of one set of actors to the coercion of another set; rules of practice in the social integration circuit can be revealed by norms and resource dependencies, and the circuit of systemic integration often produced altered routines. These power relations were revealed through the analysis of the interviews and the documents. For instance, when identifying a circuit of systemic integration, the document "Identity Assurance Principles" (GOV.UK Verify, 2014c) included the phrase "Certified companies have to work to published government standards when they verify your identity", which is interpreted as a technique employed by government to ensure compliance of suppliers. Appendix C shows more extracts of the coding of power relationships that we identified. During this phase, the three authors of the Danish MitID case and the author of the GOV.UK Verify case initially coded their data independently. The four authors then met as a group on two occasions in order to discuss the coding results. A hermeneutic process was followed (e.g. Boland, 1991; Westrup, 1994), where divergences in analysis were focused on and debated until consensus was reached concerning the identification of different circuits of power. With this shared understanding and a relatively small number of analytical constructs, inter-coder reliability was not calculated. The analysis resulted in a set of four different circuits of power for the Danish MitID case and four different circuits of power for the GOV.UK Verify case.

In the third phase, we revisited each case to identify patterns of IT governance. To do this, we used a process of open coding to label the patterns of governance that emerged for each system of digital identification. We relied on Gregory et al.'s (2018) understanding of patterns of IT governance and the examples they provided (see Section 2.3) as a sensitizing device (Klein & Myers, 1999, p. 75) to inform our search, and focussed on those IT governance patterns that our sources themselves emphasized as being significant or distinctive. Appendix D provides examples of open coding of governance patterns.

In the fourth and final phase of analysis we sought to identify generalizable claims about the processes whereby power relationships affect IT governance patterns. We used the concept of inscription to move from the individual instances of the various

circuits of power to mechanisms of power inscription. This was done by identifying mechanisms of inscription through which the circuits of power between actors involved in IT governance (as the material *substance* that is inscribed) affect the negotiation and establishment of governance patterns that are compatible with such relationships (as the material *operation* of inscribing), and the observed characteristics of IT governance patterns (as the *order* that is created through inscription). A single mechanism of power inscription was identified for each of the two cases. We identified two different mechanisms of inscription based on how the sets of power circuits between actors for each case affected the observed governance patterns. The mechanisms identified in this cross-case analysis were quite distinct, highlighting the value of using the two case studies.

4 Case analysis

4.1 Denmark's MitID

MitID is to be Denmark's next generation national digital identification system. Denmark's new digital identity system and associated governance structures are influenced by the country's history of national digital identification. On the government side, interest in a national system of digital identification was first realized in 2003 (Hoff & Hoff, 2010). This initial government digital identification solution suffered from low take up compared to online identification solutions provided by the banks that emerged in the same period. This led to the Danish Government enrolling the *Pengeinstitutternes Betalings Systemer* (PBS), an organization jointly owned by the Danish banks and later renamed Nets AS, to build a second-generation national digital identification system called NemID, shared with Danish banks. Launched in 2010, NemID is now used by all public institutions and by over 92% of Danish citizens (Digitaliseringsstyrelsen, 2016c) where secure electronic authentication is needed.

The need for MitID emerged as a result of the impending expiry of the contract for NemID. Once again, the government is partnering with the Danish banks (Digitaliseringsstyrelsen, 2016b) to build the new digital identity infrastructure, which is to be developed and managed via a public tender process to an outsourced solution provider. The solution for MitID was put out to tender in December 2017 (Digitaliseringsstyrelsen, 2017a), including an outline of the governance model. In Spring 2019, it was announced that Nets won the tender. Nets was also the outsourcing partner of the previous NemID solution. MitID is currently being implemented and its launch is planned for summer 2021.

4.1.1 Circuits of power in the Danish case

Our analysis determined that the approach to governance of the future MitID solution is affected by power relationships between three groups of actors: between Danish citizens and the government; and within a partnership consisting of the government

and the Danish banking industry. These power relationships are expressed in the following four instances of circuits of power identified in our analysis. Figure 1 provides an overview of the key circuits of power between actors engaged in the establishment of the MitID solution in Denmark.

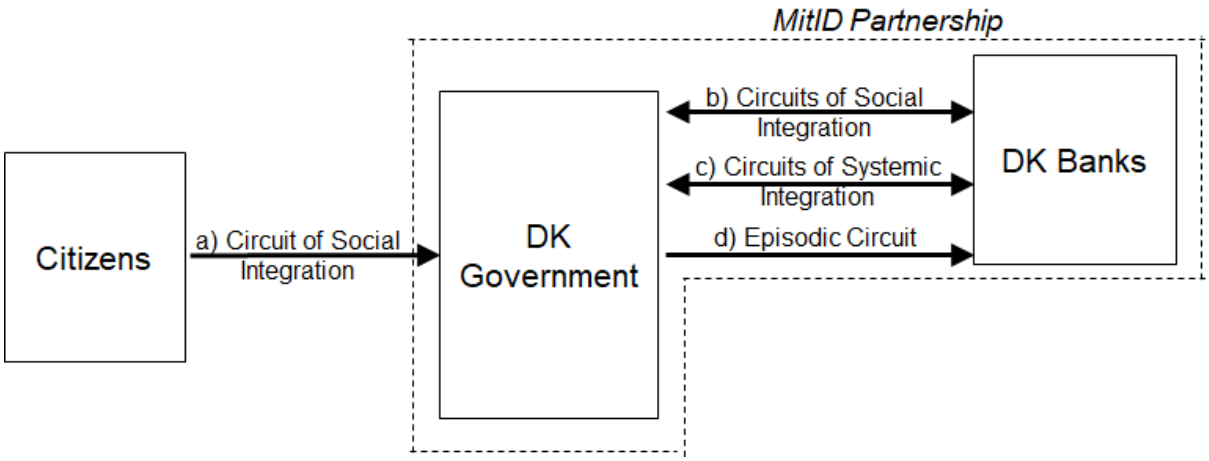

Figure 1 Denmark's MitID circuits of power

a. Societal drivers on the Danish Government to adopt a public-private partnership solution: as a circuit of social integration

There is a cultural norm of "*fælles*" (meaning, in English, common good or mutual benefit) in Danish society, which describes a tradition of cooperation between stakeholders, across sectors. The norm is explicitly stated in the agreement between the government and the banking industry, in the section "why a partnership?" (*Hvorfor et partnerskab?*) (Digitaliseringsstyrelsen, 2016b).

The benefits of *fælles* include maintaining national standing and making efficient use of resources in a small country. This was realized in NemID, the current generation of digital identity system, with the government and the banking industry sharing a common infrastructure. This is alluded to in the following quotes:

"Part of our culture is to seek common solutions, and we have a strong tradition of cooperation in the public sector in comparison to other countries. There is a recognition that we are a very small country and we need cooperate to be better than the others" – Respondent 4

"It has always been a strategy also from the Ministry of Finance that you implement this in order to get efficiency benefits and you have to reduce costs" – Respondent 5

In this way, Danish citizens possess dispositional power, expressed as a circuit of social integration (arrow a in Figure 1), over the government to maintain the norm of *fælles*.

b. Cooperation between the government and banks driven by resource interdependencies: as a circuit of social integration

The MitID partnership features a mutually beneficial interdependence of resources (Digitaliseringsstyrelsen, 2016b). The systems that emerge from these partnerships

rely on citizens identifying themselves using a government-allocated Central Person Register (CPR) number (Pedersen, 2011). The CPR number is a unique 10 number identifier and becomes the basis for the identification process. The CPR number is commonly used by Danish citizens to identify themselves in their online and offline interactions with both state and commercial organizations. The use of the number is widely trusted across Danish society. The Danish banks rely on the tacit approval of the state for the use of this government owned asset. The importance of the CPR number to both parties is indicated in the following quote:

"The CPR number has shaped the way that the public sector bases their entire interaction with citizens. The financial sector and the insurance business do the same" – Respondent 2

In parallel, the Danish government benefits from cooperating with the Danish banking industry by having access to the banks' installed base of customers. The banks' customers are accustomed to frequent use of digital authentication in order to carry out online banking transactions. The resistance of the Danish citizens to access online government services, which require digital identification, is reduced when they use the same common digital identity authentication solution employed by the banking industry. This then facilitates the adoption of online government services. In this way, the Danish government relies on the cooperation of the banks in order to share their customer base. The importance of the government having access to the banks' installed base of users is mentioned by both respondent 1 and respondent 2:

"The public sector fears that the banks make their own solution. The banks have the popular applications and the public sector needs a lot of citizens enrolled in this system" – Respondent 1

"We had a problem that public sector services were accessed very rarely by citizens. When you have a unique digital signature for the public sector and you use it maybe once a year, maybe twice, you forget how to do it" – Respondent 2

In addition, these circuits of social integration (arrow b), driven here by access to resources, are further augmented by a sense within the banking industry of the need to cooperate with the government in order to restore social capital after the recent financial crisis. This provides additional authority to the government's demands that the banks take part in the partnership and is elaborated in the following quote:

"The banks in Denmark were hit quite badly [by the financial crisis] so that for a while we had to invest in some of the banks to help them to survive. The general perception of the banks from the public sector and also public got very bad for a while. They need to improve their standing in society. I think that they look at this partnering as something to bring back the status that they actually are part of the Danish society, that they do something good" – Respondent 4

Control over each vital resource provides one side with authority and an ability to influence the other with respect to shaping governance in the partnership. In this sense this circuit of power (arrow b) is directed both ways, rather than in an asymmetric relationship of one party having 'power over' another.

c. Commitment to the terms of the MitID partnership driven by facilitative patterns: as a circuit of systemic integration.

There are several patterns associated with the MitID partnership that enable techniques of discipline that we represent as a circuit of systemic integration (arrow c). The first pattern concerns the banks' adoption of the CPR number as a general means to identify customers. However, as the government owns this asset, it has decision rights over its use. In this way, the government has the potential to sanction the banks by specifying that their use of the CPR number is limited to MitID.

