~~Date: 2023-12-19~~

~~Reference number of document:~~ **ISO/IEC FDIS 15944-~~-~~17**

~~Committee identification:~~ ISO/IEC JTC ~~001~~ 1/SC 32~~/WG 01~~

Secretariat: ~~JTC1/SC32~~ ANSI

Date: 2024-01-10

Information technology — Business ~~Operational View —~~ operational view —

Part 17: Fundamental principles and rules governing Privacy ~~-~~ by ~~-~~ Design (~~PhD~~PbD) requirements in an EDI and collaboration space context

~~*Technologies de l'information — Vue opérationnelle d'affaires — Partie 17: JTC1/SC32*~~

~~Edited DIS - MUST BE USED FOR FINAL DRAFT~~

Style Definition ...

Formatted: zzCover large, Space Before: 0 pt, After: 0 pt

Formatted ...

Formatted: Font: 11 pt, French (Switzerland)

Formatted ...

Formatted: Font: 11 pt, French (Switzerland)

Formatted: Font: 11 pt

Formatted: Space After: 0 pt

Formatted: Font: 16 pt

Formatted: Regular, Font: 16 pt, Bold

Formatted: Cover Title_A2, Space After: 0 pt, Tab stops: Not at 10.39 cm

Formatted: Font: 16 pt, Bold

Formatted ...

FDIS stage

Edited DIS - MUST BE USED FOR FINAL DRAFT

ISO ~~Copyright Office~~ copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: + 41 22 749 01 11

~~Email: copyright@iso.org~~
E-mail: copyright@iso.org
Website: ~~www.iso.org~~www.iso.org

Published in Switzerland.

Formatted: Font color: Auto, English (United Kingdom)

Formatted: Font color: Auto, English (United Kingdom)

Formatted: Font color: Auto, English (United Kingdom)

Formatted: Font color: Auto, English (United Kingdom)

Formatted: zzCopyright address

Formatted: Font color: Auto, English (United Kingdom)

Formatted: Font color: Auto, English (United Kingdom)

Formatted: zzCopyright address

Formatted: Font color: Auto, French (Switzerland)

Formatted: French (Switzerland)

Formatted: Font color: Auto

Formatted: zzCopyright address

Formatted: Font color: Auto

Formatted: Font color: Auto, English (United Kingdom)

Formatted: Font color: Auto, English (United Kingdom)

~~Edited DIS - MUST BE USED FOR FINAL DRAFT~~

Contents Page

Formatted: Font: Bold, Font color: Auto

Edited DIS - MUST BE USED FOR FINAL DRAFT

List of Figures

List of Tables

Edited DIS - MUST BE USED FOR FINAL DRAFT

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see ~~www.iso.org/directives~~www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC have not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at ~~www.iso.org/patents and https://patents.iec.ch~~www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see ~~www.iso.org/iso/foreword.html~~www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 32, *Data management and interchange*.

This document is intended to be used in conjunction with ISO/IEC 14662, ISO/IEC 15944-1, ISO/IEC 15944-4, ISO/IEC 15944-5, ISO/IEC 15944-8 and ISO/IEC 15944-12.

A list of all parts in the ISO/IEC 15944 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at ~~www.iso.org/members.html~~www.iso.org/members.html and www.iec.ch/national-committees.

Formatted: HeaderCentered
Formatted: Font: Bold
Formatted: Foreword Title, Space After: 0 pt
Formatted: Left: 1.9 cm, Right: 1.9 cm, Gutter: 0 cm, Section start: New page, Header distance from edge: 1.27 cm, Footer distance from edge: 0.5 cm
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Field Code Changed
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Field Code Changed
Formatted: English (United Kingdom)
Formatted: Foreword Text, Space After: 0 pt
Formatted: English (United Kingdom)
Field Code Changed
Formatted: FooterPageRomanNumber

Formatted: HeaderCentered

Formatted: Font: Bold

Formatted: FooterPageRomanNumber

Formatted: Font: Bold
Formatted: HeaderCentered

Introduction

0.1 Purpose and overview

The ISO/IEC 14662 and the ~~multipart~~ ISO/IEC 15944 Business Operational View (BOV) series of standards focus on electronic data interchange (EDI) and "collaboration space" among Persons. Modelling business transactions using scenarios and scenario components includes specifying the applicable constraints on the data using explicitly stated rules. The ISO/IEC 14662 Open-edi Reference Model identifies two basic classes of constraints, "internal constraints" and "external constraints".

