

SDTL

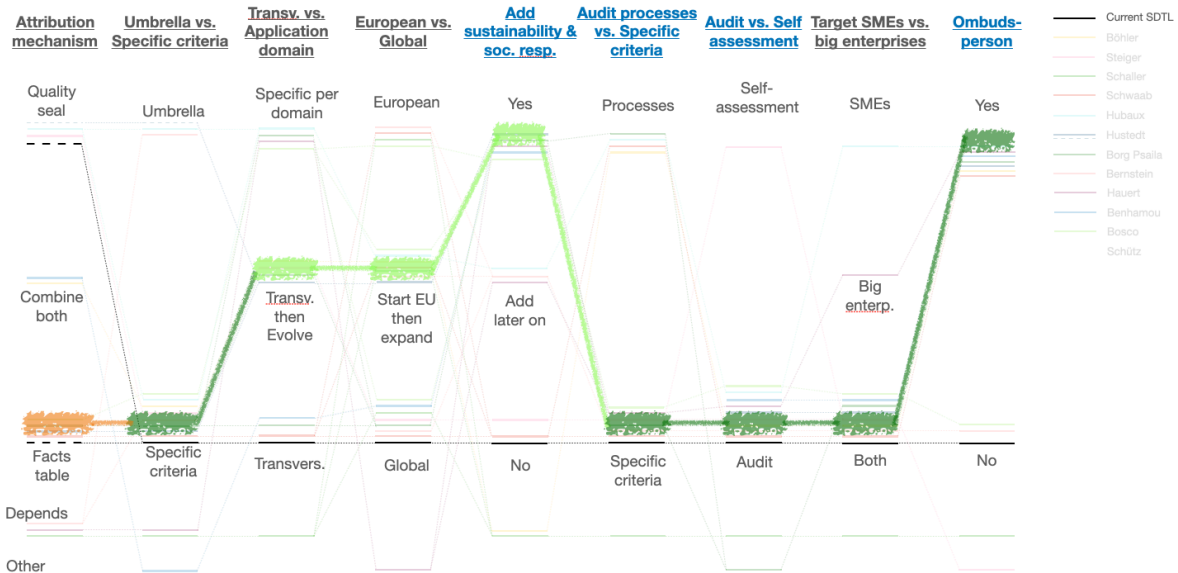
Recommendations of the Experts Committee

I. Aad, M. Rajman
Dec. 2020

Executive summary	3
1. Introduction	4
2. The experts committee	4
3. The consultation process	6
4. The design directions and their acceptance	10
5. The resulting recommendations	19
6. Opinions on each design direction	22
7. Opinions on SDTL's approach	27
8. Opinions on SDTL's current list of criteria	33

Executive summary

The SDTL Experts Committee is composed of twelve members with very different backgrounds. Their feedback on SDTL throughout various discussion rounds was very rich. Numerous opinions were brought to the table, not necessarily always aligned. The current version of SDTL served as a starting point for discussions and for identifying the design spaces. We split the current version into different "design directions", to which we added new directions proposed by members of the committee (blue titles). We gathered the opinions on these, and the result is the following.



The most supported solution, shown as the thick line (green and orange) in the graph, is a configuration consisting of:

- Listing specific criteria instead of the umbrella approach which covers complete standards and regulations
- Starting with an approach that is transversal across families of services, then moving into the specificities of each
- Going global
- Adding sustainability and social responsibility to the trust criteria, right from the start or at a second phase
- Auditing, instead of self-assessment
- Aiming at both SMEs and big enterprises
- Integrating an Ombudsperson function

Additionally, the recommended configuration includes a large support for: Open source; Whistleblowing; Establishing channels for user reporting.

The options in light green indicate a timing decision to be taken on a strategic level: "Going from European to global", "going from transversal to application-specific", and "include sustainability and social responsibility".

The last two specifically require extending the experts committee to include experts from these domains, and further work on the label criteria. **This requires strategic decisions from the SDI Board.** The most divisive option (in orange) is whether to build SDTL as a "list of trust facts", a "list of trust facts with a trust score", or a "quality seal". Each has its advantages (ex. appeal to companies and consumers) and disadvantages (ex. time to market). The ongoing user-study may help shedding the light on the way to go. The target option, together with its timing, require **strategic decisions from the SDI Board.** A dedicated section (**Section 6**) in this report details corresponding arguments. Once these decisions are taken, the list of auditing criteria must be adapted accordingly, in consultation with the Experts Committee.

Extreme care must be also taken regarding the communication (by SDI and by providers of labelled services), to avoid misleading the end-users, avoid liability issues, and avoid compromising the success of SDTL.

Design option	Description	Current positioning of the Expert Committee	Recommendation
7	Audit vs. Self-assessment	Clear support for Audit	Rely on an audit; add whistleblowing; add user reporting channel
2	Focus on a specific set of criteria	Clear support	Focus on specific criteria; add Open Source
8	Target SMEs, Corporates or both	Clear support for both	Target SMEs and large companies
6	Auditing criteria vs. Auditing processes	Clear support for auditing criteria	Audit criteria
9	Ombudsperson or not	Clear support for Ombudsperson	Consider the involvement of an ombudsperson in the labelling framework
4	EU scope vs. Global scope	Support for starting with EU scope and extending to global scope later	Start with an EU scope and extend to a global scope in a second step. Timing is a strategic issue.
3	Transversal criteria vs. Application specific criteria	Support for starting with transversal criteria and cover application specific ones later	Start with transversal criteria and expand to application specific ones in a second step. Timing is a strategic issue.
5	Add sustainability and social responsibility	Support for adding them Sustainability and social responsibility.	The committee acknowledges the considerable overhead, making the additional delay a critical strategic issue.
1	Informative approach (Fact table) vs. Normative approach (Quality seal)	Opinions are split across the options.	The target option is a strategic decision to be made. Start as an informative facts table and move to target option after learning.

1. Introduction

The SDI Board mandated the Experts Committee to make recommendations on the SDTL. To this end, this document describes the resulting recommendations, together with the detailed consultations approach and various opinions and arguments. The reader can directly jump to the section of his/her interest in this report without having to read the sections sequentially.

For further questions or comments, you can contact imad.aad@epfl.ch or martin.rajman@epfl.ch.

2. The experts committee

The Experts Committee is the successor of the Academic Committee which oversaw the creation of SDTL. The newly created Experts Committee is composed of 12 experts of multi-disciplinary backgrounds, from academia, government, international organisations, foundations, consumer protection, law firms, from Switzerland and abroad.

The Experts Committee acts independently of any other group, with the mandate of issuing recommendations to the SDI Board (see Figure 1.)

SWISS 
DIGITAL
INITIATIVE

Overall Governance Label Project Label Governance Structure

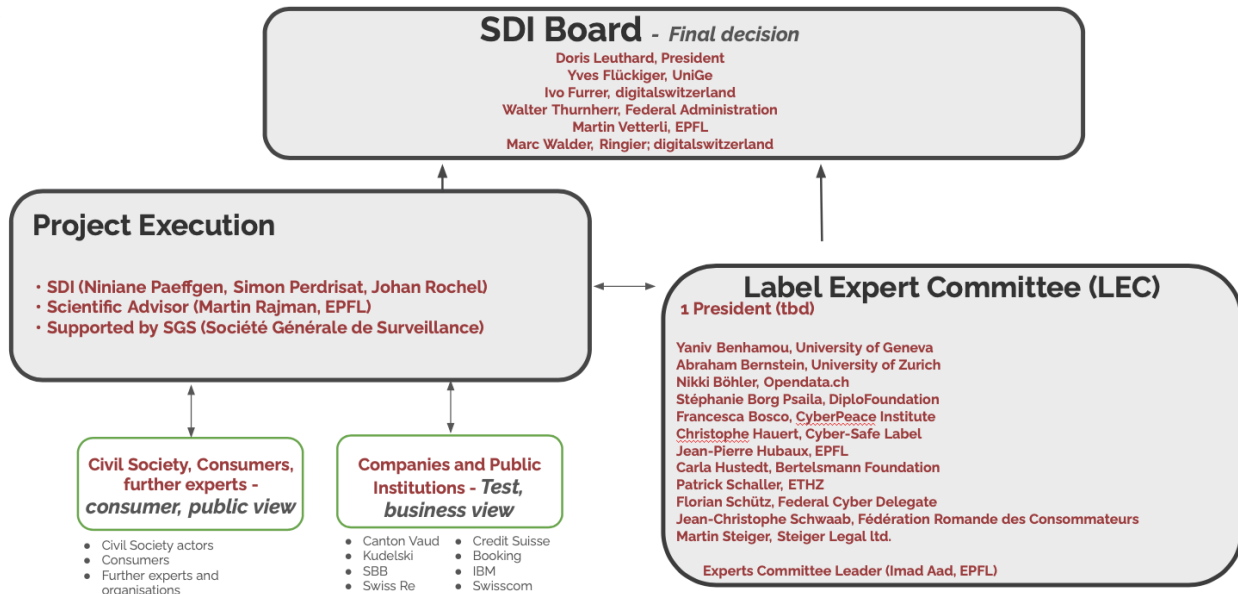


Fig. 1: SDTL project's governance, including the Label Experts Committee and the SDI Board

The members of the Experts Committee were proposed by various sources to SDI, which sent the invitations. Membership is not remunerated.

