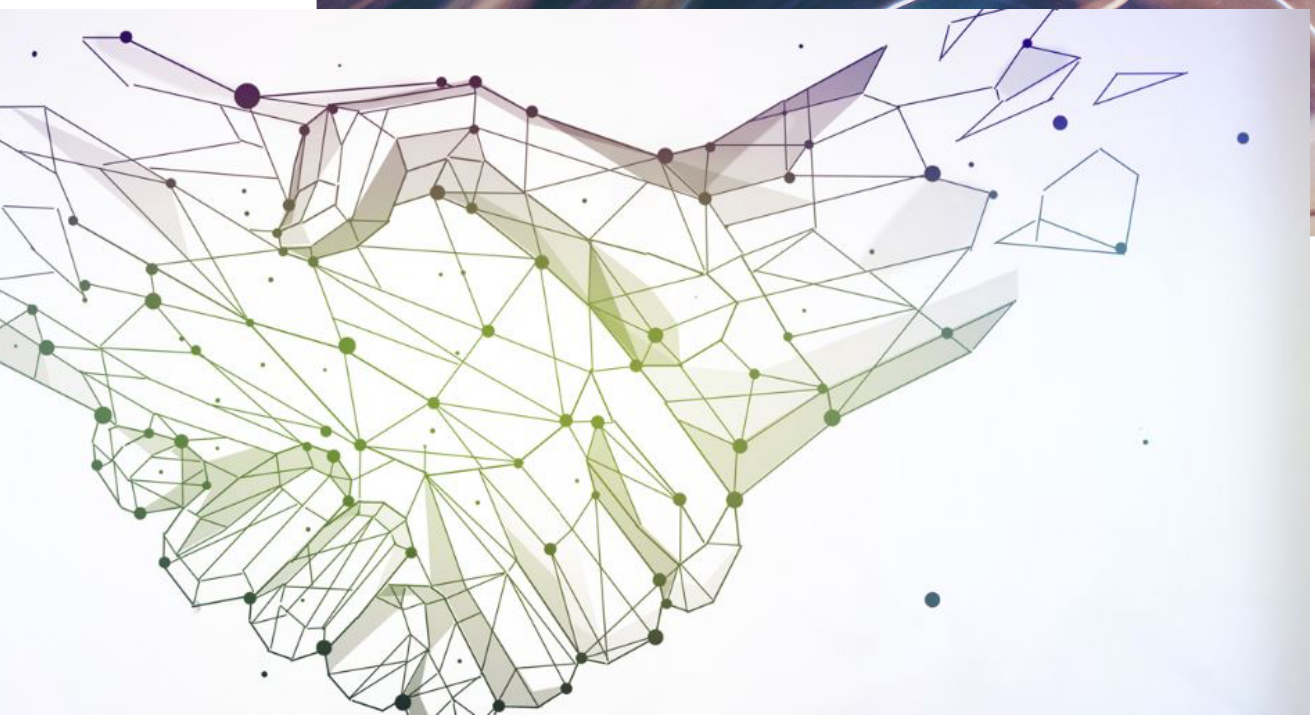
SWISS DIGITAL INITIATIVE

Digital Trust Whitepaper



SWISS DIGITAL INITIATIVE

Table of Contents

Executive Summary

Growing erosion of **trustworthiness is limiting the adoption of digital services** even in cases where they are considered beneficial for societies, e.g. in the case of Covid19 related digital healthcare services.

The Swiss Digital Initiative has been working on a **Digital Trust Label**.

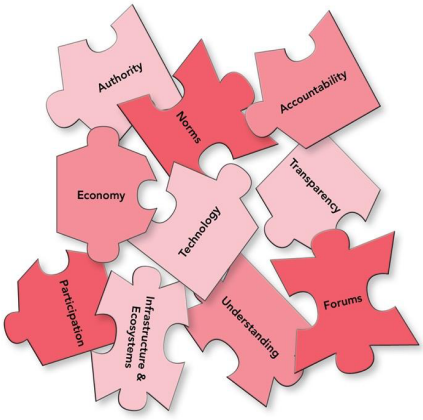
The first worldwide label **certifies the trustworthiness** of a **digital service** along four dimensions: Security, Data Protection, Reliability, Fair User Interaction.

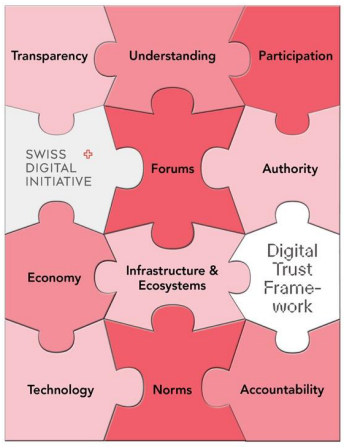
This Whitepaper presents the **main learnings** from the intense work on developing such a Digital Trust Label

- **There are no purely technical solutions to the trust deficit.**
- **There are no shortcuts: Digital Trust needs to be earned.**
- **Trust in the digital world is closely linked to offline experience with the company or provider.**
- **Digital Trust is an ongoing practical challenge and cannot be built overnight.**
- **Transparency is key in building Digital Trust**
- **In a broader sense, trust in the digital world is not limited to data protection and security alone but encompasses social and ethical responsibility.**
- **A general feeling of insecurity in a complex digital world fosters openness of users towards solutions that address the topic of Digital Trust.**
- **Building Digital Trust concerns all stakeholders and requires a holistic and iterative approach**

The Whitepaper outlines the Swiss Digital Initiative's understanding of Digital Trust and why building it matters for successful digital transformation, particularly in healthcare, public sector, the media sector, banking & insurance, HR and the education sector.

In addition to the Digital Trust Label, the Swiss Digital Initiative proposes a **Digital Trust Framework** that shows the various elements of Digital Trust:





All these elements should be addressed when working towards building Digital Trust in a coordinated fashion.

