

Chapter 7

Layers of Interoperability

In Chap. 3 we have shown that interoperability frameworks (IFs) similar to the ISO Reference Model for Open Systems Interconnection assign different standards for data exchange to three or four different layers of interoperability, which build upon each other. For our re-conceptualization we have proposed a four-layer framework (Table 3.5 and Fig. 3.7).

In this chapter we illustrate the standards on the layers of technical, syntactic, and semantic interoperability by examples from our case studies in Sect. 7.1 and further elaborate our redefinition of organizational interoperability in Sect. 7.2. On this basis we also take a look at the relationship between the four layers. The OSI Reference Model clearly assumes that standards on the different layers built upon each other, i.e., that standards on lower levels provide necessary services for functions on the next higher level, and that a standard at a higher level only function if standards from the lower layers are implemented. For the layers of interoperability this is assumed but not yet assessed empirically. In Sect. 7.3 we conduct such a test by applying a method of scalogram analysis from empirical social science research.

7.1 Technical, Syntactic and Semantic Interoperability

As shown in Chaps. 2 and 3 most IFs adopt a three-layer structure distinguishing technical, semantic and organizational interoperability. We have adopted the more differentiated four-layer model developed by the European Telecommunication Standards Institute (ETSI) which introduces the layer of syntactic interoperability above technical interoperability.

7.1.1 *Technical and Syntactic Interoperability*

Technical interoperability according to the EIF

... covers the technical issues of linking computer systems and services. It includes key aspects such as open interfaces, interconnection services, data integration and middleware, data presentation and exchange, accessibility and security services (European Communities 2004, p. 16).

This definition includes standards and protocols from all seven layers of the OSI reference model (see Table 2.1) and much more. This may be criticized or accepted from a technical point of view. The European Telecommunication Standards Institute (ETSI) works with a more narrow definition of technical interoperability and introduces the additional layer of syntactic interoperability for a simple reason: ETSI is a developer of standards for technical interoperability but only a user of standards for syntactic interoperability. This is an important point for the analysis of governance: Standards for technical and for syntactic interoperability are negotiated and issued by different institutions according to different rules and regimes. A framework that does not distinguish between these standards cannot provide much guidance.

According to ETSI technical interoperability

... is usually associated with hardware/software components, systems and platforms that enable machine-to-machine communication to take place. This kind of interoperability is often centered on (communication) protocols and the infrastructure needed for those protocols to operate (ETSI 2006, p. 5).

As explained in Chap. 2, ever since TCP/IP became available and widely accepted, technical interoperability no longer presented any relevant barrier to interoperation. For some years a basic set of protocols has evolved for the communication between back offices of separate government units, in particular, Internet protocols for secure data transmission, e.g. HTTPS (Hypertext Transfer Protocol Secure), for e-mail e.g. SMTP and SMIME (Simple Mail Transfer Protocol/Secure Multipurpose Internet Mail Extensions), and, for file transfer, FTP (File Transfer Protocol) and SSL (Secure Socket Layer).

Depending on security or performance requirements, government agencies have several options for internal and external data exchanges with regard to this layer of network/transmission service, for example, the (open and unsecured) Internet, or a virtual network (VPN = Virtual Private Networks), or even a physical extranet such as the secure European administration network s-TESTA. Some Member States have developed enhanced services for secure data transmission including digital signatures. Germany has developed OSCI-Transport (Online Services Computer Interface).

The *Road Traffic Accident Automation Project* in the UK (see case no. 8) is a good case for illustrating interoperability efforts related to the technical layer. In this e-service, the electronic transfer of data between the Compensation Recovery Unit of the Department of Work and Pensions and the Department of Health for the

compensation of victims of road accidents has been automated by employing the above-mentioned Internet protocols for secure data transmission. Another example is the *Customs Declaration System CELINA in Poland* that enables traders to submit their customs declarations in electronic form via the Internet (see case no. 9). The system includes a central repository of documents, the local application layer of the local customs offices, a jointly used payment system and the infrastructure for the use of digital signatures. Again, these functions build on Internet protocols such as HTTP with SSL and SMTP. Every trader or intermediary can send declarations from any device using a dedicated website or an email with attachment.

