
Sara Jones, Marc Wilikens, Philip Morris,
and Marcelo Masera

Trust Requirements in E-Business

A conceptual framework for understanding the needs and concerns of different stakeholders.

TRUST IN INFORMATION SERVICES AND TECHNOLOGIES HAS BECOME AN INCREASINGLY IMPORTANT issue. The development of trust between businesses, consumers, and other stakeholders is seen as crucial to the expansion of e-business markets and the full exploitation of technological developments in this area [3, 4, 10]. However, the way in which trust may be gained in this context is not yet well understood. Requirements relating to trust are seen from many different perspectives by different stakeholders, and often expressed in different terms. There is therefore a need for a common

framework or language that will support a shared understanding of the concept of trust and will allow the requirements of different stakeholders to be discussed in common terms [6].

This article aims to provide a basis for such a framework. The preliminary framework presented here is intended to be used in structuring early phases of requirements elicitation and documentation in e-business system development projects. It includes a number of different views on the origins of trust requirements and the context in which they must be defined, each of which may be used as a thinking tool, or checklist, to help break down the complexity of the problem.

Although the focus here is on requirements for trust, it will also be argued that parts of the frame-

work may also be useful in structuring the elicitation and specification of other kinds of requirements for e-business systems.

A conceptual framework specific to the needs of e-business developments is seen as potentially useful for a number of reasons. First, the widespread introduction of e-business is provoking a radical reconceptualization of the way in which businesses operate: it provides the potential for new business models in existing businesses, as well as new businesses—information brokerages and trust service providers are just two examples of types of businesses that did not exist, in their current forms, before the advent of e-business. Requirements for new e-business systems must therefore often be identified from the first principles of new business

goals, and cannot simply be carried across from existing systems. Yet such new e-business systems are often very complicated, involving numerous stakeholders with different objectives, constraints, and requirements, and the negotiation and organization of requirements for the system as a whole becomes a real challenge. A general-purpose conceptual model can help us to manage such complexity.

A second reason is the shift in emphasis in the type of systems now required for e-business. It is often important to the commercial success of a business that the systems it uses for e-business are dependable (secure, reliable, and available when needed), however, the level and type of dependability required may be different from what security and

tive consumer redress mechanisms when cross-border disputes arise [11].

Finally, because of the changes described, traditional views of key concepts such as trust and security must be re-examined and redefined for use in this new context.

The work described in this article was carried out as part of the TRUST-EC project, which was conducted on behalf of the European Commission. The project began with a review of the literature, from which a definition of e-business was formed. Initial views on trust requirements in e-business were validated in a workshop attended by 19 invited participants from European industry, universities, and public authorities, who came from different back-

REQUIREMENTS CONCERNING SECURITY, RELIABILITY, and availability must be made by trading off costs and benefits and identifying acceptable levels of risk.

safety-critical systems communities have traditionally dealt with. Requirements concerning security, reliability, and availability must be made by trading off costs and benefits and identifying acceptable levels of risk.

The environment in which e-business systems operate is also changing—businesses are no longer likely to have total control over the systems and networks upon which their e-business applications depend. It therefore becomes more important to understand, and regulate, perhaps by contractually binding statements of requirements, the relationships between stakeholders responsible for different parts of the system.

In addition, there is a real and growing problem with interoperability between different e-business solutions. Work is under way to tackle this problem (see, for example, [8]), but most of this is focusing on component and architectural levels, and is therefore not so helpful in eliciting consistent user requirements at an e-business system level. The challenge now is to establish a link between business interests and engineering work in this area.