Looking at the Digital Trust Ecosystem the Swiss Digital Initiative concludes that coordinated efforts by various stakeholders are needed. Switzerland is well positioned to play an active role globally in working towards Digital Trust.

Foreword by Doris Leuthard

When we initiated the Swiss Digital Initiative in 2019, we made Digital Trust a key issue for the organisations' work. Growing mistrust in digital services was already visible. Little did we know that a global crisis would act as a further catalyst for developments that had us already worried.

We have seen the roll-out of digital services from home office applications and videoconferencing tools to contact tracing apps and other health-related digital services as part of various countries' reaction to Covid-19. Mistrust, not just in digital services but also institutions that enjoyed high levels of trust so far, has shown that this issue needs to be addressed.

Ever since its inception, the Swiss Digital Initiative has been dedicated to advancing digital ethics through practice-oriented projects. One such project is now coming to fruition: our Digital Trust Label is about to be launched.

We thought that this milestone would be a good opportunity to reflect on our work and look ahead. What have we learned adapting an intuitive concept such as a label to the digital space? What challenges are we and like-minded organisations facing when working towards digital trust? This Whitepaper not only collects our learnings so far, but it also lays out our understanding of Digital Trust.

After all, trust, like many concepts, seems clear and intuitive at first but can mean a variety of things to different people. Therefore, we feel it is important to clearly outline our understanding of Digital Trust, why it matters and how we could help build it.

This Whitepaper also positions the Digital Trust Label in the broader context of a Digital Trust Framework. From the beginning we understood that a Label can be one contribution to the complex challenge of Digital Trust but not the only solution.

With this Whitepaper we introduce our Digital Trust Framework, a basis for continued and sustained engagement with the challenge of Digital Trust. The Framework shows what different methods we see to work towards advancing Digital Trust. It not only helps us to manage and plan our projects but also provides a blueprint to look at the ever-growing Digital Trust Ecosystem in Switzerland and around the world.

Notwithstanding all the challenges, we are at an important moment for digital transformation. The need and demand for trustworthy digital services is here and clear. We are excited to provide a conceptual basis for future projects with this Whitepaper as well as a concrete and implemented project with the Digital Trust Label. My sincere thanks go to all our supporters and partners who believe in a trustworthy digital space.

Doris Leuthard
President SDI Foundation

Introduction

Whether in our private life or in business, from grocery shopping to politics: we rely on trust in almost all our interactions. We like to trust people and institutions and we like to be seen as trustworthy by others. However, trust does not simply exist. It needs to be earned. Once betrayed, trust is extremely hard to win back.

In more and more domains, we rely on algorithms, automated decision-making and complex technologies, whose inner working remains opaque and whose criteria for trust still need to be defined. Digital Trust is a topic of major concern for all stakeholders - companies, institutions, users, and governments alike. We believe that Digital Trust is a cornerstone of successful digital transformation, and the potential of new technologies can only be exploited, if the level of acceptance is high enough. Even great technologies and robust legislation may fall short if mistrust is apparent. Accelerated through the Covid19-pandemic, societies all over the world are experiencing an erosion of trust: In institutions, the media, science, and technology.

That is why the Swiss Digital Initiative (SDI) made the issue of Digital Trust a priority for its work. The initiative aims to create the first worldwide Digital Trust Label. An instrument to foster Digital Trust by enabling users to make informed decisions through greater transparency and inciting companies to take responsibility by offering trustworthy digital services. The learning journey since the beginning of the project in 2019 has been remarkable and one objective of this whitepaper is to give a synthesis of the insights and learnings gained.

Based on theory and the practical knowledge from the project work, SDI developed a more holistic "Digital Trust Framework". SDI believes that stakeholders in every country should reflect on how to build Digital Trust. The key aim is to foster constructive digital transformation. SDI works to create an environment where people feel empowered to make decisions based on knowledge and education. It wants to communicate to society that it can use new technologies to improve quality of life. Building digital trust is a long-term investment and key requisite for sustainable digital transformation. It can neither be taken for granted, nor is there a quick tick-the-box recipe to follow.

The Digital Trust Label

History and Reasoning

The idea of creating a Digital Trust Label (DTL) was already born back in 2019 at EPFL Lausanne. With the creation of the Swiss Digital Initiative Foundation, the project was officially transferred under the SDI umbrella.

Together with its main partner, EPFL Lausanne, SDI carried out the groundwork for the development of the DTL in 2019 and 2020. The core of the Label, a sound catalogue of verifiable and auditable criteria, has been co-developed by a small Academic Expert Group (from the ETH, EPFL, Universities of Geneva and Zurich) based on a user study on Digital Trust (conducted in November 2019). An independent Swiss-based testing, verification and certification specialist, the Société Générale de Surveillance (SGS), further developed the Label catalogue to make sure that it is auditable and verifiable. The label catalogue as well as other resources can be found on our project website: https://www.digitaltrust-label.swiss

Based on this first draft of the Label Catalogue, SDI conducted the following main processes:

1. It put in place a "Label Expert Committee", consisting of independent experts[1] from academia, fields of data- and consumer protection, human rights, and digital ethics, advising the SDI Board on the Label's content and framework.

2. It conducted a co-development and public consultation process, which provided civil society bodies with the opportunity to comment on and test the catalogue of criteria through face-to-face interviews, an online survey, and workshops.

3. Six of the eight test partners tested the Label Catalogue on concrete use cases, which have contributed a great deal to the Label's improvement. This will help ensure that the Label is fit for purpose when it becomes fully operational.

4. In addition to the work on the Label Catalogue, SDI has worked on the communication and visualization of the Label. Together with the market research firm *Bruhn&Partner*, SDI conducted a user study in Switzerland, USA, Scandinavia, and Eastern Europe. This international investigation tested mechanics and determined success factors and value proposition of such a Label from the customer's perspective.

