SEVENTH FRAMEWORK PROGRAMME
Challenge 1
Information and Communication Technologies

Trusted Architecture for Securely Shared Services

D6.1 Identify the Legal Requirements – Privacy, Governance and Contractual Options

Version 1.0

1 October 2008

Table of Contents

1. Contributors

Main Contributor	ORACLE	Joseph Alhadeff
Collaborators	KUL	Griet Verhenneman
Collaborators	KUL	Brendan van Alsenoy

2. Introduction

The purpose of this deliverable is to translate the broad legal requirements related to privacy and governance into concepts that can provide technical and organizational guidance. The questions that follow each section for a course of inquiry that enables privacy concepts to be placed in operational context. This document represents the beginning of an iterative process, which will continue through the TAS3 project by way of refinement and supplement.

3. Privacy Fundamentals

There are three major documents that create the foundation of privacy in the EU:

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) ["OECD Privacy Guidelines"][1],
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 28.I.1981)[2] ["COE Convention"] and
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[3] ("EU Privacy Directive")

The last of these documents, the EU Privacy Directive, both builds upon the other two and represents a pan-European set of privacy requirements. The EU Privacy Directive must be adopted in counterpart into the national law of each of the Member States of the EU. As such, there are variances in the national implementations and interpretations of the law across the Member States, with the EU privacy Directive serving as the benchmark for review. The variability of this process means that requirements can be more detailed and in some cases more restrictive than those set forth in the Directive.

The UK and the Netherlands, the Member States focused on in the TAS3 architecture, have both implemented the EU Privacy Directive in national law.

- Data Protection Act 1998 1998 CHAPTER 29[4]
- Personal Data Protection Act (Wet Bescherming Persoonsgegevens, or the 'WBP') 2001[5]

In both cases, there is great commonality in the adoption of the EU Privacy Directive with greater and lesser details specified in the drafting.

As TAS 3 develops, greater detail will need to be paid to the specifics and nuances of both the laws at the national level as well as the implementations of any supporting regulations and relevant decisions of the data protection authorities. There will also be need for specific guidance related to sectoral applications of both the relevant data protection laws as well as specific sectoral laws related to security and/or data protection. For now, the development of a high level compendium of requirements is essential to allow developers to better grasp the nature of requirements which must be met.

A set of requirements can be developed based on the following foundation concepts:

1. Personal Data should only be collected/processed for fair and legitimate business purposes.
2. The purpose(s) for collection must be clearly specified.
3. The collection related to those purposes must be relevant and non-excessive.
4. Personal data must be accurate and, where needed, up-to-date.
5. Use, and subsequent use, of personal data cannot be incompatible with the purposes specified and should be with the consent[6] of the data subject
6. Appropriate security (technical and organizational) measures against unauthorized/unlawful/accidental access; modification, disclosure, destruction, loss or damage to personal data must be in place.
7. Controllers and processors have duties to maintain confidentiality of information.
8. Sensitive data may be subject to greater restrictions.
9. Data subjects have the right to know what types of data are being maintained and have the right to access and correct personal data.
10. Transfers of data outside of the EU may be subject to controls, limitations (adequacy) and requirements of accountability[7].

These requirements concepts, while accurate, are not defined in a manner that provides technical guidance because they lack details of operational relevance. As we delve into the operational requirements, it becomes clear that the principles summarized above are both interdependent and overlapping. Since our purpose is to provide guidance and not a legal treatise, the following sections will address these issues within the flow of how relationships and interactions occur. For the technical and business community this presents more of a workflow concept; for the data subject this represent more of the intuitive path through which a relationship with an organization or a number of organizations may develop.

Part of the challenge, which TAS3 is addressing, is the need to address privacy and security within an ecosystem, not just an enterprise. Requirements will thus contemplate both the workflow between individuals/entities as well as needs of the ecosystem. Since one of the main objectives of TAS3 is the assurance of privacy and security, we will also look at the role of policies and legal instruments in assuring that security and privacy are supported in an environment of trust supported by a governance framework.

