TAS$^3$: Business Model (Draft 06)

Editor: Luk Vervenne (luk@synergetics.be), Synergetics

January 20, 2010

Abstract

We explore the Business Models for Trust Networks. We acknowledge that there will be several Trust Networks and a given Service Provider may belong to more than one. We explore the role a Trust Guarantor plays in the network and how is this related to the concept of Trusted Third Parties. In general it is recognized that Trusted Third Parties will be needed to achieve confidence in trustability of the network. Trust Guarantor’s role is to overall coordinate the operation of the Trust Network and ensure all Trusted Third Parties as well as the Service Providers are performing their obligations. Governance aspects and stake holders of a Trust Network are examined. Some acute privacy threats are examined. Costs and sources of revenue are identified. Some recommendations for government policy are highlighted.

Disclaimer: This document has not been reviewed or approved by European Comission.

Obsolete: The editorship of the TAS3 Business Model has passed to Luk Vervenne. The document in this form is no longer maintained. Location of the new document to be announced.

Contributors

Joseph Alhadeff, Oracle
Antonia Bertolino, CNR
David Chadwick, Kent
Ingo Dahn, Koblenz
Sampo Kellomäki, EIfEL (original editor)
Luk Vervenne, Synergetics
Gang Zhao, STARLab, VUB
## Contents

### 1 Executive Summary

### 2 TAS Business Model

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>What should constitute a Trust Network?</td>
<td>5</td>
</tr>
<tr>
<td>2.1.1</td>
<td>Public vs. Private networks</td>
<td>9</td>
</tr>
<tr>
<td>2.1.2</td>
<td>Branding and reputation</td>
<td>10</td>
</tr>
<tr>
<td>2.1.3</td>
<td>Users trust perception</td>
<td>11</td>
</tr>
<tr>
<td>2.1.4</td>
<td>Quality of trust</td>
<td>12</td>
</tr>
<tr>
<td>2.2</td>
<td>How many of Trust Networks should there be?</td>
<td>13</td>
</tr>
<tr>
<td>2.3</td>
<td>Should Trust networks interact with each other?</td>
<td>14</td>
</tr>
<tr>
<td>2.4</td>
<td>Who should run them?</td>
<td>15</td>
</tr>
<tr>
<td>2.5</td>
<td>How should the governance be organized?</td>
<td>16</td>
</tr>
<tr>
<td>2.6</td>
<td>How are Trust Networks financed?</td>
<td>18</td>
</tr>
<tr>
<td>2.7</td>
<td>Form of Trust Guarantor</td>
<td>20</td>
</tr>
<tr>
<td>2.8</td>
<td>Oversight responsibility and conflict of interest</td>
<td>23</td>
</tr>
<tr>
<td>2.8.1</td>
<td>Kinds of Service Providers</td>
<td>23</td>
</tr>
<tr>
<td>2.8.2</td>
<td>Kinds of Trust Entities</td>
<td>24</td>
</tr>
<tr>
<td>2.8.3</td>
<td>Principles that Trust Network Should Adopt</td>
<td>27</td>
</tr>
<tr>
<td>2.8.4</td>
<td>Questions a Trust Network Member Has to Answer</td>
<td>28</td>
</tr>
<tr>
<td>2.8.5</td>
<td>Privacy Architecture Elements</td>
<td>28</td>
</tr>
</tbody>
</table>

### 3 Further Reading

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
</tr>
</tbody>
</table>
1 Executive Summary

In the last decade the Internet has consistently pushed the balance of power between the organization and the individual towards more user-empowerment. Today most services are being reengineered to be demand-led and user-centric.

While empowering the user/consumer/customer does create a more dynamic, agile economy, enhances consumer choice and spurs service innovation, the 180° switch from provider-led to demand-led services does come at a price.

Agile and efficient demand-led services, in fact require that users and service providers can present and exchange coherent and trustworthy information. Until now that information was collected, managed, stored and mostly kept if not shielded or stolen by the service providers. Today, at the height of using these antiquated business models in an Internet age, the truth is that your personal information sits in a 1000 databases. At best you know 10 of them.

TAS³ has set out to provide an answer to the user-controlled, trusted sharing of personal information in a user-centric, demand-led services economy.

This document explores the various Business Models for the Trust Networks (TNs) that will need to assure the trust for user-controlled Personal Information sharing. We acknowledge that there will be multiple Trust Networks. A given Service Provider may belong to more than one. This document also explores the role of Trust Guarantor in the Trust Network and its relation to the concept of Trusted Third Parties (TTP) in general. TTPs can be Identity providers, authentic (data) sources, etc. It is recognized that Trusted Third Parties will be used to link trust and identity across networks.

The Trust Guarantor’s role is to provide overall coordination of the operation of the Trust Network and to ensure that all Trusted Third Parties as well as the Service Providers are performing to their obligations. Governance aspects and stakeholders of a Trust Network are examined. Some acute privacy threats are examined. Costs and sources of revenue are identified. Some recommendations for government policy are highlighted.

2 TAS³ Business Model

TAS³ (Trusted Architecture for Securely Shared Services), aims at the creation of a secure and effective means for individuals to online monitor and control their personal information, when this is produced, used, or requested by service providers. TAS³ business models will have to provide an answer to the social innovation trends that underpin it. As such the TAS³ technological development will have to proceed alongside non-technological innovations and innovations based more on the notion of a demand-led services economy. A key task of the
Demand-led Innovation is the promotion of dialogue between users and service providers. User-led innovation is promoted in traditional business sectors, in private and public services, and in sectors which generate new demand. TAS³ aims to achieve this vision either via a distributed or central approach, however emphasizing the sharing and componentization of services and user-centricity in terms of service provision and data storage. Our working assumption is that the only robust and practical way to achieve this goal is to create a so-called "Trust Network".

