

ti&m special

digital trust 2024



Building digital trust

04

Empowering innovation
through digital trust

Matthias Bossardt, KPMG Switzerland

10

Trust is the key
to success

Andreas Tölke, Swisscom

24

"There was never any plan to replace
today's cryptographic methods"

Marc Stöcklin, IBM Research Europe



Thomas Wüst, CEO and founder of ti&m AG

Dear reader,

This ti&m special is all about digital trust: What does trust mean in the digital sphere? To understand it, we have to remember one thing: Trust has always been the foundation for all social and economic interactions. Whether within our family or among friends or colleagues, trust emerges from a mixture of emotions, behavioral patterns, and rules. Together, these elements determine the quality of the interaction.

As part of a system, such as a company or even a state, an individual also builds trust in other systems. This trust is based on the same three elements – emotions, behavior, and rules – but with a different weighting. And the larger and more anonymous the system, the less important emotions are. By contrast, rules become more important in larger systems.

Digital transactions are emotionless

A basic digital transaction does not have any emotions or moderating influences. This means that trust is based exclusively on rules and the knowledge that the parties will follow them. A digital transaction consists of just three components. And the only way to create them is using digital technologies and protocols:

- 1. Who am I dealing with?*
- 2. Does the information that I have received match the information that was sent?*
- 3. Can I agree to this transaction with a binding “yes”?*

It is these three components that have seen the greatest developments in recent years. This is because the Internet has evolved from an information medium into a transaction medium. And these three components are still powering developments. The European Union's Electronic Identification, Authentication and Trust Services Regulation, or eIDAS for short, is just one example. Developments in trust-building solutions are ongoing. They include online identification, secure digital identities, and digital seals and signatures. Effective cryptographic algorithms and new approaches to usability are making communication and data more and more secure. This naturally increases the security of digital transactions. What's more, it promotes user acceptance. And with today's blockchain technology, it's now possible to exchange digital values directly, without an intermediary. This is an important building block for the metaverse, which we could only dream of up until now.

Technological developments are creating new challenges

But we are still a long way from a completely secure digital world. Across the globe, there are only a handful of truly secure digital identity solutions – solutions that respect citizens and their data. (However, Switzerland is certainly on the right track with its planned e-ID.) What's more, artificial intelligence presents completely new trust issues: If we can no longer understand how AI produces statements and makes decisions, even in theory, how can we be sure of what is real and what is fake? And what about the new quantum computers and the threats that they could pose in six to ten years' time? According to experts, quantum computers could crack the cryptographic algorithms that we currently use for much of our online security. These questions pose huge challenges for organizations. They have to manage constantly growing quantities of data. At the same time, the regulatory framework that they must follow is also growing constantly. Plus, companies need to find ways to use this data constructively. For IT professionals, these developments also raise some tough questions: How should we build all these new technologies? How should we design the situations that we use them in? And most importantly: How can we make sure that new technologies benefit as many people as possible?

This is what we are working on at ti&m

These are precisely the kind of multidisciplinary challenges that we love at ti&m. They motivate and drive us as consultants, designers, and engineers. We have developed our mobile and e-banking suite and our patented online identification solution

to meet these challenges. These products now lead the market in the sensitive field of banking. Together with Swisscom, we have developed Swisscom Sign. It is now the de facto standard in Switzerland for qualified electronic signatures (QES). And we've created a two-factor authentication solution, the ti&m security suite. Our banking clients have been using it for many years to give many customers user-friendly and secure access to digital services. These solutions are important components of our comprehensive digital trust framework. It covers governance and consulting issues, such as information security risk management, self-sovereign identities, and compliance and ethics. But it also encompasses product and service components such as onboarding, multifactor authentication (MFA), and signing. It even includes Security Operations Center (SOC) or Security Incident and Event Management (SIEM) as-a-service and IT baseline protection for managed services. And it doesn't stop there because we're constantly expanding this framework. In this way, we address the issue of digital trust at all the levels of our value chain – just as you would expect from your trusted digital transformation partner.

We'd be very happy to talk to you about these and the other solutions that we offer. And just as you expect from the ti&m special, we've put together numerous articles by expert authors. They share their experiences in the field and their research expertise. Their articles provide diverse new perspectives on digital trust. I hope you'll enjoy reading this issue and that it'll inspire you in your work.