The explosive worldwide growth of the Internet, its vulnerabilities, and the lack of clear legal rules in international e-commerce have raised legitimate concerns with respect to the adequacy of consumer protection measures in the online environment. A key concern now is therefore the provision of effec-

grounds, including IT, retail, medicine, and law. A full account is provided in [6].¹

Characterization of E-Business

There is currently little consensus as to what exactly constitutes e-business, or e-commerce, and many different definitions of these terms are either given or implicit in the literature [7]. In this article, we use the term “e-business,” rather than “e-commerce” to describe the domain of interest, as we believe this more accurately reflects the diversity of activities affected by recent developments in the use of network and communications technologies such as the Internet. According to the *Chambers Concise 20th Century Dictionary*, the term “commerce” denotes trade, or the interchange of merchandise, and is, by implication, concerned only with the exchange of goods of financial value. The term “business,” on the other hand, denotes more general dealings or commercial activities, or a commercial or industrial concern, and therefore includes operational activities and logistics. The availability of new technologies is revolutionizing not only the way in which goods may be bought and sold, but also the way in which companies operate (for example by permitting the creation of so-called virtual enterprises), and

¹Note that although the workshop originally used the term e-commerce to describe the domain of interest, we have now adopted the term e-business to describe the same field, for reasons described here.

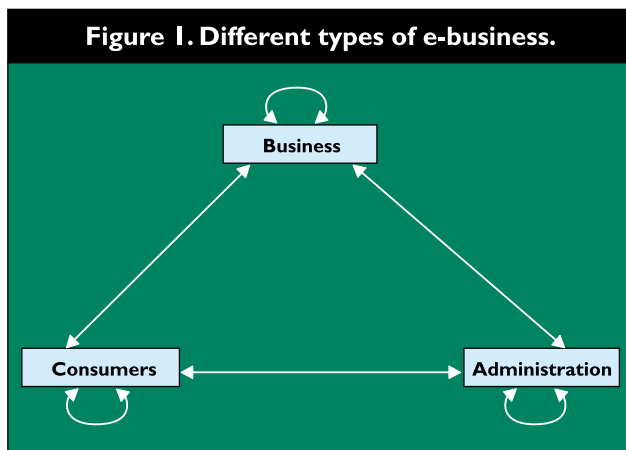


Table 1. Components of dependability [1].

Dependability categories	Effect
Safety	nonoccurrence of catastrophic events that threaten human life, health, the environment.
Reliability	continuity of service
Availability	readiness for usage
Security	authentication, confidentiality, non-repudiation, integrity

we wish to include this type of activity within our framework.

Taking an inclusive view, based on the definitions presented in the literature (see, for example, [2, 3, 5]), we therefore define e-business as follows: *E-business is the carrying out of business activities that lead to an exchange of value, where the parties interact electronically, using network or telecommunications technologies.*

In this definition, we include the exchange, not only of goods and services with a definite market value, but also of information, which is of value to partners in specific commercial activities (such as the formation or maintenance of a virtual organization), but has no market value per se. This is in line with the view of CommerceNet that: “The new paradigm of e-commerce is built not just on transactions but on building, sustaining, and improving relationships, both existing and potential.”

We intend our definition to include a set of related activities such as those referred to as electronic trading and electronic retailing, which in our view may currently be seen as types of e-business, though we note that the use of such terms is still evolving. Although most attention is currently focused on e-business conducted using the Internet (often termed Internet commerce) and the Web, we also include in our definition activities carried out using a broad range of other technologies such as narrowband (videotex), broadcast (teleshopping), proprietary corporate networks (such as those used

in banking), digital television infomercials with Internet response mechanisms (for immediate ordering), CD-ROM catalogs with Internet connections (for content or price updates), and commercial Web sites with local CD-ROM extensions (for memory-intensive multimedia demonstrations).

Thus, from the current literature (see, for example, [2, 3, 5]), we have constructed a superset of the types of e-business currently of interest or being practiced as follows—examples are included in parenthesis: business-business (electronic trading, virtual enterprises); business-consumer (online retailing); intraorganizational (management of logistics within businesses or administrations); business-administration (submission of trading information for tax purposes); consumer-administration (electronic submission of individual tax returns) and consumer-consumer (online auctions). The interactions between the different parties involved are summarized in Figure 1.

Trust and Dependability

As described earlier, the new context of e-business demands a new understanding of key concepts such as trust and dependability. According to [1], dependability is seen as a system property and consists of four attribute categories, as shown in Table 1. Security, reliability, and availability of systems are clearly important for successful e-business. Examples of requirements in these areas are given in [6]. Safety is also significant in types of e-business such as virtual hospitals.