[1] https://a.storyblok.com/f/72700/x/19cd54a0c6/members-of-the-lec.pdf

Learnings on Digital Trust from creating a Digital Trust Label

1. **There are no technical solutions to the trust deficit.**
   Trust is built in a relationship. It is how society manages risk and an uncertain future. A full guarantee is never possible, there always remains a certain risk. The gaining of trust involves a constant battle of reducing technical complexity in the experience of digital practice. Better informed and aware consumers who have a vocabulary to express their concerns will legitimise and drive the digital future. A Digital Trust Label can be one instrument to drive forward the conversation between companies and citizens, but it is not a shortcut or easy solution, which replaces the efforts and seriousness needed for building Digital Trust.

2. **There are no shortcuts: Digital Trust needs to be earned.**
   Digital Trust can neither be taken for granted, nor is there a simple "tick-the-box" recipe. Traditionally built through interpersonal relationships, it can be hard to grasp what trust in the digital realm might look like. A proxy could be the values, for which a service provider or company stands for and more importantly its actions. Discrepancy between the stated and lived values can have a negative impact on trust. Promoting Digital Trust falls short if trustworthy behaviour cannot be demonstrated. There is no easy solution: Trust takes a constant effort, and it is up to the service-providers to prove that their services are trustworthy. Once lost, it is hard to regain.

3. **Trust in the digital world is closely linked to offline experience with the company or provider.**
   Experiences in the offline world, such as the reliability of a provider or ethical responsibility as well as employee behaviour, have an influence on trust in the digital world and vice versa. If the company is present in the offline world as well, it needs to take a comprehensive approach that strengthens the trustworthiness of the whole company – in the online and offline world.

4. **Digital Trust is an ongoing practical challenge and cannot be built overnight.**
   Digital Trust cannot be mandated to a technical solution but is a long-term effort. It is a constant dialogue between users and companies, not a top-down monologue with the consumer as the end point of the conversation. Meeting this requirement in practice demands that the digital ecosystem institutionalises a sensitivity to change and a communications feed-back loop for the entire ecosystem.

5. **In a broader sense, trust in the digital world is not limited to data protection and security alone but encompasses social and ethical responsibility.**
   Trust in the digital world encompasses social and ethical responsibility – and should also be connected to the general behaviour of the service provider in this direction. Companies are expected to take on responsibility in the digital as well as the offline world. In the online world this could mean protecting customers from fraud and misinformation, protecting vulnerable groups such as children from explicit content and preventing cyber-mobbing.

6. **Transparency is key in building Digital Trust**
   For establishing a trustful relationship with the users, a solution such as a Digital Trust Label should provide transparency about the degree of criteria fulfilment. This is not to say that organisations should "overload" users with information. It is about presenting relevant information for informed decision-making in a clear fashion. There will be no trust without transparency.

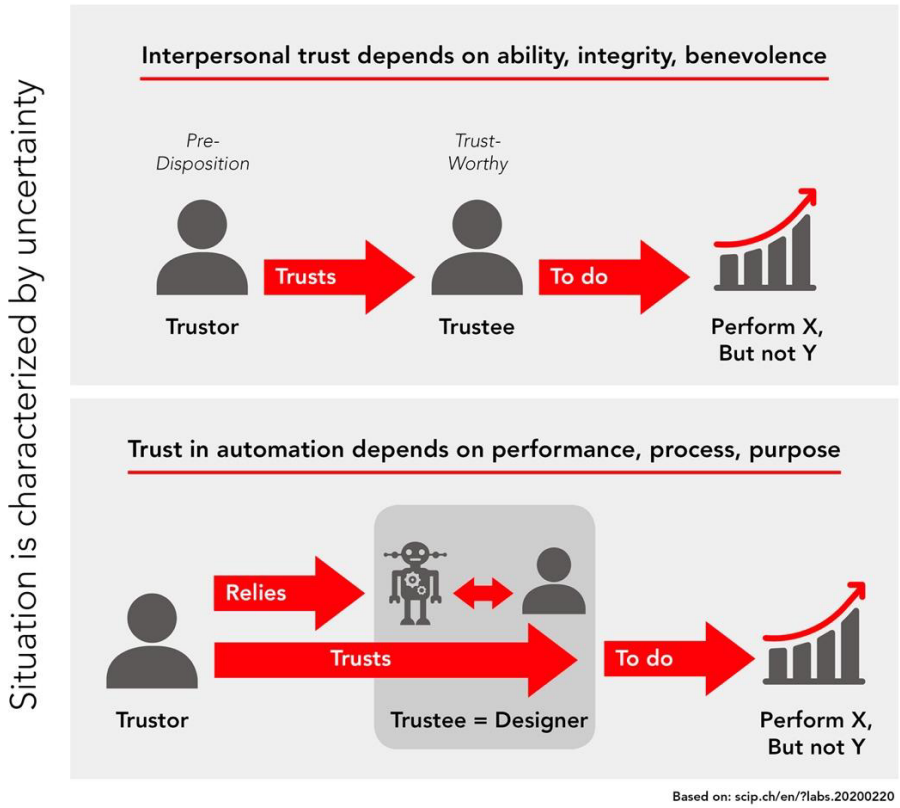
7. **A general feeling of insecurity in a complex digital world fosters openness of users towards solutions that address the topic of Digital Trust.**
   In a global user study conducted by the SDI, 80% of participants evaluate a Digital Trust Label as useful for themselves. Those that do not see an added value in a Digital Trust approach do so due to different reasons: 1) High digital competence and therefore no need for an independent assessment. 2) General mistrust on the internet and resignation about data security and usage ("You can only protect yourself")

8. **Building Digital Trust concerns all stakeholders and requires a holistic and iterative approach.** It needs a collective effort to address the trust issue around new technologies, to guarantee more transparency and accountability. Businesses must live up to their societal responsibility. Policymakers need to set framework conditions to make sure that trust can grow. To foster trust, a more holistic approach and a combination of several measures is needed. A Digital Trust Label needs constant development, feedback iterations and the criteria of trust will need to be challenged and redefined over time. From these learnings, the Swiss Digital Initiative is convinced that a Digital Trust label can be one tool to reduce mistrust. But it is also clear that our ambition cannot stop there. Therefore, the Swiss Digital Initiative proposes a generalised Digital Trust framework to guide our work in the future.