4. Privacy Concepts in Application

A workflow approach to privacy and security requirements starts with the first time an individual enters a system/ecosystem. As we start the workflow it will become increasingly clear why we have to think of both system and ecosystem needs.

4.1 Notice/Use

The first introduction of a person to a system may be in person, on the phone, via documents or online. In all cases, the individual has a right to know certain things:

- What personal information will be collected (both directly and indirectly)[8]
- For what purpose is the information being collected?
- How will the information be used?
- Who will the information be shared with?[9]
- That the information will be appropriately secured.
- How to request access to the information for correction/review.
- That the information will only be maintained for a period of time relevant to the purposes of collection.

A number of these questions are essential to allowing an individual to determine whether they consent to the collection and use of the information. In considering these questions it is essential to understand all the possible purposes of collection and uses of information by both the collecting entity and any downstream/ecosystem entity with which the information may need to be shared. The consent of the data subject to the collection and use of information is limited to those purposes specified. Thus, if an enterprise only specifies specific uses of information that it has, but then desires to share the information with other parties, or use the information for other purposes, a new notice and consent would be required[10].

Technical/Business Considerations[11]

- Need to develop a notice strategy across all channels of communication
  - Explore short-form notice options[12] to address form factor issues
  - Explore timing of online notice presentation[13]
- Understand/identify what personal data elements are going to be needed?
- Identify the persons/organizations that may get access to the information?
- How will the various data elements be used by the system and the ecosystem?

4.2 Collection Limitation/Data Minimization/Least-Means-Access

Once the appropriate notice has been provided specifying the purposes, uses and sharing of information and the data subject has provided the personal information, three privacy concepts essential to

compliance come into play. The concepts are related and are predicated on the concept that what isn't collected or shared is much less likely to be compromised.

Collection limitation, which is very related to data minimization, refers to the need to assure that only the least information needed to accomplish the purposes is collected. This is a question that requires guidance from those using the information, not just those developing systems, as they may not be aware of the possible uses and all aspects of data required.

Data Minimization is the broader concept of assuring that only the information needed to accomplish the specific business need is accessed. Data Minimization may best be explained by an example. A shipping department may need to access customer information to deliver a product, but may not require access to credit or other financial information.

Least Means Access rounds out the related concepts by providing for controls to access of information. From a security perspective this may be interpreted as a need-to-know. Only those with a need to know should be provided with access to personal information.

Taken together, the three concepts require organizations to limit information collection to those personal data elements needed to accomplish the specified purposes, to then limit use of those personal data elements to legitimate business needs related to the specified purposes and to limit access to those data elements to employees with a need-to-know.

Closely related to these concepts are tools that limit the ability of information to identify the individual: aggregation, de-identification and anonymization[14]. Where information no longer identifies a person, it is not considered personal, unless it is associated with information that may identify a person. Information elements must thus be considered both in isolation and in combination to provide the needed context to better understand how it should be treated.

Technical/Organizational Considerations:

- Are the personal data elements being collected really needed?[15]
- Are there ways of aggregating, anonymizing or de-identifying the information
- Has business need for access to information been defined?
- Are policies articulated that limit employee access to information based on business need?
- Are employees bound to those policies?
- Are there technical procedures/controls to support those policies?

4.3 Accuracy, Access and Correction

Accuracy and Access/Correction are separate, but related issues that are being treated together because they present some of the same issues. Accuracy and Correction may be some of the easiest and most problematic issues at the same time. Today's online environments facilitate compliance with these requirements because information is kept up-to-date or corrected by the data subject in self-service applications. Data in an ecosystem, however, creates different issues. For one, data that has been minimized and shared with third parties may only have some identifying characteristics and in many, if not most cases, the downstream recipients of information elements may have no direct relation or even knowledge of the data subject. In order for them to meet an access request or update information they

have only two options: One - rely on the data provider to update and correct the information thus creating a centralized resource through the entity that has the direct relationship with the data subject; or Two - collect more information from the data subject so that he/she may be able to provide that they should be given access[16]. The latter path is clearly not desirable, but may inadvertently result if no other path is provided to create a meaningful path to accuracy, access and correction.