However, in recent literature relating to e-business, the term “trust” is usually used to characterize the more general reliance of business actors and private citizens or consumers on other actors or systems within the Information Society [4, 9]. Thus, while a dependable system contributes toward raising and assuring trust in business relationships and services, trust encompasses larger issues than simply the dependability of a computing or communication infrastructure. For example, business partners need to be able to trust not just their own systems, but also other partners and the systems they use, as well as the infrastructures exploited for establishing communication. If traders in digital objects (such as musical recordings or journalistic articles) are to be trusted by their suppliers, they may need mechanisms for identifying and tracing such objects in order to prevent unauthorized copying or use. In building trust relationships with their customers, retailers may need to manage risks on an ongoing and dynamic basis based on public perceptions and commercial cost-benefit decisions. Finally, although

businesses and consumers may consider underlying systems to be completely dependable, in the traditional sense, they may not trust those systems with their business or personal interests unless there exists a suitable legal framework they can fall back on, should problems arise. Thus requirements for trust in e-business are broader than dependability requirements in other domains, and a new framework is needed in order to ensure they are fully addressed.

Four broad categories of drivers have been identified by the European Dependability Initiative [12] as shaping new perspectives on trust requirements in e-business applications, and challenging our existing understanding in this area. These drivers may be briefly characterized as increasing globalization, the complexity of large-scale open information infrastructures, the transition to a digital virtual environment, and rapidly evolving systems and environment.

For the business contexts considered in the TRUST-EC workshop (which included online retailing, virtual hospitals, online information services, and virtual enterprises), the main drivers for issues relating to trust were, in approximate order of perceived significance, as follows. Firstly, the transition to a digital virtual environment means traditional bases for trust (relating, for example, to physical characteristics of people, premises, or products) are absent, and also that businesses rely increasingly on digital assets, which must be protected from new threats. Secondly, the complexity of large-scale open information infrastructures implies the need for cooperation between a large number of different stakeholders and an increasing vulnerability to cyber-crime and fraud. Finally, the increased possibility for and exploitation of opportunities for global activity make it harder for businesses to win trust due to the geographical distribution of partners, and lack of understanding as to how differences in national legal frameworks may be accommodated.

Each of these drivers is, to a certain extent, reflected in components of the framework, which are presented in the following sections.

Stakeholders in E-Business

The first of the views in our framework focuses on system stakeholders. We define a stakeholder as “a person or organization who is, or is likely to be, significantly affected by e-business.” As noted previously, it is important that trust relationships should exist between all stakeholders in an e-business system. Since we are focusing here on general concerns, rather than requirements for particular e-business systems,

we consider general classes of stakeholders, such as service providers, consumers and businesses, between whom such relationships may need to be formed.

We have found it useful to group these different types of stakeholders into the three categories of participating, enabling, and supervisory stakeholders.

Participating stakeholders are those who are doing business by means of using e-business services and technologies. This category includes: business partners or customers (typically organizations or companies); individual customers (typically consumers, members of the public); public administrations (for example tax authorities and legal authorities); suppliers (producers, wholesalers, and individual creators of goods and digital assets such as music or film recordings) and delivery services (for physical goods such as books or groceries).

Enabling stakeholders are those who provide services or technologies to enable e-business to take place. They include providers of pre-contract services (for example, marketing, advertising), providers of financial services including electronic payment (typically banks); trust service providers (providers of digital signatures, certification authorities, copyright management facilities, trusted portals for digital content or trust seal schemes); intermediaries (information brokers that provide information about other organizations involved in e-business or their products, third-party negotiation services); providers of information and communications technology, including trust technologies; and Internet and communications service providers (providers of services using communications infrastructure).

Finally, supervisory stakeholders are those who regulate or provide advice on e-business in some way. They include regional and national advisory bodies and support centers; international advisory bodies (the OECD, World Trade Organization, G8, International Chambers of Commerce); industry-led advisory bodies (CommerceNet, the Open Group, the World Wide Web Consortium, the Trans-Atlantic Business Dialogue); technical standard-makers (the International Standards Organization, CEN/ISSS) and legislators or regulators such as the European Commission.

