SEVENTH FRAMEWORK PROGRAMME
Challenge 1
Information and Communication Technologies

Trusted Architecture for Securely Shared Services

Document type: Deliverable

Title:	**Contractual Framework**

Work Package: WP06

Deliverable Number: D6.2

Editor: Joseph Alhadeff, Oracle

Dissemination Level: PU

Preparation Date: 31 December 2008

Version: 1.0

The TAS3 Consortium

Nr	Participant name	Country	Participant short name	Participant role
1	K.U.Leuven	BE	KUL	Coordinator
2	Synergetics nv/sa	BE	SYN	Project Manager
3	University of Kent	UK	KENT	Partner
4	University of Karlsruhe	DE	KARL	Partner
5	University of Twente as NIRICT/SEC	NL	NIRICT	Partner
6	CNR/ISTI	IT	CNR	Partner
7	University of Koblenz-Landau	DE	UNIKOLD	Partner
8	Vrije Universiteit Brussel	BE	VUB	Partner
9	University of Zaragoza	ES	UNIZAR	Partner
10	University of Nottingham	UK	NOT	Partner
11	SAP research	DE	SAP	Partner
12	Eifel	FR	EIF	Partner
13	Intalio	FR	INT	Partner
14	Risaris	IR	RIS	Partner
15	Kenteq	BE	KETQ	Partner
16	Oracle	UK	ORACLE	Partner
17	Custodix	BE	CUS	Partner
18	Medisoft	NL	MEDI	Partner

Contributors

	Name	**Organisation**
1	David Chadwick	Univ. of Kent
2	Lex Polman and Kenteq Legal	Kenteq
3	Joseph Alhadeff	ORACLE

Table of Contents

1 Executive Summary

The objective of TAS3 is to develop a secure, yet adaptable technical infrastructure that enables the user-centric creation, maintenance and exchange of personal information between multiple service providers and the data subjects involved. The TAS3 infrastructure is composed of technology, policy and legal components. This paper focuses on the development of a contractual framework. When one is developing the contractual infrastructure, it is important to understand and differentiate between the elements that are best suited to be coded in technology and supported in policy and contract and those that exist in policy and contract supported by technology. A process definition to arrive at this allocation across technology, policy, and legal includes:

- Identifying needs of users and organizations
- Mapping data flows
- Defining and association roles, rights and obligations, and
- Creating system controls and governance infrastructure

It is important to understand that the contractual framework must be developed in a coherent manner to create appropriate controls at all levels of the TAS3 infrastructure from ecosystem to individual end-user. The type of contractual framework that underpins the credit card system from cardholder to issuing bank to merchant to clearing system to card provider organizations was a useful example of such a layered technology, policy and legal framework. The entities that comprise the TAS3 ecosystem can be divided into five categories:

- The end-user – this is the natural person that is often also referred to as the data subject.
- Infrastructure providers – these are providers and operators of technical system components.
- Trust infrastructure providers – these can be reputation engines, validators oversight authorities etc
- Relationship-based Service providers – these can be doctors, employment services, or other parties with whom the user has an ongoing relationship
- Transaction-based service provider – these are one off service providers which may not have any direct contact with the user.

Contractual terms will be developed to appropriately bind each of these participants based on their roles and functions as defined by the contextual needs of their relationships within a user-centric framework that incorporates the legal requirements of privacy and security. As in commercial master services agreements, the binding occurs at the ecosystem level to broad policies and requirements and is then supplemented at the functional/ transactional level by narrower contractual elements which can even include creating binding elements in the sticky policies that may be embedded in technology. As the project progresses the actual elements will be defined to create the contractual framework pursuant to this foundation blueprint.

2 Introduction to the contractual framework

2.1 Introduction

The objective of TAS^3 is to develop a secure, yet adaptable technical infrastructure that enables the user-centric creation, maintenance and exchange of personal information between multiple service providers and the data subjects involved. TAS^3 enables an infrastructure of trust, security and privacy to meet the needs of today's more global and mobile society and workforce. Changes in jobs, residences, and professional and social relationships are more frequent occurrences than ever before. Information must be portable and accessible to meet the needs of organizations, individuals and society as a whole. Providing this portability and flexibility is also a key to remaining competitive and enabling growth in the information society and digital economy. TAS^3's development is geared to compliance with privacy laws and provides for both user control and organizational functionality of records. TAS^3 thus combines security and privacy with technology, policy and law to create a trust infrastructure predicated on verifiable information governance. The TAS^{3}architecture is composed of technical, policy and legal components. This paper will set out the requirements of the contract framework. Prior to laying out the contract framework elements, it is useful to go over both some foundation elements and other relevant trust models.

Within the EU, and in a number of other jurisdictions, individuals have legal rights related to information identifying or relating to them. While these rights have been in existence for more than two decades, the ability of users to understand how to exert control over their information has been less effective than hoped for in the legislation. While laws in the EU and other jurisdictions were effective in requiring that care be taken in securing the information and rights be provided to the individual in terms of collection, sharing and use of the information, there was no real mechanism to provide any effective control over the information especially beyond the specific transaction. In many ways the legal frameworks today existed before the needs of information management over an information lifecycle became readily apparent. Currently, exercising control over the information requires a laborious and sequential oversight of each relationship. Control in such relationships is difficult to execute because of inequalities of knowledge and experience related to information of a specialist nature (medical, legal, etc.) as well as because of lack of knowledge related to the design and operation of systems. Furthermore, there are limitations in how effective the oversight of the relationship can be when information is transferred across a value chain, sometimes unbeknownst to the data subject. It should also be recognized that while organizations collecting and using the information have the benefit of better knowledge of special types of information and systems, the overhead and burden of providing security and privacy to enable trust while enabling both organizational and user functionality is highly complex and very resource intensive.

The technical details of today's backend systems and the potentially global value chains they support have grown even more complex. Part of the innovation behind the TAS^3 project is to apply technology supported by and coordinated with policy and legal frameworks at the infrastructure level to create a shared and more efficient architecture for enhanced security and privacy, which can engender greater trust. Technology has created both the potential and expectation that relevant and useful information be available across the lifecycle of these new relationships. Previously, this information, while about a specific and identified person, was either presumed to be or treated as if it was the property of the organization collecting or using the data. TAS^3 enables information to be functional and accessible in a user-centric framework.

2.2 Testing the Thesis: Employment and Health

TAS^3 creates a generally applicable secure, yet adaptable technical infrastructure that enables the processing of distributed personal information. The functionality of TAS^3, however, needs to be tested in some real world environments. To that end the infrastructure will be demonstrated in two pilot applications, one for the creation and maintenance of electronic employability portfolios and the other for electronic health records. Two of the most important information lifecycles relate to a person's educational/employment and medical/health information. New social norms related to work, flexible job functions, more routine dislocations and changes in the workplace environment coupled with the nature of education, skills and work related information which must be maintained across a work lifecycle, require greater accuracy, control and portability of records related to education, skills and work. Similarly greater longevity and mobility of the individuals coupled with advances in health care and complexity of treatment payment and operation of medical and health systems has lead to similar requirements for health records.

