SEVENTH FRAMEWORK PROGRAMME
Challenge 1
Information and Communication Technologies

Trusted Architecture for Securely Shared Services

Document Type: D6.1-2 supplement

Title: **Practitioner's guide to the Legal and Policy handbook for TAS³ implementations**

Work Package: WP6

Deliverable Nr: N/A

Dissemination: Final, public

Preparation Date: May 24, 2012

Version: 1.0

The TAS³ Consortium

	Beneficiary Name	Country	Short	Role
1	KU Leuven	BE	KUL	Coordinator
2	Synergetics NV/SA	BE	SYN	Partner
3	University of Kent	UK	KENT	Partner
4	University of Karlsruhe	DE	KARL	Partner
5	Technische Universiteit Eindhoven	NL	TUE	Partner
6	CNR/ISTI	IT	CNR	Partner
7	University of Koblenz-Landau	DE	UNIKOL	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	S&T Coordn
12	EIfEL	FR	EIF	Partner
13	Intalio	UK	INT	Partner
14	Risaris	IR	RIS	Partner
15	Kenteq	NL	KETQ	Partner
16	Oracle	UK	ORACLE	Partner
17	Custodix	BE	CUS	Partner
18	Medisoft	NL	MEDI	Partner
19	Symlabs	PT	SYM	Partner

Contributors

	Name	Organisation
1	Joseph Alhadeff	ORACLE
2	Brendan Van Alsenoy	KUL (ICRI)

Contents

1. Introduction

The Trusted Architecture for Securely Shared Services (TAS³) provides a technical architecture which enables the secure exchange personal data in a compliant manner. The combination of security and privacy functionalities in TAS³ serves to build trust among both users and providers of services. In order to provide end-to-end assurance of these properties, however, a legal and policy framework had to be developed to address the protection of information beyond the technical operations of the TAS³ architecture.

This framework was developed in TAS³ deliverable D6.1-2 ("Legal and Policy handbook for TAS³ implementations"). The following sections provide a practitioner's guide designed to supplement this framework. It is geared towards legal and policy practitioners that would be supporting either

(a) the organizers of a TAS³ Trust Network in developing the appropriate law and policy frameworks; or

(b) any organization that is considering to join an established TAS³ Trust Network.

This guide starts with an overview of the foundations of the TAS³ governance framework. It then sets forth a section-by-section guide which explains the various components of the Legal and Policy Handbook. Finally, this guide also contains an index intended to facilitate the reader's access to specific components of the Legal and Policy Handbook.

2. Foundations of the TAS³ governance framework

The Legal and Policy Handbook of TAS³ provides a governance framework that both enhances trust and facilitates the responsible exchange of information. Early in the development of TAS³, we recognized the need to work across people, organizations, processes and technology in order to create such a governance ecosystem.

TAS³ allows to co-ordinate the development of contract, policy, technology and business requirements in a manner which improves on existing models of privacy by design (which are often limited to embedding privacy technology at the design stage). This broader and earlier collaboration across the 4 elements mentioned above creates a more seamless support for privacy, which in turn enables and enhances trust for data subjects. In many design and development situations the interdependent nature of the 4 elements is insufficiently optimized. In TAS³, information collection, access and transfer proceed in accordance with data minimization; legal and compliance obligations are supported in

audit protocols[1], and mandatory enterprise policies supplement security, use limitation, and other data protection requirements. This optimization also occurs at the level of the ecosystem rather than just at enterprise/organization level, thereby providing more seamless and end-to-end integration of requirements across the 4 elements of the Trust Network.

The collaborative development of technical, policy, business and legal requirements provides a more seamless and trustworthy end-to-end architecture that enables greater compliance with privacy. Greater compliance with privacy is accomplished in mainly two ways: by taking a collaborative ecosystem approach and by providing technical means to help ensure that users' privacy preferences are enforced throughout the ecosystem. The result is a user-centric architecture that enhances privacy and security through its integrated technical, policy, business and legal requirements.

2.1 End-to-End Accountability

The development of a trustworthy ecosystem requires assurance that all participants (1) have the capacity to comply and (2) are appropriately bound to their obligations. These two concerns are also the main components of an increasingly recognized approach to data protection – accountability.

Within TAS[3], a participant's capacity to comply shall be demonstrated during an **intake process** which requires inquiry into and disclosure of practices, policies and technical implementation for service providers as well as clear acknowledgement by all participants/organisations of expectations and obligations. The disclosure of practices, policies and technologies is an important element in the evaluation of prospective service providers to assure that they can meet TAS[3] requirements[2].