Within a Trust Network information exchange and transactions are supported by guarantees in terms of both quality and the various trust & security components (authentication, authorizations, data privacy and trust management). Underpinning the Trust Network is a set of services called the Trust Network Infrastructure Services (TNIS) providing a core trust infrastructure supporting information exchange based on user control in the trust networks.

Central to the operation of the network based trust infrastructure is the use of specific Trusted Third Parties (TTPs) for mechanical & legal validation of services (providers + requesters) and (end-) users in the networks. The trusted third parties also interface with a higher level definition of trust metrics overseen by a top level Trust Guarantor. It is envisaged that cross Trust Network communication will be enabled by co-operation between Trust Guarantors. This eventually will result in a Trust Ecosystem.

1. All parties in the Trust Network (i.e. (1) end-users, (2) service providers & requesters, including (3) TTPs) will be represented by tangible legal entities that agree to the terms of the trust network before participating in it. The top level Trust Guarantor will set these terms and therefore define the laws / nature of the trust network and has to fulfill both technical and legal audit roles in the trust network.

2. All parties including end-users, service providers/requesters of application specific services (i.e. eHealth tools) and service providers/requesters...
2.1 What should constitute a Trust Network?

Figure 2: Main Components of a Trust Network Technically the top level Trust Guarantor has a fundamental role in (1) introducing, (2) monitoring, and (3) auditing the end2end assurance of trust between the transacting parties.

of TTP services (i.e. authentication) will be monitored by the overall TAS\textsuperscript{3} Trust Network Infrastructure Services (TNIS) that spans the specific trust network, its trusted services and the related and information exchange. Any party breaching of the terms of the Trust Network ecosystem and/or trust network will be reported to / monitored by the Trust Guarantor.

3. Any breaches of terms or failures of the Trust Network are the responsibility of the Trust Guarantor. Therefore the body has to act upon such cases and eject / penalize members of the ecosystem who break its rules. For example this could be done (1) via reduction of trust ranking of specific services, (2) by legal action on the basis of the TAS\textsuperscript{3} legal contract, including the expulsion of the involved party. This level of support will lead to an a-priori assumption that it is basically safe to transact with any member of the network, promoting trust in the whole network which leads to its acceptance and widespread use. This brings down (compliance) costs of doing business, reduces fraud and abuse of information, and ultimately leads to new innovative ways of transacting.

This vision raises some fundamental questions that need to be addressed:

2.1 What should constitute a Trust Network?

TAS\textsuperscript{3} is developing a generic architecture for securely shared services related to personal information. This Architecture is to be implemented in four parts:
2.1 What should constitute a Trust Network?

- business requirements
- technical requirements
- policy requirements
- Legal requirements.

The parties covered by the TAS³ architecture fall into three main categories:

- Trust (infrastructure or service) entities: trust guarantors and its certified Third Trusted parties such as authentic sources or identity providers)
- Application specific Service Providers (in TAS³ these are either employability or eHealth related)
- End-users (individuals)

All parties should consider the technical, policy and legal requirements to be the minimum requirements of the architecture.

- In the case of technology requirements, there may be limited flexibility in some implementation parameters to ensure interoperability:
- In the case of policies, they can be used in 2 ways. Participants to the TAS³ consortium can either adopt the policies promulgated as their own, or can map their policies to the model policies to assure that they meet the minimums required. The policy blocks presented by TAS³ can be used to create policies or are to use existing possible legacy policies and map onto the TAS³ definitions. Participants may need to provide evidence of the policy gap analysis if they rely on existing policies for compliance and also may need a mapping tool.
- Lastly, the legal requirements are reduced into contracts tailored to the role that each participant is playing, so they must be completed and adhered to. When registering to the Trust Network, the contract terms will bind organizations 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 trust technologies to honor the preferences and choices of users as to use and sharing of personal information.
2.1 What should constitute a Trust Network?

Trust verification and assurance are essential elements of the TAS³ Infrastructure, and thus the organization and cooperation of trust enablers in the operation and oversight of trust is essential. The co-operation is hierarchical in terms of the use of Trust Network level definitions, down to user and service definitions.

TAS³ Trust Networks are monitored & trust assured by (1) an independent Trust Guarantor supported by one of more (2) TAS³ certified Third Trusted Parties (TTPs). Both must be in an absolute position that provides them with an oversight role without having to provide services that place them in a position of conflict with data subjects.

The TAS³ Consortium members will periodically review the architecture requirements from a trust and oversight perspective or may engage in more frequent reviews as a result of changes in legal requirements, regulatory requirements, or cases that require new terms.

A TAS³ Trust Network therefore will usually consist of:

a. **Trust Network Governing Board.** The board manages the affairs of the trust network. Depending on the domain this might be a public-private-partnership (PPP) consisting for instance of the main societal eHealth or employability domain stakeholders.

For instance, in the Limburg province in the Netherlands, such PPP is currently in the making for a regional employability platform. It involves representatives of the employers, labor unions, educational sector, local governments, industry sectors,

b. **Trust Guarantor.** The trust guarantor is the technical operator of the trust network and its Trust Network Infrastructure Services (TNIS)

c. **User Representation.** The Trust Network will need some form of end-user representation. Depending on the type if Trust network this can range from existing end-user representatives such as labor unions, industry sector federations, government, grass roots user groups, ?) In essence this boils down to "organizing the communality"

d. **Governments.** We notice that governments in UK and the Netherlands (both at local and national level) are gearing up to help initiate / organize / facilitate the needed communality around user-centric data and services and the trust this requires.

The TAS³ Trust Network Governance Agreement as monitored and audited by the Trust Guarantor therefore has the following tasks:

- Monitor the governance structure of the Trust Network
2.1 What should constitute a Trust Network?