Jurisdictional domains are the primary source of external constraints on business transactions. Privacy protection is addressed as a common set of external constraint requirements coming from jurisdictional domains. Jurisdictional domains, such as UN member states and/or their administrative sub-divisions (see further ~~5.2~~5.2 on sources of requirements), have enacted various "privacy" laws, "data protection" laws, "protection of personal information" laws, etc., (as well as pursuant regulations). Some of these sources of legal requirements focus on the protection of personal information in IT systems only, (e.g. ~~,~~ "data protection"), while others focus on the protection of personal information irrespective of the medium used for the recording of personal information and/or its communication to other Persons.

The overall purpose of the PbD ~~[2]~~[2] approach is two folds: (1) to ensure that privacy protection requirements (as stated in applicable legal and/or regulatory requirements) are identified as early as possible in the business operational process; (2) are specified in a systematic and rule-based manner for those developing any IT systems within their organization.

The PbD approach has always been supported and embedded in ISO/IEC 15944 development work. The need for the multipart ISO/IEC series of standards to comply with and support privacy protection requirements was already incorporated in the1st edition of ~~Part 1 titled "*Operational aspects of Open-edi for implementation.*"~~ISO/IEC 15944-1. The development of the multipart series of ISO/IEC 15944 eBusiness standards and relevant parts of the multipart ISO/IEC standard that focus on privacy protection requirements fully supports the seven (7) foundational principles of the PbD approach ~~[2].~~ [2] In particular, it provides the detailed rules, definitions and related guidelines necessary to ensure that privacy protection requirements are identified and implemented not only throughout the entire life cycle of the recorded information involved, i.e. ~~,~~ "cradle-to-grave" information life cycle management (ILCM) but especially for any personal information interchanged via EDI among parities to a particular business transaction.

This document highlights the requirements of ISO/IEC 14662 and ISO/IEC 15944 that focus on addressing commonly definable aspects of external constraints that relate to Privacy by Design in a privacy protection requirements (PPR) context when the source is a jurisdictional domain.[1] Use of this document (and related standards) addresses the transformation of these external constraints (business rules) into specified, registered, and re-useable scenarios and scenario components.

This document also extends the requirements of ISO/IEC 14662 and ISO/IEC 15944 where relevant and describes the added business semantic descriptive techniques needed to support PbD aspects beyond privacy protection requirements (PPR) when modelling business transactions. PbD aspects are central to ensuring that PPR are embedded early on in the design, passed on and supported throughout the lifecycle of the personal information, among all the parties to a business transaction using EDI.

0.2 Use of ISO/IEC 14662 and ISO/IEC 15944

0.2.1 ISO/IEC 14662 "Open-edi Reference Model"[2]

[1] See further ~~Clause~~ sublause 0.2 below which identifies and summarizes the relevance of ISO/IEC 14662 and specific parts of the multipart ISO/IEC 15944 standard to this document.

[2] The ISO/IEC 14462 *Open-edi Reference Model* serves as the basis of the 2000 Memorandum of Understanding (MOU) among ISO, IEC, ITU and the UN/ECE concerning [harmonization of standardization in the field of electronic

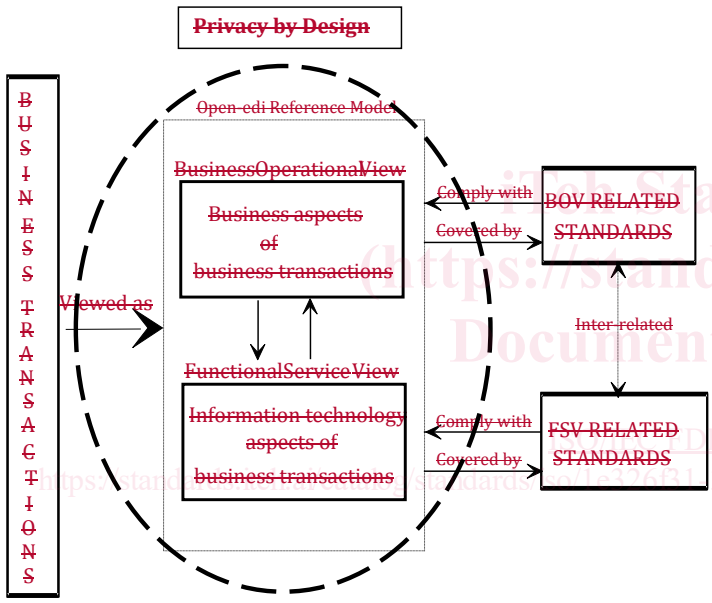
Formatted: Font: 11 pt
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)

Formatted: FooterPageRomanNumber

ISO/IEC 14662 states the conceptual architecture necessary for carrying out electronic business transactions among autonomous parties. That architecture identifies and describes the need to have two separate and related views of the business transaction. ISO/IEC 15944 is a multipart eBusiness standard which is based on and focuses on the BOV perspective of the ISO/IEC 14662 Open-edi reference model.