Technical/Organizational Considerations:

- Identify what information is provided by the data subject and can be maintained by self-service applications
- Once data elements, uses and flows are established, develop an accuracy, access and correction model for the ecosystem[17].
- Develop practices and policies to oversee appropriate access and correction[18] and legal instruments that bind the participants, as needed.

4.4 Security

Privacy and security are essential elements of user trust. Security is also an, if not *the,* essential element of privacy from a technical requirements perspective. Security requirements exist at the technical, logical and physical level and all require that appropriate policies be put in place. As a result of some very public and private sector breaches, the Information Commissioner for the UK has been putting together some detailed security guidance and his site should be consulted.[19]

Security is a topic that organizationally permeates the entire information lifecycle. Because it represents the driving force behind TAS3, it is dealt with across all aspects of the project. In this section, we will look to the concepts that stand behind security in privacy legislation as well as the current hot topics. Most privacy legislation and international instruments, including the five that are the basis of this review, do not provide detailed or proscriptive requirements as legal requirements. They do however share broad themes:

1. They relate to technical and organizational measures – technology, policies, practices and procedures.
2. They presume that state of the art is being considered, but accept gating factors that might influence decisions such as nature/sensitivity of the information, size of the enterprise, potential risk as well as risk mitigation.
3. They are looking at both external and internal threats (authorized and unauthorized access)
4. Access to information is the tripwire and wrongful access can include access by an authorized person with no legitimate need[20]
5. Information should not be maintained in an identifiable fashion beyond the time necessary to accomplish the specified purposes[21]
6. While not a specific requirement – former BS7799 now ISO 27001/2 is often referenced as an example of a set of comprehensive security practice.

Technical/Organizational Concerns:

- Major topics that should be addressed include:
    a. Intrusion detection
    b. Virus Protection

c. Firewalls
d. Encryption at rest and in motion
e. Authentication/ID Management systems
f. Authorization
g. Access control
h. Audit/logging
i. Data retention/deletion
j. Separation of duties
k. Security policies

4.5 Governance

A number of issues that are directly related to security may more properly be dealt with under the concept of governance. Beyond the complexities of making all of the elements listed above work together[22], an organization must also have a governance model. TAS3 addresses that requirement at the ecosystem level with organization binding as a basis of participation. Issues of trust do not end with just one organization, there must be the ability to network trust so that the system as a whole – the ecosystem- is trusted, not just the entity. In that way systems can grow in an efficient and organic fashion based on need and innovation without undue burdens – an issue of increasing importance in times of economic constraint. Trusted ecosystems have the ability to migrate trust across entities because individuals feel that they can rely on a governance framework to help assure trust.

The needs of the organizations; the legal rights of, and obligations to, the participants; and the risks of the environment, in which they operate, must all inform a governance framework. The framework may be developed in one of two ways. It may be organization- or user- centric. In the case of the former, the needs of organizations are tempered by the needs of the users; in the latter the desires of the users help shape and inform the needs of the organizations. Optimally system will develop over time where a win-win scenario can be developed where the desires of the users and needs of the organization can be optimized. TAS3 is an attempt at such an optimization where appropriate user control becomes an asset valued by the organizations.

A governance framework thus requires a risk analysis, a needs analysis for both users and organizations, a mapping of data flows and an identification of obligations. The operational elements of the governance framework include the polices and practices of the organizations, the legal instruments that bind the employees/agents to the organizations, the organizations to each other and[23] the users to the system. These policy and legal aspects of the system work in conjunction with the technical elements of the system.