The demonstration of capacity to comply is important because data may need to be stored outside of the TAS[3] technical infrastructure once a transaction has been completed[3]. As a result, its protection may no longer be technically enforceable by means of the TAS[3] technical architecture. Validating participant's capacity to comply is the only way to provide end-to-end assurance of compliance. Combining the evaluation of the entire operation of a service provider with the transactional security and integrity

[1] Obviously recourse to national data protection authorities and courts always remains possible in case of non-compliance. TAS[3] however also seeks to provide the data subject with more simple paths to compliance enforcement that can be accomplished entirely from within the TAS[3] Network.

[2] The information provided in this intake process will also be of importance to the developing role of a next generation of reputation engines. As part of this intake process, prospective candidates are requested to offer proof to substantiate their answers to questions posed about their practices, policies and operations. The greater the detail and validated nature of the proof, the higher the relative trust score might be.

[3] Legal compliance, audit and non-repudiation are just some of the operational rationales for maintaining records of various transaction elements.

assurance of the TAS³ technical architecture, creates a much higher level of assurance of compliance.

Accountability also requires enforceability of legal obligations. In TAS³, operational compliance supported by a **contractual framework** which binds all parties to their respective obligations. This same framework also creates a governance infrastructure for the whole ecosystem which supports verification of operational compliance through inter alia the Accountability and Oversight Committee investigations and the auditing of noncompliant behavior.

All systems require its participants to place some level of trust in each other. The more trustworthiness can be established through demonstration and validation of practices, the lower the risk of participation and the greater the likelihood of adoption. As was highlighted above, these concepts of mutual trust are supplemented by controls and demonstrable accountability mechanisms which take many components to the higher level of assurance that can exist when, as in the case of TAS³, you both *trust and verify*.[4]

2.2 Demonstration of the capacity to comply

2.2.1 End-user Intake Process

The end-user intake process binds individuals to minimal obligations through the execution of an End-User License Agreement (EULA), which also provides the user with contractual privity to the organisations participating in the TAS³ Trust Network. This ensures enforceability of individual rights against potential wrongdoers or negligent actors within the system.

Other essential elements of the end-user intake system are more operational in nature. During the registration process, the identity of then end-user is verified and bound to a TAS³ recognized credentials. Once registration is completed, a dashboard service provider is selected and an account is provisioned to serve as the user-centric / user driven control interface to TAS³.

Finally, the end-user is required to make choices among privacy and trust preferences. Because of the attempt to provide a flexible and very customized experience for each user, and because of the variety and sensitivity of personal preferences related to employment and health information, we require individuals to make personal privacy choices as opposed to merely setting defaults. That being said, defaults are maintained through the TAS³ architecture and policy controls that prevent lowering of security standards and requirements that TAS³ service providers adhere to legal and contractual obligations related to the protection and use of personal data.

[4] It should also be noted that individual end users of TAS³ (data subjects in privacy parlance), are also required to participate in an intake and contractual process. For individuals, the intake process is geared more towards awareness and de minimis obligations regarding proper use of the system. In addition, the intake process helps ensure effective credentialing and notice of privacy practices and envisaged uses of information.

2.2.2 The Service Provider Intake Process

The Service provider intake process is, as one would expect, more rigorous, tied to more substantial obligations and requires both greater effort and proof. Experience of trust/evaluation programs has demonstrated that organizations need to consider their application for membership/review in the proper context. Thus TAS³ provides guidance that sets forth the minimum policies, requirements and expectations of TAS³ membership. Once the organization has reviewed these materials, they are invited to fill out an accountability questionnaire relates to their capacity to fulfill privacy, security and technical requirements. This is the self-assessment/disclosure phase of the process. This process is then followed by a validation of the ability of the prospective service provider to meet specific privacy, security and technical requirements of TAS³. While we hope this to be a one step process, it may be iterative should insufficient demonstration of a capacity to comply be demonstrated. This phase is this called the Gap Analysis as it serves to identify potential gaps between the prospective service provider's technical and policy infrastructure with TAS³ requirements.

Once these intake process elements are satisfactorily completed, the service provider is invited to execute the TAS³ participant contract to become a recognized TAS³ service provider.

2.3 The TAS³ Contractual Framework

As noted above, the end user is bound to and gains privity with the contractual ecosystem via the EULA. The overall contractual framework is somewhat more complex as it not only creates legal binding but also underpins a governance infrastructure.

The TAS³ Ecosystem consists of three layers. Each layer is governed by an overarching set of rules, policies and procedures which must be complied with in order to render implementations of TAS³ trustworthy.

