

Knowledge of Society White Paper : 7

Globalnet as Directories of Information Security Profiles

Heikki Mäkinen
Globalnet as Directories of
Information Security Profiles
Version 3.0
30.1.2009

Globalnet as Directories of Information Security Profiles

Table of Contents

Abstract	2
1. Global Information Security – a Social Relationship	3
2. Information Security Profile and Social Binding	4
3. Global and Risk	7
4. Social Relations in Communications Network	7
Risk Management in Communications Network	7
Network Service Architecture.....	8
5. Social Relations and Knowledge	11
Knowledge Relation.....	11
Risk Management Dimensions	13
6. Social Components of Information Society Services	14
7. Information Security of Information Society Services	17
Information Security as a Social Relation.....	17
Information Security Management Systems	20
8. Information Security Profile Directories	22
9. Conclusions	23
References	24
History of Modifications	26

Globalnet as Directories of Information Security Profiles

Abstract

Global communications network cannot be protected as such. In global communications network knowledge relation has no social meaning. Social in general is specified as a continuum of global and history. They are social dimensions developed from social action. Social action is based on assessment of global risk and probability of historical continuity.

Concept 'global' has two meanings - social and geographical. 'Global', in social sense, is related to the concept 'risk'; global is object or event with risk probability equal to 1. In environments, where risks are managed, events and incidents are rational. Objects, events and incidents realize as risks if the required information security structures do not develop or are not developed.

Meaning of rational action is continuity of social relationship related to risk management, and different meanings to different environments of risk management. Without social connection and continuity incidents build not socially probable relations defined by information security. They are risks.

In global network social rationality is based on services creating global information security processes. Users can refer to information security profiles as a common basis of their secure intercommunication. A system of implementation of independent information security profiles is a social relation which makes possible the common activities of people and organizations in global network and global social formations.

In global communications network the balance between risks and trust is possible on logical network environments based on information security policy of social interaction formations. These environments are global; they are sharing the global coherent and concurrent transmission path and at the same time carrying social processes producing services or goods. These services, or social and economic relationships are 'Information Society Services'. Their security is based on information security profiles and builds the security of global network.

Meaning and forms of knowledge and social action depend entirely on relationship of risk and probability, global and history. Properties of knowledge and action are based on meaning and further on continuity; accidental knowledge or coincidental social relation have no meaning. The contents of knowledge and action are on empirical and historical foundation framed by forms of meaning.

Argumentation that global network is not controllable, is as unscientific as argument that Sun orbits Earth. Its foundation is a supposition that there exist 'absolute' social units where social is constituted; or a communications network between these units, 'network Inter networks'. Social units are all social action, interactive environments which are a relation of global and history.

Globalnet as Directories of Information Security Profiles

1. Global Information Security – a Social Relationship

Concept 'Information Security Profile'¹ considers a set of information security requirements independent of specific security implementations. User can specify her/his information security requirements by referring to the profile. Profiles can be delivered in network - which consequently means delivery of information security in network.

Profiles intended to be certified (for example according to ISO 15408 or Common Criteria) are – at least for the present and for a long time – quite technical and detailed. By the same principle can be constructed wider and more general profiles which consider various aspects of information security. This presupposes that there is created an environment where profiles can develop continuously, for example according to the principle of 'continuous improvement' ('Deming-circle', 'Kaizen-principle'). We can talk about 'dynamic', 'active' or 'learning' information security. Information security is understood as a social process approaching security implementations making possible social interaction. Security implementations are countermeasures for information security risks assessed.

Global communications network cannot be protected as such. Communications network as a transmission path is an ubiquitous and deliverable general social resource where knowledge relation has no social meaning. Social in general is specified as a continuum of global and history. They are social dimensions developed from social action. Social action in its turn is based on assessment of global risk and probability of historical continuity (Mäkinen, 2008, 25 – 31, 54 – 62, Mäkinen, 2008/12², Mäkinen, 2008/13). Continuity of social relation is realized through and in subjective meaning of social action (Mäkinen, 2009/9).

Transmission path can exist in different processes and logical networks concurrently. Global-history dimensions are constructed only in relation to human action, which develops into processes and logical networks. Also information security refers only to the activities of users' interactive formations, as organizations, and their mutual relationships in environments where it is possible to manage risks. 'Globalnet' is based on general transmission path where are specified various social network constructions with different service and information security levels (Mäkinen, 2008, 328 - 338).

¹ Information security evaluation standard ISO 15408 Evaluation Criteria of Information Security and Common Criteria for Information Security Evaluation (Version 3.1 and Version 3.0, [commoncriteriaportal.org](http://www.commoncriteriaportal.org)) introduce a concept 'Protection Profile' (CC 3.1, Ch 4). Concept is relevant (at the utmost) in technical contexts. Concept 'information security profile' is more general and necessary at discussion on topics which are considered for example profiles of network environments or organisation's processes (Mäkinen, 2008, 86 – 91). - Background of Common Criteria is on several information security evaluation criteria, as US TCSEC and EU ITSEC. - CC 3.0 represented in many respects quite a new and important approach to standard. CC 3.1, an official version, is based on former version 2.3. CC 3.0 can be used as an unofficial version (<http://www.commoncriteriaportal.org/unofficial.html>).

² Documents in yhteiskunnantieto.fi/White Papers series are referred by year and number in series. These do not correspond to each other; the updated versions of documents keep their original number.

Social is in a very non-trivial way connected with information security. The latter is relative to balance of trust and risk (Giddens, 1990, 35 – 36). In traditional and modern societies this depends on a social trust adopted through a socialization process. In global network, or risk society (Beck, 1986) and risk network (Mäkinen, 2008/3) in general, socialization itself is global, is based on knowledge relation in communications networks. Then the treatment of global risks is an essential part of socialization. In formal contexts on the other side, as for example in commercial or administrative purposes, trust must have an accepted status which is relevant in a large social context. Trust must be based on generally accepted social forms. The form of this generality is based on risk management and meaning of action (Mäkinen, 2008/13).

In network the presupposition of rational social action are services creating global information security processes. So far the most important general security creating social services in communications network are certification services. They however concern only a narrow – but important – sector of communications relationships. Based on information security profiles is possible to create general sets of information security solutions which network users can refer to as a common basis of their secure intercommunication. If these profiles are generally available in network they function as a general social service. A system of implementation independent information security solutions or profiles is such a social relation which makes possible the common activities of people and organizations in global network and global social formations.

In global communications network the balance between risks and trust is possible on logical network environments based on information security policy of social interaction formations. These environments are global too; they are sharing the global coherent and concurrent transmission path and at the same time carrying social processes producing services or goods. These services, or social and economic relationships, either commercial or administrative, are called 'Information Society Services' (Mäkinen, 2008, 303 - 318, Mäkinen, 2008/12, Mäkinen, 2008/13, Mäkinen, 2009/11).

Information security of global networks is based on delivery and acceptance of information security profiles. The forms of this acceptance process are based on forms of knowledge, information and network information, in action on information society services and information security itself.