The delivery of Privacy by Design and privacy protection requires action both at the business operational level (BOV) and functional services view (FSV) (or technology levels). Where human beings interact with recorded information once it has passed through an Open-edi transaction, they have the potential to compromise technical controls (FSV) that -have been applied. It is essential that business models take into account the need to establish overarching business processes that address issues that have not been, and/or cannot be resolved by the technical FSV controls. This is to provide the overall privacy protection demands of regulation that are required to be applied to personal data, their use, prescribed dissemination and so on. In this regard, the interplay of the BOV and FSV views of all organizations is important.

The first is the Business Operational View (BOV). The second is the Functional Service View (FSV). Figure 1 from ISO/IEC 14662-:2010, Figure 1 illustrates the realm to which PbD aligns with the Open-edi environment.



business. {See http://www.itu.int//ITU-T/e-business/files/mou.pdf }See https://www.itu.int//ITU-T/e-business/files/mou.pdf

Formatted: HeaderCentered
Formatted: Font: Bold
Formatted: Font: 11 pt
Formatted: FooterPageRomanNumber

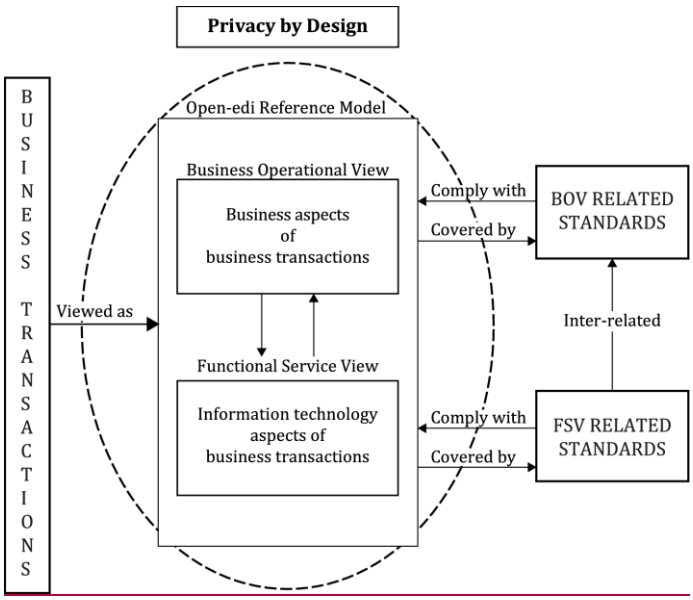


Figure ~~1~~ 1 — Privacy by Design and Open-edi reference model environment

0.2.2 ISO/IEC 15944-1 Business operational view (BOV) ~~operational~~ Operational aspects of Open-edi for implementation

ISO/IEC 15944-1 states the requirements of the BOV aspects of Open-edi in support of electronic business transactions. They include:

— commercial frameworks and associated requirements;

— legal frameworks and associated requirements;

— public policy requirements particularly which apply to individuals, i.e. are rights of individuals, which are of a generic nature such as consumer protection, privacy protection, accessibility and human rights (see ISO/IEC 15944-5:~~2017~~2008, 6.3);

— requirements arising from the need to support cultural adaptability. This includes meeting localization and multilingual requirements, (e.g. as can be required by a particular jurisdictional domain or desired to provide a good, service and/or right in a particular market). One needs the ability to distinguish, the specification of scenarios, scenario components, and their semantics, in the context of making commitments, between:

a) ~~a)~~ the use of unique, unambiguous and linguistically neutral identifiers (often as composite identifiers) at the information technology interface level among the IT systems of participation parties on the one hand; and, on the other,

b) ~~b)~~ their multiple human interface equivalent (HIE) expressions in a presentation form appropriate to the Persons involved in the making of the resulting commitments.