- Register, certify, oversee and audit of the TTPs active in the Trust Network.
- Register, certify, oversee and audit the Service Providers

The certified Trusted Third Parties, working in framework set by the Trust Network as executed by the Trust Guarantor will typically be existing actors possibly performing the following functions:

- Identity Providers (IdPs), to be certified by the TG
- Discovery and registries, to be certified by the TG
- Reputation Providers, to be certified by the TG
- PKI (q.b.) to be certified by the TG
- Authentic attribute sources, to be certified by the TG
- Etc?

Service Providers, may participate in multiple TNs (having a non-exclusive relationship), and choose their TTPs from available choice within each TN.

- Service Providers that act as data requestors
- Service Providers that act as data providers (running trusted repositories)
- Service Providers that act as data originators

End-Users can expect the following services from the Trust Network:

- Certification and audit procedures
- Branding (might/should be reputation based on live tangible metrics. Problem with brand is that it can take on a life of its own
- Secure and dependable technical infrastructure assuring trusted sharing of his personal information.

A Trust Network is built around an accountable legal entity, the Trust Guarantor (TG). Accountability implies both oversight and (legal) responsibility. The issues of obligations and liability must be clarified in the agreements that bind the party and must be appropriate to both the role and risk assumed by each party. The TG organizes and charters multiple technical Trusted Third Parties (TTPs) in order to perform specific and partial trust functions of the Trust Network.
2.1 What should constitute a Trust Network?

The sum of the delegated TTP functions may or may not cover ALL the operational functions of the Trust Guarantor. If it does, the remaining responsibility of the trust guarantor consists of overall management, certification and auditing.

A TTP will typically NOT have an exclusive relationship with TN and can operate in several TNs. TTPs should be leveraged to gain faster take-up and market acceptance of the Trust Network. Often this is also both inevitable and necessary because:

- the TG does not have all the skills needed
- there are already players in the market like:
  - Certification Authorities
  - issuing certificates
  - credit check operators
  - providing reputation

Other participants of a Trust Network are Service Providers who transact with each other, and Users who use the services of the Service Providers. Users also have a special role in that they may commit into the network data that needs special protection. The Trust Network and its Infrastructure Services only exist for the benefit of its users, not to enslave them and will be reflected in the way the user data policies are respected.

2.1.1 Public vs. Private networks

The Trust Network is generally foreseen to be a public and nonexclusive entity: anyone, User, Service Provider, or even Trusted Third Party operator, willing to be certified can participate. Trust Networks may compete on issues such as cost, trust level, terms of use and even competence of members (i.e. specialists). That being said, TAS$^3$ Trust Networks do not exclude the possibility to run private exclusive networks. Enabling such private networks however, is a non-goal, but is not an anti-goal either.

From that perspective a Trust Ecosystem (consisting of several Trust Networks) becomes possible that are made up of component TN systems. This would allow some parties to seek to develop private, closed or exclusive networks that are compatible with the TAS$^3$ infrastructure but not subject to it. In itself this may enable some information transfers across providers that are both in public and private networks in order to service particular customer needs, but would not necessarily imply that such private providers were under the TAS$^3$ Governance model or direct oversight. Thus TAS$^3$ may also be considered a portable standards-based...
2.1 What should constitute a Trust Network?

business model, but those wishing to use it for that purpose will need to appropriately adapt it and develop their own oversight models.

Each Trust Network is governed by a Governance Agreement to which all parties agree.

PS: In implementing the TAS\textsuperscript{3} requirements, two equally valid models may be used simultaneously. Some players may wish to adopt whatever criteria are created by TAS\textsuperscript{3}, where others may map their existing criteria to TAS\textsuperscript{3} to demonstrate equivalent compliance and interoperability. As we work on the development and pilots of TAS\textsuperscript{3} we shall seek to maintain whatever flexibility is possible that is consistent with governance, oversight and end-to-end security.

Trust Network participants will be subject to a general framework contract. This covers the overall rules of engagement for any user (end-user or service provider) of the Network and creates the needed relationships for obligations to be enforced against service providers. For these service providers this general framework agreement is then supplemented with role and transaction based contracts, covering not only what is allowed within the Trust Network, but also how data acquired for specific purposes should be handled beyond the reach of the TNIS monitoring capabilities (read: behind the service provider firewall).

2.1.2 Branding and reputation

Depending on the constitution of the Trust Network Governing Board the notion of branding the Trust Network may or may not be effective. If the Trust Network is merely an organization that operates the technical/legal Trust Infrastructure Services branding may or may not work.

In fact, when not backed up by a community of practice, Trust brands in some cases have shown to fail, e.g. some of the websites carrying a certification brand have never-the-less been fraudulent (even more so than sites without certification). I.e. a brand is not a guarantee in itself. This argument could go as far as recommending that no brand should be used in order to avoid inducing users into the false belief that a brand guarantees something. Users are not able to remember the historical track record of a brand and will instead trust it on basis of first impression or recent marketing.

If however the Trust Network/Guarantor is foremost setup to trust-enable a public-private-partnership, (covering for instance the employability services in a region) and this PPP is acting as the Trust Networks’ Governing Board, then such a community of practice and/or its TN may well become a solid brand.

While branding is foremost a user perception related term, more tangible trust is to be expected from real time reputation. In fact the TAS\textsuperscript{3} type of Trust Networks are based on trust which has to be user defined and real time, while brand is not defined by users nor is it real time. Nevertheless we would argue that TAS\textsuperscript{3}
2.1 What should constitute a Trust Network?

- where possible - should try to combine both approaches and in fact both are needed to produce end2end trust:

   The notion of BRAND has a connotation with user trust perception. Users are expected to perceive the brand as trusted, though if the network is mismanaged and the trust is not earned, the opposite may happen. The brand will also be used in certification: only valid participants are allowed to display the brand.