2. Information Security Profile and Social Binding

Protection profile (PP) is "an implementation-independent statement of security needs for a Product type" (Common Criteria 3.1, Part 1). By profile can be expressed the security requirements of a product – which can be equipment, program, service or guidance - in a way which is applicable to the comparable products. Profile is an information security solution which can be delivered and transferred. Profiles can be certified, they can be in network to be used by other users and they can be sold.

Protection Profile describes the general requirements for a product or service type. It is therefore typically settled by:

- A user community seeking for a consensus on the security requirements in a given situation
- A developer or a group of developers of a product or service, settling a baseline for the product type

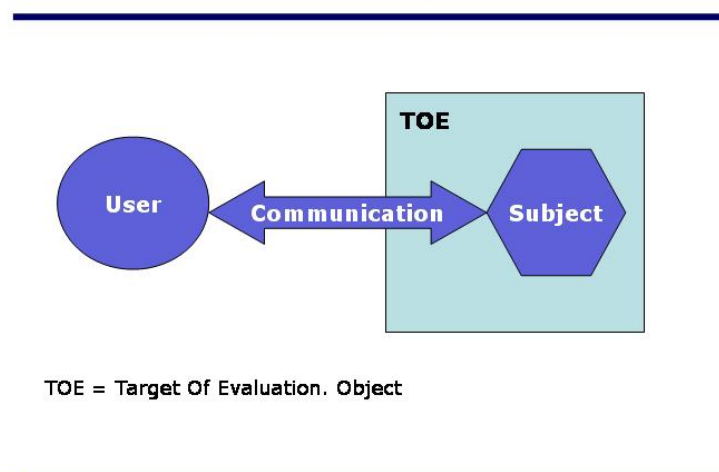
- A government or large corporation specifying its requirements as part of its acquisition process. (CC 3.1 Part 1)

Profile makers are settling their requirements for products or services in environment of mutual co-operation instead of accepting the existing independent social formation as co-operation between organizations or communications network. Profiles are based on participants' agreement on principles of information security policy and measures. If these principles are accepted, it is also possible to accept the environment of co-operation. The process follows the general principle of social selection creating rational action in general and especially in global network.

Information security profile is a generalization of concept protection profile (Mäkinen, 2008, 81 – 91). It has properties specified for protection profile, but its general characteristics are social. It can function as 'a commodity' on the market or be delivered in other social ways. Information security solutions in global network are not security measures in the fixed structures of units in social division of labour, as organizations, but common principles social actors have in network connections. They are developed on foundation of risk management, to solve a type of global risks and applied by the probable continuity social action requires.

The concept 'Binding' (Common Criteria 3.0, Part 2, Ch. 6.6.) states that User – which can be person user, node, program or service – is never directly connected with the Object of network. Object is passive, it communicates through a Subject, the active part of Object, which communicates with the User. Object has properties, as for example confidentiality classification and access or non-repudiation requirements, according to which the Binding is regulated. The elements of transmission path or information in information society service are Objects. Subjects and their Bindings and communications modes with Users compose special kinds of network environments. Objects have no social global-history dimensions; the latter are constructed only in activities of Subjects.

Binding



TOE = Target Of Evaluation. Object

Bindings are described by following examples:

- According to authentication
 - Anonymous user sends data to a node and gets data.

- User identifies and authenticates itself and gains rights to perform operations.
- According to duration
 - User sends a communications packet to the WAN-Input subject in a firewall. The binding exists only for a moment.
 - User gets through user interface rights to the system for a relatively long time (Common Criteria 3.0, Part 2).

User connected through Subject to Object, Binding, refers to a special structure between these items which Objects as such do not have. This structure can be described technically or as a social item. Binding has both structural and temporal dimension.

The essential components of Binding are:

- Identification and authentication by Subject,
- The level of non-repudiation which is presupposed in the connection of Users and Subjects³.

The concept 'Binding' can be used to define the technical information security contents of knowledge relation, also technical components of social relations and concepts 'information' and 'knowledge'. In this context 'information' or 'network information', without social connecton (Mäkinen, 2008, Mäkinen, 2008/12, Mäkinen 2008/13) is an Object of Binding, an 'information asset' (ISO 27001). For 'knowledge' is needed a Subject which is binded with information. There is created a knowledge relation whose continuity creates social relations. Usually this requires identification and authentication of Object, and non-repudiation of connection. The level these functions are required, depends on the confidentiality, availability, integrity and accountability requirements of information.

Social binding (Mäkinen, 2008, 91 – 96) creates secure, by risk management developed social formations, where social action has meaning and is rational. Such are for example social relations constituting organizations, society, state, information society services. Instead that social bindings should be created between these social formations, formations are created by social communications regulated by social bindings, also risk management and information security. Social is constituted of activities of individuals, and Globalnet about connections between them.

Binding defines an interactive communications network, where users are implementing their information security policy and measures. These are accepted by user community as information security profiles. Security requirements to be considered are effective in this network, instead of consideration of properties of binding, as identification, authentication and non-repudiation, in a given - determined for example on basis of organizations, nation states, or 'network Inter networks' - network.

In general the concepts 'Information Security Profile', 'Binding' and social communications environments based on them, are presuppositions for development of information society services. The community accepting profiles constitutes an environment where requirements of service and its risk management are possible

³ The aim of Binding is to protect information in Object and communication and to protect security functions of the Object. Further is presupposed management and audit in systems. - These functional components specify the scope of information security evaluation (Common Criteria, 3.0, 3.1, Part 2).

to implement. The other properties of communications, as protection of information in transfer, its integrity, privacy, monitoring of security and network are specified for environment build in this way.

Solutions are not made into a 'general' communications network, such exist only as risk, but on an environment determined according to required level of risk management and trust specified by bindings and interactive networks.

3. Global and Risk

Concept 'global' has two meanings - social and geographical. In social sense 'global' cannot refer into any 'absolute' and 'general' framework, where risk management should be possible infinitely, in an undetermined 'long run' exists only risks (Mäkinen, 2009/11); social is an limited property of relations. It is realized in unique historical incidents. Social is mediated by communication, by knowledge relation. When meaning of knowledge is determined in global-history dimension, it has no infinite general content, but is specified by risk management. It has different content in different environments. When activity is socially managed, incidents are local in relation to the activity in question even though they were geographically global. Without this social connection they are not socially probable relations, having information security defined. They are risks.

'Global', in social sense, is related to the concept 'risk'; global is object or event with risk probability equal to 1. Social formation of global incidents is Risk Society (Beck, 1986, Mäkinen, 2008/3). In environments, where risks are managed, events and incidents are rational. Objects, events and incidents realize as risks if the required information security structures do not develop or are not developed.

Geographically global is a special case of socially local. It requires a set of objects, events or incidents which are in a general connection with each other. Generality is then specified by social meaning and rationality (Mäkinen, 2008/12, Mäkinen, 2008/13, Mäkinen, 2009/9). It considers objects and events in a social relation specified by risk management. Then for example a resource, as network information or transmission path, which have a property of being divisible according to probable social relations into social processes and logical networks, can be global. But 'all' objects in network exist only as risks.

Social is continuum of global and history. Social binding, social relations or risk management systems exist by certain probability depending on social continuity.

4. Social Relations in Communications Network

Risk Management in Communications Network

Bindings, as social relations, exist only on historical continuity, certain probability. Meaning is a subjective condition of knowledge, that is corresponded by continuity and transferability in social relations. Continuity of social relation may be interpreted as a content of meaning; it is a probability. Social action is not coincidental (Mäkinen, 2008/13).