Best regards,



Thomas Wüst

Publisher: ti&m AG, Buckhauserstrasse 24, 8048 Zurich, Switzerland
Publication: ISSN 2235-7971
Editorial team: Thomas Wüst, Leunita Saliji, Pascal Wild, Mathias Liechti
Design/Production: ti&m AG **Circulation:** 500 copies
Printing and distribution: Multicolor Print AG



ti8m.com/blog

- 04 Empowering innovation through digital trust**
Matthias Bossardt, KPMG Switzerland
- 06 Will DeFi make banks obsolete as intermediaries?**
Thomas Ankenbrand and Denis Bieri, IFZ
- 08 Crypto as a pioneer of digital trust**
Luka Müller, MME and Sygnum Bank
- 10 Trust is the key to success**
Andreas Tölke, Swisscom
- 12 “A knowledge-based environment and supporting companies to adapt is decisive for the trust ecosystem”**
Daniel Säuberli, DIDAS
- 16 “Those who are already exploring the e-ID will have a competitive advantage in 2026”**
Désirée Heutschi, Orell Füssli
- 18 Why insurance companies need to invest in tech and data now**
Andy Maier, ti&m
- 22 How the Federal Office for Cyber Security is promoting resilience**
Florian Schütz, BACS
- 24 “There was never any plan to replace today's cryptographic methods”**
Marc Stöcklin, IBM Research Europe
- 26 Digital trust and data exchange in the housing ecosystem**
Stefan Reitbauer, NNH and Tiziano Lenoci, myky
- 28 Digital trust at ti&m: a holistic approach**
Leunita Saliji, ti&m
- 30 How ti&m creates digital trust**
Philip Dieringer and Martin Unterbäumen, ti&m
- 32 AI – a matter of trust?**
Lisa Kondratieva, ti&m
- 33 Improving the resilience of IT services with SBOMs**
Stephan Sutter, ti&m and Manuel Gysin, ISCeco
- 36 Confidential notarial services in the digital age**
Pascal Wild, ti&m and Cornelia Stengel, Kellerhals Carrard
- 38 Shaping the future in the SOC: Transforming job profiles through infrastructure as code and AI**
Ralph Keller, ti&m

Read more interesting articles about “digital trust” online in our blog!

Lukas Ruf, Head Security & Risk, Group CISO MIGROS
Gregor Hofer, Head of Cyberspace Capability Development, Swiss Army
Dominika Blonski, Data Protection Commissioner Canton Zurich

Empowering innovation through digital trust



Digital trust // In today's era of omnipresent digital transformation, the importance of trust cannot be overstated. By prioritizing secure and safe technologies and responsible governance, we can build a more trustworthy digital landscape.

Recent surveys by KPMG, and the public debate, highlight a pervasive skepticism surrounding artificial intelligence (AI) and other technologies. 61% of the respondents are wary about trusting artificial intelligence systems. Depending on the country the percentage of AI sceptics ranged as high as 84% (Finland). The resulting slowdown of digital transformation projects and technology adoption begs the question: how can we gain and maintain digital trust?

Similarly, companies and government organizations face concerns of both, their external stakeholders, such as customers, business partners, and regulators, and their internal stakeholders, such as employees, risk and compliance functions or the board of directors about the risks related to their AI systems. Typically, the concerns are related to the fairness, accuracy, safety, security, privacy, and compliance of their AI endeavors. The consequences are delayed or even failed innovation projects, longer time to market, and a slow adoption of new technologies.

This skepticism is not related to AI technology only – and it is not a new phenomenon. For example, in recent years, the Swiss people voted against an Electronic Identity Law because the public didn't trust the technology and the way it was to be deployed and operated. Concerns related to privacy and transparency were intensely debated before and in the aftermath of the public vote. Is that lack of digital trust justified? One would think so, given the high number of issues reported regarding the reliability of digital systems, as well as the number of cybersecurity and privacy incidents that make the news in Switzerland and abroad.

Why digital trust matters

If our bridges were built with the same quality as some of the digital products and services that are put in front of us users, we wouldn't walk across them. They would look too rickety and unsafe. Unfortunately, digital tinkerers, who build these untrustworthy products and services, too often enjoy a competitive advantage as they seem to deliver the expected functionality and features at a lower price point and/or with a shorter time to market while taking short-cuts on safety, security, and other quality aspects.