Very often the power of the protocols on the technical layer is overestimated. Technical interoperability only guarantees the correct transmission of bits but does not tell anything about the meaning of these bits and what they represent, not even whether it is voice, video, or data. This is the task of standards on the syntactic layer, which define the syntax of particular services.

According to ETSI *syntactic interoperability*

... is usually associated with data formats. Certainly, the messages transferred by communication protocols need to have a well-defined syntax and encoding, even if it is only in the form of bit tables. However, many protocols carry data or content, and this can be represented using high-level transfer syntaxes such as HTML, XML or ASN.12. Generally, ETSI is a user rather than a definer of generic syntaxes with a few notable exceptions, such as the definition and use of Concrete Syntax Notation (CSN) in the GSM specifications. (ETSI 2006, p. 5)

While the syntax of SMTP only allows for a distinction between a header and a body of a message, standards like XML or EDIFACT provide more differentiated structuring of the content of a message by defining not only the beginning and end of each message in a batch but also the end and the type of each data field. However EDIFACT and XML only provide the syntax for constructing message types with different content such as orders, applications, invoices, etc., which belong to the semantic layer. From a technical point of view the more recent XML syntax is considered to be more powerful and flexible. From a governance point of view however, the change from a well-established standard to a new one within a network of autonomous users is even more difficult to manage than the first introduction of a common data exchange format. Therefore quite often a conversion service is employed instead of a complete migration of all participants.

In the *road traffic accident automation project* the transfer of the compensation forms is based on XML, while the invoices and other information is exchanged according to the EDIFACT syntax. Another example is the *change of address service in civil registration in Germany*. For the exchange of deregistration data between the local registration offices a national standard X-Meld has been developed using XML schemes.

Basically, each message exchanged in the service consists of two parts: the reference data (utilization data) and the content-related data (data content). Both parts are XML documents and the latter is in OSCI-XMeld format, which is the standard for the description of the content-related data within the civil registration.

Messages are transferred between the civil registration authorities using OSCI Transport, which is the standard for the secure exchange of messages between public authorities in general.

A similar case is *lomake.fi*, the *central Finnish portal for electronic forms in the public administration* (see case no. 10). While a private company maintains the portal, public authorities use it to provide their services to citizens and businesses. The form portal is also integrated in the Finnish public-sector service portal *suomi.fi*. Public authorities interested in providing their online services through the form portal can integrate it into their workflow by technically linking their systems via standard Internet protocols. The portal offers more than 800 forms of 20 different public sector organizations. Figure 7.1 illustrates a linked system providing technical and syntactic interoperability.

One concrete application is crime declaration to local police offices. Citizens enter a crime declaration via a web interface. Data captured in PHP are transformed into XML format. A police server checks every 10 min whether new declarations have come in, downloads them by FTP, and forwards them within the police VPN to the next police station responsible for dealing with the case.

Moreover, data integrity, logical checks, conversion to XML file, temporary storing, timestamps, confirmation of application reception, etc. are done by common tools of the *lomake.fi* service. *Lomake.fi* can be seen as a typical clearing center that enables technical and syntactic interoperability between public authorities and their customers on a central level independent of a specific service application or the meaning of the data exchanged.