The second pattern concerns the potential for the Danish Government to apply competition law to sanction those larger banks who break ranks from the partnership to independently build their own solution, as alluded to in the following:

"There are two very large banks and a lot of very small banks. For the smaller banks it's very important that the large banks are not running away. We've had this situation with the Mobile Pay service where we saw Danske Bank build its own solution. The small banks have been quite eager and trying to make a situation where Danske Bank somehow got into this institutionalized partnership [for MitID]" – Respondent 4

The overall effect of these elements of facilitative power is to provide a means of discipline that leads to both parties signing up to the partnership agreement and then to abide by its terms.

d. Formation of the MitID partnership as a step towards the MitID tender: as an episodic circuit

Having the banks sign the MitID Partnership agreement was a necessary step to allow for the tendering of the MitID solution. As the tendering would involve the Danish state, it would be necessary to follow an EU tendering process for government procurement, which is a long and complex process. The banks were resistant to this process, and by implication they were resistant to signing the MitID Partnership agreement. The banks' resistance to this process is evidenced in the following comment:

"The biggest problem for the banks is to understand the public tender. It has been so complicated for them and they have no experience with doing a tender in an EU-regulated way […] They can't accept the idea that tendering takes between one year to eighteen months [...] I think in the beginning, from the banks' side, they did not think that we should do tendering together necessarily […] We had a lot of talks with the banks to convince them before we went into the tendering process" – Respondent 4

Given the distinct configuration of power relationships presented above and described as circuits of social integration and circuits of systemic integration, the entire banking industry agreed to the formation of the MitID partnership. The banks signed the MitID Partnership agreement on 1 July 2016 (Digitaliseringsstyrelsen, 2017a) and that allowed for the tendering of the MitID solution. Given the resistance of the banks to the EU tendering process, the banks' signing of the MitID partnership is evidence

of an episodic circuit of power (arrow d). The Danish government has engineered the Danish banks to sign up to an agreement that they might not otherwise have signed.

4.1.2 Governance patterns in the Danish case

In this subsection, we identify governance patterns that emerge from the power relationships between the groups of actors in Denmark's MitID.

The agreement to establish MitID explicitly as a partnership with shared ownership of a national digital identity system, rather than some other form of public-private contract, is a distinctive governance pattern of the Danish case. The need to form this partnership is driven by the societal expectation of *fælles*, whereby the public and private sector are expected to create synergies in the national interest by cooperating with each other as a cohesive entity, to develop and maintain viable national infrastructures. As a result of our analysis, we see the creation of the MitID partnership itself as a significant IT governance pattern and we identify four further detailed governance patterns inscribed in the MitID partnership that enable it to be viable and remain cohesive.

First, the public and private entities that make up the partnership have an agreement to share resources, which acts as a governance pattern. The individual members are therefore bound to each other by shared resources and the dependencies that result from this. The government is dependent on the banks' resource of an installed base of customers who regularly use digital identity systems. The banks are dependent on using the government owned resource of the Central Person Register (CPR) number that their customer use to identify themselves when using digital identity systems. Power within different sides of the partnership is fostered through maintaining the ownership of unique resources upon which the other party is dependent. These resources are unique to different actors but sharing them is essential to the functioning of the common infrastructure. The interdependency that results from this governance pattern leads to cohesion as it facilitates shared interests and common purpose when managing and maintaining the MitID solution.

Second, respondents in the case revealed a pattern of cohesive decision making. The individuals in the partnership were familiar with each other as they represent a small community within a small country, and they have established a long history of cooperation. As a consequence of this cohesion, they have built trust, shared understandings and an ease of interaction, communication and coordination. Power is nurtured within the partnership as cohesion encourages shared meaning and membership with the group and enhances their ability to produce and achieve collective goals. This was revealed in our interview data as a governance pattern where decision making is facilitated by group cohesion directed towards achieving a common goal:

"I think there is a long history of actually working together and so that is one thing. I think the pragmatic approach and I think the thing about being a relatively small country" – Respondent 4

"Because we have had so long relations with each other, and seeing each other in decision processing around each other has been also a big important step that the trust was also there when it came to form a partnership" – Respondent 5

Third, the partners agreed upon a modular organization of their solution architecture (Digitaliseringsstyrelsen, 2017b) to accommodate their divergent needs. On the one hand, the banks required that the solution have architectural flexibility to enable responsiveness and the potential for innovation in order to be competitive. On the other hand, the government required architectural stability in order to ensure that the identity solution was demonstrably secure and robust to serve the Danish public. At its core, the solution architecture contains a central module, shared across the whole partnership, and which provides functionality for basic identification and authentication. In addition, the architecture allows for members to develop and connect their own distinctive modular components. The modular organization of architecture acts as governance pattern facilitating centralized decision making of common shared functionality and decentralized decision making of specialized functionality, and in doing so it sustains the viability of the partnership. Individual members' power is sustained as they are able to maintain control of decentralized decision making concerning their own specialised modular functions, whilst taking part in collective centralized decision making regarding common functionality shared across the MitID partnership. The essence of the solution architecture is indicated in the following comment:

"So that is like modular architecture, flexibility, less complexity and in this way so that it would be easier to upgrade, that's one thing" – Respondent 3

"The idea is that we work together on a core […] and it should be possible for the ones that are in the partnership, with the public sector, but also for the banks to use that core in a lot of different ways" – Respondent 5

Fourth, the MitID partnership collaboratively agreed a set of standards and specifications with respect to the design, operation and maintenance of the MitID solution (Digitaliseringsstyrelsen, 2017b). Here individual partners' power is fostered as they control standards and specifications concerning components that meet their unique individual needs, whilst sharing the control of standard and specification of shared outsourced components that meet their common needs. Agreement of these standards and specifications was necessary for the partnership to accommodate their common and divergent needs and encouraged the viability of the solution.

4.1.3 A mechanism for power inscription in the Danish case

The previous subsection identified governance patterns that were established for the MitID partnership to function. It also identified how power is inscribed into each of the governance patterns and the effect the governance patterns have on the partnership. When the combined effect of power on governance patterns is considered

it becomes possible to synthesise an overall mechanism of power inscription in the MitID case.

The overall approach to MitID governance consists of accommodating the need to establish the MitID partnership and accommodating the implications that forming this structure has on the MitID partners. The governance patterns within the partnership are concerned with maintaining cohesion amongst the members and with maintaining the viability of the common solution. In order that this can be done, power within the partnership is *cultivated*. When taken together, the mechanism through which power relationships are inscribed in IT governance patterns in the Danish case of MitID is one of *power cultivation*. The power relationships in this case are characterized by a dominance of systemic and social integration and a relative absence of episodic circuits of power. Power is fostered within each of the governance patterns which emerge in order to encourage cohesion within the partnership and viability of the solution. In Table 4, we illustrate the power cultivation mechanism through which the circuits of power amongst actors involved in the MitID partnership affect the distinctive governance patterns that emerge from our case analysis.

Table 4 Inscription of power circuits into IT governance patterns in the case of MitID

Actors involved in power relationship	Circuits of power	Inscription mechanism	Distinctive governance patterns
Citizens and government	Social	Inscription mechanism of power cultivation	Collaborative partnership The agreement to establish MitID as a collaborative partnership with shared ownership of infrastructure is a distinctive governance pattern. This pattern is driven by the societal expectation of "*fælles*" where the public and private sector are expected to cooperate in infrastructure projects for the national interest.
Government and banks	Social + systemic + episodic		Shared resources The agreement to share resources acts as a relational governance pattern. The public and private entities that make up the partnership are bound to each other by dependencies on each other's resources. Power within different sides of the partnership is fostered through maintaining the ownership of unique resources upon which the other party is dependent. This interdependency of resources leads to cohesion as it facilitates shared interests and common purpose when managing and maintaining the MitID solution.
			Cohesive decision making Long established familiarity between the members of the partnership has built trust and an ease of interaction, communication and coordination. Power is nurtured within the partnership as cohesion encourages shared meaning and membership and enhances their ability to produce and achieve collective goals. A relational governance pattern emerges where decision making is facilitated by group cohesion directed towards achieving a common goal.
			Architectural modularity The partners adopt an architectural governance pattern of design modularity. Architectural modularity sustains the viability of the partnership as it facilitates group decision making concerning common shared modules whilst allowing individuals to shape their own specialized modular functionality. In doing so individual members power is sustained as they retain control over their unique modules, while taking part in collective centralized decision making regarding common functionality.
			Standards and specifications The MitID partnership collaboratively agreed a set of standards and specifications with respect to the design, operation and maintenance of shared and individual components within the MitID solution. Here individual partners' power is fostered as they control standards and specifications concerning their individual modular components while sharing the control of standard and specification of common components. Agreement of these standards and specifications was necessary to accommodate members' needs and enabled the viability of the solution.

4.2 GOV.UK Verify

GOV.UK Verify is the first significant digital identity system in the UK. It replaced the controversial national identity system that was scrapped by the 2010 coalition government (Whitley et al., 2014) over concerns about costs and government surveillance of its citizens. As a consequence, the government vowed not to develop an identity system that relied on a centralized database of individuals or a single unique identifier (there was no equivalent to the Danish CPR number), a vow that has been recently re-confirmed (UK House of Commons, 2019). The government also decided that it would not act as an identity provider, instead relying on private companies to undertake this aspect of the service.

GOV.UK Verify is the digital identity service that can be used to access over 20 government services in the UK as well as other services throughout Europe via the eIDAS standard. Unlike many digital identity systems, it was created from the ground up as a new service and so needed to develop an IT governance framework from scratch alongside the development of the service.

4.2.1 Circuits of power in the UK case

The approach to governance of the GOV.UK Verify solution is affected by power relationships between three groups of actors: UK citizens, the government, and private sector companies that provide key elements of the digital identity system. The power relationships can be analysed as four circuits of power. Figure 2 provides an overview of the four key circuits of power between actors identified in the GOV.UK Verify case.