   REALTIME REPUTATION however requires measurable trust metrics. TAS\(^3\) therefore builds in reputation into the system of transaction guarantee, i.e. 100% compo if you use a gold star ranked service provider or 50% if you use a grey star ranked service provider and the SLA of TAS is breached.

   Finally, to build a Trust Network, build its brand and promote its adoption, technologies and products implementing the technologies will be needed. In a mature market these may be available off-the-shelf. However in an early innovator market, such as TAS\(^3\) type of TNs, ensuring that these are available and of high enough usability and quality can be instrumental to the success of the network. The Trust Guarantor therefore needs to work with all system participants and technology developers to ensure this is the case. Similarly, even user friendly and user centric applications require some basis of familiarity or necessity for uptake among consumer/citizen users, which will have to be addressed.

2.1.3 Users trust perception

Users should be able to join trust networks by agreeing to terms and conditions of use. The User can then allow his personal information to be shared within the network in order to become part of distributed composite applications & services. It is the central focus of TAS\(^3\) that when users present their personal information to a TAS\(^3\) Trust Network, they can trust that it will be not used out of context of the terms that they agreed when joining the network and the policies set out for the actual transaction. The trust is based on the end2end assurance provided by the Trust Guarantor, and relies on a combination of technical monitoring and enforcement capabilities and legal contracts signed by all involved parties. More specifically, legal contracts extend the reach of enforcement beyond the TN perimeter and beyond the service providers’ firewall.

   The ultimate guarantee that the data will not be misused is presented by the trusted guarantor who effectively takes on the liability for their respective trust networks. When joining the network the user will agree that in the case of breach the guarantor will compensate / take action to rectify. Service providers in the domain are tied in by the same rules. The action taken might include legal actions, insurance claims, service provider depreciations of exclusion, etc?

   Beyond the brand perception of a TAS\(^3\) trust network, its’ trust model works foremost on the user defining policies for their own personal information when
2.1 What should constitute a Trust Network?

![Figure 3: Trust Perception.](image)

joining a network and at the time of the transactional network decisions based on the users’ information.

2.1.4 Quality of trust

A key business opportunity in TAS\(^3\) is the concept of user trust perception. As users present their data to TAS\(^3\) various methods of reporting can be used to keep the user in the loop. For example some users may wish to keep a close account of what applications their data is being used in or the status of their application execution. This can be achieved through the use of the trust dashboard. Trust dashboards will help the user to discover & select the appropriate trusted service providers according to specific terms and return them in trust rank order like Google.

Users could sign up for different qualities of dashboard and this will be reflected in the cost of the application. These could be scaled in terms of price. The least expensive dashboard could present users with almost a 'fire and forget' interface to TAS\(^3\) networks allowing application invocation and presentation of results when done.

A more expensive and top of the range dashboard could notify via a variety of means the various hops that the user’s data may have in a trust network as it is used in applications. This could be achieved via email, SMS, etc. Service providers could compete to provide new innovative ways to report on the progression of the users data through the network.

Overall the user’s perception of trust can be seen as related to their knowledge,
2.2 How many of Trust Networks should there be?

and this needs to be reflected in the way users can interact with TAS$^3$. It is likely
that the GUI to TAS$^3$ will not carry much weight in terms of trust perception as
users will be directed to choose from reputation rankings and elements such as
cost. Some users may interact through specific TAS$^3$ interfaces whilst others may
use TAS$^3$ embedded in existing applications. In both cases the users need to sign
off on their policy refinements and have a means by which they can be notified of
their data use.

2.2 How many of Trust Networks should there be?

First of all we like to restate that an important goal of the TAS$^3$ project is to
create documentation and software so that Trust Networks will be easy to setup,
whatever their application domain.

As argued above, we expect TAS$^3$ TNs to emerge around a clear business need,
as perceived and made operational by Public-Private-Partnerships (PPP). Early
models are likely to be government (1) initiated, (2) facilitated, (3) mediated, (4)
anchored or even (5) owned (notice the increasing governmental involvement).

PS: Of course this view has its limitations: it would for instance seem un-
reasonably stifling to outright forbid private Trust Networks. Society and public
debate should establish what distinguishes a public Trust Guarantor from a pri-
ivate one and what regulation should apply to each kind. On the other hand, let’s
not forget that a TN represents foremost the user’s interest (and personal infor-
mation).

As such a Trust Network as something similar to a bank or telecoms oper-
ator. There is room for more than one and indeed having several will promote
healthy competition. However, due to the special infrastructure utility role, Trust
Networks are likely to be heavily regulated and there would only be a handful of
them.

Conclusion: With the TAS$^3$ project initiated from a need for trusted sharing
of personal information, we see Trust Networks arise from two angles:

- With the user as the ONLY ’lifelong’ continuum within Trust Networks, the
  variety and scope of the TN is likely to be fitted around the users’ health
  wealth and happiness!

- From an service providers perspective we see two orthogonal axis or attrac-
tion pools:
  - regional development, interests & communality
  - Domain/industry sector specific interests.
2.3 Should Trust networks interact with each other?

As such we expect a bottom-up approach with smaller, local initiatives being used as reference cases and national governments overseeing the results and eventually building momentum for larger, possibly national roll-outs, where different trust networks can be interlinked into Trust Ecosystems. In fact the Trust Ecosystem level could be the goal of the TAS$^3$ project guiding principles, standards & methods (and tools?), promoting them to new candidate Trust Networks. It may also be the correct level to discuss cross-country issues.