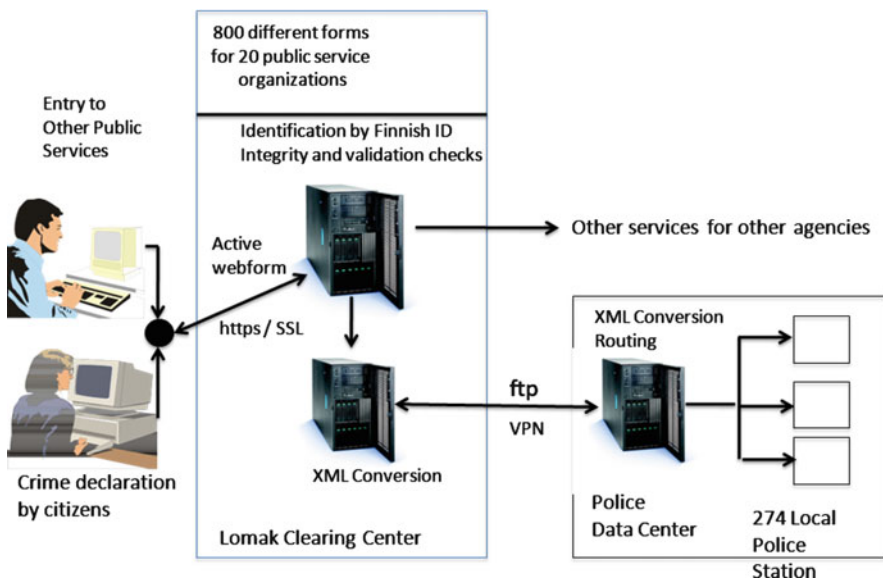


Fig. 7.1 Technical and syntactic interoperability in *lomake.fi* case (Source: own illustration, adapted from Millard et al. 2004, Vol. 3, p. 92)

7.1.2 *Semantic Interoperability*

Whereas syntactic interoperability provides for the exchange of clearly defined classes of data, semantic interoperability enables the automatic recognition of the individual data exchanged. In computer science, *syntax* refers to the grammar and formal rules for defining sets of data, while *semantics* define the meaning and the use of these data (Woods 1975). In other words, on the semantic layer data becomes information. Only if the semantics of data sets are defined and shared can these data be processed in one system, sent to another system, and there be automatically recognized and processed further.

According to the EIF, semantic interoperability

... is concerned with ensuring that the precise meaning of exchanged information is understandable by any other application that was not initially developed for this purpose. Semantic interoperability enables systems to combine received information with other information resources and to process it in a meaningful manner. (European Communities 2004, p. 16)

For example, electronic invoices sent from a supplier's computer system are automatically recognized, compared to the delivery notification by the customer, and further processed in the accounting system of the customer, by identifying the date of the invoice, its number, and the amount to pay. This requires a common definition for each data in every field of a data set. International bodies have developed common definitions for a few data related to the import and export of goods (e.g. dates, telephone number, country ID), in particular UNCTAD (United Nations Conference on Trade and Development). For example there is UPC (Universal Product Code), a classification scheme for goods, but there are also several competing product codes such as the European Article Number printed as a barcode on many brand articles, the ISBN for books, and hundreds of national branch-related product codes. In these cases, the data exchange format provides two data fields, one for the code of the code applied and another one for the attribute of the object according to the selected code.

While in e-business the problem lies in the diversity and heterogeneity of existing and often competing codes, for e-government there are only few national codes for services and the content of the respective application forms. A common data model of a service contains many more objects and attributes than an identifier and therefore is much harder to standardize across levels and domains of public administration. Computer science speaks of ontologies, which have to be developed in order to map the objects within dedicated domains (Staab and Studer 2004).

Some national interoperability frameworks (NIFs) include basic semantic standards such as a government data catalog in the British eGIF. Another approach is core directories for e-government (Welzel et al. 2011). A directory is a structured collection of data, which may serve as point of entry (Welzel et al. 2011) or as a point of reference for validation of certain data. A core directory, according to Welzel, Hartenstein and von Lucke holds information on core elements of e-government, e.g., citizens, companies, public services etc. This concept is most

widely implemented in Belgium, where public agencies according to the “unique data collection principle” are not allowed to request information from citizens or businesses, which already have been collected by other public agencies. Rather for core data there are central registries, which serve as single authentic and reliable source for all public sector agencies (see E-Government Fact Sheet Belgium at <http://www.epractice.eu/en/document/288179>).