Digital Trust in context

The concept of trust

Trust comes into play whenever we talk about relations between two parties. Trust helps us to bridge the unknown: is this object really doing what it should be doing? Is this person really going to do what she is saying? Is this institution going to interact with me the way I expect it to? If we have trust, we do not need additional answers to questions to engage in a relation and over time might not even ask these questions. We flick our light switch without thinking whether the lights will turn on, we order at a restaurant without assuming that we will be poisoned and we mail our ballots trusting that our votes count. If a certain threshold of trust is reached, we can engage in "trusted" relationships.



Based on: scip.ch/en/?labs.20200220

Trust can hence be seen as a vital resource for healthy and functioning societies and economies. Trust acts as a relational lubricant, facilitating interactions between various parties. Where there is no trust, certain types of behaviour become prohibitively expensive and are thus not undertaken. This in turn means wasting potential benefits. People end up not engaging with each other due to mistrust or refrain from using certain services. Imagine living in a world without trust at all? What dystopian scenario that would be!

As the above visualisation shows, trust involves sometimes complicated relationships between various parties. Also, trust in a person is different from trust in technologies, as the former is usually more normative while the latter focuses on reliability. Nevertheless, persons – in particular designers and coders – are also relevant when it comes to assessing whether a digital service is trustworthy. This point is also reflected in our Digital Trust Label and the broader Digital Trust Framework.

The Swiss Digital Initiative believes that in contrast to other resources, trust does not simply exist, it cannot be found and exploited like a natural resource. Instead, it needs to be built up over time through repeated interaction between parties and institutions for example. Given the benefits of trust, it is hardly surprising that societies have tried to foster trust instead of perpetuating mistrust. Nevertheless, trust – even when created over a long time – can easily be lost and should not be assumed automatically.

Trust also has a dark side that must be acknowledged. Given that trust is needed to overcome uncertainties, it can be potentially misplaced. Trusting someone always comes with the risk that this trust is abused. Trust creates vulnerability. Hence, while we do not want a world without any trust, we also do not envision a world where we are overly dependent on it. After all, how would you feel if you are constantly confronted with the assertion "trust us" or "trust me"? Rather, the Swiss Digital Initiative aims to reduce mistrust where it is blocking potential benefits for the involved parties.

Trust in the digital world

This brings us to the role of trust in the digital world. First, digital transformation has given established actors new possibilities. Newspapers can reach their audience via digital channels in addition to traditional print media. However, as a second development, digitalisation also created new challenges for established actors. Social media and data analytics have made it possible to shine a light on how certain actors behave. Various institutions have seen themselves being questioned for the first time as a result. Lastly, digital transformation has created a plethora of new actors and in turn new services that did not exist before.

What about Zero-Trust?

In the field of cybersecurity, there is an approach called Zero-Trust. The idea is, to assume that no digital service in a given system should be trusted, which has consequences on how a system interacting with digital services is set-up. Think of how a company network and its IT security needs to deal with employees bringing their own devices to the office. The company has no control over these devices and hence to increase overall security, under the Zero-Trust approach, assumes that none of those devices and digital services running on them are trustworthy. This assumption is reflected in strict security rules and tight policies. This might be a pragmatic approach, but it is rather costly, supporting our argument that we would not want to live in a world without trustworthy digital services but instead should focus on how to create better conditions for trust,

These three developments create general issues for digital policy such as data handling and security or platform governance. But they also have direct consequences for the role of trust in the digital age and for how trustworthy we see digital services. In the first case, actors might have assumed that trust earned in the analogue world will transfer over to their activities in the digital space. However, the debate around fake news shows that this is not necessarily the case. People might have trusted print newspapers before the internet but now mistrust their digital channels.

In the second case, actors that were regarded as trustworthy in the analogue world can see that trustworthiness evaporate in the digital world because their position is challenged. This may be through more technologically enabled transparency – e.g. the negative effect of WikiLeaks on the perception of states – or because digital transformation has enabled competitors to offer even more compelling services.

This brings us to the third case, where new actors have emerged through digital transformation and offer previously unseen possibilities, such as social media companies. However, because they are new and "unknown" they cannot really build up on pre-existing trustworthiness.

As a direct result of rapid digital transformation, we must talk about Digital Trust. When we say Digital Trust, we focus on a digital service being trustworthy. Our definition of digital service is aligned with the official definition by the European Commission. Digital services include a large category of online services,

from simple websites to internet infrastructure services and online platforms. Digital services come in many forms and are omnipresent. We believe that this focus is justified as it is digital services that have come to play an ever-important role in almost every aspect of our lives. And will do so even more in the future. Many digital services involve sensitive information from health to financial information and the consequences of decisions taken as part of using a digital service can be quite severe. One example is the use of AI-systems in the hiring processes. For these reasons the bar for trustworthy digital services should be set high.

There is a cynical argument to be made that all the talk about Digital Trust is simply a way of increasing costs for the providers of digital services and being a hindrance to true innovation by slowing down the pace of technological change. We strongly oppose this view and instead argue that Digital Trust is a precondition for sustainable and successful innovation. As with analogue trust, Digital Trust comes with benefits for all parties involved. People are much more likely to use digital services if they are trustworthy, instead of being convinced to do so in the face of growing mistrust. Likewise, organisations providing digital services that are seen as trustworthy can use this "trust capital" to take risks and try out new things, meaning that Digital Trust is not a hindrance but an enabler of innovation.