In these demonstrator projects, and in TAS^3 as a whole, for main variables are at issue:

- Trust in information
- Trust in the parties
- Trust in the system/infrastructure, and
- Appropriate user control

The contractual and governance framework is essential to leveraging these variables to enable the desired trust infrastructure. Since the contractual and governance framework also requires testing, this paper will focus on the demonstrator projects, but the intention is for the concepts to remain generally applicable to infrastructure deployed in other disciplines or jurisdictions[i].

2.3 Foundation issue

Technology provides great strides in securing and assuring trust during the course of a transaction between identified parties. As our lives, jobs, transactions, and social interactions become more complex we are no longer dealing with pure one-to-one relationships. Transactions today can involve multiple organizations that make up value chains. Transactions may also have multiple components and may operate across numerous value chains. There is a lack of easy predictability as to who will need to be involved in a potential transaction or interaction. This is even more acute when subcontracting takes place, as the ultimate consumer is not necessarily aware of all the suppliers in the chain. When the consumer is purchasing a physical product this may not matter, but when it is an electronic personalized service that the consumer is purchasing, then it does matter which suppliers are given access to the consumer's personal identifying information. For example, in the health care domain, whilst a routine checkup may be within the scope of prediction, when a person breaks an ankle on a flight of stairs, who treats them and where is not predicable. Therefore who is given access to the user's Personally Identifiable Information (PII)[ii] may not be known in advance, yet the consumer still needs to provide consent to these "unknown" parties. In the employability domain, whilst there may be some quantification and predictability of potential employers for a person with a defined skill set in a specific region, there is much less predictability related to the worker who is laid off or the one required to move because of family illness. Today's current technology and policy infrastructures neither map nor scale to today's societal and information needs.

2.4 Solution approach

Despite the greater number of entities and options that one needs to consider and the greater complexity of the interactions, infrastructure systems must be able to provide the information needed to accomplish the transaction and must do so in ways that:

- Allow individuals to make choices and exert appropriate controls;
- Allow individuals to provide their consent for the use of their PII;
- Assure that information systems, relevant applications and uses of information are consistent with the legal obligations of the relevant jurisdiction; and
- Provide a system/infrastructure that has the transparency and accountability to engender trust.

Technology, in the form of the TAS^3 infrastructure, will significantly enable trust, but cannot do so without an appropriate contractual and information governance framework. This is the case for a number of reasons. The first and most practical reason is that it's inefficient to try to place all of the burdens on technology. A multifaceted approach of technology, policy, practice and people, supported by audit, oversight, and accountability better distributes responsibilities across functions and uses checks and balances to assure that compliance exists. This is especially true in the more complex environments that include multiple intersecting or sequential value chains. In those cases there is no centralized point of control, as there is within an enterprise, that controls the infrastructure and related polices. In the case of a unitary value chain, there may be a large enough player, a Carrefour or Wal-Mart, which can require other value chain participants to adopt a technical infrastructure and relevant policies and procedures. In the case of multiple value chains, or ecosystems, there is no central point of control that can dictate infrastructure or polices.

2.5 Federation and Communities

Federation concepts are being applied in groups, such as the Liberty Alliance[iii], to create trust infrastructures around identity management and assurance. Approaches such as the Identity Governance Framework (IGF – see Figure 2 for a dataflow/function map)[iv] are also being developed to better deal with technical interoperability requirements across an ecosystem. Groups like Liberty are also considering the contractual and policy requirements of the ecosystem.[v] Liberty Alliance has developed approaches to policies and technical infrastructure that are predicated on the existence of federated groups of entities (communities), which are bound in circles of trust. They have also considered how Circles of Trust can help organizations comply with EU data protection requirements.[vi]

While Liberty's work on the IGF and contract framework are informative; the largest scale example that may be relevant exists in the credit card industry. The credit card industry has demonstrated a massive scalability to technology, policy and contract obligation. While everyone understands that they sign cardholder agreements, the importance of that contractual underpinning may not be evident.

Credit card networks have detailed policies related to payments, funds clearing, cardholder rights, and charge-backs to merchants, just to name a few. They also have sophisticated back end networks to verify, validate, authenticate and audit transactions (See Figure 2 for Data Flows). They have also developed some of the most advanced fraud detection technologies on the back end to find both aberrant patters of card use that might indicate fraud as well as potential issues related to internal controls. Beyond that, the major card companies/associations: AMEX, Discover, JCB, MasterCard and Visa International collaborated to develop the Payment Card Industry Data Security Standard (PCI DSS: see Figure 1). The have also develop similarly detailed standards related to payment applications[vii] and PIN Entry devices[viii].

These PCI-based standards help the card industry define the infrastructure that all players except cardholders, will need to consider and they develop and deploy infrastructure.

The credit card companies address end-user needs through security programs like Verified by Visa as well as security and identity theft training. Other card companies like American Express are looking at digital signature technologies and encryption, which are used in the Blue Card and Express Pay offerings. All of these features inure to the benefit of the consumer with enhanced security with either little burden or even enhanced convenience. The combination of these end user controls coupled with sophisticated backend systems and enhanced merchant, vendor and support requirements under the PCI standards helps create greater trust in the infrastructure and enhances compliance with numerous legal requirements.

2.6 TAS^3 Application of Concept

TAS^3 approaches the central issue of trust in the infrastructure by using many of the existing approaches in networks of trust like Liberty Alliance and the credit card clearing systems. TAS^3 however goes beyond those approaches. In the case of federated IDM, broad solutions are used to address issues related to identity at the ecosystem level, but the limitation of scope to the area of identity does not address the complexity of broad information use and governance. Credit card polices and standards are very focused on security and fraud prevention to enhance trust and do cover uses related to transactions that have as broad a scale of implementation as exists (Figures 3 and 4 show the types of services and numbers of participants). While credit information is sensitive by definition and at times may touch other sensitive fields like employment or health, credit card information is limited to information related to individual transactions resulting in choices and governance of information is thus more limited in scope, longevity and breadth. The TAS^3 infrastructure, however, covers information beyond identity that exists in multiple types of transactions over an extended information lifecycle that will be measured in decades. Furthermore the TAS^3 infrastructure must go beyond just security and choices related to identity to controlling the sharing and use of information elements that may be linked to identity.