We note that the same type of stakeholder may fall into a different category, depending on the nature of business being conducted, or on the perspective adopted. Let us, for example, consider the case of a bank or financial service provider. If we think about online retailing from the point of view of the retailer, a financial service provider is an enabling stakeholder. But when considering the per-

Figure 2. An e-business concept model.

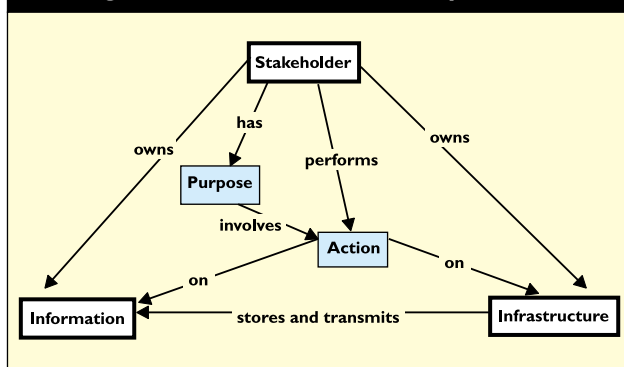


Table 2. Common e-business processes.

P1 Procurement	Making initial agreements about acquisition of systems or services.
P2 Marketing/ information search	Spreading or gathering information about products and services.
P3 Comparison of alternatives	Comparing alternative products or services.
P4 Exchange of information	Exchanging, for example, orders, invoices, contracts, or design data.
P5 Payment	Paying for products or services.
P6 Delivery of goods	Delivering goods including physical goods, such as books and groceries, as well as digital goods, such as music or video recordings.
P7 Logistics	Management of the business including, for example, stock management.
P8 Interface with public administration	Examples include submission of tax returns or payment of fines.

spective of the bank generating income through the provision of online payment services, the same financial service provider may be seen as a participating stakeholder. Thus membership to the categorization presented here is not fixed.

We also note that these different types of stakeholders are not all likely to be involved in any particular e-business system. The preceding is intended simply as a checklist of commonly occurring stakeholder types whose views may need to be taken into account in elaborating the requirements, including trust requirements, for the system.

E-Business Process Models

Another useful way of breaking down the complexity of requirements for an e-business system is to consider, in general terms, what business processes the system must support. Trust may, of course, need to be established in different ways in relation to each of these processes.

A number of more-or-less explicit process models for e-business have been presented in the literature (see, for example, [2, 3, 5]). From our understanding of the different types of e-business,

presented previously, and the various stages, processes, and activities presented in the literature, we may synthesize a very coarse characterization of e-business processes as shown in Table 2.

Once again, this list of possible processes is intended to be used simply as a checklist of business processes commonly supported by e-business systems—any particular system is likely to support only a subset of these processes, and some systems may also support processes not included in the list.

We note that, as described in [2], more detailed descriptions of the processes described here, as well as the way in which the processes are composed, will vary depending on both the type of e-business being practiced (business-business, business-consumer, business-administration, and so forth) and the viewpoint of the stakeholder (whether we are looking at the process from the point of view of, for example, a seller or a buyer, an administration, a business, or a consumer).

It should also be noted that the same system may need to support different processes in interactions between different combinations of stakeholders, or in different aspects of the business. For example, while the interaction between a retailer and a consumer may involve the processes of marketing, exchange of documentation, payment, and delivery (P2, P4, P5 and P6), that between the retailer and its supplier may involve processes of procurement, exchange of documentation, payment, delivery, and logistics (P1, P4, P5, P6 and P7). Global enterprises will predominantly involve exchange of design and production information (P4) or may involve logistics in the interaction with other businesses in the supply chain (P7).

An E-Business Concept Model

A final way in which the complexity of the problem of identifying e-business requirements may be broken down is by considering the important types of “things”—or objects—involved in an e-business transaction, and the relationships between them.

Figure 2 provides a graphical representation of important concepts and the relationships between them. Again, this model is simply a thinking tool, aimed at helping to identify significant relationships between stakeholders, information, and infrastructure in an e-business system. The relationships identified in the model do not form a complete set, and are certainly not mandatory—any particular system may embody a different subset of such relations, and will probably involve more than are shown.