Risk management environments create layers of communications network.



Historical and social incidents are occasional and singular, in principle coincidental but at the same time certain, include no risk. With meaningful knowledge, there develops conscious action at immediate experience in social time and space expressed in social relations having continuity. Meaningful knowledge has forms knowledge in action and information transferable independently of experience. It has expressions in deliverable carriers as information assets transmitted in communications or interactive network. Mediated by transferred information, a special kind of knowledge relation, action is based on risk and is meaningful in relation to management of this risk.

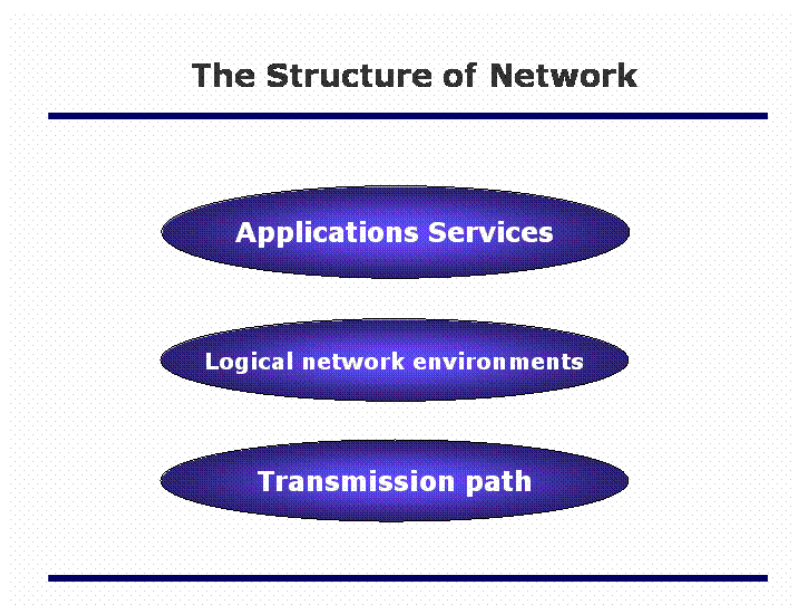
Risks are in principle coincidental, threats. Risk is assessed by its probability and consequences (ISO 27005, Mäkinen, 2008, 131 - 150). According to this are planned the measures for counteracting risks. Social formations of risk management are build on these singular risk management measures.

A Binding as a security measure is counteracting some risks. Its level and tightness, as properties of identification, authentication and non-repudiation, is constructed according to the requirements for encountering risks in the specific way action in question requires. It is a historically developed control for risks against that activity. Information security profiles and communities accepting them are historical communities for some risk management requirements. According to specified probabilities of risks and measures constructed on foundation of this, are developed formations where communications happens. Social relations and complexes build on them are developed by risk management, historical formations of established risk management measures.

Network Service Architecture

By risk management constructed social relations at networks are divided according to services offered for users - service architecture - into three layers (Mäkinen, 2008, 222 - 228, Mäkinen, 2008/13):

- Transmission path
- Logical network environments
- Services and applications of communications.



The foundation of network is transmission path. It has no special social structure but it is basis for transmission of information and building logical networks supporting social processes. Transmission path is global and ubiquitous. There is no information security – such is developed only by binding of social activities with objects in transmission path⁴.

Transmission path is deliverable concurrently between different logical networks. Thus it has no global-historical dimensions. This is the way its ubiquity works. It does not consist of connections between places or networks but of set of virtual circuits delivered concurrently into several connections of data cells. It is genuinely global in the social sense of the word, also contingency of risks. Bare connection in network, transmission path, does not imply a service which has a security or social context; this requires a Binding.

Logical network environments are specified by risk management and rational social action. There are produced, delivered and stored information and knowledge required in social action. Logical networks are knowledge relations specified at the lowest level of rationality, information security. In extension logical network environments are defined by an information security policy connected to information security objectives accepted in a social information security process.

Interactive processes are implemented by means of communications services. There are functioning already determined meaningful knowledge and global-history environments. The level they are determined may however vary, for example from connections in global ubiquitous network, where participants are unknown, into communal environments in organizations and services.

Logical network environments are constituted by Bindings required by Subjects and Objects specified. They are constituted by information security. Objects and subjects are selected sets of network entities; all properties are not relevant for the specification but it depends on service which is going to be developed. Different kinds of Bindings form network environments of several service and security levels.

⁴ In transmission path is implemented management environments of communications where are applied various technical security requirements. This is the lowest level of socially regulated logical network.

Binding having a social content, forms a genuine logical network environment. Logical network environments are social systems. Such can be for example:

- all nodes in transmission path which are able to send data when requested,
- network composed of local area networks separated by firewalls and transmitting information according to rules defined in firewalls, as for example Internet,
- network which requires identification, authentication and non-repudiation of messages and can be internal to organisation, co-operative of several organisations or based on global network.

Information, as data or explicit knowledge carried by information assets, exists in the transmission path without special social structure or information security controls attached. It may have two forms: information meaningful in social relations having a structural continuity or network information meaningful in social relations having a probabilistic continuity (Mäkinen, 2009/9). It is internalized to the human action as knowledge – even tacit – which forms knowledge assets. At the same time is formed a process which carries knowledge assets. Meaning of knowledge in all its forms is based on risk management creating continual, probable social relations (Mäkinen, 2008/13, Mäkinen, 2009/9).

Development process of knowledge, process and network environment is regulated by access control to information. Its meaning requires availability and non-repudiation of relations. This is expressed on properties of information concerning confidentiality, integrity and availability.

Bindings, including identification, authentication and non-repudiation of connection, may be done in several ways, each specified by several information security profiles, for example:

- elementary binding identifying connecting nodes through trusted paths of separate networks or cryptographic tunnelling (VPN),
- more advanced trusted path binding based on virtual circuits of ATM or MPLS,
- identification, authentication and non-repudiation service based on certificates (PKI),
- complex set of information security profiles concerning all levels of information society service and its security requirements.

Logical network environments are build on foundation of specified probability and consequences of risks. They are based on probability, but its degree may vary according to continuity of social relationship, also relation of global and history. Probability foundation is measured by concept 'acceptable risk'. The costs of risks and counteracting them are supposed to be in balance and risk is accepted by this principle (Mäkinen, 2008, 140 – 145). But it is only a probability of balance; risk regulation is not infinitely possible. If probability is trusted, the social formation will be developed. By information security developed social formations based on probability, may be 'loose' and 'wide', but it is however a social formation, not an unorganized set of contingent risks.

In a social formation based on division of labour, and production of individual organisations, logical network environments of risk management are often organization's local area networks. In information society service such networks can be only part of the service and production organization. Network must be able to form general connections with other organisations and customers; this 'generality' is limited by risk management. First this was realized in Internet as a 'network Inter (local area) networks' with security arrangements based typically on different

applications of cryptography and trusted paths (as PKI, VPN by cryptography or ATM and MPLS virtual circuits). The second phase is Globalnet as a complex of different ubiquitous networks with specified service and information security levels (Mäkinen, 2008, 328 - 338).