TAS^3 is most easily deployed as a centralized infrastructure where all participants adopt the required infrastructure and policies. However, as one considers the potential breadth of applications and requirements, TAS^3 may also operate as a specialized infrastructure within a closed network anchored by a founding or central player. Here the complexity is created by the potential intersection of independent management domains. Lastly, and most complex, TAS^3 may operate as a dynamic environment that can include new participants as well as organizations. The increased complexity is from the need to consider how to appropriately bring new players into the technical, policy and contractual fold – on the fly.

As the TAS^3 infrastructure needs to be flexible the contractual framework will need to adapt to changing conditions including new technologies, new policies and new participants. The scenarios in the design requirements document will provide useful guidance in giving direction to the initial draft of the framework.

3 Developing a Contractual Framework

3.1 Process steps

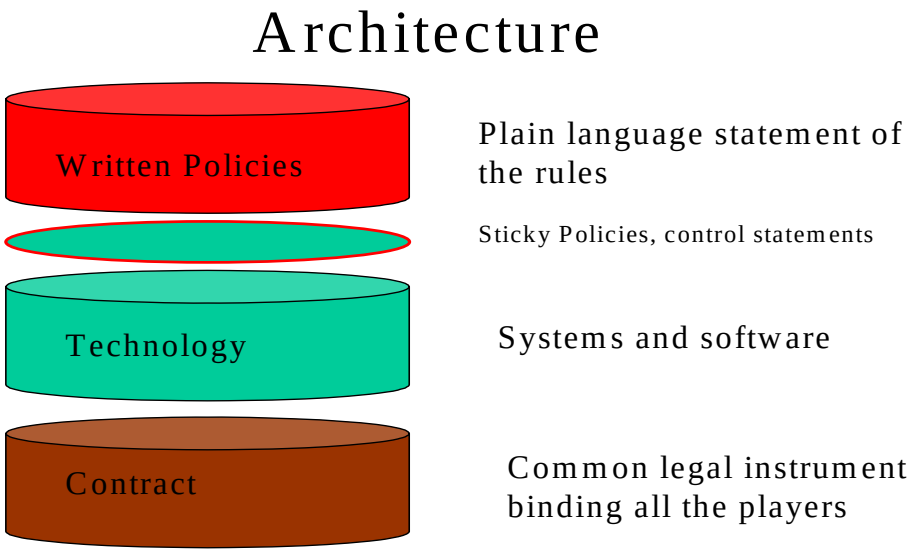
In order to develop a contractual framework four familiar terms must be established: “Who”, “What”, “Where” and “How”. The “Who” is all of the parties that will or may be involved who have rights and obligations. The “What” refers to the nature of what is being bound, or more accurately what is each party obligated or entitled to. The “Where” refers to the jurisdiction(s) involved[ix]. The “How” refers to the method and operation of the contractual framework. A term inherent in every contract is also the “what if”, which refers to needed flexibility and contingency planning. This can also be considered as methods of reducing and addressing foreseeable risk.
Error! Objects cannot be created from editing field codes.
The start of any process definition has to be an understanding of the main and ancillary purposes of a system. Defining the actors, their interests, rights and obligations is a critical second step. Thus the first two steps comprise the definition of the needs of the organizations and users. From there, understanding their interactions in terms of data flows and roles completes the foundation scoping which is required to develop a contract framework. This step then takes into account employees and other actors by associating them to roles in the ecosystem. Those roles will be critical in assigning the rights and obligations they have within the context of data flows. This foundation is needed before system controls and the overall governance framework can be specified. They in turn need to be defined before allocation across technology, policy and contract can occur. An obvious but unstated step in the process has to be an understanding of the possible role and functionality of each of the technology, policy and contract elements. This step can happen at any time as an organization goes through a number of these processes. This step will be part of the learning that should be captured at the system level to assure that it is preserved beyond personnel turnovers.

We caution that the actors, flows and roles are a foundation that is likely to change over time so that there needs to be flexibility and continuous or periodic evaluation and redefinition built into the system. The addition of new actors, the evolution of roles and the changing needs of the system are part of this change requirement. For a framework to be effective and to better understand how to structure the “How” and “What if” a dataflow map – a compendium of information flows across parties and possibly jurisdictions with associated rights and obligations related to the information flow – is needed.

The above are standard process steps in developing a contract framework. It must be stressed that a contract framework exists at the infrastructure level to create the baseline of obligations and context for binding specific choices and negotiations among the parties both directly involved in negotiation as well as relevant organization who access, control, process or store the information. It should be noted that what is described above are the ordinary process steps. Because TAS^3 is designed from the outset in a user-centric manner, TAS^3 will likely first focus on the needs of the individual users, as they will be the source of overall control in data flows. Recall that the data flow analysis will take place on a number of levels – infrastructure, community and organization/system. Data flow maps and process definition will be useful at all levels to both understand functioning and coordinate it across all levels. Even though needs may be defined from the user out, requirements will flow down from the infrastructure level with increasing granularity to cover operations. For instance individual roles are defined at the organization level while some rights may be associated at the community or infrastructure level.

3.2 Architecture

Because of the strategic nature of the contract framework to the technology, polices and process, it is also important to understand the capacity of technology to either take the place of some of the contract process or otherwise support it. The other side of that concept is the importance of knowing the limitations of technology in terms of feasibility, capacity and technology to know what functions are best allocated to contracts or polices.



It is important to understand that in the TAS[3] architecture there is the concept of sticky policies which is some way may operate as small instruction steps to enforce polices or create mini contractual bindings. In both cases these sticky policies will create some challenges in the application of contractual frameworks as the exact lineage of these sticky policies to existing legal regimes is more by example and correlation that in statute or case law[x]. Furthermore the interrelation between contracts and operational policies of the organization or infrastructure need to be defined as the project progresses.