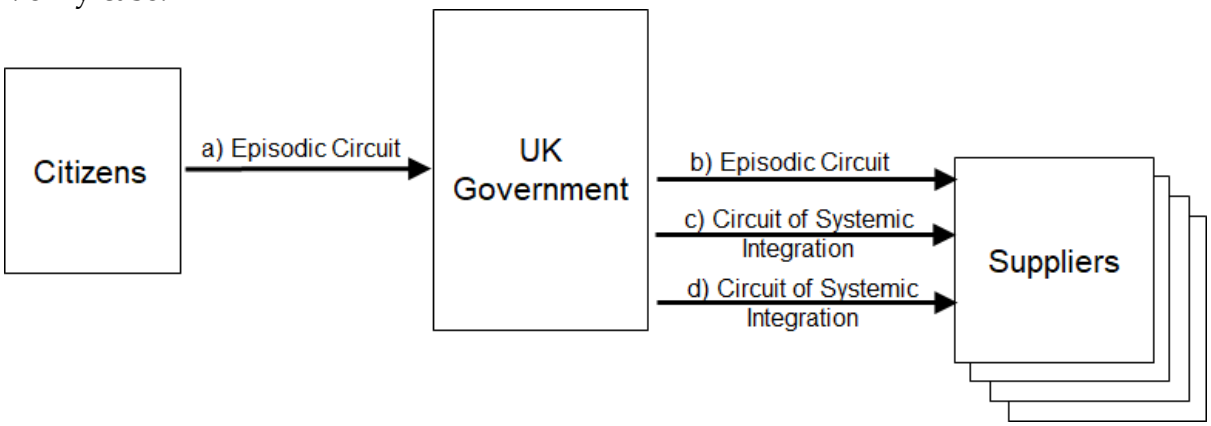

Figure 2 GOV.UK Verify circuits of power

a. Societal concerns about privacy as a driver for a new UK digital identity solution: as an episodic circuit

The approach to digital identification found in GOV.UK Verify was an explicit response to citizens' concerns about privacy and government surveillance that were associated with the UK's previous attempts to produce a digital identity system (Whitley et al., 2014). The Verify approach was implemented following the 2010 general election. During that election campaign, opposition to the previous national

identity scheme grew and a popular narrative emerged that saw the previous scheme as unnecessarily invasive. The opposition stated:

"Labour's approach to our personal privacy is the worst of all worlds – intrusive, ineffective and enormously expensive" (UK Conservative Party, 2010, p. 79).

The electorate therefore indicated its concerns with the previous approach to digital identity at the ballot box, voting for parties that were opposed to that approach. The episodic circuit of power (arrow a) between citizens and the UK government can be seen through the actions of citizens in the 2010 election. Through their choice of parties to vote for, the citizens asserted that a centralised digital identity system run by the government was politically unacceptable.

An alternative, user-centred approach had been foreshadowed by a report for the government that would help regain citizen trust and confidence in government around questions of identification (Crosby, 2008) and formed the basis for the new identity assurance approach that resulted from these power relationships. The government also put in place specific governance arrangements (detailed below) to help ensure that privacy concerns were properly addressed by the new scheme. Nevertheless, there was ongoing resistance to this user-centred approach in parts of government, with repeated consideration of introducing a national identity card.

As with the Danish case, the power relationships between citizens and the government help shape the overall approach to the governance of digital identity. In the Danish case, a circuit of social integration that emphasised "*fælles*" resulted in the creation of the MitID partnership. In contrast, the UK episodic circuit between citizens and the government highlighted privacy concerns and a desire to avoid a single database of all citizens.

b. Government requirements to avoid a single database of all citizens: Using identity proofing standards in an episodic circuit

A key feature of any identity systems is knowing the identity of the people covered by the system. In Denmark, this is achieved through the government issued CPR. In contrast, the UK does not have a single unique identifier for all citizens and has no plans to do so. Instead, the UK government exerted causal power as an episodic circuit (arrow b) over the companies it was working with, requiring them to use government-developed identity proofing standards (Cabinet Office & GDS, 2020a). These standards would help avoid a situation where a single private sector company could end up checking the identity of all UK residents and create a (private sector) centralised database of all residents.

This standard provides details of the kinds of identity evidence that would be accepted by the UK government for different levels of assurance. It also includes guidance on how to check that the evidence is genuine or valid (for instance that it has not been reported lost or stolen) and checking that the claimed identity exists over time.

c. Becoming (and remaining) a "certified company". Using standards as a circuit of systemic integration.

Facilitative power, expressed through circuits of systemic integration, comprises the means of controlling the environment of organizations. For GOV.UK Verify this can be seen in what is required to become (and remain) an authorised provider of identity services to GOV.UK Verify (arrow c). The scheme refers to such companies as certified companies and the companies must address a number of ways to assure that their services are safe for people to use (GOV.UK Verify, 2014f). For example, in addition to the identity proofing standards referred to above, certified companies also need to address the identity assurance privacy principles developed for GOV.UK Verify (GOV.UK Verify, 2014d).

The significance of this circuit of power can be seen if one of the private sector providers undertakes significant changes to its processes. As a result, their status as a certified company might be paused until the changes had been reassessed. This happened to one of the identity providers in 2016 (Bouchard, 2016). Moreover, in 2017, the same company ceased to be certified by the GOV.UK Verify framework and was no longer eligible to offer identity services for the UK Government (GOV.UK Verify, 2017).

d. Government requirements for competitive solutions: Procurement requirements as a circuit of systemic integration

Alongside concerns about single entities building centralised databases of citizens, GOV.UK Verify also sought to address efficiency concerns arising from a lack of competition in the supply of services to government. The UK government has a poor reputation when it comes to procuring IT systems (Craig & Brooks, 2006; Public Administration Select Committee, 2011) and this shaped the procurement model for identity services with an emphasis on a market of identity services provided by a range of companies. This was done to avoid an over-reliance on a small number of large system integrators. For example, in its report, the Public Administration Select Committee (2011) highlighted the need to "widen the supplier base" by promoting fair and open competition and engaging with innovative small and medium enterprises. Similarly, a report by the Institute for Government proposed a twin-track approach to involve delivering government-wide efficiencies of scale and interoperability, while facilitating rapid response and innovation at the front line through the use of platforms and agile methods (Institute for Government, 2011). The procurement process therefore explicitly included processes that sought to address power imbalances and potential vendor lock in and provides for a second, distinctive circuit of systemic integration in the UK case. Whereas the first circuit (arrow c) concerns how the government ensures that the companies it works with are deemed to be trustworthy by citizens, this circuit (arrow d) uses the procurement process as a means of monitoring and ensuring compliance with the goal of promoting fair and open competition amongst suppliers.

4.2.2 Governance patterns in the UK Case

In this sub-section we identify governance patterns that emerge from the power relationships between the groups of actors associated with GOV.UK Verify.

In a similar manner to the Danish case, the circuit between the UK electorate and the government (an episodic circuit in this case) provided a high-level framing for the governance of the UK identity scheme. Through their votes, the UK electorate indicated that they wanted a privacy friendly identity system that did not involve a single, centralised database of individuals. Unlike the Danish case, however, it did not result in a distinct IT governance pattern like the MitID partnership. Instead, it only resulted in three specific IT governance patterns between the government and its suppliers.

The first IT governance pattern identified in the UK case involves the requirement to use government standards for identity proofing. Whilst the use of standards is not an unusual IT governance approach, its application to the use of digital identity was novel at the time. The standardisation pattern in the UK contrasts with the modularity pattern found in the MitID case. The absence of a CPR equivalent meant that the UK solution had less opportunity for the kind of architectural flexibility that MitID supported. One benefit of requiring all suppliers to use these standards is that government departments that rely on these identity services simply need to specify the level of assurance they require (typically level 2) and can then accept identities from *any* approved supplier who can demonstrate that their processes meet the requirements specified in the standards. This standardisation framework helps ensure interoperability and limits the ability of particular suppliers to lock-in relationships with particular government departments (for example tax or social security) and create a centralised database of all citizens that way.

The identity proofing standards are also a part of a second IT governance pattern which encompasses the requirements an organization must address to become a certified company within the GOV.UK Verify scheme. These requirements include demonstrating compliance with the identity proofing standards and how their processes protect privacy.

In particular, to properly address the privacy and consumer concerns with the scheme the Government created the Privacy and Consumer Advisory Group (PCAG) (GOV.UK Verify, 2020) as part of the governance of GOV.UK Verify (and the Government Digital Service more generally). PCAG held its first meeting in 2011 and "is a forum that provides an independent view on issues involving privacy and wider consumer concerns" (GOV.UK Verify, 2020).

Alongside regular engagement with GOV.UK Verify, PCAG developed a set of "Identity Assurance principles" (GOV.UK Verify, 2014a). These principles are an important part of the governance patterns for Verify in terms of what it means to become a certified company. The principles were explicitly incorporated in the second round of formal procurement of identity services from private sector organizations. These companies were obliged to offer "a privacy policy (the "Provider Privacy

Policy") which is clear and easily comprehensible and which outlines (i) the steps the Provider, its Affiliates and Provider Personnel have taken to comply with the provisions in the Identity Assurance Principles which are applicable to such parties; and (ii) any measures they plan to implement in future" (GOV.UK Verify, 2016, sec. 7.2). Adherence to the PCAG identity assurance principles has also been reviewed as part of the data protection and privacy assessment of GOV.UK Verify (GOV.UK Verify, 2016) and constrains the ability of the certified companies from operating in ways that the public would not accept.

The effectiveness of the certified company governance pattern was demonstrated in the case of one company that was initially suspended from the scheme and later had to withdraw completely from the scheme because it no longer satisfied all the requirements to remain a certified company.

The final IT governance pattern identified concerns procurement requirements and relates to government concerns about vendor lock-in and an over-reliance on a small number of large systems integrators. Thus, during the procurement of services from potential certified companies, the process sought to restrict the number of organizations that "material sub-contractors" (who assess and analyse evidence and data to meet one or more of the five elements of the identity proofing and verification process described above) could work for. This IT governance pattern was explicitly designed to limit the possibility that GOV.UK Verify might end up with a situation whereby a competitive market of certified companies was locked in to relying on a small number of "material sub-contractors" to do all the work involved in verifying a person's identity (GOV.UK Verify, 2014e).

4.2.3 A mechanism for power inscription in the UK case

The previous subsection identified governance patterns from GOV.UK Verify and showed how power relationships are inscribed into each of the governance patterns and the effect the governance patterns have on the overall scheme. When the combined effect of power on governance patterns is considered, it becomes possible to synthesise an overall mechanism of power inscription in the GOV.UK Verify case.

In contrast to the Danish case, where power relationships inspired by the cultural norm of *fælles* resulted in IT governance arrangements that sought to cultivate the benefits of the power relationships found in the case study, the UK case was much more concerned about *limiting* the worst consequences of the power relationships between the government and the companies it was working with. These included limiting the possibility of creating a centralised identity database, constraining the ways in which certified companies might use identity data contrary to public expectations around privacy, and procuring services that did not result in market exploitation by specialist service providers. In this case, the (relative) absence of social circuits of power downplay the significance of power relationships that enable and support social relations and alliances. When taken together, the mechanism through which power relationships are inscribed in IT governance in this case is one of *power limitation*. In Table 5 we illustrate the power limitation mechanism through which the

circuits of power amongst actors involved in GOV.UK Verify affect the distinctive governance patterns that emerge from our case analysis.