The following three layers can be distinguished[5]:

1. the TAS³ **governance layer**: this is the layer where the rules and policies of the TAS³ Trust Network are established;

2. the TAS³ **administration layer**: this is the layer where the rules and policies which have been established for the Trust Network are enforced;

[5] This representation of the TAS³ Ecosystem is an adaptation of the model found in the draft 'National Strategy for Trusted Identities in Cyberspace', which was issued by the US Department of Homeland Security (DHS) in June 2010 (full text available at: http://www.dhs.gov/xlibrary/assets/ns_tic.pdf) . Kindred models have been elaborated by other bodies such as the Kantara Initiative (see http://kantarainitiative.org/confluence/display/GI/Identity+Assurance+Framework+v2.0) and Microsoft (see the Open Identity Trust Framework [OITF], available at http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/oitf.aspx) which have also served as a source of inspiration.

3. The TAS³ **operational layer**: this is the layer where transactions occur in accordance with the rules of the Trust Network.

Each layer of the **TAS³ ecosystem** comprises a number of actors, which each have their own roles and responsibilities. The following figure provides a conceptual overview of the types of entities that operate on each layer:

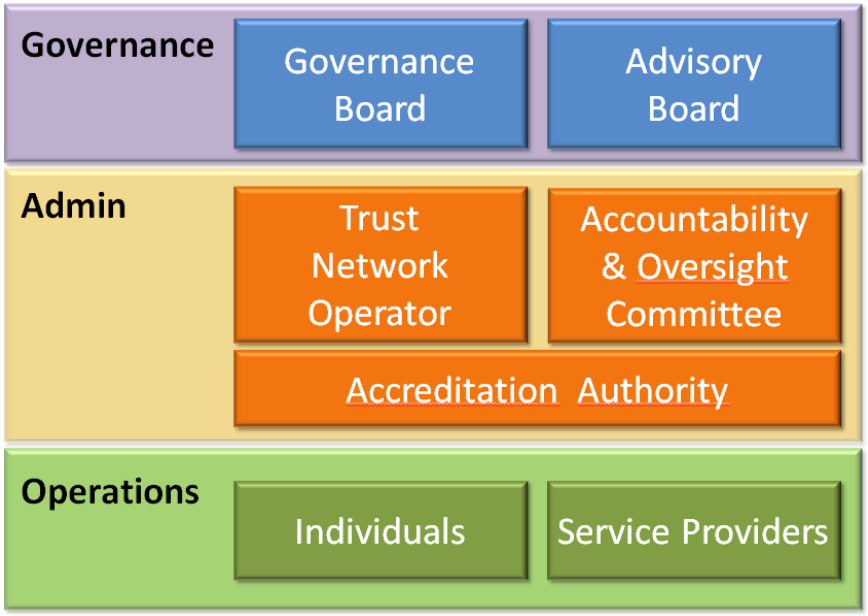

Figure 1 – Layers and Actors of the **TAS³** Ecosystem

The three layers of the TAS³ ecosystem are each covered by separate, but interactive contractual elements, that work together and in conjunction with the EULA to both create a binding of obligations across parties and define lines of oversight and responsibility.

At the highest level is the **Trust Network Agreement**. The founders of a federation can organize themselves under a variety of models, among which the three models identified by the Liberty Alliance: Collaborative, Consortium and Centralized models.[6] Once the founders have decided upon & agreed to an organisational model, they will then need to define how the Trust Network will be governed and operated.[7]

The Trust Network Agreement (TNA) is the contract among the founders that establishes the Trust Network and its organisational structure. The TNA further establishes, at a principal level, the operating rules for the Trust Network as a whole, as well as the roles, responsibilities and interactions among the top level administrative and governance bodies including: the (1) Governance Board, the (2) Trust Network Operator (and through it (3) the Accreditation Authority), (4) the Accountability and Oversight Committee, and (5) the Trust Network Advisory Board.

[6] See section 5.2.1 of part I.
[7] The organisational model that is chosen will have significant impact on the allocation of responsibilities and definition of how both power and obligation are actually apportioned.

The TNA creates the overall governance infrastructure onto which the more operational elements of the system must be specified. The general specification of overall operating rules occurs in what we call the Ecosystem Contract. The Ecosystem Contract (EC) is the contract which binds all Service Providers joining the Trust Network to their general obligations as participants of the Trust Network.

The **Ecosystem Contract** (EC) builds upon and must always remain consistent with the Trust Network Agreement. The EC must be formally adopted and approved by the Governance Board (GB).[8] Where the TNA has a more structural function (setting up the Trust Network, defining the roles and responsibilities of the major players in governance and administration and the general rules of TN operation), the EC supports the structural components of the TNA by binding all parties to more detailed statement of obligations and implementation of TN Policies as well as the high-level rules of the TN. In other words, it is an operational document that contains the general requirements related to transactions that take place within the TAS[3] ecosystem.