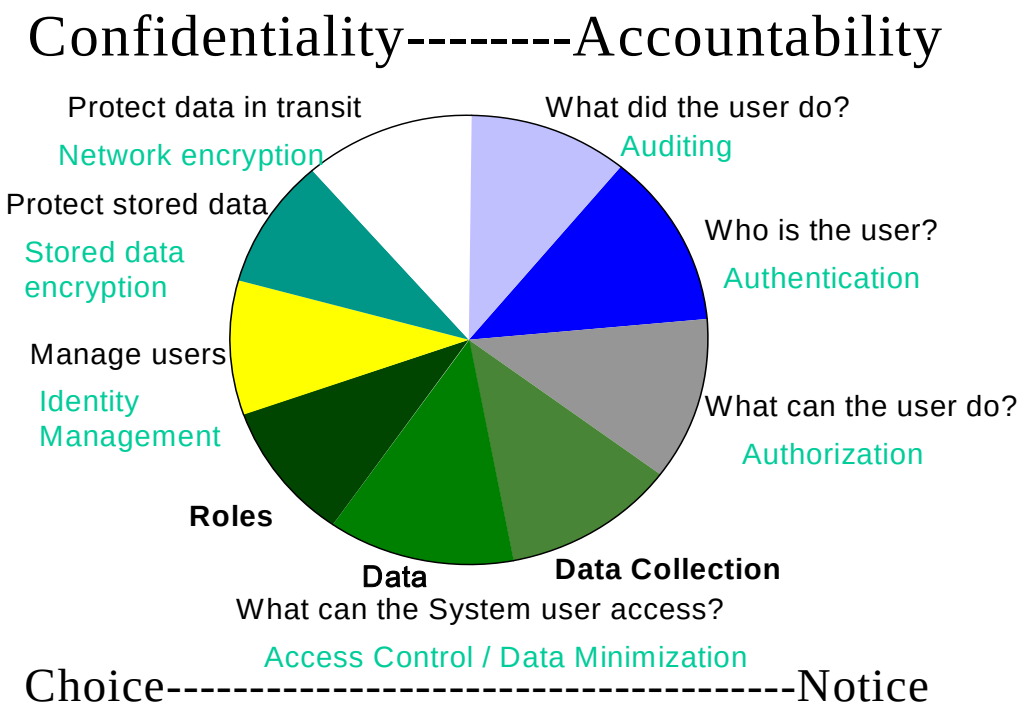
An interesting reference model to consider for this architecture is the Master Services Agreement. In the B2B commercial context, companies often enter into a Master Services Agreement (MSA) that creates the overall contractual relationship between the parties but then execute work orders pursuant to the MSA detailing specific functions and requirements. In many ways the TAS3 architecture will utilize some of these techniques – developing a master agreement at the infrastructure level supplemented by other agreements at the more transactional level that provide relevant details. An example from the education/employment demonstrator could be developing mechanisms to incorporate relevant Accreditation Prior to Learning requirements or the Common European Principles related to validation. In the context of healthcare, enabling choices related to access to records, which are by nature very context specific. Technology is essential in supporting and executing these requirements, but the contract framework is necessary to create the binding that enables remedial action to be taken against parties who fail to meet their obligations.

By way of summary the associated questions related to the contract framework in the context of the broader architecture might be summarized as follows:

- What functions can technologies do practically and efficiently?
- What functions are more efficiently enabled as part a legal framework condition?

- What conditions related to the use of or access to information should be in a plain language policy?
- What condition needs to be in more than one architectural element? i.e. linkages across the architecture
- Does oversight require a separation of duties; if so, who gets what, how and why?

When looking at architectural elements, it is also useful to associate privacy concepts and legal requirements to various technologies. The figure below makes such associations between common technologies and fundamental privacy concepts.



These technology concepts relate to the general obligations of the EU Directive[xi], which can be summarized as follows[xii]:

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

We will be referring to a number of these technologies and concepts as we delve further into the process of developing a contractual framework. They will also inform the possible binding elements of obligations.

3.3 Defining the "Who"

The essential elements of any contract are the parties - both those that sign and those that may be obligated under the contract. An organization, for example, may sign a contract that requires it to perform certain services as part of the engagement. The employees of the organization will of course perform those services. The person who engaged the organization for services can rely on that contract alone, while the organization needs to have separate contracting documents with its employees which bind them to performing services for the organization as directed by management or though appropriate processes; often in the form of work orders. The TAS^3 infrastructure creates a challenge in identifying the "Who" as was pointed out in the introductory examples because there will not always be predictable circumstances. Thus in identifying the parties to a contracting framework as opposed to a transaction, one needs to identify potential signatories and possible parties impacted by having rights or obligations. While the specific terms of a contract may need to be narrowly tailored to the facts of a situation a contractual framework that is deployed at the ecosystem and infrastructure level needs greater flexibility. After identifying possible parties from individuals to the various types of organization it is useful to categorize them in a way that rationalizes, them into a more manageable group. The categorizations are usually based on common interest, function or type with further grouping based on similarity of obligation or right.

An important organizational and classification concept comes from privacy laws, which create differing obligations based on the function provided and nature of the relationship. An information processor – one who executes instructions, but exerts no dominion over the information, has fewer obligations than does an information controller who does exert control over the information. The TAS^3 system is designed to be as user-centric as possible, but it should be noted that some information might be required by the process or to properly accomplish the purpose of the transaction/request. User control is thus an essential building block of the trust infrastructure but is subject to the concepts of need and proportionality.

The user-centricity of the TAS^3 infrastructure coupled with new technologies enabling choices made by individuals to be wired into the system to a greater degree will create interesting issues of interpretation of processor controller[xiii]. If a user can choose certain conditions and provide instructions as to use and sharing of information that are bound in technologically enabled policies and controls that the system enforces, it could be argued that entities previously considered controllers have become processors. There will of course be some areas where users will delegate decision-making – for example a patient is not likely to suggest to the treating physician what lab should be used to run tests on a blood sample. More traditional controller process relationships will still exist in those circumstances,

So transacting parties will be comprised of controllers, processors and individuals. While correct, this classification does not provide sufficient utility in application and classification of roles and functions. We may wish to consider a more detailed list of categories where their role as controller or process is used less as a classification tool and more as a way of defining obligations. We should always recall that the same entity might be either a processor or controller depending upon the context of the service or application[xiv].

Whether in healthcare, employment or any other setting five main types of parties/roles to a transaction exist:

- The end-user – this is the natural person that is often also referred to as the data subject.
- Infrastructure providers – these are providers and operators of technical system components.
- Trust infrastructure providers – these can be reputation engines, validators oversight authorities etc

- Relationship-based Service providers – these can be doctors, employment services, or other parties with whom the user has an ongoing relationship
- Transaction-based service provider – these are one off service providers which may not have any direct contact with the user.

It becomes immediately apparent that with the exception of the end-ser, an entity may play more than one role depending on context. A relationship-based service provider in one instance (an organization that provides skills training, for example) may also be part of the trust infrastructure at a later point in time as a credential validator. These classifications are not meant to be permanently linked to parties, but rather inform their obligations based on the role(s) they are playing in a particular transaction or information exchange. From a contractual architecture perspective, specific clauses specifying requirements and obligations may be associated with their role. By grouping these entities according to function it is hoped that we can define communities of interest with shared objectives and commonalities of obligations.

Accommodations, will or course, need to be made in terms of the requirements based on further factors. While general obligations across these classifications will be fairly consistent details will vary to accommodate the different types of transactions and varying nature of the information. All relationship service providers have obligations of due care and security, but the nature of that care and level of security has to be appropriate to circumstances. Thus the provider that posts a resume as part of a relocation service may be reasonable in taking different precautions to secure information than the medical practitioner exchanging diagnosis information with a hospital. Thus one of the critical features of the contractual framework is appropriately linking the "Who" with the "What".