However, in recent years, almost no action was taken to actively reduce digital mistrust. Instead, a series of scandals and poorly managed incidents have eroded the Digital Trust that existed at the start of digital transformation. Governments face push-back when rolling out digital services and technology companies face unhappy employees, critical customers, and pushy regulators. Hence, the question of how to reduce digital mistrust will not go away but only gain in importance in the future.

The limits of Digital Trust

In our understanding, Digital Trust is a facilitator for the adoption of digital services. However, it is not in essence a normative statement. The question whether a digital service is "good" for individuals or society is not our focus. Our efforts regarding Digital Trust are about making sure that people understand what is behind digital services so they can make an informed decision. A 100% guarantee does not exist, there always remains a certain risk. As in the analogue world, we cannot solve the trust issue through a purely technocratic solution and replace trust with a technical tool. With our thinking about Digital Trust – as operationalised in the Digital Trust Label – we also combine the question of reliability with the question of trust. Rather than limiting ourselves to ensuring that digital services are reliable – this is only one dimension of the label – we want to broaden the scope and include other

When to talk about Digital Trust

In a given context the question of how trustworthy a digital service offered by an organisation is can be asked at different times of its life cycle:

- Beginning of a digital service
- Development of a digital service
- Adoption of a digital service
- Continuous development and abandonment of a digital service

Ideally, the question of trustworthiness is asked and answered at each stage, especially since the "return" of "investing" in trustworthiness early in the life cycle is bigger. The earlier the issue is addressed, the easier it is to tackle and demands less attention and resources later.

Already when thinking about an idea for a digital service can organisations and employees raise the issue: will this be trustworthy? Or are we following an idea that raises fears & concerns? The same goes for the development of the service, where interdisciplinary teams for product development that also bring in non-technical expertise, is beneficial.

However, we must deal with the fact that many digital services are already rolled-out and adopted. Hence, we also need to address Digital Trust "after the fact", which is exactly the mission of the Digital Trust Label. Nevertheless, the Swiss Digital Initiative believes that going forward Digital Trust should be addressed over the whole life cycle of a digital service.

Fields to prioritise

Reducing mistrust is paramount for all areas of the society and economy. This is not only the case today but even more so for the future. In a Trend Map developed for the Swiss Digital Initiative by the Think-Tank W.I.R.E, the trends identified further increase the importance of trustworthy digital services. Priority should be given to digital services that are used in fields where:

i) the handled data is very sensitive;
ii) the consequences of using digital services matter greatly;
iii) where there is not much choice whether to use a digital service or not and
iv) where digital services are rolled-out at a high pace and on a large scale.

Following these criteria, we argue to focus, without any particular order, on digital services in the following fields

- **Healthcare:** digital services in the health sector almost always involve highly sensitive data and can have potentially lethal consequences. This is a particularly urgent field as under the recent Covid-19 pandemic situation, many digital services were rolled out on a large scale in a short timeframe. Think of automated, AI-assisted diagnosis of thorax x-rays.

- **Public Sector:** changing habits and possibilities also affect political processes and over the last years citizens and institutions of democratic societies have thought about using, or are in fact using digital services in politics, from social media to e-voting. Again, this might involve highly sensitive data – for good reason, votes are supposed to be secret – and a breach of privacy can have dire consequences. One big negative consequence being that democracy itself heavily relies on trust. If this is undermined by using digital services that are not trustworthy, it negatively affects the whole system.

- **Media Sector:** Closely linked to democratic processes is the question how trustworthy (analogue and digital) media and journalism is seen to be. Digital technologies seem so far to have been a mixed bag. Take the debate about *fake news* spreading particularly over social media as an example.

- **Banking & Insurance:** whether it's applying for a loan, payments that should remain private or activity levels for health insurance: financial services and insurance involve sensitive information and potentially severe decisions. Already in the analogue world, the bar for trust is set high and so it should be the case for the digital world.

- **HR:** from monitoring employees to assessing candidates, digital services are increasingly used in the labour market. For example, if you are applying online via a job portal, then you would probably want to know if a human or algorithm did the initial screening. Hence more transparency is needed for such tools.

- **Education:** digital technologies are also becoming rapidly widespread in the educational sector and students are exposed earlier to new digital technologies. Given the vulnerability of young students, particular attention to Digital Trust should be given in this sector.

Of course, the legal and regulatory frameworks in various countries address these questions, for instance through data privacy laws. In our quest for Digital Trust we want to go beyond what is legally required. Legal and regulatory frameworks face notorious difficulty in keeping up with technological developments and legal measures – as we explain in the section on the Digital Trust Framework – are but one piece in the puzzle.

Working towards Digital Trust: the Digital Trust Framework

As stated, increasing trustworthiness in digital services is a key objective for the Swiss Digital Initiative. We have gathered practical experience in this field through our first major project, the creation of a Digital Trust Label. To expand on this project in the future, we also propose a general framework that shows the various dimensions of Digital Trust, providing a blueprint for the direction of our future projects but also acting as inspiration for any organisation that also wants to contribute to Digital Trust.

Ways of building trustworthiness

To reap the benefits of digital transformation, we want to work towards reducing mistrust. But what makes something trustworthy? Whether in the analogue or digital world, there are several ways. When focussing on digital services, additional elements come into play to reduce mistrust, not just in a single service, but also the digital ecosystem:

- **Transparency:** as trust is used to bridge what is unknown, one way of tackling the issue is by reducing the amount of uncertainty. This can be done by being as transparent as possible: make clear to someone you want them to trust you, what is happening if they use your service. This includes clear communication, especially in times of crisis and a culture that openly admits mistakes and shows what has been learned.

