SWISS DIGITAL INITIATIVE

Report on the Label Catalogue Mock-Audits with Test Partners (companies and public organizations)

Executive Summary

From May to December 2020, six companies and public organisations took part in mock audits, using the first draft of the Digital Trust Label Catalogue, prepared by an expert group at EPFL, ETHZ and the Universities of Zurich and Geneva.

Test partners expressed their need for guidance to help them comply and better understand the aims of the criteria and implications. Some insisted they should have the opportunity to describe the full lifecycle in the audit and give the reasons why a specific implementation or process is appropriate.

Partner feedback was similar across the board, notably:

- Such a label would be something nice to have but very complex to make right
- The label should go beyond the law
- Context can be very different (private and public, with or without login, ...).
- Criteria could be nuanced in their expression (if this... do that... otherwise...).
- Criteria should be technology agnostic
- Criteria regarding manipulative and deceptive techniques are very innovative

In general, test partners were highly interested in the community built around the initiative and the possibility of networking. For the test partners, the main interest of having a Label is to be able to differentiate from their competitors and to showcase that their digital services are trustworthy. Another reason mentioned is to measure against a certain benchmark / standard and to get an idea of how trustworthy their digital services are. Most of the test partners would favour a Label which stands for a very high standard, instead of a Label available to all service providers. A Label does not make sense for all kinds of digital services, but especially for those that make automated decisions or operate with user data.

The detailed feedback can be found in the report. In each section,recommendations are made. A list of all recommendations can be found at the end of this report.

1. Introduction

The Swiss Digital Initiative (SDI) is developing a Digital Trust Label addressing the trustworthiness of digital services. A draft version of the Label was created by an Academic Expert Group from EPFL, ETH and the Universities of Zurich and Geneva.

Six national and international test partners took part in mock audits assessing one of their services. The mock-audits consisted of six online workshops. The objective of these workshops was to test the feasibility and demandingness of the first draft of the Label catalogue.

8 Test Partners are currently part of the development process: Axa, SBB, Booking.com, IBM, Kudelski, Credit Suisse, Swisscom, Swiss Re and Canton Vaud.

Guiding questions of these workshops were the following:

Challenging the Label Catalogue with a concrete use case:

1. How important are the specific criteria?
2. Is something missing?
3. How to evaluate the criteria in reality?
4. Is it practically feasible?

Feedback on additional questions:

1. How likely is it that the organisation will implement the label?
2. Would the organisation adapt the Label, if it would only be informative?
3. What benefits does the organisation see in such a label?
4. How much money would the organisation be willing to spend on labelling a
5. digital service?

Output of the workshops

- List of criticisms/challenges on the content of the label
- Feedback on the feasibility/demandingness of the label

2. General Remarks

2.1. Clarify what Swiss Digital Trust Label stands for

The initial SDTL project stands for high level of commitment: *"For companies and public institutions, the Digital Trust Label can demonstrate their **commitment to high ethical standards** and their responsible behaviour in the digital realm. To behave ethically in the digital world should become a competitive advantage."*

Yet, some test partners find the nature of the label not clear enough. For them, SDI needs to clarify if SDTL is a premium label or a certification of compliance to existing standards. If the label goes beyond existing standards and laws, this needs to be a starting point and clearly communicated. The underlying question is what SDI wants to defend; what SDI wants to push.

SDTL project has an objective of educating the user *"As a first priority, the Digital Trust Label aims to provide guidance and transparency to consumers. It aims to raise user awareness and leverage digital literacy."* This objective was often used to justify the inclusion of criteria at law level. The ideas being that users may learn those important legal rights.

Recommendations

1) Each criteria and controls should bear a high ethical standard. Educating users about their legal rights are also important objectives. But educating users should not be at the expense of the SDI commitment for high ethical standards. It's important that each criterion taken individually is fully consistent with SDI's values.

2.2. Relation with existing standards and certifications

Test partners asked multiple times if the SDTL criteria were matching existing standards. They also asked if doing a mapping of the SDTL criteria with ISO GDPR and SOC 2 was planned.