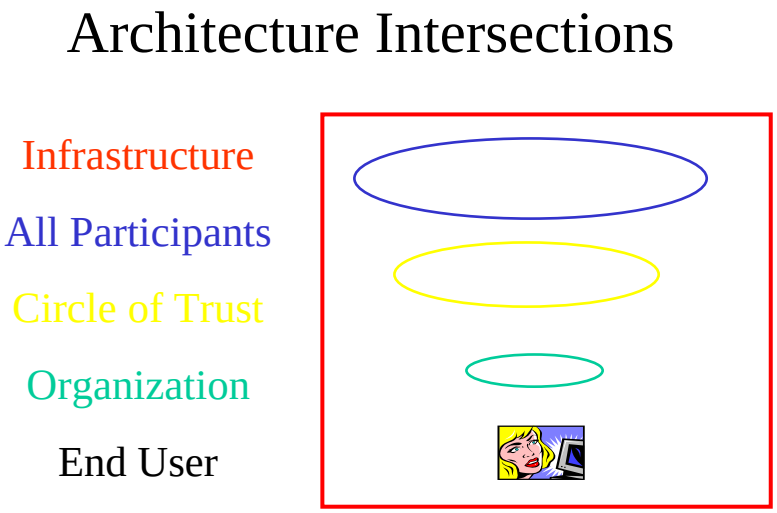
3.4 Defining the "What"

Once the parties have been identified and categorized it is important to understand their functions, rights and obligations. This will constitute the "What". For the purposes of the initial contract framework, we will presume a centralized TAS^3 trust infrastructure because the contractual framework in this situation is the most complete of the three possible architecture scenarios[xv].

All parties need to be contractually bound in order to assure that rights and obligations can be properly enforced. As in the credit card situation there are limited responsibilities on the end-user and increased responsibilities placed on those with greater control. This association between obligation, risk and control is captured in the OECD Guidelines for the Security of Information Systems and Networks[xvi] principle on responsibility:

> ***All participants are responsible for the security of information systems and networks.***
> Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. They should be accountable in a manner appropriate to their individual roles. Participants should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design and supply products and services should address system and network security and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.

There are some general architectural considerations that we need to consider prior to looking at the various obligations. The following diagram is informative in placing these obligations in context:



There are two kinds of obligations that need to be considered at all levels of the architecture above the end-user. Each group has both public-facing requirements and internal operational requirements. External requirements include privacy policies and other aspects of disclosure which are either legally mandated or discretionary and which enable persons/groups considering affiliations or transactions with the group to make informed decisions. It is in the nature of the obligations that they are natural subsets of each other. The exact dimensions of the concentric ovals will vary according to the type of participation or organization.

There is no fixed formula for the organizational dynamics of an infrastructure or ecosystem. There may be various networks of organizations that associate to create the infrastructure. The subsets of organizations are represented in our architecture chart by the term “circles of trust” most commonly used by the Liberty Alliance to refer to groups of similarly interested companies that interact or transact according to common rules.

The foundation of any ecosystem is predicated on rules established at the infrastructure level, which are subsequently bound, where appropriate and relevant, to all participants. The internal/operational elements of the infrastructure are the same as the requirements placed on participants with two exceptions. The first is the need for a compliance/oversight mechanism defined at the infrastructure level (though implemented, as appropriate, across all levels) and the second is the need for external facing documents described above. These are needed to satisfy some of the notice requirements inherent in privacy laws. In defining infrastructure requirements, and the requirements that may be imposed on other participants, subgroups will also need to create public facing as well as operational documents. Depending on the organization of the infrastructure, these may either require adoption of the pertinent parts of the infrastructure documents and procedures, or it may enable groups and organizations to develop or use their own policies and procedures that are consistent with the notice and operational requirements that apply to them. The latter course of action is more likely where existing organizations join communities of trust, or where existing communities of trust are merged together.

Service Provider (organizational) Obligations: While the focus on these comments will be on service provider/organizational obligations, they may also be applied to communities of trust and all participants except the end-user. While actual contract instruments will need to be tailored to the role of the service provider, some basic questions arise as to what infrastructure and policy requirements should be binding. A framework should consider whether the following list of major issues should be required, or at a minimum be addressed in some way:

- Use of up-to-date Anti-virus/ Spyware/ Malware detection systems
- Spam filters (may need to define settings to assure that legitimate mail is not suppressed)
- Penetration testing (may only be appropriate for largest players)[xvii]
- Encryption
  - In transit
  - At rest
- Security polices
  - Physical
  - Logical
  - Administrative
  - Separation of Duties
- Privacy policy
  - With specific obligations to honor preferences and negotiated obligations of end users
  - Notice
- Complaint handling policies / mechanism
- Compliance processes/officer
- Contact points
- Internet Access and Use Policies
- Training
- Code of ethics
- HR Policies (related to vetting of employees that have access to personal information to the extent permitted by law)
- Service Level Agreements
- Breach Notification
- Disaster recovery / Business continuity plans/exercises
- Audit/oversight
- Exceptions and Emergencies handling polices
- Government/Law Enforcement obligations/request for information policies
- Third party agreements' obligations/requirements clauses

These issues may be addressed in a number of ways. There may be a centralized policy of the infrastructure, which is deployed by all parties or there may be a model infrastructure, which parties' conform to as needed. The latter may be demonstrated by attestation or certification. Depending on the role of the service provider, some or all of these issues will be relevant, which is why the identification of functions in the who portion of the framework inquiry is so important. Understanding the nature and sensitivity of the information in question, the type of control or processing exercised and responsibility of the organization for compliance and oversight will help determine which of these factors should be binding and how.

End User Obligations: The pertinent question to ask is: what is the appropriate set of responsibilities for the end-user of the system? The end user is likely the person with the least technical knowledge, is highly vulnerable to attack at the system level, and has a high potential for compromise of his home system[xviii]. While any contract will have boilerplate

language about the need to use the service for only those purposes specified as legitimate and may have some penalties for knowingly using the system in contravention of those purposes or otherwise knowingly causing harm (spam, hacking into other accounts, defamation…) a question arises as to whether there should be some specific system requirements on the end-user that could include virus and other basic security protections. This is a final choice of the system implementers. It could either be in the contract or a requirement of the system use, for example, to log in either once or periodically. The contract terms may provide for attestation by the user of deployment of proper technologies; perhaps even types (not brands) specified by system infrastructure or may request permission to scan the system for installed software (at the directory tree level this can be done with little chance of privacy intrusion if the information is not maintained beyond the check) or may require a remote scan for viruses before allowing connection. The system will also likely check e-mail traffic for viruses and malware which provides another method for monitoring possible infection.