- **Understanding:** another way of reducing uncertainty and hence reducing mistrust is to be able to understand something. It is much easier for us to trust something we built ourselves than something we bought because we understand the first instance better. Understanding needs the willingness to understand from one party and the willingness to enable such understanding by the other party.

- **Participation:** Being able to shape developments and being involved is another way of reducing mistrust. Having a stake by participating in the development and use of a digital service makes it trustworthy. Think of the success of the open-source projects that revolve around active communities. In addition to transparency, the ability to have a say in the direction of the digital service increases trust.

- **Authority:** going back to the idea of trust as "relationship capital", if someone is already trustworthy, this can be used to reduce mistrust vis-à-vis other parties. Think for instance about product endorsements or official recommendations. This is also a leading idea behind our Digital Trust Label project and why the Swiss Digital Initiative strives to be trustworthy, e.g. by following several of these principles like transparency and being participatory.

- **Accountability:** Users need recourse options, such as legal frameworks that hold businesses and institutions accountable or focal points, ombuds or contact persons, to which users could turn in case of problems. Today, a lot of users feel overwhelmed and insecure when using digital services. Also, organisations making commitments must also be held to those standards in their practice.

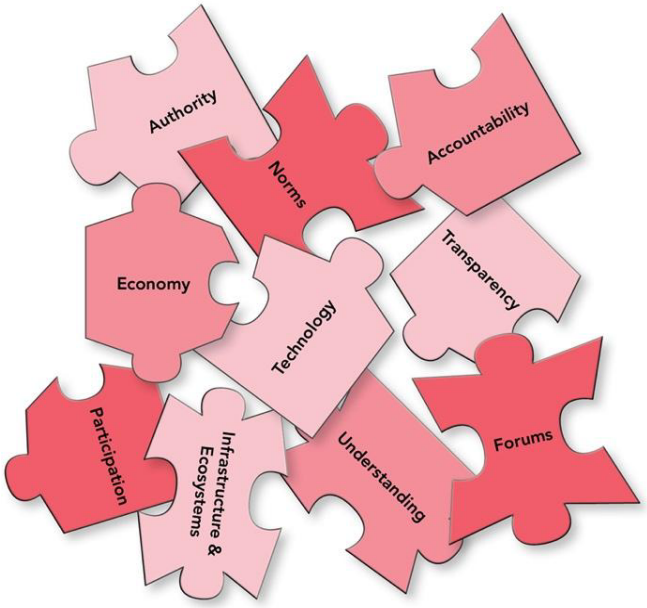
- **Technology:** the technology powering various digital services – from hardware to software – is a crucial element to be trustworthy. Is it safe or riddled with bugs? Is the technology used explainable and understandable? Does the technology used reduce uncertainty? If we can rely on technology, this is already a first step towards trustworthiness.

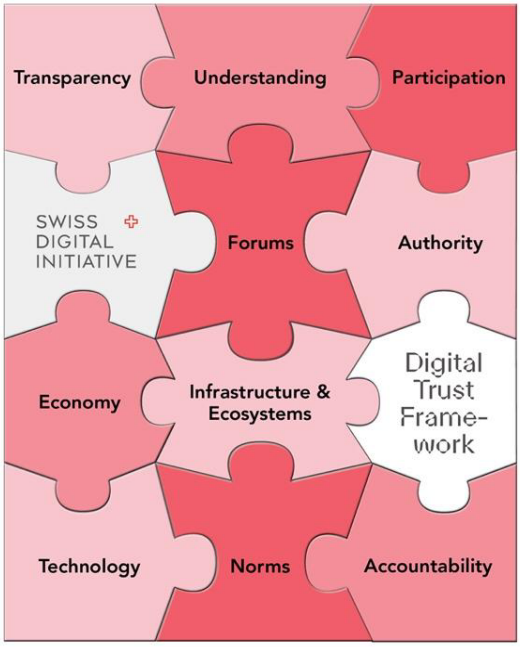
- **Infrastructure & Ecosystems:** In the digital world, digital services often rely on certain infrastructure. From the internet to standardised frameworks for identification and data sharing, such infrastructure plays a key role in the trustworthiness of digital services.

- **Norms:** While it has been decades that digital technologies have been in use, it is painfully apparent that the "rules of the game" are very much still in the making. That is why norms for digital services matter as another element of Digital Trust. Are certain digital services off limits? What is deemed acceptable behaviour in cyberspace? Clear norms in line with rules in other aspects can reduce mistrust.

- **Forums:** To debate those norms, forums are needed. Where can we address issues of Digital Trust and who is involved in those discussions? Open and inclusive forums can further reduce mistrust.
- **Economy:** as the main source of digital services, the economy also has a vital role to play when it comes to reducing digital mistrust. Are we offering a real choice to consumers instead of forcing them to adopt certain services through market power? Are business models based on exploitation of data?

Comprehensive effort needed





All these elements need to work together to complete the puzzle of trustworthiness. The issue of mistrust cannot be addressed by focussing just on one of the above-mentioned elements and methods. This is particularly evident with technologies that aim to replace the complex social construct of trust through technological means and removing human elements and factors wherever possible, e.g. certain blockchain projects. Distributed ledger technology seeks to replace the trust placed in institutions or humans with trust in technology, e.g. the code of a smart contract. However, research clearly shows that this is not enough to be seen as trustworthy.

Therefore, the Swiss Digital Initiative will start focusing on additional projects along the lines of the framework and welcomes other organisations to join in the effort to build Digital Trust and enable the adoption of trustworthy digital services. Be it through awareness and educational campaigns, research that fosters transparency, efforts to build trustworthy digital infrastructure or adapting business models and leading international debates: we need to work together on all the above-mentioned elements of the Digital Trust puzzle.

Such efforts must also break down silos that still hinder effective collaboration in various aspects of digital policy today: policymaking legal scholars and political scientists need to converse with IT specialists, AI developers and researchers need to listen and talk to civil society representatives. If there ever was a challenge demanding interdisciplinary collaboration, it is working towards a societal beneficial digital transformation with Digital Trust at its core.