Table 5 Inscription of power circuits into IT governance patterns in the case of GOV.UK Verify

Actors involved in power relationship	Circuits of power	Inscription mechanism	Distinctive governance patterns
Citizens and government	Episodic	Inscription mechanism of power limitation	No explicit IT governance patterns arise
Government and Suppliers	Episodic + systemic		<u>Identity proofing standards</u> In the absence of a central database of identities, the UK government developed and mandated a set of standards around the proofing of identity for use with GOV.UK Verify. These standards help prevent vendor lock-in and, by enforcing interoperability, help ensure that no supplier can create a centralised identity database.
			<u>Certified company requirements</u> The identity proofing standards exist as part of a broader set of requirements that suppliers wishing to become certified companies for GOV.UK Verify need to comply with. These requirements include explicitly incorporating PCAG identity assurance principles to help maintain public trust by constraining the ways in which the companies might use personal data.
			<u>Procurement requirements</u> The UK government has a poor record of achieving value for money when working with private sector organizations. The procurement process therefore put in place specific requirements around material sub-contractors who help with specific, specialist parts of the process, limiting their ability to abuse the nature of the overall scheme for financial gain.

5 Discussion

Our analysis shows the interplay between different circuits of power (Clegg, 1989), and the resulting governance of the digital identity systems. Gregory et al. (2018) identify three main dimensions of IT governance: *focus*, *scope* and *patterns*. These three dimensions allow us to reflect on the design of the study and the similarities and differences across the two cases that we investigated.

The two cases were chosen for study because they share a similar *focus*. They are both cases of digital identity systems for citizens and residents and are produced by governments working in conjunction with private sector companies.

The analysis has shown, however, that despite having a similar focus, the two cases differ in the *scope* of the IT governance and, specifically, in the *patterns* of IT governance that ensue. Differences, we argue, that are best understood in terms of the different configurations of circuits of power.

The influences arising from the circuits of power determine the *scope* of IT governance as well as power relationships between the partners within each case. Thus, for the Danish case, the initial circuit of social integration between citizens and the government resulted in the development of the MitID partnership which defined the scope of IT governance in this case. Given the social expectation of *fælles*, the consequent power relationships within this partnership between the private sector and government were relatively symmetrical. The Danish partnership favoured the relative prevalence of circuits of social and systemic integration.

In contrast, the relationship between citizens and government in the UK case was an episodic circuit that resulted in the *scope* of IT governance being more closely tied to the relationships between the government and individual suppliers. Given the UK public's expectation to minimise the potential for private partners to take advantage of their position, the consequent balance of power in the UK case was more asymmetric in favour of the public sector. This favoured the relative prevalence of episodic and systemic circuits of power.

The two cases highlight the effects of different circuits and *scopes* on the *patterns* of IT governance. In the Danish MitID case, circuits of social integration are prevalent between the different actors involved, namely citizens, the government, and the banks. The distinctive governance patterns on which the actors converge are a collaborative partnership, shared resources, cohesive decisions making, architectural modularity, and standards and specifications. In the GOV.UK Verify case, in contrast, episodic circuits of power and circuits of systemic integration are prevalent between the different actors involved, namely citizens, the government, and suppliers. The distinctive IT governance patterns on which the actors converge are identity proofing standards, certified company requirements, and procurement requirements.

While the specific actors involved and the distinctive governance patterns that emerged in this study are strongly related to the specific context of the two cases analysed, we draw implications from these empirical findings to theoretical

statements as "outputs of generalizing" (Lee & Baskerville, 2003, p. 235). We present these theoretical statements in the form of mechanisms, which are "sets of social events or processes that, under certain circumstances, bring about changes in human social relations without necessarily being reducible to the actions of individuals" (Markus & Rowe, 2018, p. 1261).

Having identified a *power cultivation mechanism* and a *power limitation mechanism* of inscription of power into IT governance, we thus put forward the following two propositions:

P1: If systemic and social integration circuits of power between actors engaged in the establishment of information systems are more prevalent than episodic circuits of power, then they are inscribed into patterns of governance through a cultivation mechanism.

P2: If episodic and systemic circuits of power between actors engaged in the establishment of information systems are more prevalent than circuits of social integration, then they are inscribed into patterns of governance through a limitation mechanism.

In these propositions, the prevalence of certain types of circuits of power compared to other circuits becomes a relevant aspect of the way power relationships are inscribed in governance patterns.

Our analysis of the way these power relationships are inscribed into patterns of IT governance has a number of key implications for research and for practice, which we discuss in the next subsection.

5.1 Implications

This study of the development and delivery of two national digital identity systems provides three types of contributions to research on power and IS in relation to IT governance: a core theoretical contribution, a methodological contribution, and a perspectival contribution.

The core theoretical contribution of our study is the articulation of two distinct mechanisms through which power relationships are inscribed into the governance of information systems: the inscription mechanism of *power cultivation* and the inscription mechanism of *power limitation*. These mechanisms provide a form of empirical to theoretical generalizability (Lee & Baskerville, 2003) by generalizing from description to theory. In doing so, we contribute to opening up the 'black box' of the ways in which power affects IT governance and provides new understandings of IS in work settings (Leclercq-Vandelannoitte & Bertin, 2018; Magnusson et al., 2020; Tallon et al., 2013; Williams & Karahanna, 2013), including for digital identity systems (Bazarhanova et al., 2020). These mechanisms allow other researchers to take advantage of our detailed analysis of cases they have not studied themselves (Barzelay, 2007). By helping unpack the power dynamics, we show how power relationships are not simply forced, or automatically transposed, into governance arrangements (Backhouse et al., 2006; Silva & Backhouse, 2003).

With the articulation of power cultivation and power limitation, we advance the understanding of the relationship between power and IT governance by

acknowledging a multiplicity of mechanisms whereby power is inscribed in IT governance. The *power cultivation* and *power limitation* mechanisms are concepts that can be used by IS researchers to more systematically explore the way power relationships are inscribed into IT governance arrangements in other cases.

Second, we provide a methodological contribution. We employ the notion of inscription to conceptualize how power relationships are included in IT governance patterns. While previous IS research using the notion of inscription argued that "any component of the heterogeneous network of skills, practices, artefacts, institutional arrangements, texts and contracts establishing a social order may be the material for inscriptions" (Monteiro & Hanseth, 1996, p. 330), in our study we operationalise power relationships between actors involved in IT governance as the material *substance* that gets inscribed; the negotiation and establishment of governance patterns that are compatible with such relationships as the material *operation* of inscription; and the observed characteristics of IT governance patterns as the *order* (Latour & Woolgar, 1986) that is created through inscription.

Using the notion of inscription to study power and IT governance has important consequences. The first is that it allows us to formulate generalizable claims, such as the ones linked to the inscription mechanisms proposed in this study. The second is that it allows us to capture situations of power relationships without making presumptions about the identification and definition of a focal actor. By focussing our analysis on inscription rather than obligatory passage points, we ensure that the outcomes of power (in our case, specific IT governance patterns) do not overly influence the analysis of the empirical data and risk hiding the influence of the full range of circuits of power in the case.

Third, we provide a perspectival contribution. Our study complements the dominant view in IS research of power as simply 'power over' with a view of power as 'power to' or 'power through', that is as a relational, productive force embedded in social relations (Avgerou & McGrath, 2007; Introna, 1997; Kärreman, 2010; Lawrence et al., 2012; Leclercq-Vandelannoitte & Bertin, 2018; Myers & Young, 1997). By moving away from the simplest form of power, we demonstrate how 'power to' can affect the outcome of information systems in an equally effective way as 'power over'. In particular, we document how different aspects of the various circuits of power in our cases are inscribed into patterns of IT governance.

5.2 Future research

Our contribution to research on power and IS and IT governance opens up a number of avenues where researchers can build upon or extend our research and address some of the limitations of our study. First, we encourage future research to test the propositions we put forward based on the two mechanisms of power inscription that we articulated. This could be done in other contexts.

While one of the downsides of engaging in context-sensitive research can be a reduction in the ability to make generalizable claims (Cheng et al., 2016), our use of the notion of inscription as a means of "bracketing off" (Latour & Woolgar, 1986) the

individual instances of power relations, to identify more abstract mechanisms as theoretical statements, leads us to believe that the identified mechanisms and the two propositions we put forward can serve as input for further research (Barzelay, 2007; Lee & Baskerville, 2003; Ruddin, 2006). Moreover, interesting contributions could emerge from the identification of additional mechanisms developed in different contexts of power influencing IT governance, such as the *focus* of IT governance (what to govern) and the *scope* of IT governance (who to govern). For example, in the case of digital identity systems, this might include cases with a different scope, such as those which explicitly choose not to use private sector organizations as part of the delivery process. There is also opportunity to examine our mechanisms beyond their application to IT governance.

Second, we call for studies that adopt a longer temporal perspective and adopt a longitudinal approach. Our study investigates IT governance patterns at a particular point in time. As live, large scale systems, the context of their use can change rapidly. For example, the UK Government has recently announced the next stages for digital identity in the UK (Department for Digital, Culture, Media and Sport, 2020) with consumer rights around digital identity strengthened to support wider use of digital identities in the UK economy. The governance patterns for this next phase will need to accommodate new circuits of power.

Finally, we call for future studies to consider using the notion of inscription to investigate the way power relationships affect IT governance in complex ecosystems, including finance and healthcare, where power relationships are likely to be particularly important. We would expect other case studies of IT governance to present very different material operation of inscription to those identified in our cases.

6 Conclusion

This paper shows, by drawing on two cases of national digital identity systems, how the establishment of IT governance is a deeply political process, where power plays a crucial role in shaping the specific governance arrangements in each case. We identify configurations of power circuits, where different combinations of social integration, episodic and systemic integration circuits of power affect patterns of IT governance, including collaborative partnership, shared resources, cohesive decisions making, architectural modularity, standards and specifications proofing standards, certified company requirements, and procurement requirements. We grasp the way power affects IT governance, by identifying two distinct mechanisms of power inscription into IT governance, namely power cultivation and power limitation, as a means through which circuits of power affect governance patterns between actors involved in the establishment of such systems.