In the model shown in Figure 2, each of the objects (shown in boxes) may have certain types,

roles, attributes, or states. For example, several different types of stakeholders may be involved in different types of e-business and different e-business processes, as described previously. Many different types of information (including, for example, payment information, consumer contact details, or company strategy) may be involved in different ways, and also many components of the supporting infrastructure (including public telecommunications networks as well as in-house intranets and servers). For example, customer contact details may be used in online retailing to support the delivery process, and may be stored on a company's in-house database, but transmitted to a separate company, to whom delivery of goods is outsourced, using the Internet. Actions may also be divided into two types: those that should be supported, and those that should not be allowed if trust relationships are to be maintained. Bona fide actions may include seeing, copying, using, sending, and receiving information, or using parts of the infrastructure. Actions to be prevented may include corrupting or destroying information or damaging the infrastructure. Similarly, a bona fide purpose for which information (such as a consumer's contact details) may be used is to deliver goods, whereas a less desirable purpose for which the same information perhaps should not be used is the sending of unsolicited mail.

Generic Trust Requirements for E-Business

In addition to general-purpose checklists and thinking tools such as those presented in earlier sections, another tool, likely to be useful to the would-be specifier of a new e-business system is a list of generic requirements that could be tailored to the needs of a particular system by using lists of stakeholders and process and concept models of the kind described previously. This section provides an initial characterization of such generic, high-level trust requirements for e-business.

Requirements have been grouped into coarse-grained categories: those relating to ensuring the identity and reliability of e-business stakeholders; those concerning the quality and protection of digital assets; and those about the dependability of services and systems. These categories correspond to the three main components (Stakeholders, Information, and Infrastructure) of the concept model presented in the previous section. A further category of requirements, relating to the overall context or environment within which e-business systems must operate, has been added. These requirements may be characterized as relating to the need for a stable and

interoperable legal and business framework for e-business. These requirements have been identified from the literature and validated in the TRUST-EC workshop as described in [6].

We list, as examples, requirements relating to the quality and protection of digital assets. As explained earlier, the transition to a digital virtual environment means that businesses rely increasingly on digital assets, which may include design or product information for virtual organizations, digital goods for suppliers of multimedia content, or simply order, invoice, and payment information for online retailers. Requirements that have been identified in relation to digital assets are:

- Confidentiality of sensitive information, including customer, payment, and product information: stakeholders may require either that the access to certain information is restricted, or that the purposes to which that information is put should be limited (for example, while consumers may be happy to give retailers their contact details to enable the delivery of goods, they may not be pleased if those same details are used for the purposes of mass-mailing).
- Integrity of critical information, including payment information and information to be used for commercial purposes: companies may require that both information (such as customer payment information) intended for internal use, and public (such as advertising) information should not be damaged or defaced.
- Availability of critical information: information (such as product information for consumers) should be accessible to those who need it within an acceptable time frame.
- Identification of digital objects: to facilitate prevention of unauthorized copying and traceability of objects (see the following).
- Prevention of unauthorized copying or use of critical information or digital assets: companies supplying digital goods (such as music, pictures, or videos) are concerned that such goods should only be available to those who have paid for them.
- Traceability of digital objects: to enable the creation of audit logs for nonrepudiation purposes.
- Quality of digital goods: both consumers and companies may be concerned that the digital goods they purchase should be of the quality agreed upon with the supplier.
- Management of risks to critical information: businesses need to identify likely threats and to decide upon how to either guard against the

threats or manage situations in which threatened events have occurred.

- Authentication of payment information: businesses need to be sure that payment information given by consumers, or even other businesses, is genuine.

Conclusion

It has been our experience that the framework presented in this article has assisted us in understanding the implications of new e-business issues for traditional concepts of trust and dependability. The framework has also been helpful in identifying a full range of high-level trust requirements for each of the four case studies discussed in the TRUST-EC workshop. Furthermore, it has permitted such requirements to be discussed by participants from a range of different backgrounds including IT, law, and retail. A more detailed account of this is provided elsewhere [6].

We argue that a significant focus on such a new understanding of trust and dependability requirements is well-justified in the situation where businesses depend for their survival on the reliability of their e-business support systems.