Members of the Experts Committee are:

- Yaniv Benhamou, University of Geneva*
- Abraham Bernstein, University of Zurich*
- Nikki Böhler, Opendata.ch

- Stephanie Borg Psaila, DiploFoundation
- Francesca Bosco, CyberPeace Institute
- Christophe Hauert, Cyber-Safe Label
- Jean-Pierre Hubaux, EPFL*
- Carla Hustedt, Bertelsmann Foundation
- Patrick Schaller, ETHZ
- Florian Schütz, Federal Cyber Delegate
- Jean-Christophe Schwaab, Fédération Romande des Consommateurs
- Martin Steiger, Steiger Legal Ltd.

(* member of the former Academic Committee)

The Experts Committee is lead by Imad Aad, Center for Digital Trust (C4DT), EPFL.

Martin Rajman, EPFL, who is active on SDTL since its beginning, is also actively participating in all the exchanges of the Experts Committee as a scientific advisor.

3. The consultation process



Figure 2: timeline and meetings

Three "main meetings" (2h each) were held with all the committee: In July, October, and December. Due to the current sanitary situation, the meetings were held exclusively online, using Zoom.

Bilateral meetings (2h each) were held with each member of the committee, in between the first two "main meetings" in order to discuss the member's point of view in depth. An additional bilateral meeting was held with Bertelsmann Foundation to gain insights from their experience in establishing a label for family-friendly employers.

Occasional exchanges with some members were also done offline.

In addition to the exchanges within the Experts Committee, this latter was continuously informed of the activities and results related to SDTL, such as the mock audits with the test partners, the workshop with the civil society, and the comparisons with similar initiatives.

The consultations with the Experts Committee were around 2 axes:

- SDTL's approach
- SDTL's content

"SDTL's approach" includes the labelling aspects, such as:

- whether the label should be transversal across digital services or specific to each family of services (e.g. finance, booking etc.)
- whether the label should be a "quality seal" or a "list of trust facts"

"SDTL's content" deals with the "Trust criteria", which are 35 in the current version, drafted prior to the establishment of the Experts Committee and overseen by the former Academic Committee.

All meeting notes (main meetings and bilateral ones) are on a Google shared folder accessible to all members of the committee.

Initial consultation round

After familiarising with SDTL during the first main meeting in July, bilateral meetings were held with each member of committee in order to get her/his opinions on the approach and content, in addition to possible recommendations.

Questions regarding the approach included:

1. Do you think that Labelling Trust is relevant? feasible?
2. Do you think SDTL's approach is good?
3. What do you think of the "identification of the areas that define digital trust"?

4. Do you think the identified categories are good? enough? (security/privacy/reliability/fairness)
5. What do you think of the transversality of the criteria? (same set of criteria for a wide range of digital services)
6. What do you think of the idea of a "Digital Trust Label" to "inform the user about the most relevant trust-related criteria"?)
7. What is your opinion on the analogy with nutrition facts?
8. Do you think the proposed method achieves this goal?
9. Do you think the proposed method is useful to build user trust in digital services?
10. Do you think SDTL would weaken or strengthen the current requirements for digital services?
11. Would you use the 'trust facts' table of SDTL?
12. Open feedback

The answers on these questions showed very diverse opinions on the approach, as shown in Figure 3.

	Bernstein	Schütz	Borg Peala	Schwaab	Benhamou	Bosco	Hustedt	Hauert	Schaller	Hubaux
relevant?	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
feasible?	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Red	Red
identification of the areas...	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
identified categories are good? enough?	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
transversality	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
most relevant trust-related criteria	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
analogy with nutrition facts	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
proposed method achieves this goal	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
useful to build user trust	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
SDTL would weaken or strengthen the current requirements	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Would you use SDTL	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
open feedback	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow

Figure 3: Feedback on the approach: Green = positive; Red = negative; Yellow = OK but...

The details of this table can be seen in [Section 7](#) at the end of this report, and on the Google shared folder.

One common consensus (first line): the issue is very relevant.

Another common point raised by most members is the importance of the communication, by SDI and by companies, towards the end-users. Giving the end-users fake impressions of trust, or misleading them in the understanding of what SDTL covers or means may lead to the failure of SDTL, besides the liabilities of various parties (SDI, companies, auditors).

Various members of the committee had questions on the strategy and on the organisational level, such as "who's going to manage the label on the long run?". These questions were transferred to SDI without being discussed in detail within the committee due to time constraints, rather focussing on the approach and on the content.

Figure 4 shows the various feedbacks on the content, which is specific to the 35 criteria in the current SDTL draft. It also shows the diversity of opinions regarding the content.

		Bernstein	Schütz	Borg Psaila	Schwaab	Benhamou	Bosco	Hustedt	Huert	Schaller	Hubaux
General feedback	General feedback	Yellow	Red	Yellow	Yellow	Yellow	Yellow	Grey	Green	Yellow	Yellow
	...						Yellow			Yellow	
	...						Green			Yellow	
	...		Red						Yellow	Yellow	
	...		Red							Yellow	
	...									Green	
	...								Red	Yellow	
	...						Yellow	Green	Yellow	Green	
	...	Yellow					Yellow	Green		Green	
	...									Yellow	
Security	Security										
	...										
	...										
	...										
	...										
	...										
	...										
	...										
	...										
	...										
Data Management	Data Management										
	...										
	...										
	...										
	...										
	...										
	...										
	...										
	...										
	...										
Reliability	Reliability										
	...										
	...										
	...										
	...										
	...										
	...										
	...										
	...										
	...										

Figure 4: Feedback on the content: Green = positive; Red = negative; Yellow = OK but...

The details of this table can also be seen in [Section 8](#), and on the Google shared folder.

Second consultation round

Besides the feedback on the first version of SDTL, the first consultation also shed the light on new possible design directions (for example: including sustainability as a category of criteria). Some design directions are complementary, others are conflicting, and all have their advantages and drawbacks.

In order to measure the level of support for these various individual proposals, we gathered them all in the "design directions" and asked all the members to give their level of support, as described in the next section. Based on the levels of support for individual directions, the overall recommendations are made and described in Section 5.

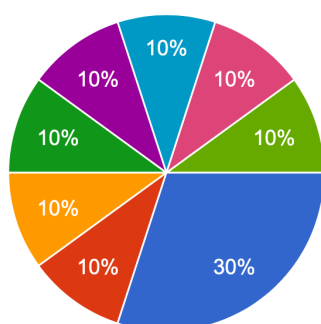
4. The design directions and their acceptance

In this section we cite all design directions that were identified, together with their advantages and drawbacks. Where applicable, the current version of SDTL is shown in blue.

Attribution mechanism: Informative "facts table" vs. Normative "quality seal"

	Informative ("facts table")	Normative ("quality seal")	Combine both
Description	With this "informative" variant, SDTL would only display which criteria are met, which ones are not, and it's left to the user to make his/her decision.	With this "Normative" variant, if all 35 criteria are met, SDTL would display something like "Control passed, service is Good"	With this variant, both variants are combined.
Pros	SDTL makes no evaluation / labelling / seal such as "good" or "bad"	Easier to grasp for the end-users More appealing for companies to buy (for differentiation and competition)	More appealing for companies to buy (for differentiation and competition)
Cons	Harder to grasp for the end-users Risks being understood as a quality seal against the current trend of trust labels with real quality seals	SDTL (with 35 criteria) is not inclusive of all legal requirements Neither of the practiced standards This gets complicated if it goes international More liability towards SDI	SDTL (with 35 criteria) is not inclusive of all legal requirements Neither of the practiced standards This gets complicated if it goes international More liability towards SDI
Questions	Does it still need to go beyond the norms? Is it still a "label" or a "trust facts table" instead?		