End User Rights: With the exception of forced virus protections, if adopted, the TAS^3 infrastructure is likely to have similar or fewer obligations on the end-user to most transactional contracts. Where TAS^3 will vary significantly is in the rights made available to the end user to control the use and sharing of his personal information. Within the TAS^3 architecture, the end user will be granted fairly granular control over the use and sharing of his personal information. The fact that TAS^3 establishes trust at the infrastructure level means that controls of the end-user will be applicable throughout the organizations participating in the information, not just the one that the end-user is in contact with. This is where appropriately defining the roles of technology, policy and contractual framework are most important.

In providing end-users with control, concepts of usability and experience must be kept in mind. How much control is enough? End-users are likely less suited to micromanaging technology specifics and may not be experienced in choosing certain professional support services. If the end user is charged for service provision e.g. resume preparation by a placement service, the end user would have no ability, and should have no ability, to determine which payment clearing service is used by the service provider, but does have the right to know that the processing is taking place and that it's being done legally and securely.

Certain issues of infrastructure are likewise beyond the scope of end user determination. The infrastructure must determine the level of transport speed and encryption that is appropriate. It is impossible for certain architecture elements to be recalibrated for every transaction. End-users have rights to know some of these parameters through a disclosure statement, and may be able to choose between security levels and privacy options in profile parameters, but they cannot create a completely individualized infrastructure at the architecture level.

Lastly, TAS^3 technology enables a user to create choices of privacy preferences related to use and sharing of information by creating rules, which we shall call personal policies. Organizations will also be able to create organizational policies. The TAS^3 infrastructure has both a discovery and negotiation function, which can include trust agents like reputation engines, to match and mediate between individual and organizational functions in order to assure that individual controls and preferences are respected. As other organizations are included different technologies may also be used to help assure that obligations are maintained. In the early stages of deployment, these continuing information flows may need to be supplemented by manual processes, which need to be considered in the contractual framework.

This blending of technology and contract framework creates a more streamlined and effective solution. Individuals and organizations are bound to their polices and the negotiation between them. The contractual framework, that includes all parties, binds all the parties to respecting both their policies and the obligations inherent in the negotiated outcomes. This is

the easiest way to address the variety of controls that are available to end-users while not requiring the end-user to become an expert in the technology or its operation, beyond the user interface. All of us use credit cards, but few of us understand the complex technology involved in payment clearing.

The role of ontologies: As part of the "what" there must be an agreed upon specification of terms both as neutral definitions and as used relationally. TAS3 will develop a privacy ontology to help create both privacy definitions and rule sets related to the use of the terms. An ontology, more broadly,

> …defines a set of representational primitives with which to model a domain of knowledge or discourse. The representational primitives are typically classes (or sets), attributes (or properties), and relationships (or relations among class members). The definitions of the representational primitives include information about their meaning and constraints on their logically consistent application. … Ontologies are typically specified in languages that allow abstraction away from data structures and implementation strategies; in practice, the languages of ontologies are closer in expressive power to first-order logic than languages used to model databases. For this reason, ontologies are said to be at the "semantic" level, whereas database schema are models of data at the "logical" or "physical" level. Due to their independence from lower level data models, ontologies are used for integrating heterogeneous databases, enabling interoperability among disparate systems, and specifying interfaces to independent, knowledge-based services. [xix]

Within TAS^3 ontologies play both a definitional and relational role. The privacy ontology will help model the overall privacy rules of the system. While the definitional nature of privacy terms[xx] can be created based on legal requirements of the region and sector, the relational requirements need to be based on well-defined relationships and responsibilities. A natural language translation tool that allows greater user control over the policy terms and conditions, which can be expressed in plain English, will make the ontologies and rules more user-friendly[xxi] whilst ensuring the user's policies are converted correctly into machine understandable rules.

3.5 Defining the "How"

As was highlighted earlier in the paper, TAS^3 will rely on a contractual infrastructure that provides proper binding of rights and obligations across all parties. The contractual infrastructure will need to be multilevel by definition: at the individual, organization/community and infrastructure level. It should be of little surprise that each of the architecture levels has appropriate binding. Master agreements will give rise to obligations that cascade down and are further specified. The granularity of bindings will also attach to sticky polices which provide the most granular operational controls. This is an essential summary of the contractual operations. Further specification of the allocation across technology, policy and contract will need to occur before the granularity of operations can be detailed. Other aspects of contract operation, which need to be supported by technology include: the ability to appropriately version and associate contract terms with transactions/interactions as well as the need to archive these terms.

At this juncture, however, it is useful to assure that we limit the boundaries between contract operations and user choices. An example may be informative. The TAS^3 infrastructure utilizes tools such as reputation engines which enable end-users to help select service providers either directly or through more automated means whereby reputation indicators will be required as part of a profile or discovery process. In either case, the choice of provider is part of the subjective nature of the system that reflects user control. The legal/governance framework is responsible for helping require that: providers post true and correct information; system parameters and legal frameworks are respected; that obligations are maintained; and that consequences exist for failures. The contractual framework supplements and informs trust negotiation, but neither controls nor replaces it.

3.6 Next steps

As case studies are further elaborated with greater detail relating to the roles and their interactions, and as the capacity of the technology and details of the polices are further elaborated, it will be possible to develop the actual contractual terms as well as populate the privacy ontology. These elements will then form the overall Governance Framework.

4 Annex

4.1 Figure 1 Core of PCI DDS

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

Build and Maintain a Secure Network
Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data
Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program
Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications

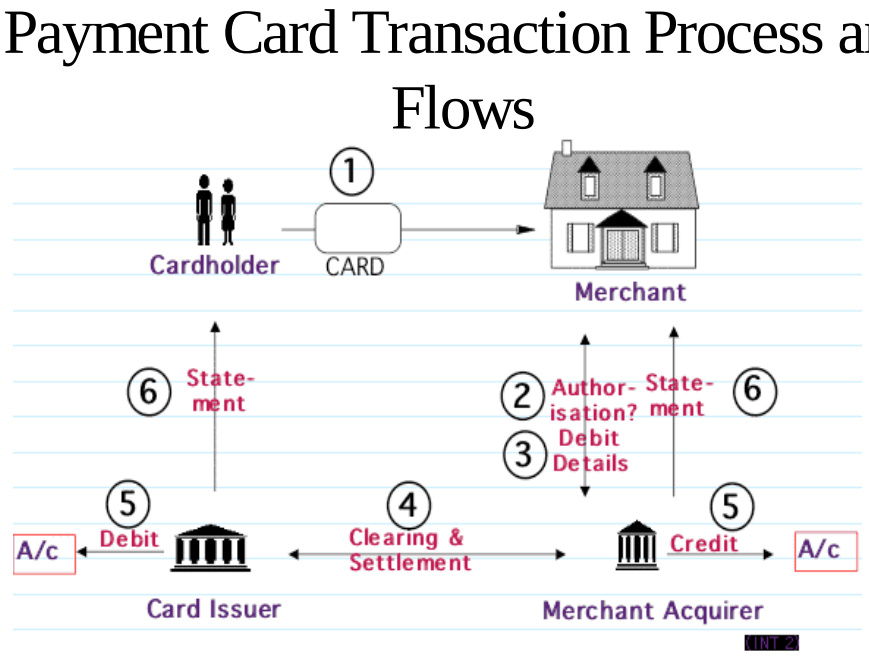
Implement Strong Access Control Measures
Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks
Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