Test partners have the legal obligation to comply with GDPR. They are also familiar with international certification on security such as ISO 27001 or SOC 2.

SDTL is for labelling digital services. Certifications may have different scope and certify the service providers instead of digital services.

Recommendations

2) Document when criteria are based or closely related to an existing standard. (This has been done by SDI in the meantime.)
3) A mapping of similar existing initiatives and standards, such as ISO 27001, GDPR, SOC2, would be useful.

2.3. Legal Responsibility and Reputational Risks

Several questions about the legal responsibilities and reputational risks for SDI that could potentially impact companies were raised, such as:

- What is the responsibility of SDI in case of an incident with a labelled service, such as a security breach?
- Malicious service providers could try to get the label by focusing only on the label criteria without caring about what the criteria try to test.

- Malicious service providers could put the label without authorisation. What will happen in such a case?
- What if SDTL provides false expectations?

During the discussions, it was proposed to have a disclaimer: "we don't have the security of the bank". But such disclaimer of trust should be evaluated.

Recommendations

4) Determine the responsibilities of each actor (SDI, auditor, service provider, users, etc.).
5) Define processes and policies for reputational incidents, legal risks, and malicious attacks.
6) Evaluate how consumers may respond to a disclaimer. In particular, if it affects consumer confidence toward the label.

2.4. Measurement and control objectives

Test partners were confused about the assessment of specific criteria of the Label Catalogue. The mock audit was based on a preliminary draft label catalogue and the Standard Operation Procedure has not yet been produced. Therefore, participants were informed of the existence but did not have access to the control objectives where this information could be found. Consequently, some criteria are hard to understand in practices and participants often said they needed more guidance.

The initial SDTL project stated that the Label should be easy to understand: "*To be credible, the Label should not only be technically sound, but at the same time easy to understand for users and reasonably implementable and auditable, so as to have good chances to be truly deployed in practice.*"

All test partners were excited by the perspective to have a Label that provides easy-to-understand information to the user. Several service providers underlined that SDI should make it hard for the providers to get the Label.

Recommendations

7) Communicate precisely what exactly needs to be "easy to understand for users". Users need to quickly understand the Label value proposition through the Label interface. The underlying content also needs to be transparent, accessible, and understandable. That does not necessarily mean that the content needs to be "simple" and "easy to understand". The mock audit showed that even for professionals, understanding the implication of some criteria was not easy. A reason for that was the missing SOP, which will be available, once the Label Catalogue is final.
8) Mechanisms can deliver contextual help and in-depth explanation. For example, a standardised and structured data format is key to deliver the underlying information in a machine-readable fashion. The same information can then be presented to the user in various ways. The user has direct access to a compact summary but can explore additional information about a given criteria or access guidance.
9) The strategy could also leverage social dynamics, such as informational relay: users may ask friends or do a quick online search. Other actors (and tools) could offer additional information and guidance to the user.

2.5. Guarantee the conformity of a service over time and ensure the Label is part of the operation

Test partners pointed that SDTL is a checklist, a collection of criteria, a snapshot of what is best practice today. There was also a feeling that things were being thrown together, very loosely coupled, as if different people had written the different parts.

Some test partners wanted the lifecycle and process, clearly and transparently described during the audit. For example, the service provider could describe what they are doing to secure user authentication and why this is the right approach in this context. The service provider could be audited against this description. It was argued this approach could also help for resilience where best practices are harder to measure: if something is happening, the provider should document what was learned. The idea was to make the label more coercive, part of the providers' operations and overreaching.

Some test partners suggested to require a description of:

- The digital service the provider wants to offer
- How the provider will deliver this service, including technical and non-technical processes
- The learning processes the provider has in place if something goes wrong

And then checking this with the auditor would be very valuable.

Recommendations

10) Objectifiable criteria were chosen because they seem easy to audit. Finding the right criteria for all contexts could be practically impossible without adding much complexity. One solution would be to have more flexible criteria where the provider documents different key processes that are then evaluated. But this could be done in the assessment of those criteria.