A good example for the standardization of messages and for core directories is the crossroads bank and its *social security services in Belgium*. It serves as an information broker for the exchange of data between local public social welfare centers in all municipalities. In this service for inter-sectoral communication, hundreds of forms previously exchanged have been reduced to three message types: “submission”, “distribution”, and “answer”. Each message type is composed of two parts: the headers (in XML or flat format) contain all necessary information for correct routing: sender and addressee, type and kind of message, mandatory information to obtain authorization, answer management. The message in itself (in XML, EDIFACT or flat format) contains the personal data (related to a Social Security Identification Number contained in the headers). The communications between back-offices rely on XML-structured messages while the CBSS (Cross-Roads Bank for Social Security) ensures protocol and syntax conversion, if necessary, as well as a validation service of identity data via a link to the central register of residents. The input from the outside (web portal, FTP, interbanking network) is collected through the Extranet and directly converted into structured messages. The connection between the CBSS and the social security institutions is made through the Extranet to which all social security institutions have a direct connection.

In the *road traffic accident automation project (case no. 8)*, semantic interoperability has been achieved by the standardization of the data-fields of the compensation forms by the hospitals, the translation of these forms for transfer between the two departments dealing with compensation, and the integration of the converted data (forms) into their respective legacy applications.

In the *company e-registration service of Sweden (case no. 5)*, applicants can apply for registration at the Swedish Company Registration Office (Bolagsverket) and the Swedish Tax Agency (Skatteverket) using the same web-service. Both agencies have agreed that the same code is applied for data entered into the web-form and then forwarded to both agencies simultaneously. Another example is the *electronic invoicing case of Denmark*, where, as of 1 February 2005, all public institutions in Denmark were required only to accept invoices from suppliers in electronic format (see case no. 11). In this case, by definition an electronic invoice is a bill converted to a format directly readable by the public sector’s accounting systems. For this purpose, standardized workflows were introduced for all public entities on different government levels and companies. A specific XML workflow was designed, which is routed by a central electronic postal service. Routing of messages from the originator to the receiver requires an electronic postal address. Different identifiers can be used, i.e., the tax registration number or a Global Location Number within an Electronic Article Number (EAN), which allows for the unique and unambiguous identification of physical locations and legal entities.

Transport of the e-invoices is based on an ebMS (ebXML Message Service), and enveloping mechanisms are built on SOAP. This means that the addressing information, mainly the EAN number, is part of the ebMS header. Thus, the introduction of the EAN location numbers for companies and public authorities and its integration in the ebMS header of the invoice provides for semantic interoperability. These identifiers also allow for the routing of invoices to the correct recipient and their integration in the respective legacy systems. In addition, a semantic validation tool checks as many integrity rules as possible providing the XML schemas with high integrity. Generally, XML schemas can go a long way regarding validation, but the technology cannot capture all rules of integrity that the legislation may contain. Thus XML schemas cannot replace the checking of integrity rules that a programmer can code. However, other schema languages like Schematron can go even further than XML schemas (for further information see: ISO/IEC FDIS 19757-3 – <http://www.schematron.com/iso/dsdl-3-fdis.pdf>), which has been deployed in the e-invoicing project.

While standards for technical and syntactic interoperability provide for content independent data exchange, semantic interoperability is highly application-specific and thus depending on the service-specific content. As shown, to achieve semantic interoperability, agencies involved in a specific e-service commonly need to agree on the use of the same data exchange formats and codes for a particular service. This can be challenging when existing legacy systems in the cooperating back offices are using different data keys but need to be aligned to a common scheme. Such a change will only be undertaken when there is a trade-off between the cost of adapting the existing system and advantages to be gained from the shift to the common standards, or if the adoption of new standards is made mandatory by higher ranking agencies or legislation. Hence, achieving semantic interoperability is much more demanding than achieving technical and syntactic interoperability. However, 29 of 31 cases of specific services surveyed have achieved semantic interoperability.

7.2 Organizational Interoperability Re-defined

In Sect. 3.6 we proposed to separate what so far was called “organizational interoperability” into three dimensions. We argued that only technical standards for the linkage of business processes should be considered as additional layer above technical, syntactic and semantic interoperability, and we proposed to rename this layer “business process interoperability,” or *BPI*. Other aspects like change management, interoperability agreements etc. we maintained could be viewed as crosscutting aspects of how to achieve and maintain the different kinds of interoperability. These can be grouped into two different areas of governance, that is, *IT governance* and *implementation of interoperability* (Fig. 3.7).