Concepts 'Information Society' and 'Information Society Service' are used to define social constructions for all situations where information exists, even those where social or security based knowledge does not. In the same way it is necessary to define transmission path without security structure. But when services exist, there is a Binding, Logical Network and Knowledge attached with them. Services based on communications networks are knowledgeServices (kServices) from inception (Mäkinen, 2008/6).

5. Social Relations and Knowledge

Knowledge Relation

Social relation is based on management of global risk. It has a probability revealing continuity. Forms of continuity are forms of social relations. Forms of knowledge and social action depend entirely on relationship of risk and probability, global and history. Meaning is subjective, but not coincidental; it exists in social continuity, accidental knowledge or coincidental social relation have no meaning. The contents of knowledge and action are on empirical and historical foundation framed by forms of meaning (Mäkinen, 2008/13).

Historical social development phases, as traditional and modern society, do differ in relation of global and history. This corresponds to the difference between knowledge forms - not in the sense that some forms should disappear or appear but that in the social continuity dominating form changes as do change the dominant dimension of social⁵. The continuity in traditional society is dominated by history. In modern society global has growing role, especially in economic relations, but it presupposes still historical probable forms related to social division of labour, as enterprises, other organizations, classes, state and even 'society' - social institutions and 'structures' (Mäkinen, 2008, 31 - 41, 324 - 328, Mäkinen, 2008/12). It is not genuinely global, not even in the economic sense, but semiglobal⁶ social relation (Mäkinen, 2009/11).

Global relation is based on meaningful knowledge created by risk management. Its continuity form is based on dominance of global dimension of social. Social relations are constituted as knowledge mediating rational action in continuous reflexion of social environments (Beck - Giddens,- Lash, 1994, Mäkinen, 2008/12). Instead of institutions and structures social relations constitute of network based relations

⁵ Such general forms of social relations and continuity are for example 'mechanic' and 'organic solidarity' (Durkheim, 1982). They are characterized in great proportion by properties of knowledge, 'common' (or 'collective') and 'individual' consciousness (Durkheim, 1982, 105). Forms of knowledge, as ideologies, religion ('mechanical solidarity', Durkheim, 1982, 31 - 67) on the other hand and contracts and laws on the other ('organic solidarity', Durkheim, 1982, 68 - 87, 149 - 174) characterize essentially these forms of social relations.

⁶ Concept 'semiglobal' is introduced here. Global relations are developed in the sense, that several means of action are available and able to be selected for achieving a certain end. This builds a global relation regarding historically determined traditional society, but not in the genuine sense of relations determined by probability based risk distributions. 'Semiglobal' denotes a social relation that is a transition phase from history dominated into global dimension dominated social.

mediating knowledge profiles making possible meaningful and rational social action. Their relation to social action is created by information security.

Social institutions and structures are as such information security arrangements. Information security in them is functioning to protect information - in forms tacit and conceptual knowledge - of institutions and organizations. In global environment such security structures do not exist. Information security functions in frame of social meaning, and guarantees this. Information security is not possible to understand as protecting information but creating forms of information which make possible the meaningful social action. This functions in the form of information security profiles but also according to knowledge forms connected to traditional and institutional social relations.

Forms of meaning are forms of generality of knowledge (Mäkinen, 2008/12, Mäkinen, 2008/13, Mäkinen, 2009/9). When social relation is based on history, knowledge transferability has same foundation. Historical event is certain (Mead, 1980, 1, Mäkinen, 2008/12). There is based continuity of social relation which on the other hand is global, based on management of global risk. Dominated by history knowledge transferability is based on certainty in immediate interaction of humans and creates conceptual forms, as ideologies, only in relation to managed risks in frame of experience.

Conceptual information applicable generally in several processes and organizations connects to continual social relations forming consolidated social structures or institutions. This presupposes wide transferability of information in conceptual and external form. There is possible to develop rules governing organizations or ideologies governing 'societies'. By these forms of knowledge are created organizational structures and general process elements, both transferable and probable social relations. They are based on probability but enough 'certain' to create structures and rules. The meaning of knowledge relation is based on information protection in social institutions. This concerns a set, 'type', of social relations, dominating social continuity constituting of probability of action, not single social formations in single form of societies. Their continuity presupposes socialization and internalization of knowledge. This forms a process for knowledge creation and development - Socialization, Externalization, Combination, Internalization - SECI (Nonaka – Takeuchi, 1995, Mäkinen, 2008, Mäkinen, 2009/9).

In global relation there exist no generality according to common structures or process elements mediated in experience. They are mediated on basis of probabilistic information, that is technically managed on network level by search engine technologies and statistical procedures and require continual social process to be accepted. Such are created according to meaning related to risk management. Its difference with 'simple' conceptual information is determined by information security, which becomes a dimension of social. Instead of structures in social institutions, the principle of formation of social is meaning of knowledge relation with operationalization at information security. These are not internal properties of knowledge or social relations but based on relationship of risk and probability creating continuity and meaning.

Social relations are determined by knowledge relation having a certain form of transferability. Transferability means continuity and continuity means probability. Knowledge in action is certain form of continuity. Generalized, conceptual information means social structures and, by transferability of information, meaning in global relations. Actually all are specific forms of continuity, subjective meaning,

but this is apparent only in global relation. In other forms meaning exists as justified truth.

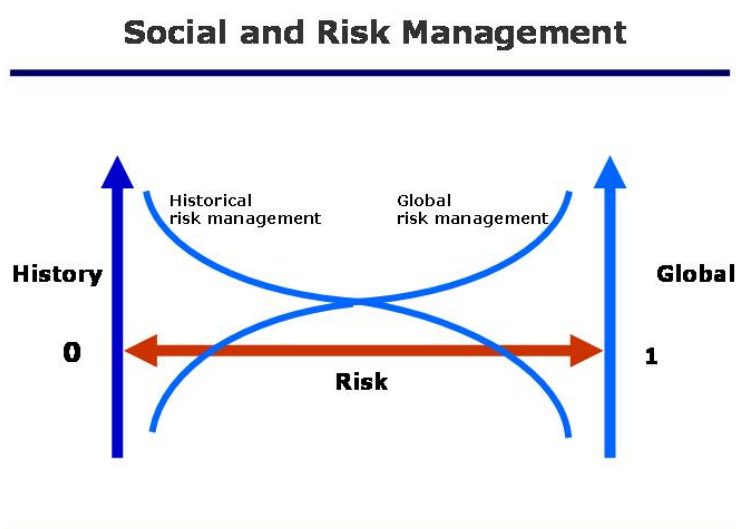
In relation to social action of subject can be defined intensity and proximity of action by its certainty. It is related to risk management in historical dimension. The general continuity of social relation is based on it, but has also form of social structure. The latter one is global. Its rules and processes, applicability in social relations is general, 'wide', or based on probabilistic continuity. Continuity is based on risk, not certainty of historical events. Social formations can be assessed and developed by principles of proximity and wideness.

Risk Management Dimensions

Social relation is global, based on risk, and a continuous relation, probability of action. 'Instantaneous' social relation is coincidental; not a relation.