10 réponses

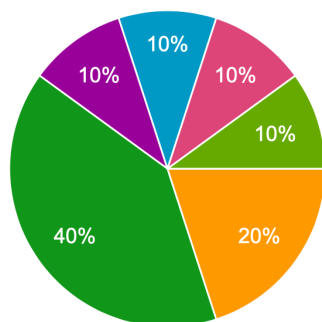


- Strong support for "Informative / facts table"
- OK for "Informative / facts table"
- Strong support for "Combine Both informative and normative"
- OK for "Combine Both informative and normative"
- OK for "Normative / quality seal"
- Strong support for "Normative / quality seal"
- Depends on the use case
- It depends on the strategic goal of the...

Umbrella approach vs. Specific criteria

	Umbrella approach (inclusion of exhaustive lists)	Specific criteria only
Description	<p>With this variant SDTL would include all criteria of the standards/regulations that relate to the trust categories. For instance ISO 27001 for security and GDPR for privacy. Other non-standardised categories (like fair user information) can be added like in the current SDTL text.</p> <p>SDTL would become an "umbrella label" covering existing standards and regulations, in addition to non-standardised categories.</p>	<p>Like in the current SDTL text, 8 criteria are taken from GDPR, 12 from ISO 27001, as the most relevant ones.</p>
Pros	<p>SDTL becomes an umbrella of existing requirements/standards -> easier to update and manage</p> <p>SDTL won't risk weakening the existing requirements.</p> <p>SDTL would not miss legal criteria which risk making a labelled service illegal -> No credibility problem of the "quality seal"</p>	<p>Easier to understand</p> <p>Easier to audit</p>
Cons	<p>Who will audit this compliance? (+costs)</p> <p>Too many criteria for the user to understand (?)</p> <p>If SDTL goes international: which law to take?</p>	<p>If SDTL is chosen to be "normative quality seal": Too few criteria for the user (?)</p> <p>Credibility problem if a service is given the "quality seal" and shows to be illegal?</p> <p>(less problematic if SDTL is "informative")</p>

10 réponses

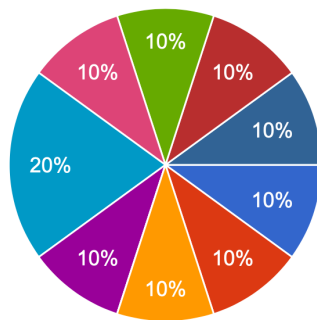


- Strong support for "Umbrella Approach"
- OK for "Umbrella Approach"
- I'm fine with any of the two
- OK for "Specific Criteria"
- Strong support for "Specific Criteria"
- Again, depends on the use case
- This decision depends on whether we go for a quality seal or a fact table.
- Strong support for "Specific Criteria" combined with an additional criteria of...

Transversal vs. Application domain / family of services

	Keep it transversal	SDTL must be specific to families of services	Start transversal, evolve later on
Pros	Easier for the user to understand Easier to manage / update	More complete, precise Gets into the specific details of each family of services	Start and learn with something small and less complex
Cons	Criteria risk being too generic	Hard to manage / update	Can make it a weak start, thus compromising the success

10 réponses

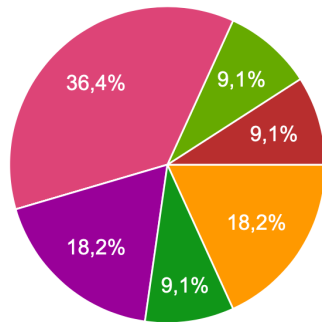


- Strong support for "Transversal"
- OK for "Transversal"
- Strong support for "Application Domain"
- OK for "Application Domain"
- Strong support for "Start transversal, e..."
- OK for "Start transversal, evolve later..."
- I'm fine with any of the three option
- Sorry, but also here: Who is the consu...
- I would say to start specific to test it in a couple of sectors and derive criteria/ lessons learned potentially applicable to others.
- do not know

European vs. Global reach (incl. China and US)

	Start and remain European	Start Global	Start European then expand Globally
Desc ription	The scope of SDTL remains European.	The scope of SDTL remains European.	SDTL starts on the smaller European scale, learn from the experience, before going global
Pros	SDTL deals with a smaller number of cultures, laws, etc.	Bigger impact More visibility	
Cons	Smaller impact Less visibility	SDTL has to be compatible with a large number of cultures, laws etc.	

11 réponses

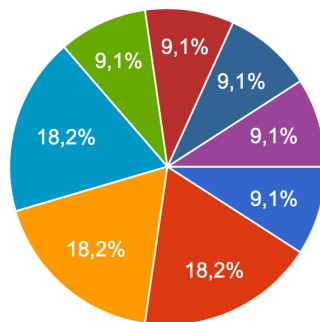


- Strong support for "Start and remain European"
- OK for "Start and remain European"
- Strong support for "Start Global"
- OK for "Start Global"
- Strong support for "Start European the..."
- OK for "Start European then expand g..."
- I'm fine with any of the three option
- transnational approach
- OK for "Start European and then see"

Add Sustainability and/or social responsibility

	Yes, add them	No, do not add them	Add them later on
Description	This gives SDTL an educational aspect in addition to the informational one. It's not only to show the users what they care about, but what they must care about as well.	Keep SDTL with the current 4 categories (security, privacy, reliability, and fair user information)	Start with the current 4 categories, then add sustainability and social responsibility at a later stage
Pros	Adds the educational impact More complete set of trust-related criteria	Less criteria, easier to manage	Start and learn with something small and less complex
Cons	They are not well defined or agreed upon, controversial. It's more about the company, not the service (remember, SDTL goes for a service, not its company) More criteria to audit (+costs)	Lacks considerable components of trust	Can make it a weak start, thus compromising the success

11 réponses

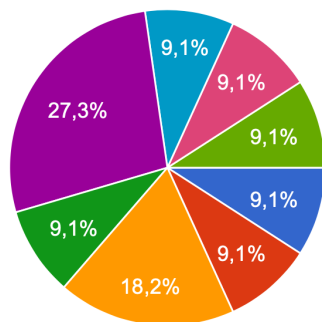


- Strong support for "Yes, add them"
- OK for "Yes, add them"
- Strong support for "No, do not add the..."
- OK for "No, do not add them"
- Strong support for "Add them later on"
- OK for "Add them later on"
- I'm fine with any of the three option
- depends on the use case of the label
- Fine with option add them now and add them later on
- Not sure, make dependent on user testing
- Strong support for "Yes, Add them", only provided that the criteria are well defined / standardized and already applied by leading companies today (which shall be assessed by experts on sustainability...

Auditing Processes vs. Specific criteria

	Processes	Specific criteria
Description	A process audit determines whether the activities, resources and behaviours are being managed efficiently and effectively.	SDTL has a list of specific criteria (Ex. 2-factor authentication, data encryption etc.)
Pros	Solves the issue of specificities of services / transversality, and the criteria dynamics over time.	More concrete and precise.
Cons	Higher level than auditing specific criteria. Implementation of the processes is less visible to the audit than with specific criteria.	Brings in the transversality issue, and keeping the criteria up to the pace of technologies.

11 réponses

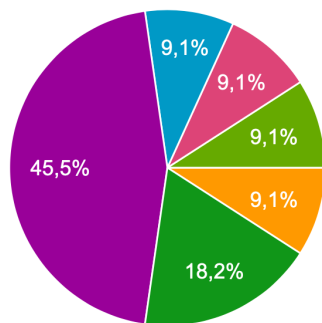


- Strong support for "Auditing processes"
- OK for "Auditing processes"
- I'm fine with any of the two option
- OK for "Auditing specific criteria"
- Strong support for "Auditing specific criteria"
- Depends on the use case of the label...
- Not sure if i understand the question correctly
- Not sure to understand this issue / diff...

Assessment: audit vs. self-assessment

	Self-assessment	Audit
Description	The assessment of the service is made by its provider, based on the SDTL's list of criteria. If the provider shows to be cheating (spot-checks, or information leaks), a penalty is applied.	A third party performs the audits.
Pros	Cheaper than audits, thus more appealing to companies	More reliable
Cons	Less reliable	Audit costs may be problematic for SMEs.