It should also be noted that the EC serves as the central repository for obligations, the myriad references to policies are references to documents either annexed or incorporated by reference. The drafting structure foresees potential for changes in policy to occur on a more frequent basis that revision of the contract.

TAS[3] encompasses a number of different service providers that may have special requirements related to their functions. These requirements are specified as needed in **Participant Contracts** which are specific to the role of the service provider.

Finally, **transaction level contracts** provide an opportunity to supplement or enhance controls and obligations in relation to a specific a transaction. Additional obligations can be put in place at the technical level through sticky policies and other privacy management and negotiation tools of the architecture. Since these obligations are expressed through technical means, they may never be explicated in writing, but they are explicitly supported and accepted by the parties as binding through agreement to the Ecosystem Contract.

This cascading contractual ecosystem helps provide both operational compliance and a basis for enforcement and redress by establishing and binding each party to their obligations. These contracts also provide for a liability and partial indemnity schema to help assure credible action can and will be taken in light of complaints.

[8] While in practice the Ecosystem Contract may be drafted by the TNO, it requires approval by the Governance Board.

3. How To Use The Legal and Policy Handbook: A Section by Section Guide

The Legal and Policy Handbook is set forth in Parts and numbered chapters. The First two parts – 'Privacy Fundamentals' and 'Legal Requirements and Policy Considerations for TAS³ Implementations' set the scene for the privacy and policy issues that need to be considered by the practitioner. They are up to date to the end of 2011. In this guide we also highlight some evolving issues that have resulted from more recent policy and legislative developments.

The Third and Fourth Parts, 'From Theory To Practice' and 'Implementing the Contractual Framework' are more practically oriented and set forth the essentials of a TAS³ implementation. A final part which is entitled Epilogue: Delivering End-to-End Accountability goes into further detail on the 'lessons learned' from developing the TAS³ Legal and Policy Handbook: specifically, how the interrelation between technology, policy and contracts is supporting an end-to-end trust ecosystem.

Finally, a number of useful annexes are set forth with supporting materials. In order to enhance ease of use, we have included an Index at the end of this Guide to highlight and reference the main tools and points of reference that are set forth throughout the Handbook.

Part I: Privacy Fundamentals

While the Legal and Policy Handbook was developed for those experienced in law and/or policy, it does not presume detailed knowledge of privacy or the creation of trust networks. To that end, the first part of the Legal and Policy Handbook addresses the fundamentals of privacy and data protection. This section includes an overview and comparison of Fundamental Privacy texts from OECD, Council of Europe and EU (see Annex 1) and develops a set of Common Privacy Principles as well as an overview of common concepts and definitions. The Legal and Policy Handbook was drafted to address the needs of TAS³ implementations, but also recognized the state of privacy flux at the time of its creation in a section entitled 'Evolving Fundamentals'.

Policy and regulatory practice related to privacy and data protection are in an unprecedented state of evolution. The founding documents of privacy and data protection – the OECD Guidelines and the Council of Europe Treaty 108 – are both being reviewed and revised[9]. In the EU, the Data Protection Directive (Directive 95/46) is undergoing a major revision, being broken up into a proposed Regulation to cover most processing of personal information and a proposed Directive to cover law enforcement activities. In Canada, aspects of PIPEDA, the main Canadian Privacy legislation, are under review

[9] For OECD see: *www.oecd.org/sti/privacyreview* ; For COE see April revisions at: http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp

and the Federal Privacy Commissioner, in conjunction with the BC and Alberta Commissioners, has issued a paper setting out governance frameworks for accountable organizations[10]. In the Asia-Pacific, APEC has finished the major work on its cross-border privacy rules and is continuing work on interoperability – facilitating data flows between economies with different privacy frameworks, as well as understanding how to recognize compliance with other privacy requirements in partial or complete satisfaction of local requirements.[11] Thus any practitioner should take caution to consider how these changes may impact legal obligations, evolving trends and the requirements that should be incorporated into TAS[3] legal and policy frameworks.

While the part on Privacy Fundamentals is based on fundamental texts and established practices, it also recognizes the need to apply those practices and concepts in context in the section entitled 'Privacy and the Information Society in Context' (section 4). A major evolving trend and context for privacy over the last years is accountability – the need to develop, implement, support and enforce policies and practices that support compliance with legal obligations.