Appendix A – Overview of data sources

Denmark

Online sources	Documents	Interviews
• Nets Denmark: https://www.medarbejdersignatur.dk/ • Danish Agency for Digitisation: http://www.digst.dk • NemID: https://digst.dk/it-loesninger/nemid/	• Next generation NemID (Digitaliseringsstyrelsen, 2015) • The Next Generation of National Electronic and Signing in Denmark (Digitaliseringsstyrelsen, 2016c) • Partnerskab om MitID (Digitaliseringsstyrelsen, 2016b) • Afsluttet udbud af partnerskabet (Digitaliseringsstyrelsen, 2016a) • MitID sent out to tender (Digitaliseringsstyrelsen, 2017a) • The future infrastructure for digital identities in Denmark (Digitaliseringsstyrelsen, 2017b) • Four suppliers are now competing for MitID (Digitaliseringsstyrelsen, 2018) • MitID (Digitaliseringsstyrelsen, 2020)	• 11/09/2015 – Respondent 1: Business Development manager at Nets AS • 12/11/2015 – Respondent 2: Head of Division at Digitaliseringsstyrelsen • 02/02/2017 - Respondent 1: Business Development manager at Nets AS • 10/05/2017 - Respondent 2: Head of Division at Digitaliseringsstyrelsen • 21/06/2017 – Respondent 3: IT Architect at Digitaliseringsstyrelsen • 22/06/2017 – Respondent 4: Director at Digitaliseringsstyrelsen • 22/09/2017 – Respondent 5: Head of Division at Finans Danmark

United Kingdom

Online sources	Documents	Interviews / Participant Observation
• UK Digital Strategy: https://www.gov.uk/government/publications/uk-digital-strategy • Introducing GOV.UK Verify: https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify • GOV.UK Verify blogs at https://identityassurance.blog.gov.uk/	• How to prove and verify someone's identity (Cabinet Office & GDS, 2020a) • Using authenticators to protect an online service (Cabinet Office & GDS, 2020b) • Challenges and opportunities in identity assurance (Crosby, 2008) • Guidance on Framework Agreements (Crown Commercial Service, 2016) • Requirements for secure delivery of online public services (GOV.UK, 2012) • Identity Assurance Principles, No. Version 3.1 (GOV.UK Verify, 2014a) • GOV.UK Verify: IPV Operations Manual (redacted) (GOV.UK Verify, 2014c) • GOV.UK Verify: checks identity providers must perform - Detailed guidance (GOV.UK Verify, 2014b) • System error: Fixing the flaws in government IT (Institute for Government, 2011) • Digital Transformation in Government (NAO, 2017) • JustGiving and GOV.UK Verify: Exploring JustGiving information as part of the GOV.UK Verify process (OIXUK, 2016) • How Digital Identities Which Meet Government Standards Could be Used as Part of UK Bank's Customer On-Boarding and KYC Requirements (OIXUK, 2017) • Government and IT- "A Recipe For Rip-Offs": Time For A New Approach (Public Administration Select Committee, 2011)	One author is a key member of the GOV.UK Privacy and Consumer Advisory Group which has involved regular participations in meetings and receiving monthly updates from key stakeholders (developers, users etc.) since 2011. Information from interactions with this group that can be made public, was then published in the GOV.UK Verify team's blogs, and informs this study.

Appendix B - Examples of open coding of events, actions and outcomes from phase 1

Coding categories	MitID	GOV.UK Verify
Events	The pending expiry of the NemID partnership contract (Digitaliseringsstyrelsen, 2015).	The outcome of the 2010 general election is a new UK government with a different policy for digital identity, explicitly scrapping the previous ID card scheme (Cabinet Office, 2010).
Decisions and actions	The Danish government responds to the pending expiry of the current NemID partnership contract by deciding to tender for a new MitID partnership (Digitaliseringsstyrelsen, 2016a). The new MitID partnership (Danish government and Danish banks) respond to the requirements of EU procurement law by deciding to tender for an MitID solution provider (Digitaliseringsstyrelsen, 2017a).	The UK government undertakes assessment of identity services needs in the private sector (GOV.UK Verify, 2015b). The UK government responds to failure of an identity provider to conform to government standards by suspending its participation in GOV.UK Verify (GOV.UK Verify, 2017).
Outcomes	Following the MitID partnership tender, the Danish government forms the MitID partnership with the Danish banks (Digitaliseringsstyrelsen, 2016b). Following the MitID solution tender, the MitID partnership selects Nets A/S as the solution provider for the future Danish digital identity system (Digitaliseringsstyrelsen, 2018).	Following the certification of a selection of companies as identity providers, the UK government is no longer dependent on the performance of any one supplier (GOV.UK Verify, 2014e). Development of on-boarding processes for government services that wish to use it (GOV.UK Verify, 2015a).

Appendix C - Examples of coding of power relationships from phase 2.

	Example of empirical data	**Power relationship**
Episodic circuit of power	The DK government is able to have the DK banks enter an EU approved procurement process as a necessary part of the digital identity partnership, when they might not have otherwise done so. *"They [the banks] can't accept the idea that tendering takes between one year to eighteen months [...] I think in the beginning, from the banks' side they did not think that we should do tendering together necessarily […] We had a lot of talks with the banks to convince them before we went into the tendering process" – Respondent 4*.	Government power over banks
	Most UK political parties, seeking citizen votes, listed scrapping identity cards in their election manifestos as a reflection of citizens concerns about right to privacy and risks of over-surveillance (Whitley & Hosein, 2010). *"Labour's approach to our personal privacy is the worst of all worlds – intrusive, ineffective and enormously expensive" (UK Conservative Party, 2010, p. 79).*	Citizens power over government
Social circuit of power	DK citizens influence government to conform to cultural norms (in Danish: "*fælles*") of public-private partnership. *"Part of our culture is to seek common solutions, and we have a strong tradition of cooperation in the public sector in comparison to other countries. There is a recognition that we are a very small country and we need cooperate to be better than the others" – Respondent 4*.	Norm conditions for citizens to exercise power on government concerning the use of public resources
	Group of invited experts and nominated representatives from privacy organizations created in the UK *"to ensure that the programme engages effectively with its stakeholders to incorporate issues related to privacy, trust and confidence during each of the design phases from requirements specification through to delivery with the aim of improving the eventual design and implementation of the ID Assurance Programme" (Private email to author 4. 6 July 2011).*	Dispositional power of experts legitimised by (personal) status or position (representatives of privacy organizations)

	Example of empirical data	Power relationship
	UK government creates new norms for framing levels of confidence in identity evidence. *"By reaching a level of confidence:* • *you'll know how well your organisation or service is protected against identity risks* • *your identity checking process can be understood and reused by other organisations and services"* *"Low confidence in someone's identity* *Compared to not doing any identity checks, having low confidence in someone's identity will lower the risk of you accepting either:* • *synthetic identities* • *impostors who do not have a relationship with the claimed identity"* *"Very high confidence in someone's identity* *Having very high confidence in someone's identity will protect you against the same things as high confidence. It will also lower the risk of you accepting impostors who are trying to look like the claimed identity, for example by wearing a mask or make up."* (Cabinet Office & GDS, 2020a)	Development of new rules of practice for identity proofing activities
Circuit of systemic integration	DK government's techniques of discipline over the MitID partnership using law. *"As a result, the Danish banks, represented by FR I of 16 September 2015" A/S (subsidiary of Finans Danmark), have entered into an agreement with the Digitaliseringsstyrelsen to jointly procure and make MitID available to the entire public and private sector in Denmark" (Digitaliseringsstyrelsen, 2016b)*	Techniques employed by government to ensure compliance of banks
	UK Government applies standards (Cabinet Office & GDS, 2020a) in accordance with an "operations manual" (GOV.UK Verify, 2014c) to define what it will accept as proof of identity for a particular level of assurance. *"Certified companies have to work to published government standards when they verify your identity"* (GOV.UK Verify, 2014c).	Techniques employed by government to ensure compliance of suppliers

Appendix D - Examples of open coding of patterns of governance from phase 3.

Example of empirical data	Governance pattern (open coding)
The cultural norm of "*fælles*" describing a tradition of public and private sector cooperation to benefit Danish society. *"I think there is a part of our culture to seek common solutions, we are a very small country and we need cooperate to be better than the others" - Respondent 4*	Collaborative Partnership – Public private partnership fulfils societal expectation of collaboration
The Danish banks reliance on the Danish government for the use of citizens' government-allocated Central Person Register (CPR) number. *"I would say that it has shaped it in a way that not only the public sector bases their entire government, e-government and government on the personal registration numbers. The financial sector does the same" – Respondent 2* The Danish governments reliance on the Danish banks for access to their installed base of customers. *"The banks have the popular applications and the public sector needs a lot of people enrolled in this system, so they can use it. So the public sector, I think they accept more requirement from the banks to be sure that they still have 4.8 million users that can use the public system" – Respondent 1*	Shared Resources – to encourage collaboration
UK Government applies standards that define what it will accept as proof of identity for a particular level of assurance. These standards must be met by certified companies to provide identity services to government (GOV.UK Verify, 2014b) *"This guidance will help you choose the authenticator that will give you the right level of protection for your service" (Cabinet Office & GDS, 2020b).*	Identity Proofing Standards – standards-based approach to managing verification and authentication requirements
UK government sought to restrict the number of identity providers that sub-contractors could work for (GOV.UK Verify, 2014e). *"For the next round of procurement, a single organization will only be allowed to be a 'material sub-contractor' for a maximum of three certified companies" (GOV.UK Verify, 2014e)*	Procurement requirements – used to demand multiple sourcing to avoid supplier lock-in

References

Allen, D. K., Brown, A., Karanasios, S., & Norman, A. (2013). How Should Technology-Mediated Organizational Change Be Explained? A Comparison of the Contributions of Critical Realism and Activity Theory. *MIS Quarterly*, *37*(3), 835–854.

Almeida, R., Pereira, R., & Mira da Silva, M. (2013). IT Governance Mechanisms: A Literature Review. In J. Falcão e Cunha, M. Snene, & H. Nóvoa (Eds.), *Exploring Services Science* (pp. 186–199). Springer Berlin Heidelberg.