11 réponses

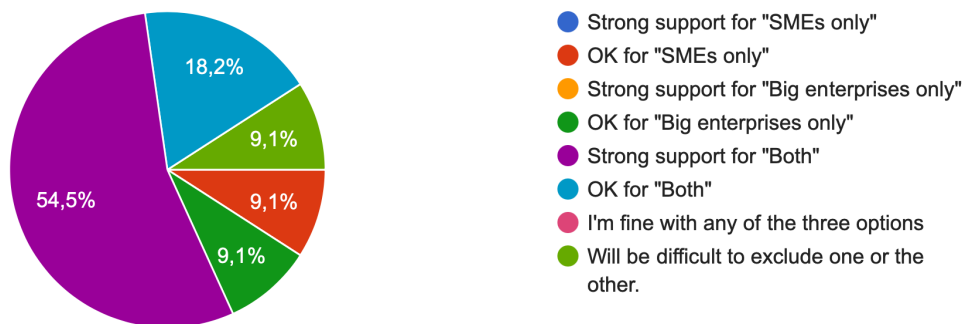


- Strong support for "Self-assessment"
- OK for "Self-assessment"
- I'm fine with any of the two option
- OK for "Audit"
- Strong support for "Audit"
- Both
- I would expect, that if it is "self-assessment" there would need to be a kind of audit for the self-assessment o...
- third party audit

Target: SMEs vs. Big Enterprises

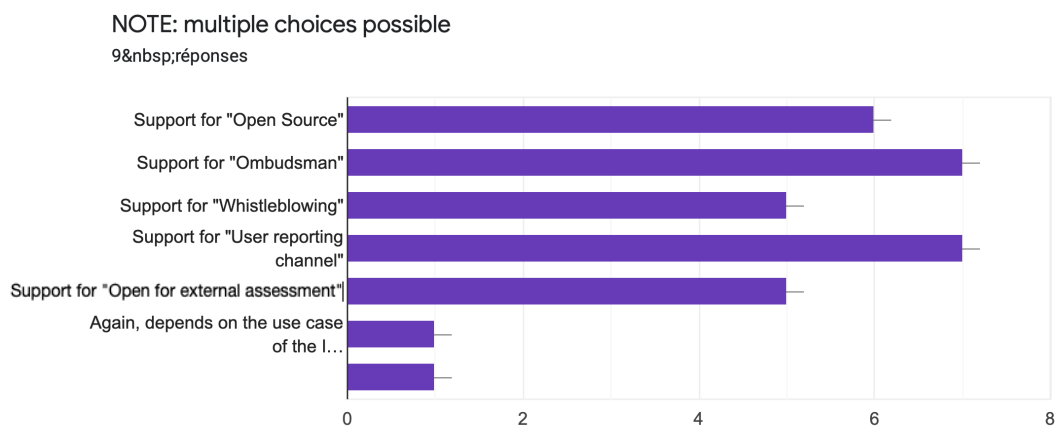
	SMEs only	Big enterprises only	Both
Description	The set of criteria is adapted accordingly, in order to reduce the audit costs.	Audit costs are not an issue, allowing the set of criteria to be more extensive.	The set of criteria, and the audit costs, are at an intermediate level.
Pros	SDTL is appealing to SMEs, increasing its adoption, and promoting good practices	Criteria can cover more trust categories, and can be more exhaustive.	Intermediate level between the two "Pros"
Cons	The set of criteria gets too small, missing some important criteria in standards/ regulations.	SDTL is restricted to big companies, reducing its adoption and the spread of good practices.	Audit costs may be costly for SMEs, making SDTL accessible to big enterprises only.

11 réponses



Open Source ; Ombudsperson ; Whistleblowing ; User reporting channel ; Open for external assessments

	Open source	Ombudsperson	Whistleblowing	User reporting channel	Open for external assessment
Description	The source code of the service is made open	The role of an ombudsperson is defined, for investigating, reporting, and resolving user complaints	Include the whistleblowing possibility within a company, in SDTL criteria	Establish a channel/contact for end-users to report observations to the label body (ex. SDI). For example: "the service stopped using 2-factor authentication."	Not only auditors are mandated to perform the checks. Organisations like Chaos Computer Club, or researchers, can perform specific checks on the service.
Pros	Provides high transparency. Makes the verification of the criteria easier.	Complements the task of raising the awareness of users, connecting them to the service providers, while raising the accountability of the service providers.	Complements or replaces audits in a very efficient manner.	Enables continuous observation of some criteria beyond the audit periods. More people (than the auditing body) can watch for the good practices.	More transparency Wider range of checks Reduces audit costs
Cons	Possible issues with IP rights	The work load of the ombudsperson is considerable.	Hard to implement in SMEs.	Adds the load of managing and checking the user reports to the label body (ex. SDI)	Adds considerable load to SMEs Adds the load of managing these checks to the label body (ex. SDI)

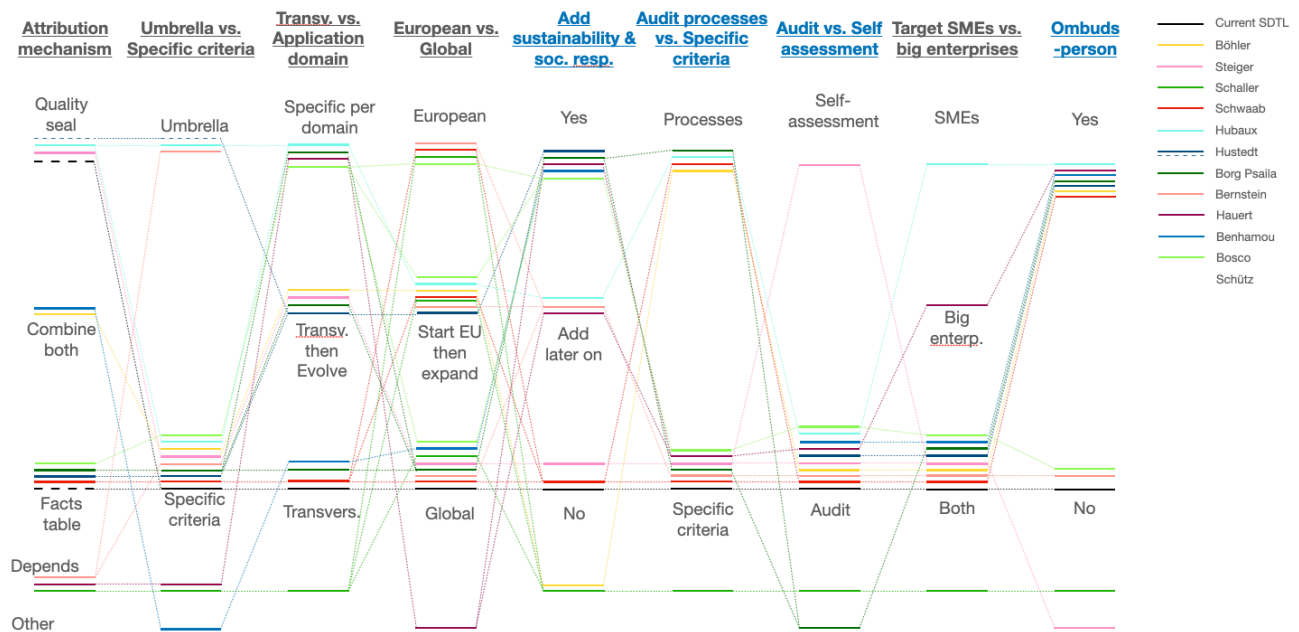


5. The resulting recommendations

Note that the design directions described in the previous section are not all independent from each other. For example, a "quality seal" is likely to require "extensive lists / umbrella of criteria". Therefore, the resulting recommendations cannot be based on the support level of individual design directions, but rather they must take the dependency into consideration. This aspect is reflected in this section.

The following figure shows:

- The design directions and the corresponding possibilities (summarising the previous section)
- The choices made by the individual members of the Experts Committee
- The levels of support for the current configuration of SDTL
- The recommended solutions, consisting of the "paths" with the largest consensus.



The 2 widths of lines correspond to the choices "Strong support..." and "OK for..."

The levels of support for the current configuration of SDTL

The graph shows that the most supported components of the current version of SDTL are:

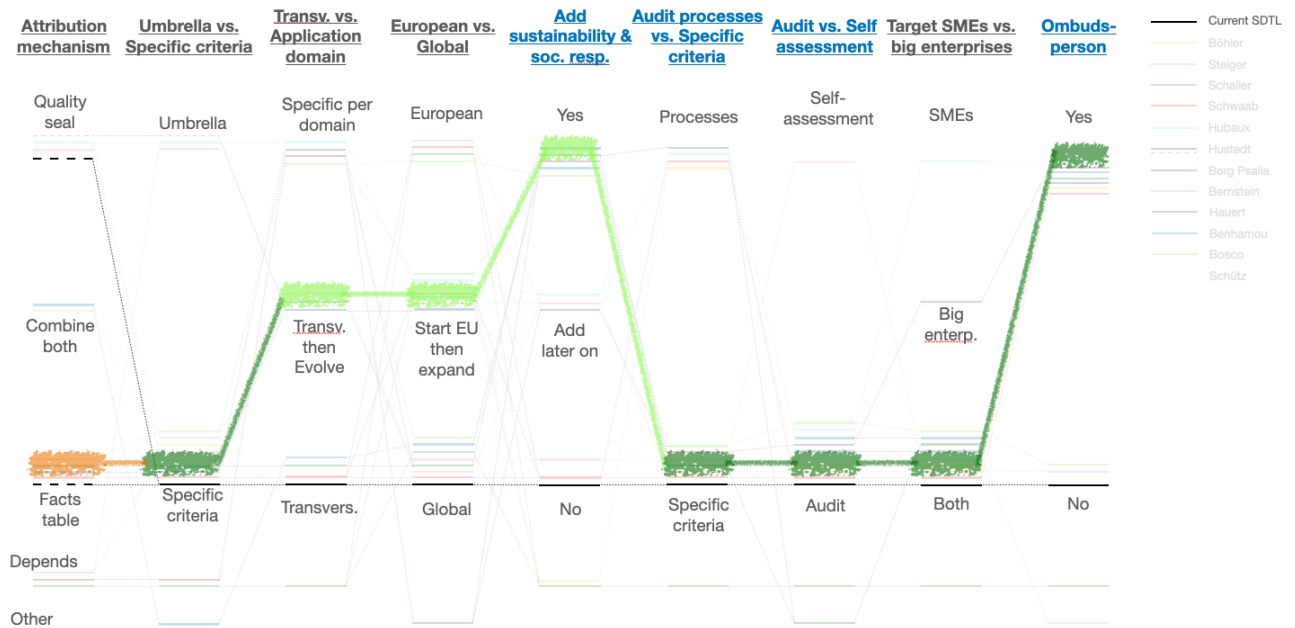
- Targeting both SMEs and big enterprises
- Based on audits (vs self-assessment)
- Based on lists of specific criteria (vs umbrella of existing standards and regulations)

On the other hand, the least supported components of the current configuration are:

- SDTL does not include sustainability and social responsibility
- SDTL is transversal across various families of services (ex. Financial, social networks etc.), and does not tackle domain specificities

These can be improved by opting for the more supported counterparts, making the configuration closer to the recommended solution described below.

The recommended solution



We can see that the most supported solution, shown as the thickest line in the graph, is a configuration consisting of:

- Listing specific criteria instead of the umbrella approach which covers complete standards and regulations
- Starting with an approach that is transversal across families of services, then moving into the specificities of each
- Start European and go global afterwards
- Adding sustainability and social responsibility to the trust criteria
- Auditing, instead of self-assessment
- Aiming at both SMEs and big enterprises
- Integrating an Ombudsperson function

Additionally, there is a large support for:

- Open source
- Whistleblowing
- Establishing channels for user reporting

The expert committee acknowledges that the decisions for the three directions (in light green) are typically strategic. For instance, "adding sustainability and social responsibility" is a considerable added value which makes SDTL stronger and more appealing, at the cost of requiring further work and the inclusion of experts in the field, hence further delays to go to market. On the other hand, excluding them would make SDTL's deployment faster, while potentially making it weaker and prone to failure. More detailed arguments can be found in [Section 6](#) below.

Making SDTL specific per domain requires the implication of experts in these domains in order to write down the corresponding criteria. On one hand it avoids having SDTL "too generic", but at the same time it introduces a huge overhead to onboard these domain experts, and then to keep SDTL up-to-date with the changes in these domains. More detailed arguments can be found in [Section 6](#) below.

The most divisive question (in orange) is whether to make and communicate SDTL as a "quality seal" or as a "list of trust facts", or as an intermediary option "list of trust facts with a trust rating". Each option has its advantages, drawbacks, and specific overhead/delay before going to market. During the interactions with the (8) test users, some of them showed interest in the "quality seal" option, while others pointed to the risk of raising false expectations when using a quality seal with non-exhaustive criteria. User preferences is another major factor in this decision. The ongoing

user study is expected to shed more light on this regard. Besides the split in the opinions on this question, it is also a strategic decision on which the SDI Board can decide. In order to help the SDI Board making the decision, we list here the related arguments.

- "I strongly speak out against a quality seal only approach since this will not provide the necessary differentiation and might create a false sense of trust. Under certain circumstances I could maybe see a combined approach as feasible. In that case we would need to carefully check again the criteria that need to be met to get the quality seal."
- "A label should offer information and facts. It is the user/recipient who should then make his/her own judgment based on the facts the label is offering. The efficacy of any normative function is lost when applied to such a fast-evolving environment such as digital technology."
- "I imagine a public SDTL report (informative, comparable to the nutrition facts) and a systematically deducted scoring per category (normative, comparable to the nutri score). The normative scoring is important to give individuals a clear indication on how to judge the digital service, as most people won't want to invest too much time. The scoring per category allows for a more nuanced scoring. A company can e.g. be bad in data security, but good with responsible user interaction. The informative report is important to convey relevant background information to make sure that interested individuals can understand the evaluation and scoring system and make up their own mind."
- "From a legal perspective, the distinction between the two is blurred / a bit artificial. Both would have the legal effect of indicating properties of a product / service vis-à-vis consumer. The major difference being the business perspective, as the informative approach would possibly help to save control and auditing expenses."
- "The fact table is easier to achieve and makes no claim about the degree of testing. The label requires strict quality control otherwise its not really trustworthy. Also, if one chooses the label then it needs to make clear that it does only check for a limited number of claims."
- "To be defined on the basis of use cases"
- There's an issue in the label design when you say "this website *has earned...*", it makes it normative across all 4 labels. As a user I don't want someone to judge on my behalf. I just want the information/rating of each criteria and I make my own judgement. This is an "informative" label. All the rest is normative.
- Note that all the projects that have failed, it's because they were not clear since the beginning, from the users' perspective. It is a key element to understand how the users will perceive it.

Communication

Several members of the expert committee raised the point of communications around the label, and its extreme importance conditioning to the success of SDTL. We can split it 3 parts:

- How SDI (or the organisation managing the label) communicates or advertises the label to the users
- How SDI (or the organisation managing the label) governs how the label is being used
- How companies communicate the label

Common note regarding the three points above is that extreme care must be taken such that the label does not give, or is not used to give, a false impression of trust. For example, if "facts table" is opted for, the communication around the label, by SDI or by a company, must not hint that "the facts table is awarded, therefore the service is trustworthy". Even with the "quality seal" option, care must be taken for communicating to the user what is covered or not by the quality seal.

Besides the risk of misleading the end user, intentionally or unintentionally, the issue of wrong communication brings in the liability of SDI, and the success of SDTL in general.

6. Opinions on each design direction

In the previous sections we listed the arguments related to the undecided component (quality seal vs facts table). In this section we also list the main arguments related to the other components.

Attribution mechanism: Informative "facts table" vs. Normative "quality seal"

(Some arguments were listed in the previous section, repeated here for completeness of the section)

- A label should offer information and facts. It is the user/recipient who should then make his/her own judgment based on the facts the label is offering. The efficacy of any normative function is lost when applied to such a fast-evolving environment such as digital technology.
- There's an issue in the label design when you say "this website HAS EARNED...", it makes it normative across all 4 labels. As a user I don't want someone to judge on my behalf. I just want the information/rating of each criteria and I make my own judgement. This is an "informative" label. All the rest is normative.

Note that all the projects that have failed, it's because they were not clear since the beginning, from the users' perspective. It is a key element to understand how the users will perceive it.

- As I have already pointed out, I would really like to understand who is supposed to use the the label and how the label is supposed to be used. Depending on that, one or the other (or even both) makes sense or not. At the current state, I get the impression that we want to write a book, but don't know who the audience is...
- To be defined on the basis of use cases
- I imagine a public SDTL report (informative, comparable to the nutrition facts) and a systematically deducted scoring per category (normative, comparable to the nutri score). The normative scoring is important to give individuals a clear indication on how to judge the digital service, as most people won't want to invest too much time. The scoring per category allows for a more nuanced scoring. A company can e.g. be bad in data security, but good with responsible user interaction. The informative report is important to convey relevant background information to make sure that interested individuals can understand the evaluation and scoring system and make up their own mind.
- I strongly speak out against a quality seal only approach since this will not provide the necessary differentiation and might create a false sense of trust. Under certain circumstances I could maybe see a combined approach as feasible. In that case we would need to carefully check again the criteria that need to be met to get the quality seal.
- From a legal perspective - however in my view and as indicated in a previous meeting, the distinction between the two is blurred / a bit artificial. Both would have the legal effect of indicating properties of a product / service vis-à-vis consumer. The major difference being the business perspective, as the informative approach would possibly help to save control and auditing expenses.
- As mentioned above, this is a strategic decision as to what the SDI wants to achieve.
- The fact table is easier to achieve and makes no claim about the degree of testing. The label requires strict quality control otherwise its not really trustworthy. Also, if one chooses the label then it needs to make clear that it does only check for a limited number of claims.
(Informative) Most attainable-to work on the narrative for the end-users

Umbrella approach vs. Specific criteria

- More or less fine with both, verging slightly toward specific criteria
- Compliance with GDPR etc. could not be audited. Reliance on existing certifications would rule out participation of most SME. (Many important companies in the digital space are SME.)
- Same as in the last point
- To be defined on the basis of use cases
- I don't think that including "all criteria" is an option, that wouldn't be possible anyways. I think a label is always about taking decisions and defining priorities. But of course, the priorities need to be well reflected and on point.
- In case of the fact table I believe the "specific criteria" might be the right way to go. The challenge in that case will be to identify the criteria that are relevant and easy to interpret through the users. In the case of a normative quality seal, I would strongly vote for the umbrella

approach. We cannot risk giving out a seal for a product that does not comply with standards and laws like GDPR.