All too often, we consumers become aware of these short-cuts only when the equivalent to a collapsing bridge has occurred, typically accompanied by a communication of the responsible company or public entity stating that this incident comes as a surprise.

Clearly, this is not a sustainable approach. Earning and maintaining the trust of customers, business partners, regulators, and the public will become increasingly important for the success of digital products and services and for the adoption of new technologies in general.

What is digital trust?

In a recent report that KPMG wrote in collaboration with the WEF¹, digital trust is defined as follows. Digital trust is the expectation by individuals that digital technologies and services — and the organizations providing them — will protect all stakeholders' interests and uphold societal expectations and values.

There are two key ingredients to digital trust:

1. *Secure & safe technologies, resilient infrastructures*

Digital products and services must be based on a sound fundament, which ensures that data is kept confidential and cannot be manipulated; that products and services do not harm its users or the environment; and that products and services are resilient against disruptive events, including human errors, (cyber-) attacks, etc.

2. *Responsible use*

As with any technology, be it a knife or a digital system, it can be used for good and bad. Hence, it is critical that digital products and services are provided under a governance that ensures users are served responsibly, i.e. ethically, transparently, and in good faith.

A differentiator for digital products and services “made in Switzerland”?

Trustworthiness should be treated as a quality attribute and can serve as a differentiator for products and services. Many successful Swiss companies across different industries have understood this and justify their premium price tag with it. However, the fact that a product or service is “Swiss made”, doesn't necessarily mean that it is trustworthy. Particularly for digital products and services, more than enough cases that prove such an assumption wrong have made it into the media in the past.

To earn and maintain the trust of users and benefit from it in a sustainable way, developers and providers of digital products and services should take an active approach:

Digital products and services should be developed with trustworthiness in mind from the design phase (“trustworthiness-by-design”), incorporating specific requirements for security, reliability, accountability, oversight, as well as ethical and responsible use.

Trustworthy digital products and services should be developed and operated through engagement and

communication with stakeholders. Demonstrating adherence to these standards can be achieved by having products and services audited by knowledgeable, independent third parties. This may include compliance with standards and best practices in the form of certificates and SOC-2 attestations issued by trusted organizations.

Developers should hold their suppliers and business partner ecosystem to the same standards.

Education of buyers, procurement organizations, legislators, and the general public should be promoted. Trade associations may be able to play an important role here.

Our choices determine whether digital trust gets the attention it deserves

As buyers and consumers of digital products and services, our choices are critical to support and accelerate the transition to a more trustworthy digital environment. We must look under the hood to challenge providers and developers and make trustworthiness part of our requirements when procuring or subscribing to digital services and products. Often, we must be ready to pay an upfront premium for it, but the payback may come faster than expected in form of accelerated time-to-market, smoother execution projects and less costs to managing incidents as demonstrated.

In the end, it is the responsibility of all of us consumers to demand the transparency required to inform our choices. Let's buy and consume services and products from those organizations and tech ecosystems that are able to demonstrate that they deserve our trust. ●



Dr. Matthias Bossardt

Head Cyber & Digital Risk Consulting and Partner, KPMG Switzerland

As partner and head of Cyber & Digital Risk Consulting at KPMG Switzerland, Matthias Bossardt advises his clients in managing data and using digital technologies in a trustworthy, responsible, safe and secure way. He is a member of KPMG's global Trusted AI steering committee. He chaired the cybersecurity

working group of economiesuisse and is a member of the cyber advisory board of the Swiss Academy of Engineering Sciences (SATW).

In 2016 he was voted one of Switzerland's 100 most influential Digital Shapers by Bilanz, a leading Swiss business publication. [kpmg.com](https://www.kpmg.com)



Will DeFi make banks obsolete as intermediaries?

Decentralized finance // A stable, functioning financial system is essential for the economy and prosperity. Up to now, banks have played a crucial role in this. But will it stay that way?

The financial system ensures that different market participants can access their money: Private individuals want to save or invest money. Companies need equity or loan capital to expand their production. The state is also an important market participant, whether as an investor or borrower. Trust is vital to a functioning financial system. It becomes clear just how important it is when trust vanishes. Financial crises can have a severe negative impact on the real economy, for example through a decline in investment. Restoring confidence after such a crisis can take a long time. It often requires additional measures to build confidence in the form of state guarantees and loans, or regulation.