11) A criterion could ensure the provider has good internal processes to keep all the label criteria in check in the long run. This could also be part of the assessment instead of a specific new criterion.

3. Feedback on the Scope of the Label

3.1. Private and public sector, B2B or B2C

The SDI current assumption is SDTL would be limited to B2C digital service. However, two B2B services were included in the tests to see if there is an added value. There were discussions about whatever B2B service should be labelled or not. Having access to trusted labeled B2B service could help provide certified B2C digital services.

Partners highlighted that differentiating between B2B and B2C is not always easy. For example, clients may have to install the Java SDK, which is primarily a B2B service, to run a specific program. Businesses are also heavily using consumer products as part of their operations and to provide digital service to the final user.

Private and public sectors compliance may diverge. For example, data collection by a private actor must be based on informed consent and predominant requirement, while similar data collection by a government department must have a legal basis.

Recommendations

12) Check all content with the specificity of the private and public sector in mind. If the criteria must diverge in different contexts, this needs to be documented.
13) Strongly communicate to partners the label is strictly limited to B2C services. Eventually help them to select a service to test.
14) Provide examples of existing digital services that would be considered or excluded for the label. Also provide examples that are not easy to distinguish at first.

3.2. What is a “digital service”, granularity and perimeters

Test partners need a definition of “digital service”. Some asked if a product such as a *software development kit* (SDK)[1] could be considered as a digital service. SDK is a B2B product and is out of the scope, but a similar question could be asked for a plugin.

The context in which the services are provided is important. The associated risk may greatly diverge, and the Label must be appropriate for the purpose of the underlying service. Cantonal services are connected to other services (such as the services of the Confederation, for example). Similarly, SBB and booking provide a website/app which gives access to all the functionality of the company. Services could be accessed both with and without a login, which are two very distinct contexts was another given example by a test partner.

SDTL abstracts away from a lot of details, but how much is enough? What if someone is fulfilling the standards, but is very bad in all the aspects SDTL is not covering? There is a tension between auditing numerous criteria or reducing their number through abstractions and picking criteria that appear the most important for the end user.

Recommendations

15) Provide definitions of key concepts and an extensive glossary. Some definitions – at the core of the Label – seem necessary to avoid misunderstanding and to move forward.

[1] A software development kit (SDK) is a collection of software development tools in one installable package. Some SDKs are required for developing a platform-specific app. SDKs can be unsafe (because they are implemented within apps, but yet run separate code). Malicious SDKs (with honest intentions or not) can violate users' data privacy or damage app performance.

16) Consider the context in which the service is provided. The potential risks, the legal framework that apply and responsibilities can be significantly different depending on the type of service.

3.3. Third-Party Components and External Service Provider

Most participants are using external service providers such as AWS and some rely on a private cloud infrastructure. Similarly, the code depends on (thousands) third-party libraries and SDK.

Digital systems are by nature a stack of interlaced technologies. When digital systems are networked and deployed on client devices, this complexity and interdependence raise exponentially.

Building a digital service developer also relies on various toolchains and services (compiler, IDE, code repository like GitHub, local and server OS, virtualisation, and many more).

This raises the question on how to assess the service provider. What are the criteria to demonstrate a third-party component is trustworthy? How can we generate trust in a post-Snowden world where state agencies are secretly exploiting citizens' device security flaws on a massive scale?

4. Feedback on the Content of the Label

Feedback on the content of the label is much more concrete. Thefeedback can be light or strong objections. But the level of the objection is not an indicator of the difficulty and/or feasibility to solve a given issue. For example, some of the strongest objections were resolved directly during the interview.

4.1. General Remarks on the Content of the Label

The following section contains general remarks on the content of the Label raised by the test partners.

General

- Everyone must respect the law. But some points are the legal minimum (GDPR). Why including them?
- Provide good cases and bad cases as examples, for example it would help for security parameters.

The notion of "best practices" has raised many questions.