Business process interoperability purely focuses on the technical side of automated processing of sub-functions to one single (inter-organizational)

automated workflow. This may be achieved through common service architecture and securing interoperability on the three lower layers.

A prominent example of how BPI can be achieved within a service is the use of a Service-Oriented-Architecture (SOA), which allows for the common description of inter-organizational processes, when business process definition languages are standardized, e.g., web services defined in WSDL (Web Services Definition Language) or BPML (Business Process Modeling Language). In the *road traffic accident automation project* the filing of the compensation forms by the hospitals was centrally secured as a web-service. The inter-organizational workflows with automated data integration between the two national departments were jointly agreed upon, modeled in SOA, and finally rolled out. Routing the forms to the receiving insurance companies was also done based on SOA. Another example is the *certificate of residence service in Austria* (see case no. 12). Quite a few institutions like social security administrations, schools, universities, or insurance companies require this type of certificate as proof of residence. The service can be fully provided electronically and automated as illustrated by the workflow diagram in Fig. 7.2.

In order to apply for a certificate of residence, a citizen has to pass an identification and authentication procedure before filling in and signing an online application form. For this purpose the citizen has to allow the server application to extract the identity link from the e-signature card or from the server of a specific mobile phone provider (in case the citizen has an active contract with the provider). The browser then displays the form, which the citizen had used before, updated with additional personal information from the server. The citizen does not have to enter any personal information. The server module uses the identifier from the e-signature card to search the central register of residence (CRR) for the citizen's personal information. In the next step the citizen signs the form using a personal e-signature card again (including the entering of a PIN) and submits it. By generating a hash value of the message and encrypting it with the sender's private key the Austrian PKI specifies that the application form was signed. Alternatively to the e-signature card, authentication and digital signing can be provided by mobile phone. The procedure makes use of the fact that the mobile phone provider already identified the user when subscribing him to the network. Therefore a digital signature can be safely linked to a person's identity. The workflow with the mobile phone function contains SMS service and requires the entering of PIN and TAN transmitted by the payment provider. After identification, authentication, digital signing, and form submitting, the certificate of residence service is immediately and automatically processed. Accessing the CRR and generating the certificate can be completed in a matter of seconds. Also, the payment procedure is fully integrated via a private payment provider. This provider asks the citizen for authorization of payment, which is given by sending a SMS containing a PIN. The payment application then sends a payment confirmation to the administration's application, which automatically hands the certificate over to the delivery services of the citizen. Payment confirmations are standardized XML messages conforming to the Electronic Payment Standard (EPS2). Finally, the citizen receives a notification from