The Digital Trust Ecosystem

Having established the elements of Digital Trust through our framework, we can position the efforts of various organisations and actors within the framework to see where lots of efforts are already undertaken and which elements of the framework might require more attention going forward. Different stakeholders will be working on different elements given their backgrounds, capabilities, and interests. Although this is a very dynamic space with many actors in Switzerland and internationally, we try to generalise the various contributions.

As a multi-stakeholder organisation itself, the Swiss Digital Initiative is convinced that an effort from all stakeholders is needed towards Digital Trust: Academia and research lay the foundation for the technological infrastructure and functioning. Businesses must live up to their societal responsibility in their own interest: being trustworthy contributes to the adoption of the digital services offered and hence to the potential revenues. Policymakers need to set framework conditions to make sure that trust can grow, and vulnerable groups are protected. Civil society and independent media can function as watchdogs and counter-power. In short: It needs a collective effort to address the trust issue around new technologies, to guarantee more transparency and accountability.

While additional involvement in the Digital Trust field is generally welcome, there is also a danger of "too many cooks" and reinventing the wheel. As the Swiss Digital Initiative has learned in conversations with other initiatives around the world, exchange of information and learnings is seen as beneficial, and efforts should be better coordinated. This Whitepaper and our Digital Trust Framework can hopefully act as a contribution towards better coordination.

The role of Switzerland

Travel to any place in the world and ask someone what they associate with Switzerland? Trust stands a good chance of making into the top ten, from its democratic institutions to reliable watches.

So how does Switzerland fit into the Digital Trust landscape? Switzerland enjoys high trust in its institutions and the economy nationally and is seen as a trustworthy actor internationally. An open economy with strong SMEs leads to export-oriented growth but struggles with digital transformation and digital competitiveness. Nevertheless, the presence of leading universities and research facilities also positions Switzerland as a technology hub for cybersecurity, cryptography and other technologies generally linked to "trust", from bias detection in AI data sets to self-sovereign identities.
With more organisations joining the Geneva ecosystem, Switzerland also acts as host for various forums for global debates on norms with participants ranging from leading tech companies to NGOs and international organisations increasingly dealing with digital policy and the question of Digital Trust.

There is already a strong basis with many elements in place. What is now needed is connection of the dots and "doubling down" on the potential of transferring the Swiss quality of trust towards the digital age. Players in the Digital Trust ecosystem need to collaborate and coordinate their efforts. The Swiss Digital Initiative will be monitoring the evolving digital ecosystem in Geneva and around the world and is looking forward to cooperating with other stakeholders towards the common vision of Digital Trust. Having recognised the challenge of Digital Trust and its importance for successful digital transformation early on, ideally positions Switzerland to play an active role in this field. Just as was the case with other challenges, confidence-building measures for the digital space are needed and more projects along the line of our Digital Trust Framework can contribute to a world where citizens and users feel: the digital space is trustworthy.

Conclusion

The importance of Digital Trust is only increasing. On one side, mistrust in digital transformation is growing given repeated scandals and revelations about unethical business practices. On the other side, the need for digital services is growing and we have seen widespread rollouts of digital services in various sectors in recent years.

With the Digital Trust Label, the Swiss Digital Initiative provides a concrete and practice-oriented approach for the issue of Digital Trust. Digital services can be certified for their trustworthiness. This can contribute to Digital Trust, but as this paper shows, trust is a complex issue that defies simple solutions.

With the growing need for Digital Trust and based on the learnings from the Digital Trust Label project, SDI proposes a Digital Trust Framework that incorporates various elements that contribute towards Digital Trust.

The framework acts as a blueprint for mapping current activities and planning future projects. Such a mapping helps to identify areas with need for coordination or need to address a gap.

With the spread of digital services, priority in addressing Digital Trust should be given to digital services that are used in fields where:

i) the handled data is very sensitive;
ii) the consequences of using digital services matter greatly;
iii) where there is not much choice whether to use a digital service or not and
iv) where digital services are rolled-out at a high pace and on a large scale.

This concerns in particular digital services in healthcare, public sector, the media sector, banking & insurance, HR and the education sector.

The growing need for Digital Trust has also created a dynamic Digital Trust Ecosystem that is starting to take shape. With various projects and initiatives along the lines of our Digital Trust Framework – from awareness campaigns to technology start-ups - SDI hopes to contribute to the future evolution of this ecosystem and looks forward to implementing additional projects to tackle Digital Trust in a comprehensive way.

About SDI

The Swiss Digital Initiative (SDI) is an independent, non-profit foundation headquartered in Geneva and set up in 2020 by the association digitalswitzerland and under the patronage of Federal Councillor Ueli Maurer. The SDI pursues concrete projects with the aim of safeguarding ethical standards and promoting responsible behaviour in the digital world.

The SDI's location in Geneva is no coincidence. The SDI is very much Swiss at heart and embodies many of the Swiss qualities of security, reliability, and trust. At the same time, we recognize that the issue of digital ethics and trust is a global one. With this in mind, we believe our location in international Geneva puts us in a great starting position to combine Swiss values and perspectives with a global debate and international impact.

Authors

This Whitepaper was written by Nicolas Zahn and Niniane Paeffgen.

Acknowledgments

The authors would like to thank the SDI team, experts, and community for their support. This Whitepaper has been made possible thanks to the generous support of the Mercator Foundation Switzerland.

We would also like to thank Marisa Tschopp (scip AG), Johan Rochel & Jean-Daniel Strub (ethix – Lab for innovation ethics), Christian Budnik (University of Zurich) and Anna Jobin (Alexander von Humboldt Institute for Internet & Society) for their helpful inputs.

References

Atlantic Council (2019), 'Breaking Trust', Technical report, Cyber Statecraft Initiative.