- Best practices are highly contextual. For example, SBB doesn't encrypt communication inside their private cloud, but access to this cloud is highly secure. Participants emphasise the importance of being able to explain technical and strategic choices considering the context of the digital service.
- Best practices constantly evolve. How to guarantee the conformity of a service over time?
- It's very difficult to arrive at a gold standard as you use technique where it makes sense, it's not black or white.
- In the public sector, the legal framework is not necessarily in line with the best practices in the scientific literature but remains a priority.

4.2. Specific Remarks on the Content of the Label

The following section contains remarks raised by the test partners related to a specific category of the Label catalogue.

Security

- There is always old tech in the system. You can minimise risk with a well-organised management system.
- There was resistance for a standard with “fixated solution or technology.”There is a need to include different possibilities like “long password” or “short password + 2FA” or using “magic password link”, perhaps the best way for some service is to abandon the requirement for an account altogether.
- For encrypted data, the question is how much inside knowledge you need to decode.
- A lot of services are containerised, one participant commented that secure computation may be important. (Yet no technique seems practicable today. This question should be verified with an expert in security/cryptography).
- Keys management may be an important criterion.
- For IBM, anonymisation makes no sense as anonymisation is not possible and de-anonymization is often easy. There exist some use cases where it’s useful, but they would prefer something like “How do I make sure your privacy is respected”. You need to know the purpose: “Clearly describing what you are doing to preserve the privacy of the person you are providing a given service”.
- On 12 “*Vulnerabilities and/or personal data breaches shall be communicated to relevant authorities and impacted data subjects within 72 hours.”,* it was suggesting using the word "incident."

Fair data management

- The provider may not have the legal right to delete the data. In practices, you delete what you can and return to the subject explaining why there is partial retention.
- We can describe what we do and what we need based on what our partners (banks) tell us what the minimum data requirement is.
- How do you not qualify for point 20 *“The service provider shall ensure that the user can access their data and can exercise their rights with clear instructions to make the request. From this process users shall receive confirmation of the actions taken?”*

Reliability

- Why do we ask for the version number to be sure the software is up to date? Does it apply to web service?

Interactions with users

- Having criteria on manipulative and deceptive techniques (i.e., dark patterns for example) is interesting and not covered by other certifications.
- They may be discrimination (i.e., service only for part of the word or for a given profession). The question is if the discrimination is justified and moral.

5. Business Model and Cost

Test partners acknowledged the digital industry suffers from a general mistrust among users. They see a clear benefit in communicating to the user their digital services quality and the service trustworthiness. It also shows a commitment by the company. A trusted third-party is necessary to achieve this as digital service may be impossible to assess from the outside.

For large companies and government agencies, a financial cost between 10’000 to 50’000 CHF is not a barrier. They also would have the necessary resources to allow time. Finding the perimeters of the service could be more complicated.

The situation is very different for SMEs and startups where financial cost is an issue. They may also have difficulty to allocate the necessary resources.

Test partners perceived advantages in auditing digital service, instead of auditing the full company. Companies may maintain digital services in operation for a long time that may not immediately be ready for an audit. But they could start with service still in the development

phase or newer services. Limiting the perimeter of an audit to a digital service could be a unique value proposition of SDTL.

Test partners raised the question if a different label should be provided for different types of service.

Test partners will likely implement such a Label if it exists and seem to have a good chance of success.

The added value for the test partners must be clear. A question, which has been raised several times is how a combination of various Labels can generate an added-value. The additional benefit, in comparison to existing labels and standards, would be if the Label provides the user with simplicity. One challenge that has been mentioned several times is the question of who is behind such a Label. In general, Labels are coming from very established organisations, which have built up their reputation over the years.

6. Lessons Learned from the Process

Analysis of the process related with test partners highlighted the complexity of such a Label. The SDTL project was organised in separate sequences. After the first draft, time was spent getting feedback. Now the feedback will be integrated. This approach has advantages. It's easy to communicate and make a clear agenda. But there are also drawbacks, notably a lot of points get discussed multiple times, even once that was fixed. The feedback, once integrated, could also raise new questions and objections. The current workflow does not document the reasons for each change (no change record). This could lead to difficult onboarding processes in the future.