Important work is also being done in the development of policy and technical standardization of privacy. The Handbook covers both the work lead by the Spanish Date Protection Commissioner in developing an International Privacy (Policy) Standard and the ISO work on privacy standards. While formally the work on the Privacy Framework (29100) has been completed; it has yet to be meaningfully implemented or applied. Further work items are underway however. In light of the ongoing activities related to standards, practitioners are advised to monitor these developments as such standardization is likely to enhance both current and future interoperability across systems and policies.

Finally, the Privacy Fundamentals part ends with a section on Privacy and Technology which provides practical resources that consist of policy tools and principles related to the development and deployment of technical solutions. Topics include: privacy principles for identity management, concepts of privacy by design and default, privacy impact assessments (both as applies to a systems and across systems) and a privacy maturity model that can help organization benchmark where they are in a privacy development and maturity cycle.

---

[10] *Getting Accountability Right with a Privacy Management Program*, http://www.oipc.bc.ca/pdfs/public/Getting_Accountability_Right(Apr2012).pdf

[11] For a good overview see: Bruening, Paula: *APEC Passes Privacy Policy Milestones; New challenges await in 2012,* BNA World Data Protection Report, V12 No. 1, January 2012 http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/News/BNA_International_APEC_January_2012_Bruening.pdf.

Part II: Legal Requirements and Policy Considerations for TAS³ implementations

While Part I provided many of the theoretical underpinnings of privacy as, well as some of the policy tools related to organizations and systems, this Part was not geared towards implementation as such. Part II sets out more tailored legal requirements (see Annex 5 for a complete list of these TAS³ requirements) and drills down into the application of fundamental privacy principles such as notice, collection limitation/data minimization, access/correction, security, governance and compliance. The section then addresses the role of fundamental concepts to employment and health scenarios, applies some of the fundamentals such as accountability to TAS³ and begins to introduce important concepts of user orientation – user-centricity, data subject perspective and complexity of data flows.

Part III: From Theory to Practice

Part III provides step-by-step guidance for the creation of a TAS³ Trust Network. The first step is to identify and decide upon the initial actors/founders and organizational forms. Both the Liberty Alliance and The Credit Card Industry provided interesting organizational and contracting models setting forth possible constructs of hierarchy, control and obligation.

The section on 'Developing a Contractual Framework' introduces many of the basic concepts and organizational issues that will be encountered in contract formation. That being said, the entire process of consortia formation creates an issue of order and prioritization. As we discovered in the process of drafting the Legal and Policy Handbook, there is no magic order in formation. We have presented what we believe to be the most logical order, but practitioners should determine what issues to tackle in what priority and order in the context of the specific circumstances of their implementation.

In developing the contractual and governance framework; it is important to understand the nature and roles of the various potential actors – the "Who", from the founders of the Trust Network, through those administrating Trust Network policies until the service providers and users to whose these policies relate. To understand the potential compliance obligations of each actor; it is important to be able to identify them as controllers or processors of data. A substantial section is dedicated to addressing these roles, but practitioners should note that the new Draft Data Protection Regulation has introduced the potential for new obligations, so continued review is advisable.

Once actors are appropriately identified and categorized (recognizing that the roles may be context dependent and the same actor may take on different roles depending on context) certain obligation and requirements – the "What" – must be clarified. Issues addressed include: liability among the service providers and governance entities,

including concepts of insurance and some liquidated damages, security and architecture requirements as well as data protection, mandated disclosure and e-discovery requirements.

While the requirements are important, it is equally important to specify obligations in a way that participants can better understand their obligations. This is an important element of both user centricity as well as assuring that smaller, less sophisticated service providers are cognizant of their obligations. Thus in "Applying the "What" to the "Who" section, both end user and service provider rights and obligations are spelled out in an inclusive but high-level manner.

Establishing trust and credibility in a system is very important, and the need to assure that service providers can understand their obligations and demonstrate their capacity to comply with those obligations is an essential element of accountability. The section on "Defining the "How" sets forth the rationale of the intake process for organizations, which starts with a general guidance section, followed by a self-assessment questionnaire, gap analysis process and contractual binding of the parties. This section also outlines an intake process for end users which involves execution of an End User License Agreement (EULA) which provides the nexus between the end user and other participants to the TAS^3 consortium, binding all of them to the legal and consortia compliance obligations and enabling the end user to hold participating organizations accountable (even if they are not in direct contact with them). The completion of the intake process results in the creation of Dashboard account which is the end-user interface and central point of control.