Requirement 12: Maintain a policy that addresses information security

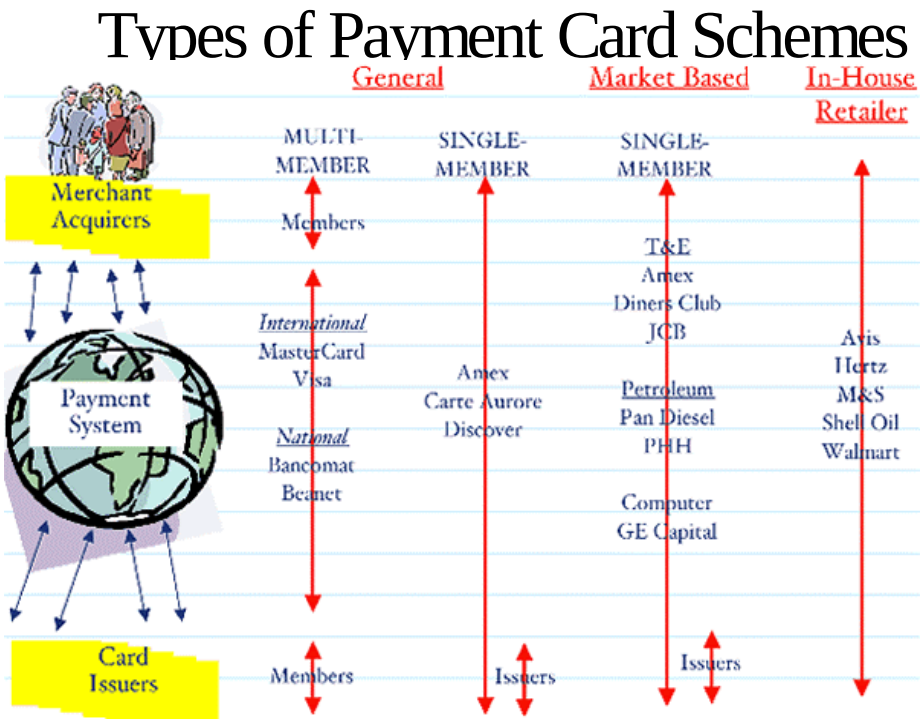
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

4.2 Figure 2: Payment Card Transaction Process and flows



.gtnews.com/paymentcards/paymentcardsguide1.cfm

4.3 Figure 3 Types of Payment Card Schemes



www.gtnews.com/paymentcards/paymentcardsguide1.cfm

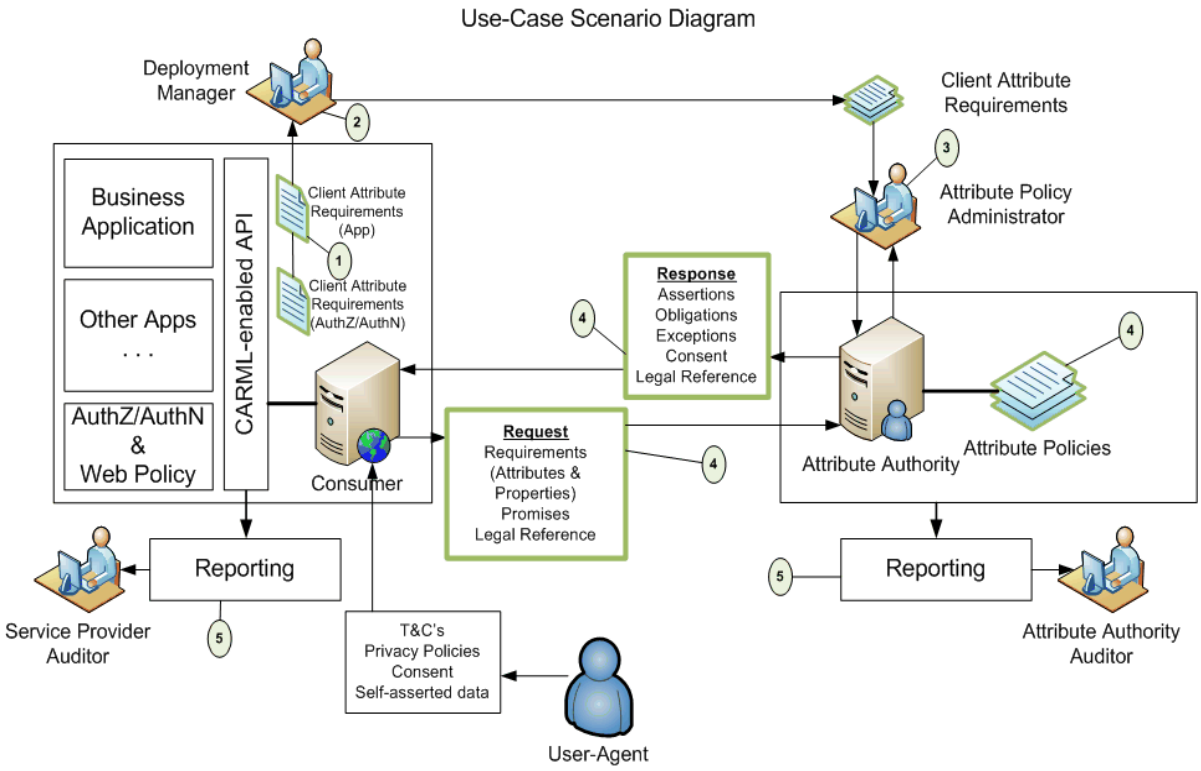
4.4 Figure 4 Payment Card Scheme Scale and Coverage

Payment Card Scheme Scale and Coverage (End 2003)

	Visa	Master Card	American Express	JCB	Diner's Club
Members	21,000	21,000	1	44+	60
Countries	180+	180+	150+	145	175+
Acceptance Locations	21.6m	22m	8.3m	11.4m	8.4m
ATMs	800k+	750k+	200k+	220k+	162k+
Cards Issued	1,208m	632m	60.5m	49.6m	8.6m
Purchase Transactions	30bn	13.1bn	3bn	0.4bn	0.14bn
Purchase (US$) Volume	$1,892bn	$891bn	$351bn	$40.5bn	$29.5bn

http://www.gtnews.com/paymentcards/paymentcardsguide1.cfm

4.5 Figure 5 Use-Case Scenario Diagram



In the diagram, above, the relationships between the deployed application environment, the attribute authority, and the end-user are shown:

1. Developer – the developer declares the attribute requirements of the application.

2. Application Deployment Manager – determines how attributes will flow to/from the application, what information is gathered directly from the user under what Ts and Cs, and what information will come from back-end systems and federated partners.