A document owner and a clear modification process seem critical. SDTL could also set up a more scalable, modern, and transparent contribution system or use the help of a partner such as ISO with established processes and infrastructure.

Ethics washing, intentional or not, is a major risk associated with the SDTL project. Debates about ethics are frequently seen as an easy alternative to government regulation, both by companies and governments.[2] Companies might exaggerate their interest in systems that work for everyone. The SDTL label may be instrumental in this objective. A company could promote a "Tech 4 Good" approach on one side while selling surveillance capitalism tech to governments and corporate customers on the other. This is especially a risk as SDTL is a label for digital services not the company.

The Label content is not shielded from interested influence. Private or public actors could try to influence the content of the Label to make it compatible with specific business models that are in their interest.

SDTL needs to stay relevant with rules adequate and ambitious enough. The field can move quickly, this was particularly true in 2020. For example, GitHub removed all tracking cookies.[3] Most browsers provide solid built-in anti-tracking protection. Apple is moving forward with their App Tracking Transparency (ATT) requiring app developers to notify users if their app collects a unique device code, known as an IDFA (ID for Advertisers), and require that collection to be an opt-in setting.[4] SDTL needs to find a strategy to keep-up with technologies, norms,

[2] https://www.cohubicol.com/assets/uploads/being-profiled-16-wagner.pdf

[3] https://github.blog/2020-12-17-no-cookie-for-you/

[4] https://arstechnica.com/tech-policy/2020/11/apple-moving-forward-with-plan-to-limit-creepy-user-tracking/

and policy changes. What was not even discussed a year ago could become unacceptable practices a year later.

Recommendations

17) Business models should be evaluated. There is a risk when enterprises' incentives are not fully aligned with the Label values. SDI needs to be cautious with actors practicing with targeted advertising based on personnel data.

18) When an enterprise claims they anonymise data, they should be fully transparent about the data they collect and how. Especially when those data are then used to make personal decisions.

19) The business's track record needs to be considered.

7. Concluding Remarks

The idea of the Label is garnering a strong interest from the partners and its timing makes it clearly relevant. Such a Label would without a doubt be very welcome by the industry and other stakeholders. Consumers may be ready to pay a premium for higher quality. But product differentiation and assessment are very hard on features such as security or privacy. There is also a need to improve the industry image.

However, this report demonstrates the complexity of this project and the extremely broad range of aspects that need to be taken into account. Some of these may appear contradictory and their resolution might prove extremely time-consuming.

Exercises based on open discussions are prone to bias. Even academics trained in social science often get inadvertently biased results. The author of this report suggests being particularly cautious about potential bias in the future. Proven methods, such as changing the order of the questions during mock audits, would improve the robustness of the results.

Integrating and responding to external ideas and critics is a challenge. A semi-public living document and an open-participation process could be an approach to improve the process. This would require specifying the license of the content in accordance with the future business model by using for example a BY-NC-SA Creative Commons license.[5]

A Label is only part of the answer to improve trust. The assumption is that it gives a competitive advantage to providers that have it. It's then the consumer who influences the market. Such schemes may only work on a competitive market where users have different options. This is not always the case in the digital realm where monopolistic positions are common, notably because of high cost of entry, network effect or lock-in. More administration could potentially reinforce those monopolistic positions.

The Label is taking services independently of the ecosystem. Yet, it's often the interactions and interdependence of different services, platforms and specific contexts that create problems. We currently lack a cross-service data exchange layer infrastructure, enabling users to have an overview and be in control of access to their data. Other initiatives such as SITRA's "Fair Data Economy" project[6] or aNewGovernance[7] think tank are working on the foundation for a fair data economy, "in which successful digital services are based on trust and create value for

[5] https://creativecommons.org/licenses/by-nc-sa/4.0/

[6] https://www.sitra.fi/en/topics/fair-data-economy

[7] https://www.anewgovernance.org

everyone." For them, to reach the full potential of the digital economy we need the creation of a new kind of ecosystem. This is also in line with the current EU data strategy.[8]

Some aspects of the label may require technologies that do not exist yet, which complexifies the discussions with the partners. Nevertheless, the SDTL label seems a practical and efficient way to attract attention to those issues and foster those discussions, change perception, and push for further technical development.