We also argue that, despite its roots in work on trust and dependability, such a framework will in the future be useful in identifying and structuring other types of requirements for new e-business systems. This will be especially important in the case where such systems instantiate new business models, so that requirements cannot simply be carried over from existing systems and must be identified from first principles, using high-level business objectives. For example, the list of stakeholders and process models provides a first step for scenario or use-case analysis enabling the identification of functional requirements. The concept model may help to bring out nonfunctional requirements or constraints regarding portability (perhaps relating to the storage of a particular kind of information on systems belonging to a number of different stakeholders) or performance.

Our next step will be to investigate the feasibility of developing a requirements process for e-business, based on the framework, which will assist developers in structuring both the process of eliciting trust requirements (by providing a checklist of issues to be discussed with different stakeholders), and the way in which such requirements are documented. We anticipate that further applications of the framework in a broad range of cases may enable us to develop the basic framework presented here, perhaps by providing different versions for use in different e-busi-

ness scenarios. As experience is gained, we envisage that patterns of requirements, centered around the framework, will begin to emerge. These could in the future form the basis for requirements templates relating to particular activities, such as electronic retailing or electronic trading, or to core business models, such as e-shopping, e-mail, or e-auction. **C**

REFERENCES

1. Avizienis, A., Kopetz, H. and Laprie J.C., Eds. *Dependability: Basic Concepts and Terminology, Volume 5*. Springer-Verlag, 1993.
2. EBES/EWOS Project Team. *Building Blocks for Electronic Commerce: Final Report*. Brussels, 1997; www.cenorm.be/iss/Workshop/ec/Projects.htm.
3. Information Society Project Office. Memorandum of understanding "Open access to electronic commerce for European SMEs" EN 1.3, (Apr. 1998) and followup and impact of the memorandum of understanding; www.ispo.cec.be/ecommerce/mou/default.htm.
4. Hoffman, D.L., Novak, T.P., and Peralta, M. Building consumer trust online. *Commun. ACM* 42, 4 (Apr. 1999), 80–85.
5. Information Society Project Office. *Electronic Commerce: An Introduction*; www.ispo.cec.be/ecommerce/introduc.htm.
6. Jones, S. and Morris, P. *TRUST-EC: Requirements for Trust and Confidence in E-Commerce: Report of the Workshop held in Luxembourg, April 8th–9th, 1999*. Issue 2. European Communities EUR Report, EUR 18749 EN.
7. Riggins, F. and Rhee, H. Toward a unified view of electronic commerce. *Commun. ACM* 41, 10 (Oct. 1998).
8. Steiner, M., Ed. *SEMPER Consortium: Advanced Services, Architecture and Design, Deliverable D10 of ACTS project AC026*. Public Specification, March 1999; www.semper.org.
9. Tan, Y. and Thoen, W. Towards a generic model of trust for electronic commerce. In *Deception, Fraud and Trust in Agent Societies*. Castelfranchi, C., Tan, Y., Falcone, R. and Firozabadi, B.S., Eds., *Proceedings of Agents'99*, workshop 7, May 1st, 1999, Seattle, published by the National Research Council, Institute of Psychology, Rome, Italy.
10. U.K. Department of Trade and Industry. *Building Confidence in Electronic Commerce—A Consultation Document*. March 1999; dti.gov.uk/CII/elect/consfn1.pdf.
11. Wilikens, M., Vahrenwald, A., and Morris, P. Out-of-court dispute settlement systems for e-commerce: Report of an exploratory study. European Communities EUR Report, September 2000.
12. Wilikens, M., Morris, P. and Masera, M., Eds. *Defining the European Dependability Initiative: A Strategy Document*. European Communities EUR Report, EUR 18139 EN, May 1998.

SARA JONES (S.Jones@herts.ac.uk) is a principal lecturer in the Department of Computer Science at the University of Herfordshire, UK.

MARC WILIKENS (marc.wilikens@jrc.it) is a staff researcher responsible for information dependability research at the Joint Research Centre of the EC in Ispra, Italy.

PHILIP MORRIS (bam@skylink.it) is a member of the staff at the Joint Research Centre of the EC in Ispra, Italy.

MARCELO MASERA (marcelo.masera@objectway.it) is an independent consultant specializing in requirements engineering and software processes.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