3. Identity Services Manager/Attribute Authority Manager – Attribute authorities are contacted for permission to use information by providing an appropriate declaration. If the Attribute Policy Administrator approves, then the attribute policy for the Attribute Authority can be revised to enable access by the client business application.

4. Client application – Access identity information sources using CARML declarations and AAPML policy enforced providers.

5. Audit Reporting – Auditors on both sides audit the consumption and publication of identity-related information.

Liberty Alliance: An Overview of Id Governance Framework v1.0

www.projectliberty.org/liberty/content/download/3500/23156/file/**overview-id-governance-framework-v1.0**.pdf

4.6 Figure 6 Definitions

Article 2 Definitions

For the purposes of this Directive:

(a) 'personal data 'shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b)'processing of personal data'('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d)'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h)'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

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.

Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31.

Data Protection Act Definitions

Data Controller

A Data Controller either alone or jointly with others determines the purposes for which data is to be used. If you wish to use data for a new purpose you should seek guidance from the Head of Information Compliance & Policy.

Data Processor

Any person or organization (other than an employee of the data controller) who processes the data on behalf of the data controller. An example of this might be a payroll bureau.

Data Subject

The living individual to whom the data relates who is therefore the subject of personal data.

Personal Data

Data relating to a living individual who can be identified from the information, or any other data likely to come into the possession of the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Processing

The collecting, amending, augmenting, deleting or re-arranging of the data or extracting information by means of reference to the data subject to whom they will/may be disclosing. Basically anything that can be done with data!

Sensitive Data

The Act introduces categories of sensitive personal data, namely, personal data consisting of information as to:-

- the racial or ethnic origin of the data subject,
- their political opinions,
- their religious beliefs or other beliefs of a similar nature,
- whether they are a member of a trade union,
- their physical or mental health or condition,
- their sexual life,
- the commission or alleged commission by them of any offence, or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Where such data is being processed not only must the controller meet the requirements of the Principles and Schedule 2, but processing is prohibited unless at least one of the conditions in Schedule 3 can be satisfied. The explicit consent of the individual will usually have to be obtained before sensitive data can be processed unless the controller can show that the processing is necessary based on one of the criteria laid out in Schedule 3 of the Act.

Subject Access Request

Every living individual has the right of access to personal data held about them by City University and to be informed whether personal data of which that individual is the data subject are being processed. This is known as a SAR (Subject Access Request)

Third Party

Any person other than the data subject, the data controller, any data processor or other person authorised to process data for the data controller or data processor.

City University of London – Data Protection Act Definitions -
http://www.city.ac.uk/ic/dataprotection/dpadefinitions.html

Document Control

Amendment History

Version	Baseline	Date	Author	Description/Comments
0.1		28-11-2008	Joseph Alhadeff	First draft
0.2		12-12-2008	Joseph Alhadeff	Draft
0.9		31-12-2008	Joseph Alhadeff	Comments of reviewers incorporated
1.0		31-12-2008	Theo Hensen	Deliverable in template TAS3

5 End notes

[i] It should be noted, however, that sectors and jurisdictions have variances in their legal requirements, which must be addressed in the contractual framework as applied.

[ii] The concept of PII or personal or private information does not refer only to the person's name, but also includes information associated with the name or from which the person's identity may be derived.

[iii] http://www.projectliberty.org/

[iv] www.projectliberty.org/liberty/content/download/3500/23156/file/overview-id-governance-framework-v1.0.pdf

[v] www.projectliberty.org/liberty/content/download/2962/19808/file/Liberty%20Legal%20Frameworks.pdf

[vi] http://idmashup.org/schedule/conferencesession.2006-06-12.7080164057/conferencefile.2006-06-16.0742495181

[vii] https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml

[viii] https://www.pcisecuritystandards.org/security_standards/ped/index.shtml

[ix] Less attention will be paid to the Where in this process because the projects have been limited to a defined group of jurisdictions. As TAS 3 deploys in greater scope this issue will become more important, but even our limited country scope should prove informative for purposes of developing a contract framework.

[x] The challenge is less in the actual binding since that will be done at a higher level, but rather is in the situation where an end-user claims the negotiated outcome was not consistent with his preferences and to demonstrate in court the operation of the system and legal chain of obligation through the operation of the application.

[xi] **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; http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf**

[xii] These rules will also help inform requirements between actors depending on role. They will likewise be useful in developing/reviewing the privacy ontology.

[xiii] The Data Protection and Electronic Communications Directives of the EU are currently under review and the implications of new systems on these definitions and their possible revision should be taken into account.

[xiv] A novel issue enabled by technology , which is beyond the current scope of TAS^3 consideration, but which may have relevance for future iterations is how to deal with individuals that become part of transactions in a non-commercial fashion. Through social networking and other participative web technologies individuals may participate in transaction either as pats of communities of trust, reputation engines, referral sources or any number of ways that we can even imagine today. Those individuals and their actions may have significant impacts on the privacy, security and trust infrastructure, but because of their noncommercial nature, may not be contractually bound to any

obligations. Legal frameworks currently in place are not designed to address their roles or actions beyond concepts of defamation and libel.

[xv] See Page Three for discussion of architecture options

[xvi] http://www.oecd.org/dataoecd/16/22/15582260.pdf

[xvii] Will likely require consent of the party being tested and may require reasonable notice to avoid potential disruption to business if a real attack were perceived.

[xviii] Recent press releases from Panda Security and Symantec suggest that home computers that are infected and part of botnets are significantly on the rise. Various reports also suggest that more that 23% of home computers are infected with one or more viruses.

[xix] Gruber, Tom, Ontology; to appear in the Encyclopedia of Database Systems, Ling Liu and M. Tamer Özsu (Eds.), Springer-Verlag, 2008. http://tomgruber.org/writing/ontology-definition-2007.htm

[xx] See figure 6 for privacy definition examples from the EU and UK

[xxi] Plain English in this case refers to the use of plain language, but certain expression formats are required in order for terms to be properly parsed.