The last section of Part III addresses the question of jurisdiction. While this work envisioned transfers within the EU, issues of jurisdiction and applicable law still exist. It should be noted however, that the EU Draft Data protection Regulation would be more harmonized by definition – Regulations unlike Directives do not need to be transposed into national law; and because the Draft Regulation introduces the concept of a lead authority which may further address jurisdictional complexity for the service provider and end-user.

Part IV: Implementing the Contractual Framework

Part IV reflects the most practical and operational section of the Handbook. The layers of the TAS^3 ecosystem are defined in layers addressing Governance, Administration and Operation. To form the appropriate governance structure, the practitioner is provided with information on developing a Trust Network Governance Board as well as a Trust Network Advisory Board to assure that external expertise is available to the Board.

Practitioners are then provided guidance on the development of an Administration layer that executes the requirements of the Governance Structure and oversees day-to-day operations. The Administration layer is comprised of the Trust Network Operator, the

TAS³ Accreditation Authority and the TAS³ Accountability and oversight Committee. Finally, the operational layer is defined, comprised of the end users and service providers including: Identity Providers and Attribute Authorities, Trust Network Infrastructure Service Providers, and Application-specific service providers.

After addressing the conceptual formation issues, Part IV focuses on the instruments and processes in the order that they need to be considered. The first topic to consider is the need for a Trust Network Agreement which creates a general rules and responsibilities of the consortia. The Intake processes are revisited again because of the need to understand how an organization's capacity to comply is evaluated. Their general obligations and operational requirements are set forth in the Ecosystem Contract which is also outlined in this section. Subsidiary to the general service provider obligations which are captured in the Ecosystem contract are participant contracts which are based on special processing operations or special categories of service providers. These contract concepts are set out as detailed outlines as opposed to specific forms because they need to be tailored to circumstances of the consortia and the specific roles of the actors.

In further support of informing all the parties of their rights and obligations, Part IV sets out the terms of the of the End User License Agreement and the Notice of Privacy Practices which better informs the obligations and expectations related to the services. Finally, Part IV sets forth frameworks for oversight and compliance.

Epilogue: Delivering End-to-end Accountability

This final section of the handbook, discusses in greater depth how technology, policy and law work together to provide end-to-end accountability. An important element of this analysis is how TAS³ as an architecture and policy solution maps well to evolving requirements of accountability. In order to address end-to-end accountability, this section also looks at user-centricity, employment and health as examples and how trust is supported in an end-to-end fashion. This section was set apart at the end of the handbook, because it reflects the lessons learned during the course of the developing TAS³ about how the various components (technical, policy, business and legal) can create a set of benefits that are greater than the mere sum of the parts.

4. INDEX

TAS³ Contractual framework

What is it?

The TAS³ contractual framework is the combination of legal instruments which ensure appropriate binding of TAS³ participants to TAS³ requirements and policies. It consists of:

- the Trust Network Agreement;
- the TAS³ Ecosystem Contract;
- TAS³ Participant Contracts; and
- TAS³ End-User and Licensing Agreements.

How should it be used?

The TAS³ contractual framework is intended to operate at three levels: Trust Network, Ecosystem and Transaction level (whereby the latter is supplemented by the technical architecture). The Trust Network Agreement (TNA) reflects the organizational model of the Trust Network and creates the general governance and oversight framework. The Ecosystem Contract deals with the operational rules of the implementation and provides the general binding of rights and obligations across all parties, including general terms and conditions, required technical implementations and requirements for policies at the level of individual organizations. The Ecosystem contract is executed in counterpart forms adapted to the role of each individual entity, but with large commonalities for the core aspects of the TAS³ Ecosystem. These counterpart contracts are referred to as TAS³ Participant contracts. The TAS³ Terms and Conditions is the counterpart of the Ecosystem contract for end-users, which outlines their rights and responsibilities and also provides them with privity of contract towards the other Ecosystem participants.

More detailed explanations regarding the envisaged use of each of the aforementioned instruments shall be elaborated over each of the following subsections.

Where can it be found in the document?

A detailed outline of Trust Network Agreement can be found in section 3 of Part IV (p. 163).

A detailed outline of TAS³ Ecosystem Contract can be found in section 5 of Part IV (p. 172).

A conceptual outline of TAS³ Participant contracts can be found in section 6 of Part IV (p. 181).

A reference template of the TAS³ End-User and Licensing Agreement can be found in Annex 7 (p. 268).

Trust Network Agreement (TNA)

What is it?

The Trust Network Agreement is the agreement through which the founding members establish a Trust Network and its organizational structure.

How should it be used?