Social action has meaning, continuity, it is rational. Human may act according to features of certain rationality accidentally, but only continuity makes it a social form of action. It is related to other social actions, based on risk. Risk management has dimensions global and history. They are constituted about same actions. Being meaningful and rational they have dimensions global and history.

Risk management dimensions, which function also as dimensions of information security, create dimensions of social, history and global⁷.



Global dimension of risk management is unlimited when risk has probability equal to one. Absolute generality, or absolute risk regulation, should be possible only on that condition. Idea of infinite regulative effects is incompatible with existence of

⁷ One picture confuses more than by thousand words can be explained. There is several ways to describe this relationship and no-one is better than the others. Some principles must be taken into account when considering the description: 1) Global, history and risk management forms exist only together, they are based on same events, 2) Social relations are never only historical or global; concept 'relation' requires global and its continuity in action, 3) Risk is not specified at all levels of social interaction but there exist also 'chaotic' (Mäkinen, 2005/1) social relations.

social relation. In historical, unique processes, based on rational action, are developed risk probabilities smaller than one, social relations. In the limiting case they are approaching certainty, however it never reaching: social relation is always mediated by knowledge. Global dimension has a social meaning at continuing social relation. Then it is limited, determined, which is equal to social meaning.

Social relation is impossible without rational action, whether it is valuerational or instrumental – or based on probabilistic, either scientific knowledge. 'General laws' of social, independently of this, exist not (Mäkinen, 2009/9, Mäkinen, 2009/11). The meaning of knowledge, where continuity of social relation is based, is not developed on basis on coincident, unmanaged risks.

Action, however rational, is coincidental in relation to global. It is single, and is social only with continuity. Considering knowledge action is mediated by meaning dependent on risk management. It is certain in immediate interaction, conceptual in social structures and probabilistic in global relations. At the two latter cases it is transferred in external forms, requiring explicit risk management. These forms of continuity are based on historical component of risk management, actual actions.

To have social continuity, remarkable enough to build a social relation, events must fulfil the requirements of global risk management. This is the continuity principle of probability exceeding socially meaningfully zero. But it never is certain as actual action. On this basis are developed forms of social continuity, are they based on tradition, social structures and institutions, or probabilistic systems of social profiles.

6. Social Components of Information Society Services

Information assets are deliverable social resources which can be divided into several networks and processes concurrently. This specifies the special form of transferability of conceptual information - in simple information by information assets as entities, although possibly complex as databases, and network information by probability managed assets. Information which assets carry is deliverable by restrictions considering information development process, especially socialization and internalization. These do mean that information has meaning and builds the forms of social continuity and at the same time knowledge. These restrictions are not bound into special forms of social meaning or continuity but their existence in general.

Socially determined networks are constituted in deliverable transmission path; logical network is a view of it according to the requirements specified by risk management. Information based dimensions of interaction processes are deliverable at least internal to the risk management environment. Part of them, especially components connected with information management and protection, are deliverable also between risk management environments. Process components define a special degree of interactivity and information transfer process requires.

Social continuity and relations require knowledge and logical network in special forms. Where is network information, there are global social relations of information transferability; where is information, there are global structures relative to experience and knowledge relation relevant in it, as organizations, their rules and mutual relationships. In both cases social relation and continuity are based on probability. Their continuity builds history and development based on risk. Network information has meaning only based on probability. It is possible to define only on basis of information security.

Information society service is defined as a service based on networks' information and knowledge resources and social processes determined by continuity of risk management environments producing certain goods or services to the customers (Mäkinen, 2008, 303 - 318). It is independent of experienced social place and time, global and history, in frame of social meaning of knowledge relation based on transferability of information and network information.

Information society services, or 'eServices', are often planned according to the level of on one hand process repeatability and consistency and on the other hand complexity service requires. This determines for example the level of 'automation', also ICT-solutions, formal production arrangements of implemented services and the security solutions planned for the service components.

Repeatability and consistency mean that service is mainly constituted of resources based on information, which are socially deliverable and divisible and 'widely' applicable in communications network. Then services are still divided into ones realized in social structures and those realized in network as accepted profiles. Their difference is in information security applied. The latter ones constitute genuine information society services. Complexity of service means that service is mainly constituted of interactive social resources which are based on knowledge. Their applicability is limited by conscious resources of communications network. They do not include risk to be managed independently of actual social communication.

There is no way to define global relation, transmission path or network information, than information security. Information is constituted in consciousness applied in continual social relations. These form social structures and institutions, where information is applied. Same information assets are functioning in network, only with difference, that their meaning is determined by risk management and information security.

Information society service is build on components of three types:

- Probabilistic components concerning risk management and information security in global environments,
- Technological components concerning information and its carriers,
- Functional components concerning knowledge and interactivity.

Each component follows social processes in global and historical risk management. These build a general, formal and service specific factors of services and their information security. They are connected with each other: general and formal do not mean anything instead of rational history at events. The principle of limited social relations means in this connection that no service cannot be based on some form of knowledge, but always on all forms, with different emphasis. Any components, including technological, of service cannot be generalized or applied infinitely.

Technologically the foundation of service is communications network as general transmission path, its definition according to processes in interactive connections and their risk management – logical networks – and services accomplished in this totality. Functionally service is constituted of processes which are divided into components of formal processes and information systems serving them and personal interactive contribution and knowledge attached to it. Both have specification as meaningful social formation according to information security defining their relation to global.

Information security is a dimension of service as social relations and action. It is in global environment a social relation and continuity comparable to social structures in institutions at social relations dominated by social division of labour or tradition in premodern societies. In global environment knowledge relation is based on network information, whose applicability is probable only by continual reflexion of social conditions. 'General' social conditions are possible to define as profiles of social forms applied in actual action.

This builds dimensions of information society service:

- Deliverable technological and information resources,
- Historical technological and knowledge resources,
- Information security of former dimensions defining their applicability as continual, meaningful and rational social formations.

These dimensions are social relations. It is not relevant to talk about them as properties of certain service - as is not relevant to talk about 'knowledge' or 'information' as properties, or 'organic solidarity' as a property of single organization or process in division of labour. Continuous meaningful rational action in information society service is dependent of information security. 'General' components of services, are they based on deliverable or historical social resources and respective forms of knowledge, do not form information society service, but only their continuity based on information security – in the same way as 'accidental' behaviour according to features of certain rationality does not form social action, but only its probability. In global relations meaningful in information society services this presupposes continuous probability evaluation. Information security represents global in these formations, makes them restricted, defined and limited global relations. 'Deliverable resources' are not absolutely deliverable; they are based on history dimension specified by social meaning and continuity.

Social continuity of deliverable resources may form generality based, in limits of risk management, social relations that are not scarce in the economic sense of the word. They can be used in different networks and processes concurrently. Knowledge based resources are scarce in any social relation. In traditional economy, based on division of labour and hierarchical organisational forms, these resources are intertwined but in information society service, based on processes and logical networks, they can be separated. Economic activity is thus based on socially scarce resources and emphasized into service production. This is a central characteristic specifying information society.

At information society service can be defined extent and intensity, proximity of action by level of risk and certainty.