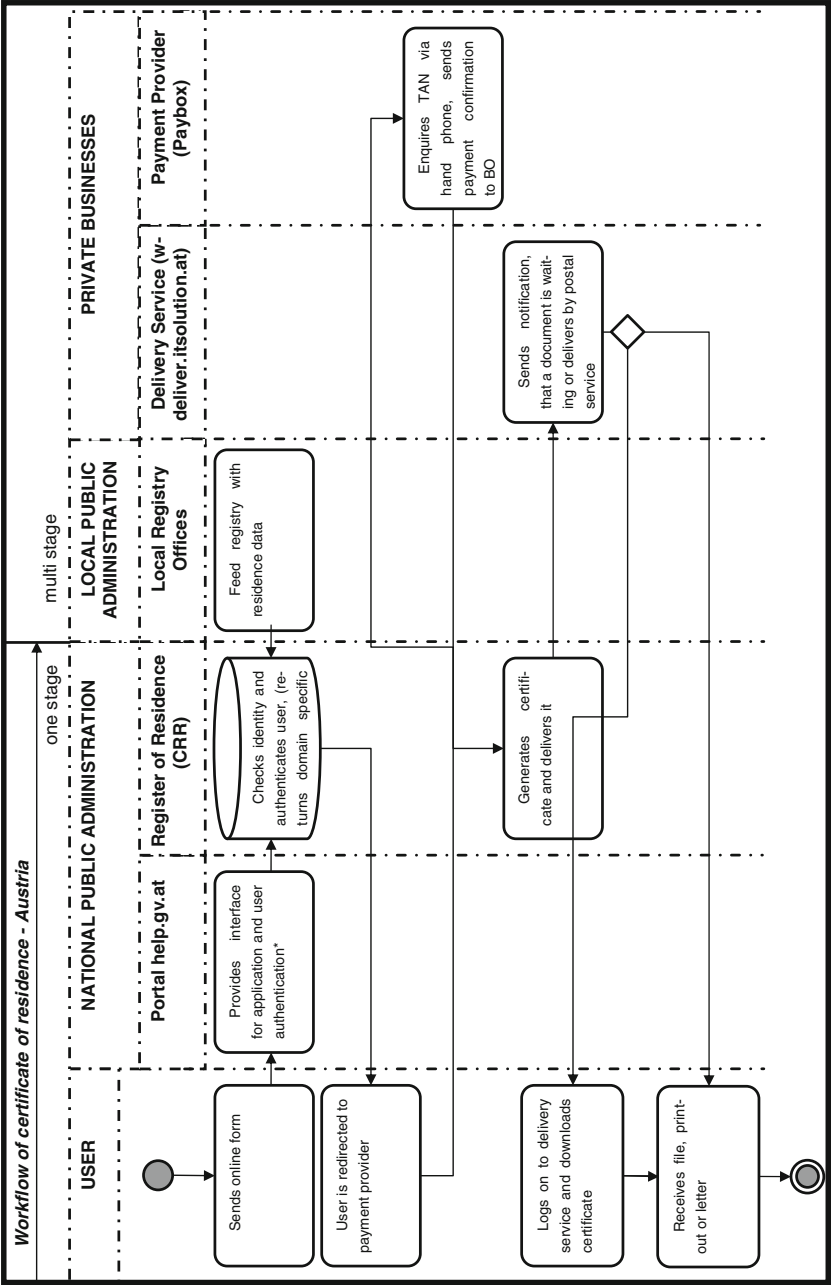


Fig. 7.2 Workflow of certificate of residence in Austria

the delivery service that a certificate is ready for downloading. The citizen has to pass through another authentication procedure either by e-signature card or via mobile phone. The downloadable document is an encrypted XML file, which can be downloaded to the citizen’s system, saved in a secure data box or printed on paper in legible form. If required by the agency, a delivery confirmation is automatically returned for receiving the certificate.

Like semantic interoperability BPI is application or service-specific. It requires cooperation among the agencies involved in the particular service, or, if agencies are part of a specific domain within the public sector, the same challenges for governance. The above example of linking different workflows related to the certificate of residence service in Austria perfectly illustrates the application-specific dependencies to achieve semantic interoperability and, on top of that, BPI (Fig. 4.2).

Obviously the integration of jointly used workflows is and remains complex, in general. Service oriented architectures including web services provide the basis for achieving BPI. Modeling languages like WSDL or BPML can facilitate standardized rules and framework conditions for the creation and linkage of back-office workflows enabling automated service delivery. Moreover, further processes can be integrated more easily to extend service provision. Establishing BPI is the most mature achievement in automated online service provision. In our survey, 20 of 31 specific-service cases had advanced towards full BPI.

7.3 Cumulative Structure of Interoperability Layers

As mentioned in Chap. 3, IFs assume a kind of maturity hierarchy with regard to the four technology-related layers of interoperability. A higher layer allows for a higher degree of automation of a multi-unit workflow and the corresponding service. Following the construction principle of the OSI reference model (Fig. 2.1 and Table 2.1) one would assume that a higher level of interoperability can only be achieved if the subordinate layers are enacted. In other words, semantic interoperability can only be achieved when standards for syntactic and technical interoperability have successfully been implemented.