- I changed my mind: before I understood that the SDTL wanted to go with an umbrella approach (kind of a gold-platinum labelling covering all aspects, including the GDPR-certifications) and I strongly supported to ask for a GDPR as a prior-requirement for entering into the SDTL. After consideration and further to our meetings, it seems that a specific criteria approach is good too, as (i) there will be several GDPR-certifications anyway, so that we want to make the difference with other criteria, (ii) we want to go glocal (i.e. first local then global, with companies not specifically subject to the GDPR) and (iii) an umbrella that includes the GDPR-compliance would mean a more detailed SDTL with more GDPR-criteria and a delicate audits / controls to enter and maintain the label. This being said, as an alternative approach, we could consider having a GDPR-prior certification as an additional criteria.
- This is mostly a communication challenge.
- If the umbrella option is chosen, then it will be the "only" label consumers have to look for.
- If the other option is chosen, then one needs to make consumers aware of the incompleteness of the label and that they should look for the combination of labels (e.g., SDI + GDPR + ???, etc.) to ensure their needs.
- Both have their merits but require precise communication.
- (Specific criteria) Easier to develop and deploy-including auditing

Transversal vs. Application domain / family of services

- Feasibility is a big issue. There is a huge number of criteria to be defined to make the label meaningful across domains. Take for instance Facebook, Uber, and airbnb. Criteria from one won't really apply to the others. One has to start with a subset that is clearly identified. This is a formidable challenge to be conveyed to the SDI Board: make a meaningful label across services, and the efforts this requires. These domains grow extremely fast, and following them is a noble but difficult ambition.
- 'Iterate Fast and Release Often' approach
- It is not clear what is meant by transversal; does it mean the label would address IoT, web services, apps and all kind of connected devices?
- How is family of services defined? A possible option would be to target a specific type of services (search engine or mobile apps for instance) to start with. Regarding the "evolve later on", whatever the option chosen the Label has to evolve later on according to consumers demands, business needs and opportunities that will raise in the course of the project.
- I would start with the umbrella approach in order to keep it simple enough (it's complex already) for the beginning. I can imagine that at a later stage we notice that it makes sense to start more specific labels for family of services.
- The check, whether a transversal approach makes sense should be conducted shortly after the introduction!
- (i) From the beginning the transversality was the idea, (ii) that is where we can make the difference (e.g. compared to ISO-norms or other seal projects), (iii) understandable and reassuring from the consumer perspective, which is the most important criteria in my view, (iv) and we have the capacities within this Expert Group to solve this issue of complexity.
- (Other) I would say to start specific to test it in a couple of sectors and derive criteria/lessons learned potentially applicable to others.
- We've been working so far on a transversal label. Do we have the time to include experts from 4-5 different domains to write criteria for these specific domains? just keep it as it is.
- I'm not sure it's a good idea to go domain-specific and compete with the EU's efforts in this domain already.

European vs. Global reach (incl. China and US)

- Fully agree with "Start EU then evolve" but let us be clear about the question. Are we talking about the clients/companies? about the beneficiaries/end-customers? or about the criteria?
- I don't see why we need to limit the scope to EU as long as we don't stick to GDPR
- It depends on the international partner you choose. ISO and IEEE won't make european specific standards.
- The ambition should be Global. How we get there is a different question.

- If the label will consider specific criteria (rather than an umbrella set of criteria), then I see the global approach as offering added value to the label's aim
- There's no such thing as 'Europe' in the digital space. Everything (OK, almost everything) digital in Europe is related to China and the US anyway.
- Of course this depends if both options are feasible or make even sense...
- Not sure what is meant here - let's see what is feasible and existing opportunities rather than take a principle decision. What does it mean for the scope of SDTL to remain European: are we talking about the content? The targeted business? Or benefiting consumers? Is there not anyhow an ambition to be globally recognised?
- A clear focus (target area & group) is relevant for the beginning of every projects. I don't think the STDL can start global, but it might be able to expand globally at some point. For the moment I would focus on Europe, evaluate the learnings and progress and then decide how to continue.
- Double strong support for Global, as (i) digital is global, (iii) Switzerland & Geneva have their role her to play and (iii) we observe about the convergence of norms (e.g. for data protection with GDPR, Californian Act), also due to the extra-territoriality of more and more norms, so that there is a need to have a consistent global approach.
- This largely depends on the strategic answer to the first two questions (normative vs. informational & umbrella vs. collection of subset).
- Whichever option is key since will have a big impact on process/actors/timeline

Add Sustainability and/or social responsibility

- (Having chosen not to include them) I am fine including them IF the proper criteria are there, written by trustworthy experts in the field. There are different organisations with different views on these matters, with no consensus. Choosing the right partner organisation is crucial for the trustworthiness and success of SDTL if it includes sustainability and social responsibility.
- Again, both add value to the label; with the additional two (or one) categories, the label provides a more holistic set of parameters
- Mon expérience montre que de tels critères sont impossibles à certifier.
- To be considered with the opportunity to gain support from or integrate existing private and public regulatory initiatives
- I would evaluate this after the first feedback of the public & user testings. Personally, I would love to add them right now, but maybe user testings show that this is not a priority and that it would overwhelm users anyways to include even more information in the label.
- If the seal wants to be taken serious in the expert community (and particularly civil society) I strongly advise for the inclusion of these factors. In addition I so actually think that these factors matter to a lot of consumers already and that they will matter even more in the close future.
- Strong support for "Yes, Add them", as it is a key topic and SDTL could make here the difference (originality compared to other existing labels), however only provided that clarity (see above), otherwise to be completely removed. I am very happy to see this topic, at least thematized, as I personally brought this issue at several occasions / meetings and consider it as an important one.
- This is -- again -- a strategic choice. In particular, it depends on whether SDI is an umbrella label or one label in a collection that people will be looking for.
- Try to be bold and innovative
- How about adding Green-IT instead of focussing on sustainability? (<https://ec.europa.eu/energy/intelligent/projects/en/projects/green-it>)
- This can cover a very wide range, and it becomes very tricky if we adopt the informative approach, identifying what to cover exactly.
- I can add a counter-argument, which is from the trademark and IP perspective. We speak of strong or weak trademark. If you're too broad, you loose strength.
- SDTL (digital dimension of services) should be part of sustainability, rather than the opposite way round.
- Add sustainability criteria related to what we have in the label, not overall sustainability.
- Adding sustainability would definitely add value, because people link trust to sustainability. It will depend on the time-frame for the development of the label since this needs time to be included.

Auditing Processes vs. Specific criteria

- Note: I'm not 100% clear on what a process audit entails specifically. The concept is slightly elusive to me...
- Note that specific criteria might refer to processes
- I don't think specific criteria will be enough to judge the elements we currently want to include in the label. Plus, an independent auditing process creates trust.
- I do believe that there will be a need for both, technical requirements as well as requirements for the process (i.e. when it comes to transparency).
- In the mind of most people a label usually conveys state not process.
- (Auditing specific criteria) More manageable

Assessment: audit vs. self-assessment

- Why not provide both options, with a clear indication on the label itself? Cost should not be a barrier for participation; at the same time, larger companies may prefer outsourcing (and paying for the service). In practice, the end-result should be the same (ie, label should indicate values or grades for the same set of parameters, regardless who conducts the audit).
- Maybe two different levels?
- I don't know any self-assessment schemes that work properly. Especially when it comes to digital corporations, mistrust is too big, to my mind.
- I understand, that audits can be costly for SMEs. We should look for mechanisms to support them in this regards because the label can be a great way for SMEs to differentiate themselves from more mainstream products.
- Strong support for "Audit", as I am not even sure we can go for a "Self-assessment", or before we should analyze first some complex legal: (i) the certification trademark requires that the owner, i.e. SDI, keeps a certain control over its trademark, which would exclude a "self-assessment" approach and would mean to have no trademark, hence lose control over the SDTL and (ii) a pure self-assessment could be even more complex in terms of liability.
- One might be able to mitigate the cost for SMEs by setting up some subsidy scheme.
- (Audit) More reliable-it can be the starting point moving into self-assessment on the long run