Money is allocated in various ways. Banks and stock exchanges are the traditional channels for this. Alongside them, there are now some new alternatives: peer-to-peer platforms and decentralized finance (DeFi).

Banks and stock exchanges

Banks bring investors (or lenders) and borrowers together. They perform various functions. One of them is maturity transformation: accepting short-term deposits and turning them into long-term loans. Another is lot size transformation: bundling small deposits to fund larger loans, for example. Banks also serve as a risk buffer between borrowers and lenders. This means that if the loan defaults, the bank bears the loss, and not the investor. To make sure that banks can bear these risks, they must have sufficient capital to back their transactions. There are also specific regulations governing banks. Problems arise when investors lose confidence in a bank and want to withdraw their money. As a result, the bank cannot settle all the claims immediately: Usually, maturity transformation means that claims mature at different times. These bank runs can lead to a chain reaction in the financial system: One bank's insolvency can have negative consequences for other financial services providers. This can spread to the wider financial sector and affect customers. It is crucial to avoid this domino effect.

Stock exchanges also play an important role in the financial system. You can think of them like a major intersection or central market where borrowers and lenders gather to transfer money. This can be in the form of equity (shares) or loan capital (bonds). Stock exchanges enable investors to invest in companies, for example. This supports the flow of capital in the economy. Stock exchanges do not actually transform maturities or risk. They are usually regulated, which gives investors greater confidence. But the investor still bears the risk of the issuer defaulting. Stock exchanges have close links to clearing and settlement infrastructures. Financial professionals and policymakers often refer to them collectively as "financial center infrastructure." Special regulations govern this infrastructure, and supervisory authorities oversee it.

Peer-to-peer platforms

Peer-to-peer platforms offer an alternative to traditional financing channels such as banks and stock exchanges. They connect businesses or organizations that are looking for capital directly with investors. For organizations seeking capital, these platforms offer various benefits: They are easier to access than stock exchanges and ideal for raising smaller amounts. Investors on the other hand can invest directly without having to pay a professional broker. The unregulated or less regulated peer-to-peer platforms handle a smaller volume of transactions than the traditional exchanges. They are mainly active in the primary market – less so in the secondary market. As with banks and stock exchanges, it is essential that investors and borrowers can trust the operators of a peer-to-peer platform. These operators must ensure that transactions are fair and transparent. Most importantly, investors need to know that their money is safe.

Decentralized finance (DeFi)

Traditional finance is merging with distributed ledger technology, also known as the blockchain. Industry professionals call this “decentralized finance.” Among other things, DeFi aims to offer traditional financial services without centralized intermediaries such as

banks, stock exchanges, or peer-to-peer platforms. This means that investors and borrowers transfer their funds directly and independently via a blockchain. The products and services offered in DeFi are based on smart contracts. These contracts are written automatically and enforced autonomously. The rules are stored on the blockchain. This represents a paradigm shift in how we manage trust in financial transactions: In traditional finance, for example with banks or stock exchanges, having trust in how these central institutions operate is crucial. Likewise with peer-to-peer platforms, investors have to be able to trust the operators. In DeFi systems by contrast, it is the security and transparency of the blockchain technology that creates trust.

Will we still need banks in the future?

Banking or financial services are regulated, risk-bearing intermediaries. They perform important functions for the real economy and will probably continue to do so for two reasons:

1. *Various banks, central platforms, and markets also coexisted in the past. DeFi is another option for allocating financial resources. It will probably complement existing systems rather than replacing them. It gives investors and borrowers an alternative to traditional channels for certain financial products and services. Investors and borrowers will select the most suitable offering based on their preferences and trust. What's more, not all products and services are available on all channels.*
2. *Not all participants want to and are able to make all their financial transactions independently on the blockchain. Some participants still need support. They therefore sometimes turn to banks for assistance. For these participants, banks are trustworthy intermediaries offering both traditional and blockchain-based financial services. In addition, there are hybrid forms such as central exchanges based on the blockchain.*

Traditional financial intermediaries will probably continue to enjoy the trust of customers in the future. However, some people value the transparency, efficiency, and autonomy of the blockchain. These individuals have more trust in the technology than in the established, regulated financial system. And this group of customers is growing. ●



Thomas Ankenbrand

Head of the Competence Center for Investments, IFZ

Thomas Ankenbrand has a master's degree from the University of St. Gallen and a doctorate from the University of Lausanne. He is currently researching financial technology (fintech) and investment management at the Lucerne University of Applied Sciences and Arts. He is particularly interested in applying AI, agent-based modeling (ABM), decentralized finance (DeFi), and quantum computing in financial markets.