2.3 Should Trust networks interact with each other?

As TAS$^3$ services mature, the focus will shift towards building efficient larger trust ecosystems, which means connecting different context networks and avoiding overlapping functions. Again TAS$^3$ is build from the ground up as a generic & domain-independent architecture. Multiple Trust Networks (say a European wide and interlinked employability trust networks) can be linked into for instance a larger European Employability Trust Ecosystem. This requires that the involved Trust Networks cooperate and have established a set of common rules of engagement, both at technical and legal level. Besides providing first insights and comments, the TAS$^3$ project however considers the Trust Ecosystem level to be outside of the scope of the project and of its demonstrators.

We are presuming sectoral/national trust ecosystems at the outset. But these ecosystems may be comprised of trust network solar systems in galaxies that in turn make up the universe of the national sector. The business, technological, policy and legal contractual root of these interlocking players will be the architecture defined by TAS$^3$ which will enable interoperability, where needed. Not all players will interact with each other, but rather interact as required by need. It is impossible to predict in advance all of the specific participants to any transaction type, as user needs and preferences must be factored. The idea of parallel, but disjointed Trust Networks lacks credibility in today’s globalized world. The users would not be able to understand why the networks do not talk to each other and a multitude of kludgy or illicit "gateways" would spring into existence whether we want or not. Much better policy is to foresee the interaction directly in the architecture.

However roaming the trust concept from one TN to another is quite challenging and requires standardization of the different trust concepts. Nevertheless commercial systems have proven to be quite adequate in solving these types of unclean interfaces. As long as someone is willing to carry the liability for occasional mismatches and leaks, it can be made to work. Risk management is good enough if you can’t prevent the risks entirely. This is for instance how the credit card system works.
2.4 Who should run them?

Initially we expect the involved (innovating) project authority to govern the TN. Later on the powers that be will take over, unless the initiators manage to cross the chasm.

Figure 4: Crossing the Chasm: Marketing and Selling High-Tech Products to Mainstream Customers (1991, revised 1999), is a marketing book by Geoffrey A. Moore that focuses on the specifics of marketing high tech products. Moore’s exploration and expansion of the diffusions of innovations model has had a significant and lasting impact on high tech entrepreneurship. In 2006, Tom Byers, Faculty Director of Stanford Technology Ventures Program, described it as "still the bible for entrepreneurial marketing 15 years later”. This success resulted in several follow-up books and a consulting company, The Chasm Group.

Trust Network should be run by a credible and long lasting legal entity, with the necessary strong user community impact. Without government backstop, there might be a question of credibility to oversight, for instance. As such Trust Network is likely to be a non-for-profit PPP or Consortium type of organization, run by a representative governing board. The Trust Guarantor on the contrary has a specialist operational task probably best suited for a commercial entity, contracted by the TN.

Nevertheless, just for the sake of it, we list some other alternatives:

- Public-Private partnership with a user community impact
- New for profit company founded for the purpose (needs to build reputation)
- New non-profit foundation or association created for the purpose (needs to build reputation)
- Existing non-profit foundation or association
2.5 How should the governance be organized?

- Certification Authority
- Other major (consumer) player
- Government institution
- Government
- EU
- Charity
- Bank (they run your money, why not you personal data?)
- Insurance Brokers (you honest broker represents users)
- United Nations

A special peril would seem to be that the Users are easily left without representation (they are not foreseen to sign the Governance Agreement). Part of this problem is that there is no obvious party that could represent the users. Should they be represented by some consumer organization? We noted that Labor unions stepped up for the employability use case in the Netherlands, but on a more general level, outreach to privacy and consumer organizations would be recommended.

2.5 How should the governance be organized?

Since the Trust Network 'polices' the sharing of services and personal information exchange between multiple parties, it seems natural that the representative societal stakeholders that traditionally help manage users, providing them with a service offering, are the prime candidates to be brought onboard.

a. On the one hand will TAS³ enable them to evolve into demand-led service providers (representatives) and on the other hand they are needed create momentum for the trust network to become accepted as the 'new way forward'.

b. Overall we see national and local governments as the possible initiator and the most likely facilitator to help engage the stakeholders in adhering to the Trust Network compliance. Some caution is needed in defining the role of governments, since in a user-centric service economy they are also service providers like any other.

C. Hence the need for a society-wide Public-Private-Partnership, where all representative parties involved will need:
2.5 How should the governance be organized?

1. a clear win-win for their members and constituency (why)
2. adhere to TAS$^3$ compliance and its common rules of engagement (how)
3. a board seat and a responsibility in governing the Trust Network, following the Trust Network governance agreement (what)

The basic premise of Trust Networks is that transactions of monetary value will be involved. There will also be data protection issues to which liability is attached. Liabilities will eventually bring the Trust Guarantor, Service Providers, Trusted Third Parties or indeed even an end-user in court. Law and legal contracts will therefore provide the ultimate safety nets.

All parties are bound by contracts which set out rights and obligations. Users will sign documents related to terms and conditions, but they will be geared to the exercise of their rights and recourse, although it will also set out the need for them to be bound to their choices and act in ways that nobody undermines the system or attempt to defraud or otherwise injure other parties literally or figuratively. It therefore seems logically that governments sooner or later are going to regulate the Trust Networks.

To stave off excessive regulation and to delay regulation in general, Trust Guarantors have active interest to self-regulate. This places heavy emphasis on the Trust Network’s Governance Agreement.