Target: SMEs vs. Big Enterprises

- The cost factor would be solved if both self-audit and third-party audit are permitted (previous q)
- Criteria should be general anyway. Example: Requirement to publish a transparency report.
- SME's might use services of "big enterprises" (e.g., a Google service). How would that be handled in either case?
- Mais attention aux coûts d'audit, qui pourraient être impossible à assumer pour les PME
- Trust issues either arise with regard to big company, the effort to adress SME might not be worth of the impact; Choices of company targeted might also be framed according to the number of users of a services worldwide: does it concern 1k person or 5000k people on earth? We should target digital services that are widely implemented and used
- I would try a gradual pricing, which increases with the size of the company. Thereby, there would be no cons.
- Success depends on voluntary adhesion of the SDLT, including major companies. A way to be faire would be adapt the costs depending on the size of the companies (which would be justify, if we have audits / controls, as bigger companies would mean more work / audits by the auditing firms).
- The goal should be to have the label be used by any participants. If cost for SMEs are prohibitive then we need to find other means to lower the cost.
- (Both) It's meant to assess the services/products, not the companies

Open Source

- As argued via email, I think we absolutely need to mention open-source to be taken serious as a label. And to make it feasible, we don't have to make it count for the scoring.
- The fact that the source code is open is enough to show how transparent things are.

Ombudsperson

- Ombudsperson and whistleblowing are relevant and trustable elements, plus, they make the label criteria more unique.

Whistleblowing

- Ombudsperson and whistleblowing are relevant and trustable elements, plus, they make the label criteria more unique.
- Whistleblowing can suggest that the process can be easily exploited. Even if loopholes were to be found, this can lead to unwanted assumptions, and can erode people's trust in the label itself.

User reporting channel

- The user reporting channel is highly relevant to be open, inclusive and trustworthy. This are crucial values for the SDTL.
- I would go for rather being sure to have the two selected in place since the beginning and then to possibly invest in the others

Open for external assessments

- No go for “external assessment“ at least we go for a certification trademark, as the trademark owner (i.e. SDI) is required to keep a control over its trademark, which would hence exclude external non recognised and controlled third parties.
- I'm not sure how the open for external assessment would work, but the short description here sounds good. Including trustworthy, well-known civic society organisation would definitely be a plus for the label.
- External assessment would also be going too far
- I would go for rather being sure to have the two selected in place since the beginning and then to possibly invest in the others

7. Opinions on SDTL's approach

Color coding: Good; Good but...; Bad; Proposals for improvement underlined

Do you think that Labelling Trust is **relevant**?

- The initial idea is good. It's the feasibility that is difficult (see general comment below)

- It is relevant, especially that it is aimed to users, since there is not enough awareness. It is also relevant for the service providers, since it provides measures of accountability. It also provides a differentiating advantage.

Martin: why do you think people or companies would care?

Stephanie: it's the network effect. If a lot of people care about it, the others will start doing so. Moreover, for companies, the differentiation factor means more profits.

I see SDTL clearly applicable to B2C, not B2B where it is not detailed enough. SDTL is very basic, fits B2C.

- Defining what should be in "Trust" is essential. (Jump to the analogy with the nutrition facts). The educational factor is excellent.

Martin: example of credibility of SwissCovid.

JC: supporters and critics were coming from all directions for SwissCovid. Having an external trustee like SDTL would be excellent.

Imad: Currently there is a lack of reference with which users can compare SwissCovid to Facebook, for instance.

- Labelling trust is a good and important problem to conduct, yes.

- Trust is a recurring issue that is extending from sector to sector. In addition there is a wide usage of technology. The general public is more knowledgeable and tech savvy, and trust is taken into consideration. The label is definitely relevant. Even for the less tech savvy people, there is a kind of appetite for this type of labels. There is also nowadays an overwhelming amount of information, so a label will help the lazy ones to make their choice.

Where it becomes very challenging is the compromise between the technical specification and the human-centric approach (being technically deep and at the same time palpable to the users).

On the educational effect of SDTL: yes indeed. I have seen similar effect with the release of GDPR. After its release and all the changes to T&C, people started being more aware about privacy, asking questions they never thought of before. People had privacy in the back of their minds, and such initiatives make it concrete. That's why I am a big fan of this initiative. It's a tough road, but it's worth the pain.

It won't be easy to have the same level of technical assessment and perception of the end-users, because they have very different levels.

- labelling digital services, especially with criteria, is very important.

Linking trust and transparency can be complicated: people may get suspicious if there is a lot of details provided (like short motivation vs over-explaining).

- Sure, many people are getting concerned about the use of their data. There is however a mismatch between the discourse and the practice. For example people are skeptical about SwissCovid app, while at the same time they use WhatsApp and don't care about the trust issues behind. The consumers are not mature to act according to their words but probably this will come in the next years. So yes, the problem of having trustworthy applications and digital services is relevant.
- It is highly relevant. I'm not sure it is feasible.

Do you think that Labelling Trust is **feasible**?

- It becomes feasible if it is self-driven, not as an audit by a 3rd party. Count on spot-checks, whistleblowers, not on audits. But it must be verifiable, yes.
- Try to test SDTL on some products (ex. hardware, which are not the original aim), not on services (ex. Booking a hotel room), and you'll see where the weaknesses are.
You may encounter difficulties in feasibility if you don't focus on one area like "e-commerce" (e.g. booking.com) rather than infrastructure/technology providers (e.g. IBM, Swisscom) for instance. In e-commerce, users rely a lot on other users' reviews. This is not the case for infrastructure/technology providers where a label can have a bigger impact.
Imad: the criteria of the label are the same, but the impact would be different.
Stephanie: exactly

- In SDTL there may be too many criteria to be readable. It's not like the bio label for instance, where the same philosophy applies everywhere. With SDTL there are a lot of categories that are independent, and cannot compensate each other. If the label is not readable the users would be lost.

Martin: this is essential. Indeed, the users won't see this list of criteria but a simplified representation. We have to avoid specific things while reaching other. We have to avoid that the user misunderstands that the label is given then he/she can trust the service. SDTL cannot guarantee security/reliability etc. What SDTL wants to reach is to show "what's inside" the service, such as the user can decide whether to use or not. Would this work you think? Does it meet your expectations?

JC: this will depend on how companies will use it and advertise having the label. "This is the label, make your choice" vs. "We have the label, trust us". Governance of the label, its usage, and possible sanctions play an important role here. I'm looking forward to see what SDTL will propose on this regard because this is the core of the problem

Imad: conditions of usage of the label must be set.

The core question is how to provide a friendly and accessible and understandable criteria for the consumer, as well as auditable criteria for the auditors.

- Where I see the label difficult is the process, and making the label understandable to the general public.

Martin: we already received the critic of some experts, about raising false expectations from the users, about the trust level w.r.t. the list of criteria vs. in general, for example on the security side, where SDTL does not check everything.

Francesca: it's a very valid point. It goes back to my observation regarding the process. The communication may be a tricky part. It must be scientifically and technically strong enough, and at the same time being an effective tool for the general public, user-friendly.

- you can never portray all aspects of trust, but it is important to try. It can have a positive effect if we do it well. If it is made wrong, it can create more harm, false believes of trust. It's not black/white, we have to constantly work on it.

- On the other hand it is a big challenge and I have strong doubts about the feasibility of creating a meaningful and sustainable label. This is not against SDTL specifically but in general. A nice

example is e-voting. Cryptographically it is amazing, and in the end it should be doable. But the question is if we deploy an e-voting system, only a few people would understand why such a system should be secure. Cryptographers would understand them and tell you that this is secure, you can trust. Compare it to the current ballot voting system, more people would understand it more and its security. In the first case people must trust what the few cryptographers say about the system (and the math proofs) without understanding it. People won't trust with their own understanding. If somebody comes and says "no there is a problem in the system", is it false claims?

Same with SDTL (or any other label): how to make people trust the label (the few people saying it's good) despite other people making false claims?

There will be situations where there will be problems with SDTL, applications declared good/secure and someone finds a vulnerability, showing the label is wrong. What does this mean for the reputation of the label? Do you know how you'd re-establish the reputation of the label?

Imad: SDTL is informative, not a stemple "service good"

Patrick: what is the understanding of the user? If the application has the label, he'll perceive it as "good".

Niniane: Now we're working on the technical content. At a second step we'll make a big user study to see how we can communicate properly with the users. We're also thinking of what todo when a company breaks it commitment to the label criteria (risk for the label)

Patrick: These don't always come on purpose. Look at the vulnerabilities that showed up in the last years (meltdown, spectra etc.). Every web application running in the cloud became vulnerable.