The Trust Network Agreement (TNA) should be used to create the contractual underpinning of the organizational structure of the Trust Network. The TNA should further establish, at a principal level, the operating rules for the Trust Network as a whole, as well as the roles, responsibilities and interactions among the top level administrative and governance bodies including: the (1) Governance Board, the (2) Trust Network Operator (and through it (3) the Accreditation Authority), (4) the Accountability and Oversight Committee, and (5) the Trust Network Advisory Board.

The TNA creates the overall governance infrastructure onto which the more operational elements of the system must be specified. The general specification of overall operating rules occurs in what we call the Ecosystem Contract.

Where can it be found in the document?

A detailed outline of Trust Network Agreement can be found in section 3 of Part IV (p. 163). The various organizational models under which a Trust Network can be established are described in section 2.2 of Part III (p. 74).

TAS³ Ecosystem Contract (EC)

What is it?

The TAS³ Ecosystem Contract is the agreement between the Trust Network Operator and every entity offering services within the Trust Network that binds these service providers to the rules and policies that apply within the Trust Network.

How should it be used?

The TAS³ Ecosystem Contract (EC) should be used to bind all Service Providers joining the Trust Network to their general obligations as participants of the Trust Network. It is to be executed in counterpart forms through the TAS³ Participant Contracts which are tailored to the role of each service provider.

The EC should build upon and must always remain consistent with the Trust Network Agreement. The EC must be formally adopted and approved by the Governance Board (GB). Where the TNA has a more structural function (setting up the Trust Network, defining the roles and responsibilities of the major players in governance and administration and the general rules of TN operation), the EC supports the structural elements of the TNA by binding all parties to more detailed statement of obligations and implementation of TN Policies and high-level rules of the TN; it is an operational document that implements TN requirements related to transactions.

The EC should contain the common baseline of obligations among TAS³ participants. It must also contain third-party beneficiary clauses that will allow end-users to seek enforcement against service providers of their obligations under this contract.

Where can it be found in the document?

A detailed outline of TAS³ Ecosystem Contract can be found in section 5 of Part IV (p. 172).

TAS³ Participant Contract

What is it?

A TAS³ Participant contract is a contract which details the specific obligations of a service provider in light of its role within the Trust Network and the transactions it is likely to engage in.

How should it be used?

A TAS³ Participant Contract should be used as a role-based addendum to the TAS³ Ecosystem contract. It should contain the specific obligations of a service provider in light of its role within the Trust Network and transactions it is likely to engage in.

A TAS³ Participant Contract should also bind service providers to technical and policy requirements, both in terms of those expressed at the intra- and inter-organizational level as well as in terms of using the appropriate technologies to honour the preferences and choices of users as to use and sharing of personal information.

Transaction level contracts provide an opportunity to supplement or enhance controls and obligations in relation to a specific a transaction. Additional obligations can be put in place at the technical level through sticky policies and other privacy management and negotiation tools of the architecture. Since these obligations are expressed through technical means, they may never be explicated in writing, but they are explicitly supported and accepted by the parties as binding through agreement to the Ecosystem Contract.

Where can it be found in the document?

A conceptual outline of TAS³ Participant contracts can be found in section 6 of Part IV (p. 181).

TAS³ End-User and Licensing Agreement (EULA)

What is it?

The TAS³ End-User and Licensing Agreement is a contract between an end-user and the Trust Network Operator (TNO) which outlines the rights and obligations of the end-user as well as the warranties and disclaimers made by the TNO with regards to operations that take place within the Trust Network.

How should it be used?

Agreeing to the EULA is part of the intake process for end-users (registration phase), and is executed between the TNO and the prospective end-user. The TAS³ EULA should enumerate all those rights and obligations which remain consistent across TAS³ service providers. The EULA shall be supplemented by additional terms which govern the individual transactions of the end-user with participating service providers.

Where can it be found in the document?

The TAS³ EULA and its role is described in section 7.2.1 of Part III. A reference template of the EULA itself can be found in Annex 7 (p. 268).

The complete intake process for end-users is described in section 7.2 of Part III (p. 129).

Tools

TAS³ Notice of Privacy Practices (NPP)

What is it?

The TAS³ Notice of Privacy Practices is a document which sets forth the privacy practices of the Trust Network. This includes types of information collected, purposes of collection, uses, access rights.

How should it be used?

The primary purpose of the NPP is to inform potential end-users of the privacy practices that apply within the Trust Network. As such, it should be agreed to by end-users as part of the intake process for end-users.

The NPP should also play a role in the intake process for TAS³ service providers as they are obliged to ensure that their organizations can support the practices outlined in the NPP; both in terms of their participation in the TAS³ Trust Network and more broadly in their general operations.