*Adjekum, A., Ienca, M. and Vayena, E. (2017), 'What Is Trust? Ethics and Risk Governance in Precision Medicine and Predictive Analytics', Omics: a Journal of Integrative Biology **21**(12), 704-710.*

Australian Government (2021), 'Digital Service Platforms Strategy', Technical report, Digital Transformation Agency.

ARM (2021), 'Security Manifesto'. https://interactive.arm.com/story/security-manifesto-2021/

Cave, S., Craig, C., Dihal, K., Dillon, S., Montgomery, J., Singler, B. and Taylor, L. (2018), Portrayals and perceptions of AI and why they matter, The Royal Society.

CoT (2021), 'Charter of Trust'. https://www.charteroftrust.com/

Deloitte (2021), 'Future of Digital Trust - Digitalization of public sector organissations', .

European Commission (2019), 'Ethics guidelines for trustworthy AI'. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

European Commission (2021), 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts', COM/2021/206 final.

*Adjekum, A., Blasimme, A. and Vayena, E. (2018), 'Elements of Trust in Digital Health Systems: Scoping Review', Journal of Medical Internet Research **20**(12).*

Haataja, M. and Bryson, J. (2021), 'What costs should we expect from the EU's AI Act?', SocArXiv.

Hoff, K. and Bashir, M. (2014), 'Trust in Automation: Integrating Empirical Evidence on Factors That Influence Trust', Human Factors: The Journal of the Human Factors and Ergonomics Society.

IMD and St. Gallen Symposium (2021), 'Strengthening Trust in Technology When It Matters The Most', Joint White Paper. https://a.storyblok.com/f/72700/x/6f57f16650/strengthening-trust-in-technology_a-joint-imd-and-sgs-white-paper.pdf

*Janssen, M., Rana, N., Slade, E. and Dwivedi, Y. (2018), 'Trustworthiness of digital government services: deriving a comprehensive theory through interpretive structural modelling', Public Management Review **20**(5).*

*Gille, F., Jobin, A. and Ienca, M. (2020), 'What we talk about when we talk about trust: Theory of trust for AI in healthcare', Intelligence-Based Medicine **1**(2).*

*Kelton, K., Fleischmann, K. and Wallace, W. (2007), 'Trust in digital information', Journal of the American Society for Information Science and Technology **59**(3), 363-374.*

Küderli, U. (2019), 'Digital Trust drives business growth', PwC. https://www.pwc.ch/en/insights/digital/digital-trust-drives-business-growth.html

NGI Forward (2020): Report - Digital Trustmarks. https://research.ngi.eu/wp-content/uploads/2020/01/NGI-Forward-Digital-Trustmarks.pdf

OECD (2014), Recommendation of the Council on Digital Government Strategies, OECD Publishing Paris.

OECD (2017), 'Trust and Public Policy: How Better Governance Can Help Rebuild Public Trust', OECD Public Governance Reviews.

OECD (2019), Digital Government Review of Sweden: Towards a Data-driven Public Sector, OECD Publishing Paris.

O'Neill, O. (2002), A Question of trust: The BBC Reith Lectures, Cambridge University Press.

*O'Neill, O. (2017), 'Intelligent Trust in a Digital World', New Perspectives Quarterly **34**(4), 6-31.*

Paris Call (2018), 'Paris Call'. https://pariscall.international/en/

PwC (2021), 'Global Digital Trust Insights Survey 2021: Cybersecurity comes of age'. https://www.pwc.ch/en/publications/2020/ch-Digital-Trust-Insights-Survey-2021-report.pdf

*Eisenhauer, S. (2019), 'Trust in Innovation', ethix White Paper **2**.*

Swiss Digital Initiative (2019), 'Digital Trust from the customer's perspective: a qualitative study in Switzerland'. https://a.storyblok.com/f/72700/x/55feac39be/booklet-digital-trust.pdf

Nuremberg Institute for Market Decisions and St. Gallen Symposium (2021), 'Challenges for Human Trust in a connected and technology-driven world', Voices of the Leaders of Tomorrow.

Söllner, M., Hoffmann, A., Hoffmann, H. and Wacker, A. (2012), 'Understanding the Formation of Trust in IT Artifacts', International Conference on Information Systems .

Söllner, M., Hoffmann, A. and Leimeister, J. M. (2016), 'Why different trust relationships matter for information systems users', European Journal of Information Systems ***25****, 274-287.*

Tschopp, M. (2020), 'AI & Trust: stop asking how to increase Trust in AI', scip. https://www.scip.ch/en/?labs.20200220

Tschopp, M. (2020), 'Trust and AI: three wrong questions', scip. https://www.scip.ch/en/?labs.20201112

Tschopp, M., Scharowski, N. and Wintersberger, P. (2021), 'Do Humans Trust AI or Its Developers? Exploring Benefits of Differentiating Trustees Within Trust in AI Frameworks', Extended Abstract.

UVEK (2016), 'Strategie "Digitale Schweiz"'. https://www.digitaldialog.swiss/de/

van Haasteren, A. (2019), 'Trust in Digital Health', PhD thesis, ETH Zürich.

Vestager, M. (2021), 'Trust and Technology in a new digital age''Internet Week Denmark'.

Zavolokina, L., Spychiger, F., Tessone, C. and Schwabe, G. (2018), 'Incentivizing Data Quality in Blockchains for Inter-Organizational Networks - Learning from the Digital Car Dossier''Thirty ninth International Conference on Information Systems'.

Zavolokina, L., Zani, N. and Schwabe, G. (2020), 'Designing for Trust in Blockchain Platforms', IEEE Transactions on Engineering Management.

Contact

Swiss Digital Initiative
c/o Campus Biotech
Chemin des Mines 9
1202 Genève

https://www.swiss-digital-initiative.org
info@sdi-foundation.org