Such a Governance Agreement should address:

- Governance structure, such as advisory and audit boards
- Criteria to join and stay on the network, including certification and audits
- Process for removal from the network
- Process for complaints
- Commercial liability and its fair appropriation
- Liability due to negligence in criminal cases and its fair appropriation
- Privacy protection, including redress for users (Req. $D1.2-6.10$-$Redress$)
- Minimal mandatory security practices (Req. $D1.2-6.11$-$Confid$)
- Acceptable use for Service Providers
- Acceptable use for Users
- Licensing of Trusted Third Parties, and their liability
2.6 How are Trust Networks financed?

a. A TAS³ Trust Network represents the trust assurance for a new way of working between service providers and users. The Trust Network therefore is merely an instrument and, at best, "a conditio sine qua non" for supporting a new demand-led services economy model. The TN therefore foremost replaces (and claims to improve) the existing services and their underlying business processes by changing them into trusted, online web services. We do believe tough that by putting the user in the center, new, and innovative user-centered services will be developed, which did not exist in the old service economy.

b. Financing the Trust network and its operational Trust Network Infrastructure Services (TNIS) therefore is foremost a replacement cost & benefit issue. The two main questions then are:

- How much money is saved by using a user-centric online trust network, compared to the scattered service provider centric services?
- How much of these saving can be spend on financing the Trust Network?

c. There is no easy answer. Firstly, one has to calculate the REAL and often hidden cost of let’s say, the lifelong employability of a worker. Today that cost is not even considered from a lifelong perspective! It is spread over any number of service provider cost models.

d. The way forward therefore seems to be to define the specific win-win benefits for the separate main stakeholders that come onboard to found the Trust Network.

By now it is clear that Trust Networks will have operational costs:

- Procurement and maintenance of technical infrastructure
- Member acquisition costs
- Member management costs
- User acquisition costs
- User management costs
- Trust branding costs (marketing)
- Audit costs
2.6 How are Trust Networks financed?

- Legal costs
- Liability and insurance costs
- General management costs

Trust Network can be financed in a variety of ways

- Initial capital injection for
  - Procurement of technical infrastructure
  - Procurement of legal contract framework
  - Initial trust branding costs (marketing)
  - Initial member acquisition
  - General set up

- Fees from Service Providers: there is a need to accommodate many types of Service Providers:
  - Fixed yearly fee
  - Per transaction
  - Per number of Users
  - Per yearly business volume
  - Revenue share
  - Member management fees
  - Audit fees

- Fees from Trusted Third Parties
  - Trusted Third Parties are allowed to have a fee structure of their own
  - Need to accommodate many types of TTPs; for

- Fees from Users:
  - Fixed yearly fee
  - Usage fees from Users. (The tricky part is to collect them)
  - Per transaction
  - Per number of Users
2.7 Form of Trust Guarantor

- Per yearly business volume
- Revenue share
- Member management fees
- Audit fees

- Advertisement
  - Placement of advertisement in authentication steps
  - Right to place advertisements in Service Providers
  - Revenue share from Service Provider advertising revenue

- Proceeds from foundation grant investment portfolio
- Government subsidy, research funding, taxes in a fair way. Perhaps a model where bill for broadband
- Internet connection includes some fee.

The TAS³ architecture should enable all of the above forms of raising revenue, or at least not block any of them.

2.7 What form of Trust Guarantor is most suited to operate and manage the Trust Network Infrastructure Services, a centralized or shared trust model?

The Trust Network Governance Board will appoint a Trust Guarantor to oversee, operate and technically & legally manage the Trust Assurance guaranteed by the Trust Network. While the Trust Guarantor will likely use a centralized model for starters, it is clear that there are already several third trusted parties guaranteeing identities, or authentic sources, etc... Today they are scattered, each having their own - often offline - trust models. The Trust Guarantor will have to incorporate and enable these existing third trusted parties all while providing the end2end trust assurance for sharing personal information. This capability will be build upon the stakeholder engagement

The Trust Guarantor will likely be a privately held, for-profit company that holds the technical and legal and business skills to operationally oversee and promote the Trust Network, on the request and on behalf of the Trust Network Governing Board. The Trust Guarantor architecture and compliance requirements will need to be matched to Government requirements & regulation.

The Trust Guarantor tasks include:
2.7 Form of Trust Guarantor

A win for All Trust Network Parties

- Authentic, coherent, dynamic, automated and up to date
- User controlled sharing of personal information
- Employability self

- Authenticate & direct process employee data
- Training & Career planning
- Meaningful matching
- Manage multiple
- Assessment & recruitment processes

Educational, Governmental

- Engage in demand
- Support user
- Facilitate employers
- Matching of unemployed

Figure 5: Example of Employability Trust Network win-win benefits.

1. Assure Compliance to TAS³ specification. This includes:
   a. Operate or outsource the certification program for software products to be used in the Trust Network.
   b. Operate or outsource the certification program for deployments, i.e. the participating Service Providers, and possibly others like IdPs.
   c. Operate or outsource an audit programme for the deployments
   d. Process complaints and arrange for arbitration or disciplinary action
   e. Market the network to both Service Providers and Users
   f. Maintain government compliance & endorsement as "The Trust Network"
   g. Guarantee minimal cost participation for non-profits

2. Operate necessary technical infrastructure.
   Depending on how the Trust Guarantor organizes (1) its business and (2) the Trust Network this may include:
2.7 Form of Trust Guarantor

a. Execute an IdP function or arrange for others to operate IdPs in the network

b. Authentication providers, in as far as this is not integrated into IdP.

c. Discovery and registry functions

d. Dashboard and audit results publication portal

e. Possibly a certification authority of some sort - this is likely to be outsourced. Certificate or credentials validation or revocation will be a central responsibility of Trust Guarantor.

f. Network level PDP

g. Reputation system, or arrange for someone to run the reputation system.

h. Where users have choice of multiple providers, the Trust Guarantor will need to ensure all in fact work and if not, may need to provide an integration solution, such as a gateway.

i. Where interaction between networks happens, the Trust Guarantor may operate a gateway that mediates.