Participating service providers may need to provide additional notice or information related to their processing or specific transactions. Such notice should be provided to the individuals concerned in the form of a Supplemental Notice of Privacy Practices.

Where can it be found in the document?

The TAS³ NPP and its role is described in section 7.2.1 of Part III (p. 130). A reference template of the NPP itself can be found in Annex 8 (p. 187).
The complete intake process for end-users is described in section 7.2 of Part III (p. 129).
The complete intake process for organizations is described in section 7.1 of Part III (p. 121).

Participant Questionnaire

What is it?

The Participant Questionnaire is a self-assessment questionnaire for prospective TAS³ participants which enables a determination as to whether or not the applicant meets the criteria for TAS³ participation in relations to privacy, security and technical capacity.

How should it be used?

Completion of the Participant Questionnaire is part of the intake process for organizations. The TAS³ Accreditation Authority should require the applicant to complete this questionnaire and then assess its credibility. This validation is one of the steps preceding accreditation as a 'TAS³ recognized service provider'.

Applicant service providers have a number of options in how they demonstrate their capacity to comply with privacy requirements. Where the applicant is confident that they already have compliant policies, they can just provide copies of the policies/documents with a short description of how they comply with requirements. For those applicants with fewer privacy support staff or less experience in drafting policies, the TAS³ Accreditation Authority should provide sample policies which may be used as starting points for policy development.

Where can it be found in the document?

The Participant Questionnaire and its role is described in section 7.1.2 of Part III (p. 122). The participant questionnaire itself is provided in Annex 9 (p. 295).
The complete intake process for organizations is described in section 7.1 of Part III (p. 121).

IT security requirements checklist

What is it?

The IT security checklist is a compendium of security requirements relating to the general operations of TAS³ service providers. It outlines the minimum requirements for security which participating organizations must adhere to for all of its operations.[12]

How should it be used?

Completion of the IT security requirements checklist is part of the intake process for organizations. The TAS³ Accreditation Authority should require the applicant to complete this questionnaire and then assess its credibility. This validation is one of the steps preceding accreditation as a 'TAS³ recognized service provider'.
Applicant service providers have a number of options in how they demonstrate their capacity to comply with security requirements. Where the applicant is confident that they already have compliant policies, they can just provide copies of the policies/documents with a short description of how they comply with requirements. For those applicants with fewer technology support staff or less experience in drafting policies, the TAS³ Accreditation Authority should provide sample policies which may be used as starting points for policy development.

Where can it be found in the document?

The IT security checklist can be found in Annex 10 (p. 313).
The complete intake process for organizations is described in section 7.1 of Part III (p. 121).

TAS³ Privacy impact assessment

What is it?

The TAS³ Privacy Impact Assessment (PIA) is a risk evaluation tool intended to assist both the design and implementation of privacy protecting measures in new applications, products or practices.

How should it be used?

Privacy Impact Assessments (PIAs) should be undertaken prior to deployment of any new application, product or practice which involves the processing of personal data. It can be used both at the level of the Trust Network and at the level of participating service providers to validate that privacy and data protection requirements have been met prior to the launch of any new application, product or practice.

[12] Not all of the operations of service providers participating in TAS³ are related to TAS³ (or necessarily executed through the TAS³ technical architecture). Those operations should, however, meet certain minimal security requirements in order to mitigate risk of compromise of those functions or components which do interact with TAS³ components.

Where can it be found in the document?

The TAS³ Privacy Impact Assessment (PIA) can be found in Annex 4 (p. 220).

Reference documents

Privacy Maturity model

What is it?

The Privacy Maturity Model is a tool to help organizations better understand the development, implementation and comparative positioning of their comprehensive privacy program.

How should it be used?

The Privacy Maturity Model is intended to act as a compliance measurement tool. It could be used as an auxiliary measurement tool during the intake of service providers when evaluating an applicant's capacity to comply and status of their privacy program.
It can also be used:

- to monitor the status of privacy initiatives and their implementation/deployment
- to compare an organization or departmental implementation of privacy across other departments or groups; and
- as a basis for benchmarking among comparable entities.

Where can it be found in the document?

The AICPA/CICA Privacy Maturity Model can be found in Annex 3 (p. 219).

Overview of foundation documents on privacy

What is it?

The overview of foundation documents on privacy is a table containing a high-level comparison of major principles and requirements of five legal instruments which are directly relevant to TAS³.

How should it be used?

The overview of foundation documents on privacy should be considered as background material to help understand the common concepts and principles underlying the contractual framework of TAS³.

Where can it be found in the document?

The overview of foundation documents on privacy can be found in Annex 1 (p. 215).