Table 7.1 shows the number of good-practice cases in our sample, which achieved respective levels of interoperability:

The figures support the assumption of a hierarchical or cumulative structure as the number of achievements of semantic interoperability is smaller than the number of cases achieving syntactic interoperability, and the number of cases reaching business process interoperability is even smaller. However, this is not a definitive proof because some cases may show BPI without providing semantic interoperability.

Table 7.1 Distribution of interoperability layers achieved among 77 cases

Layer of interoperability	Technical	Syntactic	Semantic	Business process
No. of cases	77	77	60	44

For testing the relationship between the four layers of interoperability, we borrow a method from scale construction in empirical social science. A cumulative structure exists if a number of items in a questionnaire is uni-dimensional and can be combined into an index in a way so that every respondent who agrees to a certain item also agrees to a number of other items. Scales of such a cumulative structure are called Guttman scales after Louis Guttman who developed the test method in the 1940s represented in so-called scalograms (Guttman 1950). In a ‘perfect’ Guttman scale all surveyed cases are characterized by the same cumulative structure of the items of a questionnaire. Therefore this structure can be reproduced in every case of a sample and hopefully beyond that sample.

For a less perfect scale the pattern of responses can only be reproduced for a certain percentage of cases. The measure for the degree of perfection is expressed by the reproducibility coefficient with a range between 0 and 1. It is calculated by the formula: Reproducibility coefficient = $1 - (\text{number of errors} / \text{number of cases} \times \text{number of items})$ (cf. Kenny and Rubin 1977, or Grimm and Yarnold 1995).

We apply this method to test for the existence of standards on different layers of interoperability in our good-practice cases. According to our hypothesis, whenever an interoperability standard is detected in a project on a higher layer of interoperability, also the interoperability standards on all lower layers will be found. We coded our cases accordingly (yes = 1, no = 0) and ordered the cases according to the number of standardized interoperability layers detected in decreasing order. We also calculated the reproducibility coefficient. The table in Annex 3 shows the complete listing of all 74 cases with the decreasing number of standardized interoperability layers involved in each case, starting with cases where standards from all four layers were found followed by cases with standards on the three lower layers etc. Table 7.2 shows the summary:

Table 7.2 Cumulative structure of layers of interoperability

Number of cases	Technical	Syntactic	Semantic	Business process
40	1	1	1	1
20	1	1	1	0
13	1	1	0	0

The table shows the verification of a cumulative structure for 73 out of 77 cases. The pattern of score with the Figure ‘1’ comes very close to a triangle. For this distribution a reproducibility coefficient of 0.97403 has been calculated.

There are only four cases, which do not fit to the overall pattern: the *Mobile Government Infrastructure of Malta* (see case no. 13), *Electronic Service Delivery Toolkit* (UK) (see case no. 14), *ELAK im Bund* (AT) (see case no. 17), and *Hamburg Gateway* (DE) (see case no. 16). These four systems have achieved business process interoperability without providing semantic interoperability (Table 7.3).

These four cases are not about providing a specific public service to citizens or business but deal with providing an infrastructure for an undefined number of services, which is something quite different. Infrastructures only provide some generic preconditions, which always have to be completed by service-specific

Table 7.3 Cases not fitting to the cumulative structure

ID	Name of case	Technical	Syntactic	Semantic	Bus procs	Faults
31	Mobile government infrastructure	1	1		1	2
67	ESD – electronic service delivery toolkit	1	1		1	2
89	ELAK im BUND	1	1		1	2
100	Hamburg Gateway – The digital gate to the city	1	1		1	2

elements, and most likely these have to do with the semantics of the respective service. If we ignore these four infrastructure-related cases, the four layers of interoperability as defined before form a perfect Guttman scale. Wherever a higher level of interoperability was achieved, we found all lower layers with standardized interoperability as well.



<http://www.springer.com/978-3-642-22501-7>

Organizational Interoperability in E-Government
Lessons from 77 European Good-Practice Cases

Kubicek, H.; Cimander, R.; Scholl, H.J.

2011, XIV, 185 p., Hardcover

ISBN: 978-3-642-22501-7