SDTL could benefit in rethinking how it could articulate internal and external management processes around tangible artifacts (label catalogue, documentation, tools, ...). First the functional objective of those artifacts needs to be defined. To move forward some options must be closed and put aside. An overview table of the Digital Trust Label features and what it will do, or not do, could be a good starting point. Typically, future change in this table would need to be justified and documented.

8. All recommendations

For convenience, you can find below the list of recommendations made in each section.

Clarify what Swiss Digital Trust Label stands for

1) Each criteria and controls should bear a high ethical standard. Educating users about their legal rights are also important objectives. But educating users should not be at the expense of the SDI commitment for high ethical standards. It's important that each criteria taken individually are fully consistent with SDI's values.

Relation with existing standards and certification

2) Document when criteria are based or closely related to an existing standard. This has been done by SDI in the meantime.
3) A mapping of similar existing initiatives and standards, such as ISO 27001, GDPR, SOC2, would be useful.

Legal responsibility and reputational risks

4) Determine the responsibilities of each actor (SDI, auditor, service provider, users, etc.).
5) Define processes and policies for reputational incidents, legal risks, and malicious attacks.
6) Evaluate how consumers may respond to a disclaimer. In particular if it affects consumer confidence toward the label.

Measurement and control objectives

7) Communicate precisely what needs to be "easy to understand for users." Users need to quickly understand the label value proposition through the label interface. The underlying content also needs to be transparent, accessible, and understandable. That does not necessarily mean that the content needs to be "simple" and "easy to understand."The mock audit showed that even for professionals, understanding the implication of some criteria was not easy. A reason for that was the missing SOP, which will be available, once the Label Catalogue is final.
8) Mechanisms can deliver contextual help and in-depth explanation. For example, a standardised and structured data format is key to deliver the underlying information in a machine-readable fashion. The same information can then be presented to the user

[8] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

in various ways. The user has direct access to a compact summary but can explore additional information about a given criteria or access guidance.

9) The strategy could also leverage social dynamics such as informational relay: users may ask friends or do a quick online search. Other actors (and tools) could offer additional information and guidance to the user.

Guarantee the conformity of a service over time and ensure the Label is part of the operation

10) Objectifiable criteria were chosen because they seem easy to audit. Finding the right criteria for all contexts could be practically impossible without adding much complexity. One solution would be to have more flexible criteria where the provider documents different key processes that are then evaluated. But this could be done in the assessment of those criteria.

11) A criterion could ensure the provider has good internal processes to keep all the label criteria in check in the long run. This could also be part of the assessment instead of a specific new criterion.

Private and public sector, B2B or B2C

12) Check all content with the specificity of the private and public sector in mind. If the criteria must diverge in different contexts, this needs to be documented.

13) Strongly communicate to partners the label is strictly limited to B2C services. Eventually help them to select a service to test.

What is a "digital service", granularity and perimeters

14) Provide definitions of key concepts and an extensive glossary. Some definitions – at the core of the label – seem necessary to avoid misunderstanding and to move forward.

15) Consider the context in which the service is provided. The potential risks, the legal framework that apply and responsibilities can be significantly different depending on the type of service.

Lessons Learned from the Process

16) Business models should be evaluated. There is a risk when enterprises' incentives are not fully aligned with the label values. SDI needs to be cautious with actors practicing with targeted advertising based on personnel data.

17) When an enterprise claims they anonymise data, they should be fully transparent about the data they collect and how. Especially when those data are then used to make personal decisions.

18) The business's track record needs to be considered.

This report was written in December 2020 by Simon Perdrisat as part of his internship at SDI.