Divisibility of service transaction or solution and their extent in communications network indicates repeatability. This is based on deliverable resources as information and communications network and their carriers. Intensity of transaction or solution requires interactivity and indicates weak divisibility. Interactivity however makes possible to produce complex solutions. They are based on historical risk management of knowledge, its carriers and the mutual relationships and processes of people.

If transaction is applied widely, repeated often and is simple enough, the most economic and sufficiently good service level is reached by utilizing deliverable resources to build standard solutions. The more knowledge is involved with the human action, the more intense and complex service is. Then interactivity must be

increased. This presupposes varying technological solutions. When intensity and complexity are increasing, the possibility to treat the service by a general solution diminishes. Finally it is got into the individual treatment of service.

Deliverable resources are based on two factors:

- Technologies of information carriers as information assets, their presentation in data bases, equipment and programs.
- Formal process elements and information applied in them.

These resources are deliverable in social structures, as in organizations, based on conceptual information and between them⁸.

On historical dimension of resources are composed specific process implementations and logical network environments where knowledge required in these processes is created, delivered and stored. Interactive process includes

- the actual process and knowledge used in it,
- the carriers of interactive processes.

The knowledge of process is focused on the special purpose process has. It is highly specified knowledge. The carriers of interactive processes include for example arrangements for developing and maintaining creative environments. Network solutions must in last instance serve interaction. This presupposes flexibility of network structure.

7. Information Security of Information Society Services

Information Security as a Social Relation

The main technologies of network information treatment are so far search engine technologies. The principal question however is not how information is found but how it is, or becomes socially meaningful. This requires subjective meaning of knowledge and continuity of social relations. It concerns principally information security.

This presupposes the change in the understanding of information security – it cannot be seen as protection of organization's or other interactive form's information, but a presupposition for knowledge creation and essential part of knowledge relation. Accidental knowledge exist not, neither accidental rationality; their continuity is their meaning. This is based on risk management and information security. Continuity principle defines social relation.

Information society change means that information processing technologies develop into more general knowledge creation and development technologies (Nonaka – Takeuchi, 1995, Takeuchi – Nonaka, 2004, vonKrogh – Grand, 2000, Mäkinen, 2008, 45 – 48, 62 – 67, Mäkinen, 2008/13). Foundations of information processing in bureaucratic organization are not an exception; organization's knowledge consists of 'justified true beliefs' (vonGrogh – Grand, 2000, 14). Knowledge creation is a social process where is created meaning and content of knowledge. In

⁸ In management based on process approach these process elements are often described 'support processes'. Such an expression is misleading. They include for example knowledge governance as specifying the common principles of knowledge creation and development or information security in preserving the value of developed knowledge and creating meaningful knowledge relations. These are components of social relations in all cases and principal forms in information society services.

developed social institutions and structures this is expressed in a dialectical process of tacit and conceptual knowledge or knowledge and information. In general social relations is considered further network information. Information security is the essentially global dimension of knowledge and services specifying their finiteness and social content. On the other hand it is essentially the continuity dimension of knowledge and services

This principle becomes important in information society services, where exist not organizational structures, which as such guarantee information protection and its meaning in organization's activities. They have history, where these functions are developed, but in actual action in organization it is given. Information society services are constituted of components specified by deliverable and interactive knowledge relations which as such do not compose continuity. Information security and meaning for knowledge and information used must be separately specified in the service processes. From network is available immensely information which has no a priori meaning. It must be defined in service processes. This becomes the main problematic of information security.

In single organization or process this can mean the evaluation of usability of knowledge on foundation of objectives. It may be called historical risk assessment and evaluation of information. But the meaning of knowledge requires continuity of social relation. In information society service this continuity is created by a form of information security which requires specification of access, confidentiality and availability criteria of information in relation to rational action in service. It may require delivery of information as well as its protection.

Risk is an objective relation of specified threat and continuity. It is built on set of events creating social relation by continuity. Probability and consequences distributions of risk are known. This is based on assessments but realized in actual information security measures building management systems. Information security requires specification of bindings which determine the 'structures', actually processes and networks service uses.

Information security is always composed of two components: in bindings realized technical and management component. These components can consist of network, application and process solutions. On the other hand information security has characteristics related to the mode of resources applied and in last instance to the mode of information managed in controls. Both types of resources presuppose technical and management components of information security

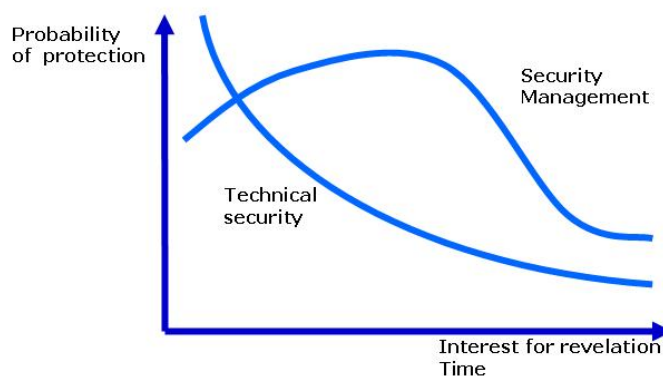
With information security based on deliverable resources can be created solutions based on global dimensions of risk management and security. They do not have a history dimension specified. To have continuity or be long-lasting solutions presuppose the use of interactive resources and information security procedures. Actually both are necessary forms of security solutions. Then they have history and make possible social action and information or knowledge storage and transference.

The forms of social can be used as characteristics of information society, as follows: "the information society is not primarily a society in which the production of information displaces the production of goods. It is also not primarily a society in which knowledge or information becomes the most important factor of production. It is instead an order in which the principle of 'society' becomes displaced by the principle of 'information'. An order in which sociality becomes displaced by a certain 'informationality'. Sociality is long-lasting and proximal. Informationality is of short duration and at a distance" (Lash, 2002, 75).

The problem is how to compare distance and time; what are 'long-lasting' and 'proximal' on the other hand and 'short duration' and 'at the distance' on the other? Duration can be expressed only in terms of probability of a social relationship and distance only as a risk involved with a relationship (Mäkinen, 2008/12).

Rather than about 'sociality' and 'informationality' the question is about varying forms of social which have at least statistical connection to the social and geographical distance and time in experience. The more solutions are socially global, also based on technical solutions and information, the more they are possible to 'spread out' in society but the time their duration may be reducing. 'Instantaneous', or – a paradox – coincidental protection, has a high probability in relation to social distance. With management functions and based on acceptance in interactive processes, also continuity components, information security solutions can have also duration in experienced time, they are considered long lasting. This may concern technical concepts and information based solutions.

Information security, time and interest



Social management of information security in communications network is composed of the security of Information Society Services. Several organisations can be participants on a service. On the other hand, if organisation's process utilizes communications network, it can be interpreted as information society service. Based on information and communications network it is always global.

Information security as relation can be operationalized by information security profiles which are based on 'material relations' as bindings in technical sense, and by management components. These profiles can define security objectives and controls at several levels according to the requirements of users and suppliers of services. Profiles describe several network environments with different service and security levels. Totality of these network environments is called **Globalnet** (Mäkinen, 2008, 244 – 247, 280 – 281, 328 - 338).