Astley, W. G., & Sachdeva, P. S. (1984). Structural Sources of Intraorganizational Power: A Theoretical Synthesis. *The Academy of Management Review*, *9*(1), 104–113. https://doi.org/10.2307/258237

Avgerou, C., & McGrath, K. (2007). Power, Rationality, and the Art of Living Through Socio-Technical Change. *MIS Quarterly*, *31*(2), 295–315.

Azad, B., & Faraj, S. (2011). Social power and information technology implementation: A contentious framing lens. *Information Systems Journal*, *21*(1), 33–61. https://doi.org/10.1111/j.1365-2575.2010.00349.x

Backhouse, J., Hsu, C. W., & Silva, L. (2006). Circuits of Power in Creating De Jure Standards: Shaping an International Information Systems Security Standard. *MIS Quarterly*, *30*, 413–438.

Barzelay, M. (2007). Learning from second hand experience: Methodology for Extrapolation-Oriented Case Research. *Governance*, *20*(3), 521–543.

Bazarhanova, A., Yli-Huumo, J., & Smolander, K. (2020). From platform dominance to weakened ownership: How external regulation changed Finnish e-identification. *Electronic Markets*, *30*(3), 525–538. https://doi.org/10.1007/s12525-019-00331-4

Bekkers, V. (2009). Flexible information infrastructures in Dutch E-Government collaboration arrangements: Experiences and policy implications. *Government Information Quarterly*, *26*(1), 60–68. https://doi.org/10.1016/j.giq.2007.09.010

Beresford, A. D. (2003). Foucault's Theory Of Governance And The Deterrence Of Internet Fraud. *Administration & Society*, *35*(1), 82–103. https://doi.org/10.1177/0095399702250347

Bertot, J., Estevez, E., & Janowski, T. (2016). Universal and contextualized public services: Digital public service innovation framework. *Government Information Quarterly*, *33*(2), 211–222. https://doi.org/10.1016/j.giq.2016.05.004

Boland, R. J. (1991). *Information system use as a hermeneutic process* (H.-E. Nissen, H. K. Klein, & R. Hirschheim, Eds.; pp. 439–458). North-Holland.

Bouchard, L. (2016). *Verizon "temporarily removed" as GOV.UK Verify ID provider*. Government Computing Network. https://www.governmentcomputing.com/central-government/news/newsverizon-temporarily-removed-as-govuk-verify-id-provider-4955500

Brown, A. E., & Grant, G. G. (2005). Framing the Frameworks: A Review of IT Governance Research. *Communications of the Association for Information Systems*, *15*(1). https://doi.org/10.17705/1CAIS.01538

Cabinet Office. (2010). *The Coalition: Our programme for government*. The Coalition documentation

Cabinet Office, & GDS. (2020a). *How to prove and verify someone's identity*. GOV.UK. https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

Cabinet Office, & GDS. (2020b). *Using authenticators to protect an online service*. GOV.UK. https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services

Callon, M. (1984). Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay. *The Sociological Review*, *32*(1_suppl), 196–233. https://doi.org/10.1111/j.1467-954X.1984.tb00113.x

Cheng, Z. (Aaron), Dimoka, A., & Pavlou, P. A. (2016). Context may be King, but generalizability is the Emperor! *Journal of Information Technology*, *31*(3), 257–264. https://doi.org/10.1057/s41265-016-0005-7

Chi, M., Zhao, J., George, J. F., Li, Y., & Zhai, S. (2017). The influence of inter-firm IT governance strategies on relational performance: The moderation effect of information technology ambidexterity. *International Journal of Information Management*, *37*(2), 43–53. https://doi.org/10.1016/j.ijinfomgt.2016.11.007

Clegg, S. R. (1989). *Frameworks of power*. SAGE Publications.

Clegg, S. R., Courpasson, D., & Phillips, N. (2006). *Power and Organizations*. Sage.

Constantinides, P., & Barrett, M. (2014). Information Infrastructure Development and Governance as Collective Action. *Information Systems Research*, *26*(1), 40–56.

Cordella, A., & Willcocks, L. (2010). Outsourcing, bureaucracy and public value: Reappraising the notion of the "contract state." *Government Information Quarterly*, *27*(1), 82–88. https://doi.org/10.1016/j.giq.2009.08.004

Craig, D., & Brooks, R. (2006). *Plundering the public sector: How New Labour are letting consultants run off with £70 billion of our money*. Constable.

Crosby, S. J. (2008). *Challenges and opportunities in identity assurance*. HM Treasury. http://webarchive.nationalarchives.gov.uk/20120906144256/http://www.hm-treasury.gov.uk/d/identity_assurance060308.pdf

Crown Commercial Service. (2016). *Guidance on Framework Agreements*. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/560268/Guidance_on_Frameworks_-_Oct_16.pdf

Dahl, R. A. (1957). The concept of power. *Behavioral Science*, *2*(3), 201–215. https://doi.org/10.1002/bs.3830020303

De Haes, S., & Van Grembergen, W. (2004). IT Governance and Its Mechanisms. *Information Systems Control Journal*, *1*, 7.

Deng, X., Joshi, K. D., & Galliers, R. D. (2016). The Duality of Empowerment and Marginalization in Microtask Crowdsourcing: Giving Voice to the Less Powerful Through Value Sensitive Design. *MIS Quarterly*, *40*(2), 279-A19.

Department for Digital, Culture, Media and Sport. (2020). *Next steps outlined for UK's use of digital identity*. GOV.UK. https://www.gov.uk/government/news/next-steps-outlined-for-uks-use-of-digital-identity

Dhillon, G. S., Caldeira, M., & Wenger, M. R. (2011). Intentionality and power interplay in IS implementation: The case of an asset management firm. *The Journal of Strategic Information Systems*, *20*(4), 438–448. https://doi.org/10.1016/j.jsis.2011.09.003

Digitaliseringsstyrelsen. (2015). *Next generation NemID*. https://en.digst.dk/digitisation/eid/next-generation-nemid/

Digitaliseringsstyrelsen. (2016a). *Afsluttet udbud af partnerskabet*. https://digst.dk/it-loesninger/nemid/naeste-generation/partnerskab/afsluttet-udbud-af-partnerskabet/

Digitaliseringsstyrelsen. (2016b). *Partnerskab om MitID*. https://digst.dk/it-loesninger/nemid/naeste-generation/partnerskab/

Digitaliseringsstyrelsen. (2016c). *The Next Generation of National Electronic and Signing in Denmark*. https://digst.dk/media/15232/introduction-national-electronic-identity-and-signing.pdf

Digitaliseringsstyrelsen. (2017a). *MitID sent out to tender*. https://en.digst.dk/news/news-archive/2017/december/mitid-sent-out-to-tender/

Digitaliseringsstyrelsen. (2017b). *The future infrastructure for digital identities in Denmark*. https://en.digst.dk/media/14836/english_fremtidens-infrastruktur-for-digitale-identiteter.pdf

Digitaliseringsstyrelsen. (2018). *Four suppliers are now competing for MitID*. https://en.digst.dk/digitisation/eid/mitid/

Digitaliseringsstyrelsen. (2020). *MitID*. https://digst.dk/it-loesninger/mitid/

Doolin, B. (2004). Power and resistance in the implementation of a medical management information system. *Information Systems Journal*, *14*(4), 343–362. https://doi.org/10.1111/j.1365-2575.2004.00176.x

Eaton, B., Elaluf-Calderwood, S., Sørensen, C., & Yoo, Y. (2015). Distributed Tuning of Boundary Resources: The Case of Apple's Ios Service System. *MIS Quarterly*, *39*(1), 217-A12.

Eaton, B., Hedman, J., & Medaglia, R. (2018). Three different ways to skin a cat: Financialization in the emergence of national e-ID solutions. *Journal of Information Technology*, *33*(1), 70–83. https://doi.org/10.1057/s41265-017-0036-8

Emerson, R. M. (1962). Power-Dependence Relations. *American Sociological Review*, *27*(1), 31–41. https://doi.org/10.2307/2089716

European Commission. (2016). *Trust Services and eID - eIDAS*. https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

Fleming, P., & Spicer, A. (2014). Power in Management and Organization Science. *The Academy of Management Annals*, *8*(1), 237–298. https://doi.org/10.1080/19416520.2014.875671

Foucault, M. (1977). *Discipline and punish: The birth of the prison*. Pantheon Books.

Foucault, M. (1980a). The Subject and Power. In C. Gordon (Ed.), *Power/Knowledge: Selected Interviews and Other Writings 1972-1977*. Pantheon Books.

Foucault, M. (1980b). Truth and Power. In C. Gordon (Ed.), *Power/Knowledge: Selected Interviews and Other Writings 1972-1977*. Pantheon Books.

Fragos, C., Karyda, M., & Kiountouzis, E. (2007). Using the Lens of Circuits of Power in Information Systems Security Management. In C. Lambrinoudakis, G. Pernul, & A. M. Tjoa (Eds.), *Trust, Privacy and Security in Digital Business* (pp. 228–236). Springer. https://doi.org/10.1007/978-3-540-74409-2_25

Gelb, A., & Diofasi Metz, A. (2018). *Identification Revolution: Can Digital ID Be Harnessed for Development?* Center for Global Development. https://www.cgdev.org/publication/identification-revolution-can-digital-id-be-harnessed-development

George, J. F., & King, J. L. (1991). Examining the computing and centralization debate. *Communications of the ACM*, *34*(7), 62–72. https://doi.org/10.1145/105783.105796

GOV.UK. (2012). *Requirements for secure delivery of online public services*. https://www.gov.uk/government/publications/requirements-for-secure-delivery-of-online-public-services

GOV.UK. (2020). *Introducing GOV.UK Verify*. GOV.UK. https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify

GOV.UK Verify. (2014a). *Identity Assurance Principles* (Version 3.1). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/361496/PCAG_IDA_Principles_3.1__4_.pdf

GOV.UK Verify. (2014b). *GOV.UK Verify: Checks identity providers must perform - Detailed guidance*. https://www.gov.uk/guidance/govuk-verify-checks-identity-providers-must-perform

GOV.UK Verify. (2014c). *GOV.UK Verify: IPV Operations Manual (redacted)* (2.3.1). https://www.gov.uk/government/publications/govuk-verify-ipv-operations-manual-redacted