What would happen then? Would you un-label all these services?

Martin: the label does not provide a guarantee of quality. It is, like the nutrition facts, informative. Not so many people understand these, like in the examples you gave. This information provides them information to help them decide as they wish.

Patrick: this is the right approach, but it can be that this is not what the people expect from the label. They expect that the label tells them if an app is good or not, and we know this is not possible. If SDTL marks a service as "it meets these criteria", half of the population would understand that it's a green light, app is secure. If later on a library used by the service shows to be faulty, there's a reputation risk for the label. I fear this is what most of the people would expect, secure/unsecure.

- I'm not sure this is feasible (in the absolute sense), as pointed out in the study "digital services are not bananas".

Besides, there is the feasibility of SDTL considering the body backing it (see the General Comment below).

What do you think of the "identification of the areas that define digital trust"?

- These are good categories. The main concern for the user is transparency, and how his/her data is treated, and his accesses to it.

- "I would think trust is a monolithic concept, rather than splittable in order to get it quantifiable. Trust is the conclusion the user puts on a service.

Imad: you are distinguishing between trust (from the user side) and trustworthiness (the value, on the service side)

Stephanie: exactly. Still, even if you're talking about trustworthiness, it is a monolithic concept, a single umbrella covering the categories you're listing here. The user does not require this or that category, he/she care about the whole thing."

- The identification of the areas that you made in SDTL is very good. The splitting into the domains is very helpful.

- It is a wide area / many categories, this is why we need to map it into a few to make it more tangible (they also used the same approach for their label). What is also good in SDTL is that scoring well in one category does not balance a bad in another category.

- I think these are the right fields. For all these fields it's a challenge to bring them to a "label" (ex. Security is OK, privacy is OK...). Privacy may be labeled "OK", but then the user posts whatever, assuming it's OK with Privacy. Again, there is a problem of what the user understands in the label.

Do you think the **identified categories are good? enough?** (security/privacy/reliability/fairness)

- The categories are fine. I'd just use "fair use" instead of fairness. (Btw "Fair use" has a connotation in the copyright world)

Martin: how about digital sustainability and social responsibility? These were proposed before.

Stephanie: Good points, they are good to have, and they are easy to assess.

Martin: the issue is that these are more related to the service providers rather than to the services themselves, that's why they were not taken.

Stephanie: I don't agree with that. It does not fly as a justification why sustainability is not there. If you're distinguishing between service and service provider, you're removing the notion of accountability. You may be providing escape routes with this distinction. Start with the 4 categories and eventually introduce the 5th one which groups sustainability and social responsibility under one name.

- To me it looks quite complete.

Martin: we were told to include sustainability and social responsibility also.

Imad: it's not only to show what people care about, but also to include the educational factor and show what people should care about also.

JC: who are the experts who would say if a company is socially responsible? This would multiply the size of the committee x4. There are many controversies regarding social responsibility and different definitions, approaches, and metrics depending on the organisations. It is almost impossible to certify.

- I really like the categories.

Martin: we have been criticised for not having sustainability or social responsibility in the categories.

Francesca: I wonder if these need to be criteria in the label...

Martin: these criteria apply to the company, not to the service.

Francesca: exactly

- Maybe it is more clear for the users to use "Privacy" instead of "Data management. "Fairness" is better than "interaction with users".

Accountability is not specific to reliability.

Fairness: it should not mean that the system is fair but that the fairness was accounted for during the development process.

Carla: Sustainability is missing from the categories

Imad: this has been considered in the past but kept away for simplicity, and because sustainability does not link directly to Trust.

Carla: sustainability is important for transparency and to help people choose. The 4 categories came from the user-study and this is what they want, but such a label should have an educational aspect, to make them care, to tell them what they should care of.

- I looked at the list of criteria, and I find it quite exhaustive, not missing important aspects.

- I think these are OK. The problem is the interdependence between services using each other (ex. App using google ads). Is this covered? The application itself may not have any privacy issues, but it uses an API from another provider that is not good in privacy. How would this fit in these categories? Or are there new categories to be introduced for this?

Imad: this is an issue in each of the categories

Patrick: there could also be a category regarding ethics. Would a porn website be labeled or not?

Martin: there were initially discussions about this. Facebook provides a fair service, they provide what their users want, but it is not necessarily ethical in terms of filter bubble. So we restricted the label to what impacts the user directly. It would also include whether companies are behaving socially responsibly, but this would open a pandora box. This is why we restricted SDTL to fairness.

- I'm happy with these four areas.

Reliability is the least important one. People can see it by themselves and drop/leave the service. For the 3 others there can be hard or soft legislations around them, to really encourage companies to behave because it's very easy to cheat.

Martin: NGI's proposal include sustainability. Do you think this is important?

J-P: Consumption habits will evolve, and services should not be decremental to this goal (ex. Plastic wastage, energy consumption), but it's not at the same level of importance. The project is so complex and so loaded, that I wouldn't include sustainability. This can be added at a later stage. Let's concentrate on few ones: security, privacy, fairness. Reliability will be regulated by the market.

What do you think of the **transversality** of the criteria? (same set of criteria for a wide range of digital services)

What do you think of the idea of a "Digital Trust Label" to **"inform the user about the most relevant trust-related criteria"**?

Imad: how about the situation where a service has the SDTL label, but is not GDPR compliant (Ex. Does not provide data portability)?

Yaniv: this is why we have to be very careful about the communication of the label and SDI's liability. If the communication is not clear enough then SDI can be made liable.

Martin: how about the proposal of Thomas Schneider about formulating SDTL towards transparency, not about guaranteeing that there is a given level of security/privacy/reliability....? SDTL forces companies to say which level of security/privacy/etc. they are ready to provide? Of course this must be above the legal minimum. Can this fly?

Yaniv: this is the pure informative approach which does not exclude to commit legally to some terms. Even though it's a informative note, it's still a legal commitment. Due to this legal confusion, I highly recommend SDI to have an insurance.

Imad: SDTL now has an informative component, and a normative one. The informative one seems to be safer than the normative one. For instance, if SDTL defines an aspect as good enough, while it is less than the legal minimum, SDI may be branding something "good enough" while it's in fact illegal. (Example of Martin of the data breach notification period of 92h for SDTL, for example, vs. 72 of GDPR)

Yaniv: SDTL should stick to the minimum legal requirement. SDTL can put a very clear visible disclaimer about a criteria being less than the legal requirement. But still a user can claim being misled by SDTL, raising his expectations about the service despite the presence of the disclaimer. Expectations is the key word here, not the exact content. Expectations of the consumers w.r.t. the label.

What is your opinion on the **analogy with nutrition facts**?

Do you think the **proposed method achieves this goal**?

Do you think the **proposed method is useful to build user trust in digital services**?

Do you think **SDTL would weaken or strengthen the current requirements for digital services**?

Would you use the 'trust fact' table of SDTL?"

General open feedback

Initial discussion was around liability and governance in the setting-norm process (democratic legitimacy).

1. Liability

When a company does not comply with a criteria:

which is GDPR and SDTL (ex. notification of data breach) -> Company can be made liable based on GDPR and on commitment to SDTL, as a contract. SDI can be liable.

Which is SDTL only (ex. non-discrimination) -> Both company and SDI can be made liable.

Solution:

Care must be taken of the communication of the label to reduce SDI liability

Very strong contract with SGS (the auditor) to move liability to them. Attention to sub-contracting the audits to 3rd parties.

SDI does the job well choosing and checking the auditors.

An alternative to that, is to draft the criteria and not to be involved anymore in the auditing processes (like it is the case for creative commons)

2. Governance

As the main scepticism about labelling and self-regulation is the governance and decisional power of the stakeholders involved (e.g. with the Facebook oversight board, main criticisms are that such board does not have, or only a limited decisional power vis-à-vis Facebook), the key question for Yaniv is to have a transparent and clear governance structure in the setting-norm process (including a precise roadmap, role, scope and decision power of each stakeholder involved in the setting-norm process as well publicity of their statement, such as meetings, workshops and bilateral meeting).

Such governance process shall ensure procedural legitimacy. In this respect, Yaniv raises concerns about the role and decisional power of the Academic Expert Group, in particular if the SDI Board can just acknowledge and reject its proposals without justification and publicity. He recommends either to have a specific decisional power or at least to be able to issue recommendations that shall be made publicly available & (if rejected by the Board) justified. A solution could be to get inspired by the CJUE with the general attorney statement, that is always published and justified by the CJUE.

8. Opinions on SDTL's current list of criteria

General feedback