A social relation, and profile, should be described by risk and security distributions (Mäkinen, 2008, 118 – 122, Mäkinen, 2009/10, Mäkinen, 2009/11). Single factors of security are related to social division of labour. In social relation nothing is done according to unique factor but according to meaning of action related to security created continuity. Global relations in general cannot be defined by single factors as

division of labour or commodity production. Instead in information society services are defined general welfare functions in relation to customer.

Information security level of a relation can be defined on security distributions having profile definitions of several factors⁹. At relation and dimension, especially in information society service, security evaluation and its implementation should be defined by social meaning. This is related to risk management which is a dimension, where components can compensate each other and have a same total effect in different proportions.

Information security profiles can be strict in technological matters and concerning formal process security. The more interactivity increases the more flexible profiles are. This is however a matter of application and implementation more than a principal condition. Information security solution is constructed relative to the complexity of service and duration of security arrangements. Profiles as such do not differ from each other. With deliverable resources and technical security it is possible to apply them 'directly' whereas in other components application is based more on development processes, consultation and training. Profiles, as possibility to deliver service resources, are based on information applied, its stability and presentation in external carrier. In this sense information security profiles follow the general components of information society services. Economic activity is emphasized into the service processes.

When information security is evaluated as a social relation, the whole concept becomes problematic. Question is actually of a form of social. Same thing however is true in social form where organization and 'society' in form of nation state are dominating. Then however is developed social relations in form of structures and institutions, whose security is object of protection, which has also other forms than information security. In information society services information security is the only form creating social rationality.

Concept 'information security' is however used onwards. There is two reasons: 1) special technical means and 2) special management systems for information security. These make it reasonable to develop the conception.

Information Security Management Systems

Foundation of information society service is in modern society value creating processes based on networked environments. Even process of one organization uses network. Value creating process has been replaced by value creating network.

In a social formation based on division of labour the specified probability of risk and measures it presuppose are realized in organization and its communications network. Information society service presupposes a set of social relations, network of interaction, where are specified risk the service encounters and trust it requires. This presupposes specification of service's logical network environment for processes included.

Information society service is a new type of social organization of production and administration. Its characteristics is that the separation between organizational and

⁹ 'Information security level' in comparative sense can be defined also on other grounds, as for example in SSE-CMM, 2003 and IMS3, 2007. Then must however be defined a fixed requirement level, where security status is compared. This is important in connection where for example organizations are planning a mutual co-operation. In general such definition is impossible as unlimited risk management is.

social, or communications, level of interaction is not reasonable. From the point of view of information security management this means that in organization, processes and networks carrying them must be acted according to the same principles. Separation between organisation's management systems and communications network's so called 'Internet-security' exist not. Or rather the latter does not exist but information security of communications through security of information society services.

In its current standardized form Information security management system (ISMS, ISO 27001/ISO 27002, Mäkinen, 2008, 106 - 111) describes a system of an organization with a specific division of labour and information processing facilities. If security system is described according to knowledge and processes in information society services the same principles, which apply to an organization, apply also to processes within an organisation or between them, based on agreement or general social services. In this sense ISMS-standards can be seen as standardisation of the content of information security profiles.

When information society service is developed, in the first phase organizations start probably co-operation based on information, knowledge and communications network with customers and other organizations.

In a simple process and co-operation of organizations in frame of organizational rationality information security management is respective to organization's information security management system. Some relevant emphasis should be defined:

- organizations must have agreements on internal principles between different processes and of co-operation between organizations,
- information security objectives and measures should be integrated with the use of information in process,
- organization is responsible for principal know-how on information security, process is responsible for special information security know-how

Co-operation with other organisations and customers presupposes specification of interface for external relations in information security management system (Mäkinen, 2008, 176 - 181). In it relevant emphasis is on:

- agreements,
- use of information and knowledge assets and access control,
- management of operations and communications,
- management of know-how.

In co-operation information society service presupposes processes or process elements which are independent of an organization and form a relation between them. This composes the mutual architecture of co-operating organizations. According to architecture is constructed a system based on expertise which is a presupposition for trust required in co-operation.

The general form of information society service is based on network, also organizational rationality is no more its foundation; it is possible to talk about 'network rationality' (Mäkinen, 2008/12). Then process - which is compatible with network rationality, actually its first form - has to be defined also at network level. It is based on knowledge relation developed by deliverable information and historical knowledge. Its evaluation as social relation is based on information security which in its turn should be defined as a distribution of risk and consequences; it is not possible to evaluate by singular security measures.

In this case principles of ISMS standards are not valid as such, although the contents of information security measures are principally same. Also global dimension of risk management and information security constitution must be considered. Then problematic is based on formation of network's service architecture by risk management and security relations based on bindings. The information security content is not specified concerning measures in social structures or institutions but on information security profiles requiring social acceptance process.

8. Information Security Profile Directories

Meaning and forms of knowledge and social action depend entirely on relationship of risk and probability, global and history. They mean continuity of social relation, not properties of knowledge or action. In information society service continuity forms by information security specified relations. These are implemented in access and trust into profiles. The former is a technical question and the latter a matter of social process, where by selections is created foundations for social action.

Social rationality develops in general on basis of selections, which are coincidental – in relation to risk, and rational – in relation to probability. Rationality forms depend on relation of risk and probability. In traditional social relation this is dominated by history, in modern instrumental relations by global and history together – semiglobal relations - and in information society entirely by global (Mäkinen, 2008/12, Mäkinen, 2008, 25 - 53). Commodity production is not based on utilitarian orientation of human, but on by selections developed rationality form, which is dependent on global but has social structure on basis of social division of labour. Information society service is developed on entirely global basis, having no social structures involved but based on continual, rational selection and acceptance process.

In global network exists no centre or hierarchy. Social is totally distributed, constructed through information society services. These can be constituted ad hoc by probabilities or be based on historically developed proximal and stabile social formations for example in a nation state – and anything between these. However in every information society service risks and trust must be in balance. This balance varies according to the proximity and stability of the service, but it exists anyhow. If the balance does not exist, it is indeed questionable is it possible to talk about social in that relationship. Information society services such a relationships are not anyhow.

The balance between risk and trust, risk and probability of social relation, is based on assurance¹⁰ and acceptance of the information security solutions. This is the form social selection process has. Solutions, profiles to be applied in concrete processes, must be available and users must have ability to evaluate them. Assurance based on evaluation is basis for trust and reason for rational action. It cannot be based solely on expertise. Depending on service applied the principles must be understandable also to 'laymen'.

The objective for development of information security profiles, is to make information security solutions deliverable and transferable, generally available and accepted. These properties mean that profiles are realized in continual rational action. The aim of standards – as ISO 27000 and ISO 15408/Common Criteria - is

¹⁰ "Assurance – Grounds for confidence that an entity meets its security objectives" (Common Criteria, 3.1 Part 1, Ch. 4.).

that systems and applications according to them are certified by an independent body and mutually accepted in international contexts. In this case profiles have an 'official' status. They have a general acceptance which makes possible their use in communications and processes in general. Acceptance rests upon the mutual recognition of certifying parties.

Social relation based on selection and on assurance based acceptance is a general social process. Networks and directories serve a technical means for a social relations and processes in risk dominated, 'large', global distributed environment.