GOV.UK Verify. (2014d). *How we're embedding the Identity Assurance Principles in GOV.UK Verify*. https://identityassurance.blog.gov.uk/2014/12/04/how-were-embedding-the-identity-assurance-principles-in-gov-uk-verify/

GOV.UK Verify. (2014e). *Making sure we have a range of certified companies*. https://identityassurance.blog.gov.uk/2014/12/10/making-sure-we-have-a-range-of-certified-companies/

GOV.UK Verify. (2014f). *What it means to be a "certified company."* GOV.UK Verify. https://identityassurance.blog.gov.uk/2014/12/11/what-it-means-to-be-a-certified-company/

GOV.UK Verify. (2015a). *Helping services integrate with GOV.UK Verify: Improvements to our onboarding process*. GOV.UK Verify. https://identityassurance.blog.gov.uk/2015/03/17/helping-services-integrate-with-gov-uk-verify-improvements-to-our-onboarding-process/

GOV.UK Verify. (2015b). *Exploring private sector identity assurance needs*. GOV.UK Verify. https://identityassurance.blog.gov.uk/2015/09/02/exploring-private-sector-identity-assurance-needs/

GOV.UK Verify. (2016). *GOV.UK Verify Data Protection Impact Assessment*. https://identityassurance.blog.gov.uk/wp-content/uploads/sites/36/2016/05/GOV-UK-Verify-DPIA-v1.0.pdf

GOV.UK Verify. (2017). *The latest improvements across GOV.UK Verify's certified companies*. GOV.UK Verify. https://identityassurance.blog.gov.uk/2017/01/06/the-latest-improvements-across-gov-uk-verifys-certified-companies/

GOV.UK Verify. (2020). *Privacy and Consumer Advisory Group*. https://www.gov.uk/government/groups/privacy-and-consumer-advisory-group

Gregory, R. W., Kaganer, E., Henfridsson, O., & Ruch, T. J. (2018). IT consumerization and the transformation of IT governance. *MIS Quarterly*, *42*(4), 1225–1253.

GSMA. (2016). *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*. http://www.gsma.com/mobilefordevelopment/programme/digital-identity/digital-identity-towards-shared-principles-public-private-sector-cooperation

Hislop, D., Bosua, R., & Helms, R. (2018). *Knowledge management in organizations: A critical introduction* (4th edition). Oxford University Press.

Hoff, J. V., & Hoff, F. V. (2010). The Danish eID case: Twenty years of delay. *Identity in the Information Society*, *3*(1), 155–174. https://doi.org/10.1007/s12394-010-0056-9

Huber, T. L., Kude, T., & Dibbern, J. (2017). Governance Practices in Platform Ecosystems: Navigating Tensions Between Cocreated Value and Governance Costs. *Information Systems Research*, *28*(3), 563–584. https://doi.org/10.1287/isre.2017.0701

Institute for Government. (2011). *System error: Fixing the flaws in government IT*. http://www.instituteforgovernment.org.uk/sites/default/files/publications/System%20Error.pdf

Introna, L. D. (1997). *Management, Information and Power*. Macmillan.

Jasperson, J. (Sean), Carte, T. A., Saunders, C. S., Butler, B. S., Croes, H. J. P., & Zheng, W. (2002). Review: Power and Information Technology Research: A Metatriangulation Review. *MIS Quarterly*, *26*(4), 397–459.

Joshi, A., Bollen, L., Hassink, H., De Haes, S., & Van Grembergen, W. (2018). Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role. *Information & Management*, *55*(3), 368–380. https://doi.org/10.1016/j.im.2017.09.003

Karhu, K., Gustafsson, R., & Lyytinen, K. (2018). Exploiting and Defending Open Digital Platforms with Boundary Resources: Android's Five Platform Forks.

Information Systems Research, *29*(2), 479–497. https://doi.org/10.1287/isre.2018.0786

Kärreman, D. (2010). The Power of Knowledge: Learning from 'Learning by Knowledge-Intensive Firm.' *Journal of Management Studies*, *47*(7), 1405–1416. https://doi.org/10.1111/j.1467-6486.2009.00898.x

Keen, P. G. (1981). Information systems and organizational change. *Communications of the ACM*, *24*(1), 24–33.

King, J. L. (1983). Centralized Versus Decentralized Computing: Organizational Considerations and Management Options. *ACM Computing Surveys*, *15*(4), 319–349. https://doi.org/10.1145/289.290

Klein, H. K., & Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly*, *23*(1), 67–93. https://doi.org/10.2307/249410

Klievink, B., Bharosa, N., & Tan, Y.-H. (2016). The collaborative realization of public values and business goals: Governance and infrastructure of public–private information platforms. *Government Information Quarterly*, *33*(1), 67–79. https://doi.org/10.1016/j.giq.2015.12.002

Klievink, B., & Janssen, M. (2014). Developing Multi-Layer Information Infrastructures: Advancing Social Innovation through Public–Private Governance. *Information Systems Management*, *31*(3), 240–249. https://doi.org/10.1080/10580530.2014.923268

Kling, R., & Iacono, S. (1984). The Control of Information Systems Developments After Implementation. *Communications of the ACM*, *27*(12), 1218–1226. https://doi.org/10.1145/2135.358307

Kumar, N., Stern, L. W., & Anderson, J. C. (1993). Conducting Interorganizational Research Using Key Informants. *Academy of Management Journal*, *36*(6), 1633–1651.

Lapke, M., & Dhillon, G. (2008). *Power Relationships in Information Systems Security Policy Formulation and Implementation*. European Conference on Information Systems, Galway, Ireland.

Latour, B. (1986). Powers of association. In J. Law (Ed.), *Power, action and belief: A new sociology of knowledge?* (pp. 264–280). Routledge & Kegan Paul.

Latour, B. (1987). *Science in Action: How to Follow Scientists and Engineers Through Society*. Harvard University Press.

Latour, B. (1999). *Pandora's hope: Essays on the reality of science studies*. Harvard University Press.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford University Press.

Latour, B., & Woolgar, S. (1986). *Laboratory life: The construction of scientific facts*. Princeton University Press.

Lawrence, T. B., Malhotra, N., & Morris, T. (2012). Episodic and Systemic Power in the Transformation of Professional Service Firms. *Journal of Management Studies*, *49*(1), 102–143. https://doi.org/10.1111/j.1467-6486.2011.01031.x

Leavitt, H. J., & Whisler, T. L. (1958). Management in the 1980's. *Harvard Business Review*, *36*(6), 41–48.

Leclercq-Vandelannoitte, A., & Bertin, E. (2018). From sovereign IT governance to liberal IT governmentality? A Foucauldian analogy. *European Journal of Information Systems*, *27*(3), 326–346. https://doi.org/10.1080/0960085X.2018.1473932

Lee, A. S., & Baskerville, R. L. (2003). Generalizing Generalizability in Information Systems Research. *Information Systems Research*, *14*(3), 221–243. https://doi.org/10.1287/isre.14.3.221.16560

Lessig, L. (1999). *Code and other laws of cyberspace*. Basic Books.

Levina, N., & Arriaga, M. (2014). Distinction and Status Production on User-Generated Content Platforms: Using Bourdieu's Theory of Cultural Production to Understand Social Dynamics in Online Fields. *Information Systems Research*, *25*(3), 468–488. https://doi.org/10.1287/isre.2014.0535

Lukes, S. (1974). *Power: A Radical View*. The Macmillan Press Ltd.

Magnusson, J., Koutsikouri, D., & Päivärinta, T. (2020). Efficiency creep and shadow innovation: Enacting ambidextrous IT Governance in the public sector. *European Journal of Information Systems*, *29*(4), 329–349. https://doi.org/10.1080/0960085X.2020.1740617

Malaurent, J., & Avison, D. (2016). Reconciling global and local needs: A canonical action research project to deal with workarounds. *Information Systems Journal*, *26*(3), 227–257. https://doi.org/10.1111/isj.12074

Marabelli, M., & Galliers, R. D. (2017). A reflection on information systems strategizing: The role of power and everyday practices. *Information Systems Journal*, *27*(3), 347–366. https://doi.org/10.1111/isj.12110

Markus, M. L. (1983). Power, Politics, and MIS Implementation. *Communications of the ACM*, *26*(6), 430–444. https://doi.org/10.1145/358141.358148

Markus, M. L., & Rowe, F. (2018). Is IT Changing the World? Conceptions of Causality for Information Systems Theorizing. *MIS Quarterly*, *42*(4), 1255–1280. https://doi.org/10.25300/MISQ/2018/12903

Medaglia, R., Hedman, J., & Eaton, B. (2017). Public-Private Collaboration in the Emergence of a National Electronic Identification Policy: The Case of NemID in Denmark. *Proceedings of the Hawaii International Conference on System Sciences (HICSS-50)*, 2782–2791.

Monteiro, E., & Hanseth, O. (1996). Social Shaping of Information Infrastructure: On Being Specific about the Technology. In W. J. Orlikowski, G. Walsham, M. R. Jones, & J. I. Degross (Eds.), *Information Technology and Changes in Organizational Work: Proceedings of the IFIP WG8.2 working conference on information technology and changes in organizational work, December 1995* (pp. 325–343). Springer US.