This coordination is one of the elements of TAS3 that sets it apart. In most cases these concepts are backed into over time. In the case of TAS3, these elements are a prime consideration of the design process. This level of coordination takes the concept of privacy by design to a higher level. That being said, this will be an interactive and collaborative process through the development cycles and will also require continued refinement and optimization. The benefit from designing both security and privacy into technology, policy and legal requirements at the outset enables an optimization of resources to assure that all three project aspects are complementary and mutually supportive. In some cases, technology enables an organizations compliance with policies to be demonstrated; in other cases,

polices underpin concepts difficult to code and lastly, contracts may be required to bind organizations and users to both policy and technical requirements.

After appropriate needs and risk analyses, policies are the next logical step, which help define the obligations and rules of behaviour that will be supported by the technology and contractual framework. A broad variety of policies may be required, or considered that relate to security, privacy, compliance and operations. While not relevant to specific EU obligations, Annex 2 provides an example of policies that were either considered required or addressable under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the US. While the policies are not surprising and approximate requirements of ISO 27002, they do specify agreements/contracts as required elements of the security matrix.

Among the most notable polices that need to be considered from a privacy/trust perspective:

1. Privacy policy
    a. Data subject
    b. Employees /third parties
    c. Personal information of other customers transferred for processing
2. Employment/HR Policies
    a. Policies related to employee screening
    b. Workplace monitoring (includes systems)[24]
3. Security Policies
    a. Security policy
    b. Internet Access and Use
    c. Incident Response Policies
    d. Encryption
4. Business continuity/disaster recovery

As these and other required polices are being considered, recall that they must be considered at the enterprise and ecosystem level so that assurances of trust can be made.

Technical/Ecosystem Considerations:

- Can you identify technical minimum requirements for participation?
    - Are they ecosystem-wide or do they vary by type of participant, nature of information flow etc.
- Are there minimum security requirements for all participants?
    - Are they ecosystem-wide or do they vary by type of participant, nature of information flow etc.
- What privacy promises were made or legal obligations are owed to data subjects that need to be respected across the Ecosystem?
- Once these factors are identified can they be supported by contract.

While we have discussed many of the inputs to developing a governance framework, we have not focused on the important operational factors of compliance and oversight. Again, under normal circumstances, these issues are more complex at the ecosystem level, but the fact that these considerations are being taken into account at the legal, policy and technical level of project development, the compliance overhead related to these burdens may be lessened. In the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, the

principle of “each according to their role” was highlighted and reminds us that all participants to a system, even users, have some security obligation that should be proportional to their role[25].

From a privacy perspective, two main points need to be stressed. All privacy laws require that there be an effective mechanism for complaint. Thus an essential element of a governance framework is an easily accessible and usable complaint process. Good practice often favours the inclusion of a dispute resolution or mediation process. The other critical aspect is a compliance/oversight process. It is hoped that appropriate compliance and oversight processes can help address issues before they result in complaints.

Compliance and oversight in TAS3 will be assisted to a larger degree than usual by the technical infrastructure. Concepts of “sticky polices” and other automated means inherent to the architecture assure more correct use of, and access to, information. This is an important example of how technology, policy and legal issues considered at the outset can enable greater compliance with lower overhead. That being said compliance and oversight are multifaceted concepts that must exist in dimensions beyond technology – no matter how good the technology is.

Organizational/Ecosystem Considerations:

- Are there specific persons appointed to the various tasks and are there appropriate separations of duties, reporting lines etc.
- Is all the information needed to prove or investigate compliance being logged?
    - What are the investigatory polices?
    - What are the retention periods?
    - Can any of the information be retained in an anonymized or de-identified fashion?
- Have audit procedures been defined that provide backing for compliance?
- Can you audit across transactions and interactions involving multiple parties?
- Where issues do occur[26], do you have a complaint mechanism that is easily accessible?
- Do you have a process to handle, escalate and archive complaints?
- Are there mechanisms that facilitate reporting/registration requirements with data protection authorities?[27]

5. References

1 http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

2 http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

3 http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm (link to EU data protection site)

4 http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

5 http://www.dutchdpa.nl/indexen/en_ind_wetten_wbp.shtml?refer=true&theme=purple (DPA site link to act)

6 It should be noted that consent often bears important adjectives of clear, unambiguous or explicit. From a technical point of view, this requires that the user "opt in" to the collection of personal information.