3. Managing liability

**Panopticon threat** One especially pertinent risk in running a Trust Guarantor is that it may gain excessive knowledge to the operations of the SP members or the Users and their business processes. This is the so called "panopticon" threat. It can be mitigated by careful division of responsibilities using externally contracted Trusted Third Parties, each of which operates in its own isolated, regulatory scheme.

**Government regulation** Governments should consider regulating sound operation practices for Trust Guarantors. For example, it might be mandatory to outsource the IdP function. It may also be that regulation will require Users to be able to choose their dashboard or audit provider from choices that are available within the network.

The Trust Guarantor should also be able to make ultimate decisions on suspensions of parties, and will be liable to the core functionality of the trust networks it is responsible for.

**Outsourcing** Trust Guarantor is a business entity that has liability. The actual running of the Trust Network may involve several outsourced, franchised, or otherwise farmed out functions. The most obvious of these are Identity Provider (IdP), Authentication Provider (usually same as IdP), Discovery Service (DS), Reputation Provider (Rep), and Audit Function.

Thus an actual network will be configured to trust a number of IdPs, DSes, and Reps. In a strict view, all of these entities should be viewed as
2.8 Oversight responsibility and conflict of interest

Trusted Third Parties (TTP), but from business perspective what matters is that they are endorsed by the Trust Guarantor. As such the Trust Guarantor is the ultimate TTP policing the other TTPs and allowing them to enter the network. A clear legal definition of shared and accountability and responsibility will be paradigm in order to foster public trust in the network.

4. The Trust Guarantor monetary streams are:

- Trusted Third Parties contracted on case-by-case basis.
  - Most of these will involve cash outflow
  - Some cases cash inflows may be possible. Never-the-less, to be negotiated.
- Government Service Providers pay a yearly fee, to be negotiated
- Commercial Service Providers pay as negotiated, but preferred basis is revenue share or per transaction
- Small Service Providers pay small
  - yearly fee
  - an one-off Service Provider setup fee
  - support fees once initial support package has been exhausted
- Value added telephone & (first/second level) helpdesk support for users
- Advertising in authentication process where feasible
- Licensing fees or Revenue Sharing from Trusted Third Parties
- Insurance against liability

In the above listing, there are many charter requirements to guarantee that the Trust Guarantor will operate ‘within reason’. Since TAS is in position to license its brand and possibly some of its IPR, it should be in position to negotiate with prospective Trust Guarantor to get these charter items included.

2.8 How do you differentiate between parts of the trust network with oversight responsibilities and service providers that are relevant to trust but may have conflicting interests?

2.8.1 Kinds of Service Providers

All business actors, other than end-users, are modeled as Service Providers. Obviously there are different types of Service Providers with different legal require-
2.8 Oversight responsibility and conflict of interest

Requesters or Clients and agents  Provide some service to the end-user and in performing this service, will invoke other services, some to perform an action, others to store or retrieve data.

Infrastructure specific service providers  In case the Trust Guarantor does not execute these services which are core to the functionality of the trust network, they can be outsources to Infrastructure Service providers. They provide the core application functions such as accounting, monitoring etc on behalf of the trusted Guarantor. A generic TTP can also be seen as infrastructure specific. The business model / price they operate on may be fixed with the trusted Guarantor in order to guarantee availability.

Application specific services  These services provide the main functions of the network and make it domain specific. For example in an employability network you will have application specific services such as job matching services and CV translator. These types of services can offer a variety of prices and may compete in service selection brokering and negotiation; the cost may reflect a more real-time supply and demand / market place model.

Authentic Data Sources (Data Originators)  These are authoritative / authentic source of data may certify its veracity. They may also wish to control where and how the data is used. An originator may use a repository to store the data, or it may act as a repository by itself.

Data (Repository) Providers  These store data on behalf of the user or service provider, but the data in itself may have originated or is referenced outside the repository. Effectively the data provider’s repository is handling data on behalf of someone.

2.8.2 Kinds of Trust Entities

Trust entities will fall out of the TAS³ architecture, i.e. the business model should not nail them down before architecture is decided. However, we can say with fairly good degree of confidence that at least following types of trust entities will exist:

1. PKI Certification Authorities (CAs)
   - Issue SSL and signing certs to system entities
   - Potentially issue certs to users as well (we should avoid this if at all possible)
2.8 Oversight responsibility and conflict of interest

- Handle certificate revocation and online status checks (OCSP)
- No particular conflict of interest seen. TG could well be CA.
- However, established players exist on market, so it makes sense to leverage them.

2. User registration authorities. (PS: Sometimes IdPs perform the user registration function as well, but this need not necessarily be so)

3. Identity Providers (IdPs)
   - Authentication
   - SSO
   - Possibly some initial attributes
   - Possibly a discovery and/or token issuance service bootstrap

Main problems with IdPs are
   - Visibility to federation relationships
   - Traffic analysis, know who’s customer and how often
   - Potential visibility to authentication credentials

Since IdP can see so much, its best of there is no single IdP. The Trust Guarantor therefore probably should not perform this role itself. Instead it should charter or license others to do it. However, to avoid Conflict of Interest, an IdP SHOULD NOT be run by a SP.

4. Discovery service, service registry, or token mapper
   - Who provides what service to whom
   - Where do users keep their data
   - Indirection layer in providing end point URLs
   - Credential mapping, from original to specific use

Problems are similar to IdP. Further technical reasons usually dictate that that Discovery is operated by same entity as IdP.