Myers, M. D., & Young, L. W. (1997). Hidden agendas, power and managerial assumptions in information systems development: An ethnographic study. *Information Technology & People*, *10*(3), 224–240. https://doi.org/10.1108/09593849710178225

NAO. (2017). *Digital Transformation in Government*. National Audit Office. https://www.nao.org.uk/report/digital-transformation-in-government/

Nyst, C., Pannifer, S., Whitley, E. A., & Makin, P. (2016). *Digital Identity: Issue analysis* (ReferenceType09; PRJ.1578). Consult Hyperion for Omidyar Network; OmidyarReport2016.pdf. http://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1_6-1.pdf

OIXUK. (2016). *JustGiving and GOV.UK Verify: Exploring JustGiving information as part of the GOV.UK Verify process*. http://oixuk.org/blog/2016/05/28/justgiving-and-gov-uk-verify/

OIXUK. (2017). *How Digital Identities Which Meet Government Standards Could be Used as Part of UK Bank's Customer On-Boarding and KYC Requirements*. OIXUK. http://oixuk.org/wp-content/uploads/2017/02/How-Digital-Identities-which-meet-Government-Standards-could-be-used-as-part-of-UK-Banks%E2%80%99-Customer-On-boarding-and-KYC-Requirements-FINAL.pdf

Ojo, A., & Mellouli, S. (2018). Deploying governance networks for societal challenges. *Government Information Quarterly*, *35*(4, Supplement), S106–S112. https://doi.org/10.1016/j.giq.2016.04.001

Olson, M. H., & Chervany, N. L. (1980). The Relationship between Organizational Characteristics and the Structure of the Information Services Function. *MIS Quarterly*, *4*(2), 57–68. JSTOR. https://doi.org/10.2307/249337

Orlikowski, W. J. (2000). Using Technology and Constituting Structures: A Practice Lens for Studying Technology in organizations. *Organizational Science*, *11*(4), 404–428. https://doi.org/10.1287/orsc.11.4.404.14600

Pedersen, C. B. (2011). The Danish Civil Registration System. *Scandinavian Journal of Public Health*, *39*(Supplement 7), 22–25. https://doi.org/10.1177/1403494810387965

Pettigrew, A. M. (1985). Contextualist research and the study of organizational change processes. In *Doing Research that is Useful for Theory and Practice*. Jossey Bass.

Pouloudi, N., Currie, W., & Whitley, E. A. (2016). Entangled Stakeholder Roles and Perceptions in Health Information Systems: A Longitudinal Study of the UK NHS N3 Network. *Journal of the Association for Information Systems (JAIS)*, *17*(2), 107–161. JAIS2016.pdf.

Pozzebon, M., & Pinsonneault, A. (2005). Global–local negotiations for implementing configurable packages: The power of initial organizational decisions. *The Journal of Strategic Information Systems*, *14*(2), 121–145. https://doi.org/10.1016/j.jsis.2005.04.004

Pozzebon, M., & Pinsonneault, A. (2012). The dynamics of client–consultant relationships: Exploring the interplay of power and knowledge. *Journal of Information Technology*, *27*(1), 35–56. https://doi.org/10.1057/jit.2011.32

Public Administration Select Committee. (2011). *Government and IT- "A Recipe For Rip-Offs": Time For A New Approach*.

http://www.publications.parliament.uk/pa/cm201012/cmselect/cmpubadm/715/715i.pdf

Ruddin, L. P. (2006). You Can Generalize Stupid! Social Scientists, Bent Flyvbjerg, and Case Study Methodology. *Qualitative Inquiry*, *12*(4), 797–812. https://doi.org/10.1177/1077800406288622

Sabherwal, R., & Grover, V. (2010). A taxonomy of political processes in systems development. *Information Systems Journal*, *20*(5), 419–447. https://doi.org/10.1111/j.1365-2575.2009.00341.x

Sambamurthy, V., & Zmud, R. W. (1999). Arrangements for Information Technology Governance: A Theory of Multiple Contingencies. *MIS Quarterly*, *23*(2), 261–290. https://doi.org/10.2307/249754

Sarker, S., Sarker, S., & Sidorova, A. (2006). Understanding Business Process Change Failure: An Actor-Network Perspective. *Journal of Management Information Systems*, *23*(1), 51–86. https://doi.org/10.2753/MIS0742-1222230102

Sarker, S., Xiao, X., Beaulieu, T., & Lee, A. S. (2018). Learning from First-generation Qualitative Approaches in the IS Discipline: An Evolutionary View and Some Implications for Authors and Evaluators (Part 1/2). *Journal of the Association for Information Systems*, *19*(8), 752–774. https://doi.org/10.17705/1jais.00508

Saunders, C. S. (1981). Management Information Systems, Communications, and Departmental Power: An Integrative Model. *Academy of Management Review*, *6*(3), 431–442. https://doi.org/10.5465/amr.1981.4285782

Schlosser, F., Beimborn, D., Weitzel, T., & Wagner, H.-T. (2015). Achieving social alignment between business and IT – an empirical evaluation of the efficacy of IT governance mechanisms. *Journal of Information Technology*, *30*(2), 119–135. https://doi.org/10.1057/jit.2015.2

Scupola, A., & Zanfei, A. (2016). Governance and innovation in public sector services: The case of the digital library. *Government Information Quarterly*, *33*(2), 237–249. https://doi.org/10.1016/j.giq.2016.04.005

Silva, L. (2007). Epistemological and theoretical challenges for studying power and politics in information systems. *Information Systems Journal*, *17*(2), 165–183. https://doi.org/10.1111/j.1365-2575.2007.00232.x

Silva, L., & Backhouse, J. (2003). The Circuits-of-Power Framework for Studying Power in Institutionalization of Information Systems. *Journal of the Association for Information Systems*, *4*(1).

Silva, L., & Fulk, H. K. (2012). From disruptions to struggles: Theorizing power in ERP implementation projects. *Information and Organization*, *22*(4), 227–251. https://doi.org/10.1016/j.infoandorg.2012.06.001

Simeonova, B. (2018). Transactive memory systems and Web 2.0 in knowledge sharing: A conceptual model based on activity theory and critical realism. *Information Systems Journal*, *28*(4), 592–611. https://doi.org/10.1111/isj.12147

Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). Circuits of Power: A Study of Mandated Compliance to an Information Systems Security De Jure Standard in a Government Organization. *MIS Quarterly*, *34*(3), 463–486.

Star, S. L. (1991). Power, Technologies and the Phenomenology of Standards: On Being Allergic to Onions. In J. Law (Ed.), *A sociology of monsters* (pp. 27–57). Basil Blackwell.

Tallon, P. P., Ramirez, R. V., & Short, J. E. (2013). The Information Artifact in IT Governance: Toward a Theory of Information Governance. *Journal of Management Information Systems*, *30*(3), 141–178. https://doi.org/10.2753/MIS0742-1222300306

Tilson, D., Lyytinen, K., & Sørensen, C. (2010). Digital Infrastructures: The Missing IS Research Agenda. *Information Systems Research*, *21*(4), 748–759.

Tiwana, A., & Kim, S. K. (2015). Discriminating IT Governance. *Information Systems Research*, *26*(4), 656–674. https://doi.org/10.1287/isre.2015.0591

Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Research Commentary—Platform Evolution: Coevolution of Platform Architecture, Governance, and Environmental Dynamics. *Information Systems Research*, *21*(4), 675–687. https://doi.org/10.1287/isre.1100.0323

Tiwana, A., Konsynski, B., & Venkatraman, N. (2013). Information Technology and Organizational Governance: The IT Governance Cube. *Journal of Management Information Systems*, *30*(3), 7–12. https://doi.org/10.2753/MIS0742-1222300301

UK Conservative Party. (2010). *Invitation to Join the Government of Britain: The Conservative Manifesto 2010*. https://conservativehome.blogs.com/files/conservative-manifesto-2010.pdf

UK House of Commons. (2019). *Digital Government: Government Response to the Committee's Eighteenth Report* (HC 2673). House of Commons Science and Technology Committee. https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/2673/2673.pdf

Walsham, G. (1995). Interpretive case studies in IS research: Nature and method. *European Journal of Information Systems*, *4*(2), 74–81.

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems*, *15*(3), 320–330. https://doi.org/10.1057/palgrave.ejis.3000589

Walsham, G., & Sahay, S. (1999). GIS for District-Level Administration in India: Problems and Opportunities. *MIS Quarterly*, *23*(1), 39–65. JSTOR. https://doi.org/10.2307/249409

Wareham, J., Fox, P. B., & Cano Giner, J. L. (2014). Technology Ecosystem Governance. *Organization Science*, *25*(4), 1195–1215. https://doi.org/10.1287/orsc.2014.0895

Webster, J. (1995). Networks of collaboration or conflict? Electronic data interchange and power in the supply chain. *The Journal of Strategic Information Systems*, *4*(1), 31–42. https://doi.org/10.1016/0963-8687(95)80013-G

Weill, P., & Ross, J. W. (2005). A Matrixed Approach to Designing IT Governance. *MIT Sloan Management Review*, *46*(2), 26–34.

Westrup, C. (1994). Practical understanding: Hermeneutics and teaching the management of information systems development using a case study. *Accounting, Management and Information Technologies*, *4*(1), 39–58.

Whitley, E. A., & Hosein, G. (2010). *Global challenges for identity policies* (ReferenceType00). Palgrave Macmillan.

Whitley, E. A., & Hosein, I. R. (2008). Doing the politics of technological decision making: Due process and the debate about identity cards in the UK. *European Journal of Information Systems*, *17*(6), 668–677. http://dx.doi.org/10.1057/ejis.2008.53

Whitley, E. A., Martin, A. K., & Hosein, G. (2014). From surveillance-by-design to privacy-by-design: Evolving identity policy in the United Kingdom. In K. Boersma, R. van Brakel, C. Fonio, & P. Wagenaar (Eds.), *Histories of Surveillance in Europe and Beyond* (pp. 205–219). Routledge.

Willcocks, L. P. (2006). Michel Foucault in the Social Study of ICTs: Critique and Reappraisal. *Social Science Computer Review*, *24*(3), 274–295. https://doi.org/10.1177/0894439306287973

Williams, C. K., & Karahanna, E. (2013). Causal Explanation in the Coordinating Process: A Critical Realist Case Study of Federated It Governance Structures. *MIS Quarterly*, *37*(3), 933–964.

Winkler, T. J., & Brown, C. V. (2013). Horizontal Allocation of Decision Rights for On-Premise Applications and Software-as-a-Service. *Journal of Management Information Systems*, *30*(3), 13–48. https://doi.org/10.2753/MIS0742-1222300302

Wu, P.-J., Straub, D. W., & Liang, T.-P. (2015). How Information Technology Governance Mechanisms and Strategic Alignment Influence Organizational Performance: Insights from a Matched Survey of Business and It Managers. *MIS Quarterly*, *39*(2), 497-A7.

Xiao, J., Xie, K., & Hu, Q. (2013). Inter-firm IT governance in power-imbalanced buyer–supplier dyads: Exploring how it works and why it lasts. *European Journal of Information Systems*, *22*(5), 512–528. https://doi.org/10.1057/ejis.2012.40

Xue, Y., Liang, H., & Boulton, W. (2008). Information Technology Governance in Information Technology Investment Decision Processes: The Impact of Investment Characteristics, External Environment, and Internal Context. *Management Information Systems Quarterly*, *32*(1).