7 Please note that while this issue is perhaps the most contentious and important in the global/multinational context it is less relevant to TAS3 and will not be the subject of significant discussion.

8 This includes information provided knowingly as well as information that may be collected in less obvious ways on line or on the phone. In employment and health cases issues of video surveillance and audiotaping also come into play. Depending on the jurisdictions there may be special requirements of notice related to the latter. Issue of third party information sources used to supplement information obtained directly are also covered.

9 At least in terms of types/categories

10 There are some uses/sharing that are permitted within the original collection – those purposes not incompatible with the purposes of the collections/processing or needed to accomplish the transaction. Good practice would favor listing those uses in the notice.

11 This is where the overlapping and interdependent nature of the requirements comes into play; some elements that must be noticed are more suitably discussed under other topics.

12Article 29 WP paper on notice options. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf

13 Laws require at or before time of information collection which becomes more problematic as questions arise whether IP address is personal data

14 The operational benefit of each of these approaches is predicated on the likelihood of re-identification. Aggregation and de-identification are some of the more popular approaches to anonymization.

15 Recall that this inquiry starts with the initial online collection – the technical handshake, cookies etc. While these elements may or may not be personal at the time of collection they could later be associated with a persons identity and as such need to be considered at the outset.

16 As TAS3 develops, the greater level of user control afforded by the systems may limit the scope of this issue.

17 These considerations will raise issues related to how information is stored, separation of duties and other technical topics dealt in greater depth under security.

18 There may also be rights to request supplement of information, blocking and deletion, but those must be appropriate to purposes and circumstances. A data subject does not have a unilateral right to block and accurate credit report for being used in the accepted course of transactions, merely because the report is negative.

19 Good practice note on security: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/security%20v%201.0_plain_english_website_version1.pdf; see also http://www.ico.gov.uk/Home/about_us/news_and_views/current_topics/Our%20approach%20to%20encryption.aspx for guidance on approach to encryption.

20 This may be an especially prevalent concern in medical systems where people may try to glean information on a celebrity or VIP for non-medical reasons

21 There is no hard and fast rule as to what the proper period of retention is related to a specific purpose. Interpretations rely on concepts of appropriateness and proportionality. One must also be aware, however, that certain information like communication headers and medical records have minimum retention periods.

22 Recall that the elements work in unison and greater strength in one may allow fewer resources deployed in another with no negative impact to overall security.

23 By way of example, one could consider the credit card system. There are agreements and policies that control relations between banks, processors, merchants and cardholders. There are likewise policies and agreements that bind what employees can do with card-member/institutional information. All parties are bound to an ecosystem that does not require any prior contact or relationship between transacting parties. This is why a tourist from the US is able to purchase a watch in the EU from a merchant he has never met by using a credit card. The governance framework that also controls onward transfers and other uses of the information is one of the factors in enabling the user to trust the system with sensitive personal information. Similarly in the EU healthcare arena the desire to be able to have access to needed records to treat an ever more mobile population is spawning the development of governance frameworks for e-health records.

24 Guidance from the UK Information Commissioner http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/employment_practices_code/part_3-monitoring_at_work_1.html

25 http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html

26 The complaint system should be able accessible from across the workflow as issues are not solely generated at the close of a transaction.

27 These reporting and registration requirements start with the need to register system that collect and process personal information (the detail of these requirements vary by country) and go to consideration of breach notification.