5. Relationship Service
   - Who has invited whom to have sharing relationships
2.8 Oversight responsibility and conflict of interest

- Social network
- Groups
- Delegation use cases
- Almost certainly should be distinct from IdP to avoid accumulating too much information in one place
- Technically easy to have multiple PS

6. Organizational PDPs

- Local to organizations operating the SPs
- Authorizations must be trusted blindly
- The PDP gets to see quite a lot of traffic analysis info

7. TAS³ network-wide PDP

- Enforces the network wide rules
- Authorizations must be trusted blindly
- The PDP gets to see quite a lot of traffic analysis info

8. Reputation Providers

- Reputation based trust scores are computed from usage pattern data and from PII. Both sensitive, but both can also be influenced by savvy users.
- Multiple instances encouraged to avoid accumulation of too much info of this nature in one place

9. Authorative data sources

- Sometimes known as Policy Information Points (PIPs)
- PDPs and reputation scoring can rely on authorative attribute data, thus supplier of this data has to be trusted
- The way the data was collected in the first place has to be trusted

10. Policy Authorities

- Where do the policies that drive various PDPs come from?
- Are they dynamic or field upgradeable?
2.8 Oversight responsibility and conflict of interest


- Many TAS\(^3\) components are driven by business models, so whoever programs these and has ability to update the installed base, has a lot of power
- Dynamic BPM where the actual model itself can change and be propagated instantaneously to the consumers of the model

12. Ontology authorities

- When trying to compare apples to apples, e.g. to make authorization decision, the authority that defines the equivalence classes of terminology can control the outcome.
- Field upgradeable or dynamic ontologies are likely to be used, thus it matters what authority lies behind them.
- This threat is similar to the process model one

13. The domain name system

It may arise that in some situations integrity of DNS will affect trust. Usually we should be able to avoid relying on this by using digital signatures, but there may be special cases, e.g. error situations where signature is not applied, which could then open the door to phishing or hijack attacks. Please note that the audit dashboard, while probably trusted by the user, need not be trusted in process of making any access decisions. The dashboard can, however, be one of the channels from which the reputation system gets its information.

2.8.3 Principles that Trust Network Should Adopt

A TN should adopt following principles:

1. Personal Data should only be collected and/or processed for fair and legitimate business purposes.

2. The purpose(s) for collection must be clearly specified.

3. The collection related to those purposes must be relevant and non-excessive.

4. Personal data must be accurate and, where needed, up-to-date.

5. Use, and subsequent use, of personal data cannot be incompatible with the purposes specified and should be with the consent of the data subject

6. Appropriate security (technical and organizational) measures against
2.8 Oversight responsibility and conflict of interest

7. Unauthorized/unlawful/accidental access; modification, disclosure, destruction, loss or damage to personal data must be in place.

8. Controllers and processors have duties to maintain confidentiality of information.

9. Sensitive data may be subject to greater restrictions.

10. Data subjects have the right to know what types of data are being maintained and have the right to access and correct personal data.

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

2.8.4 Questions a Trust Network Member Has to Answer

1. Are you collecting/using PII as part of the service?

2. Do you have a privacy policy that you are bound to follow?

3. Do you use PII for any purpose other than providing the service?

4. Do you get my consent or let me opt out before my information is used for other purposes than providing the specific service?

5. Do you share my information beyond your company or family of companies?

6. Do you get my consent or let me opt out before your share my information with any other company not needed to provide the specific service?

7. Do you allow me to manage these preferences over time and change my options?

2.8.5 Privacy Architecture Elements

1. Identify why information is needed

2. Provide appropriate notice and obtain consent for use of information

3. Limit information collected to that which is required for the legitimate business need

4. Limit access to information to those that need it for the business function
5. Retain information only as long as reasonably needed to complete the business function and securely delete it (or possibly anonymise it).

6. Secure information as required in a manner proportionate to its nature and sensitivity

7. Maintain the integrity and accuracy of the information

8. Provide access and possibility of correction

3 Further Reading

To further understand TAS³ Trust Networks, you should read (in roughly this order):

1. The Governing Agreement of the network you plan to participate in (this depends on the network, no single answer exists)

2. The Compliance Requirements [TAS3COMPLIANCE]

3. The TAS³ high level architecture [TAS3ARCH]

4. The TAS³ protocol and concrete architecture [TAS3PROTO]

5. Any architecture and compliance documents of your Trust Network

References


REFERENCES

[REFERENCES]


Revision History

 06 30.3.2009 Sampo
  • NOT PUB
  • Post-handover tweaks
  • Incorporated new version of biz model from Luk

 05 25.3.2009 Sampo
  • Formatted for handover to Luk

 04 23.3.2009 Sampo
  • Incorporated comments by Joseph (JHA) from "biz model v3jha.rtf"
  • Dropped mention of private trust networks
  • Added concept of Trust Ecosystem

 03 15.3.2009 Sampo
  • Multipolar Trust Network
  • Changed Trust Operator to more general Trust Guarantor
  • Explicitly foresee TTPs, but subordinate them to to TG
  • Explicitly mention that TTP and SP may participate in other/multiple TNs
  • Reference the rest of the architecture documentation

 02 13.3.2009 Sampo
  • Incorporated comments from David and Ingo
  • Formatted headers and footers to include TAS3 logo
REFERENCES

01  11.3.2009 Sampo (sampo@symlabs.com)

  • First draft out of blue

Document ID draft-tas3-biz-model-2009-v06.pdf

Repository path repo.tas3.eu:/var/lib/tas3repo/tas3-biz-model.pdf

(1.32)

    export CVSROOT=:ext:repo.tas3.eu:/var/lib/tas3repo
cvs co arch
cd arch
# modify tas3-*.pd
cvs ci -m 'What changed...'

URL path https://portal.tas3.eu/arch/review/tas3-biz-model-v06.pdf

Commenting

  • Please comment on the TAS3ALL@LISTSERV.CC.KULEUVEN.AC.BE
    mailing list, or that failing, send your comments to the editor.
  • Any footnotes in this document will not appear in final version. They
    are editorial comments that may help reviewers to put material in con-
    text.