Information society service uses a set of information security profiles with an acceptance suited to the service in question. They can be official, general on some other basis, based on agreements or internal to the service in question. Actually they are in every case situated in all these categories. But for compatibility reasons certain part of profiles must be official and general. On the other hand, official character and generality means that the development of system is slow and expensive. For example in certificate services systems based on only quality certificates of official services (ETSI, TS 101, 456) are too gauche to fulfil the various needs of networking. To a certain extent every participant in network must be 'Certificate Authority' or authority offering information security profiles in the same way as firms are accepting signatures written by hand in traditional commerce. General and perfect solutions exist not, but only probable solutions based on accepted risk.

This kind of service should function by distributed directory principle (X.500) as certification services do (X.509); if not exactly then actually. When information society service is global service composed of independent parties, must also services supporting it be constituted in the same way.

Information security profiles describe only the general features of security solutions. They must be applied. Economic activity based on them is always a service. The information, profile, itself is the same in every application, and directs the application, but the environment of it determines the way information is used.

If no form of social trust on information security profiles is present, we live in a chaotic network and social. There is no reason why that should not be possible at least in parts of global formations. This would form at least a risk society and risk network, if not something more (Mäkinen, 2008/3).

9. Conclusions

Argumentation that global network is not controllable is as unscientific as argument that Sun orbits Earth or that God created world 6000 years ago. Its foundation is a supposition that there exists 'absolute' units where social is constituted; structures, as family, gender, community, organization, enterprise, society, state, or a communications network between them, 'network Inter networks'. This should presuppose that risk management is possible in infinite framework and knowledge would have an absolute meaning. All these forms are social action, interactive environments which are a relation of global and history.

Social is always constituted of rational management of global risk establishing probable social relations - were they family, gender, community, organization, enterprise, society, state, or a communications network between them, 'network Inter networks'. Information society service does not differ from other established

forms of risk management in any other way than in it global and risk are apparent and presented also as a special form of management.

References

- Beck, Ulrich: Risikogesellschaft. Auf dem Weg in eine andere Moderne. Suhrkamp, 1986
- Beck, Ulrich – Giddens, Anthony – Lash, Scott: Reflexive Modernization. Politics, Tradition and Aesthetics in the Modern Social Order. Polity Press, 1994
- Common Criteria for Information Security Evaluation, Version 3.1, (commoncriteriaportal.org)
- Common Criteria for Information Security Evaluation, Version 3.0, Revision 2,
- Durkheim, Emile: The Division of Labour in Society. The Macmillan Press, 1984 (Original 1893)
- ETSI, European Telecommunications Standards Institute: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, Technical Specification, TS 101 456 (www.etsi.org)
- Giddens, Anthony: The Consequences of Modernity. Polity Press, 1990
- IETF, Internet Engineering Task Force, RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- ISM3 Consortium: Information Security Management Maturity Model, v. 2.0. Handbook, 2007, (<http://www.ism3.com/>)
- ISO/IEC, International Standardisation organisation, Standard 15408: 2005 Evaluation Criteria of Information Security, (commoncriteriaportal.org)
- ISO/IEC, International Standardisation organisation, Standard 27001: Information Technology - Security techniques- Information Security Management Systems – Requirements, 2005
- ISO/IEC, International Standardisation organisation, Standard 27002: Information Technology - Security techniques. Code of practice for information security management, 2007
- ISO/IEC 27005, International Standardisation organisation, Standard 27005: Information technology - Security techniques - Information security risk management, 2008
- ISO/IEC 9594-1/ ITU-T, International Telecommunication Union, Recommendation X.500 (02/01), Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services, 2001
- ISO/IEC 9594-8/ ITU-T, International Telecommunication Union Recommendation X.509 (08/05): Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, 2005.
- von Krogh, Georg – Ichijo, Kazuo – Nonaka, Ikujiro: Enabling Knowledge Management. How to Unlock the Mystery of Tacit Knowledge and Release the Power of Innovation. Oxford University Press, 2000
- von Krogh, Georg – Nonaka, Ikujiro – Nishiguchi, Toshihiro (eds): Knowledge Creation. A source of Value. MacMillan Press, 2000
- von Grogh, Georg – Grand, Simon: Justification in Knowledge Creation: Dominant Logic in Management Discourses, In voKrogh – Nonaka – Nishiguchi, 2000
- Lash, Scott: Critique of Information. SAGE Publications, 2002
- Mead, George Herbert: The Philosophy of the Present. The University of Chicago Press, 1980 (original 1932)
- Mäkinen, Heikki: Yhteiskunnan tiedon turvallisuus, Versio 2.0, 2008, yhteiskunnantieto.fi, (In Finnish, Knowledge of Society: Security, Version 2.0)
- Mäkinen, Heikki: Risk, Trust and Security, Version 1.0, 2005, yhteiskunnantieto.fi, White Papers 1
- Mäkinen, Heikki: Risk Society and Risk Network, Version 2.0, 2008, yhteiskunnantieto.fi, White Papers 3

- Mäkinen, Heikki: Knowledge Society of Information Society?, Version 2.0, 2008, yhteiskunnantieto.fi, White Papers 6
- Mäkinen, Heikki: The Social Foundations of Knowledge Management, Version 2.0, 2009, yhteiskunnantieto.fi, White Papers 9
- Mäkinen, Heikki: The Social Foundations of Information Security, Version 2.0, 2009, yhteiskunnantieto.fi, White Papers 10
- Mäkinen, Heikki: The Social Foundations of Information Society Services, Version 2.0, 2009, yhteiskunnantieto.fi, White Papers 11
- Mäkinen, Heikki: Information Society Services and the Change of Social Rationality, Version 2.0, 2008, yhteiskunnantieto.fi, White Papers 12
- Mäkinen, Heikki: Global, History and Social, Version 1.0, 2008, yhteiskunnantieto.fi, White Papers 13
- Nonaka, Ikujiro - Takeuchi, Hirotaka: The Knowledge-Creating Company. Oxford University press, New York, 1995
- Nonaka, Ikujiro – Teece, David J. (eds): Managing Industrial Knowledge. Creation, Transfer and Utilization. SAGE Publications, London, 2001
- Nonaka, Ikujiro – Toyama, Ryoko – Konno, Noboru: SECI, Ba and Leadership: a Unified Model of Dynamic Knowledge Creation. (In Nonaka – Teece, 2001).
- Systems Security Engineering: Capability Maturity Model. SSE-CMM. Model (ISO/IEC 21827), Description Document, Version 3.0, June 15, 2003 (Carnegie Mellon University), <http://www.sse-cmm.org>
- Takeuchi, Hirotaka: Towards a Universal Management Concept of Knowledge. (In Nonaka-Teece, 2001).
- Takeuchi, Hirotaka – Nonaka, Ikujiro (eds): Hitotsubashi on Knowledge Management. John Wiley & Sons (Asia) Pte Ltd, 2004

History of Modifications

Date	Version	Writer	Modification
15.8.2006	1.0	Heikki Mäkinen	1. version
5.12.2006	2.0	Heikki Mäkinen	Main modifications in presentation of risk environments and components of information society services
30.1.2009	3.0	Heikki Mäkinen	Modifications according to 'Yhteiskunnan Tiedon Turvallisuus', Version 2.0 Definition of social continuity by network, probability and social processes