Denis Bieri

Lecturer, IFZ

Denis Bieri completed his doctorate at the University of Basel and is currently a lecturer at the Lucerne University of Applied Sciences and Arts. His research focuses on financial services, and he has a special interest in fintech.

hslu.ch/ifz

Crypto as a pioneer of digital trust

Dr. Luka Müller

Co-founder of MME and Sygnum Bank AG

Dr. Luka Müller is an expert in FinTech and RegTech, founding partner of MME, and co-founder and Chairman of the Board of Directors of Sygnum Bank AG. He is also co-founder of daura AG and KYC Spider AG, which deal with digital assets, share tokenization, and digital compliance.

mme.ch / sygnum.com



Distributed ledgers // Cryptocurrencies are often mentioned in the context of speculation and money laundering. As a result, the crucial importance of the underlying technology for trustworthy digital information and functionalities (digital trust) is often forgotten. A look at the history of securities illustrates the importance of state-of-the-art technology for the development of the format and legal concepts surrounding trustworthy information – from deeds to digital trust.

Even as far back as the Roman Empire, deeds were often used to record legally binding information. A deed acts as paper evidence of the authenticity and veracity of its content. Back then, the state-of-the-art medium was parchment and later, paper. With the increase in trade in the late Middle Ages, there was a growing need to add further functionality to these deeds. They were used not only to make a right binding, but also to mobilize it, i.e. by transferring them from person to person (peer-to-peer). This led to the creation of the security.

According to the current understanding of Swiss law, a security is a deed linked to a right in such a way that the right can neither be asserted nor transferred without the deed. Possession of the deed is proof of the assertion of the right, and the transfer of ownership is the prerequisite for transferring the right.

Central computers and trust in their operators

Paper securities began to become widespread in the 16th century and experienced their first heyday in the early 20th century. Millions of deeds had to be physically stored and exchanged. The limits of the mobilizing function of the paper-based security soon became apparent. In 1970, Swiss banks founded a joint venture, Schweizerische Effekten-Giro AG (SEGA – a predecessor of today's SIX Group AG), for the central safekeeping of physical share certificates. This holding of securities by an intermediary meant that they no longer had to be physically delivered to the new owner in order to transfer the right. The security was rendered immobile by its holding, and the rights to it could now only be transferred by means of credit entries (book entries). These book entries were recorded on the central computers of banks and depositories as digitalization progressed. Thus the first foundation stone for digitally recording, holding, and transferring a legal claim to a security was laid. A central digital database was and still is the "holy grail" when it comes to this original form of digital trust.

The importance of state-of-the-art technology

The history of the security has been shaped by the efforts of market participants and legislators to protect security ownership and the associated rights under civil law in the most effective way, and at the same time to ensure secure transfers even with high volumes and large numbers of market participants. The legal concepts developed over the years must always be understood in the context of the "gold standard" technology available at the time. The focus always has been, and remains, on the question of which digital information and functions can be trusted. The technology surrounding this has developed rapidly since the beginning of the 21st century, and has also influenced the next stage in the evolution of digital trust.

With the introduction of the ledger-based security (Article 973d of the Swiss Code of Obligations, CO) in 2021, Swiss lawmakers demonstrated an astonishing openness to a new technology. The new ledger-based security is based on the realization that it is now technically possible to program digital functions and operate them so reliably on digital infrastructures that they are – as an information carrier – functionally comparable to a deed or security. Using this technology, legally relevant information can be entered unalterably and made available for transfer exclusively to the authorized party. The beneficiary can thereby also verify themselves to the debtor and third parties as the holder of the right. Swiss lawmakers have thus created a legal concept for an important application of digital trust.

To remain as technology-neutral as possible, lawmakers summarized these digital functions and infrastructures under the term "distributed ledger technology" (DLT), which also covers technologies known as blockchain. Blockchain protocols such as Bitcoin from 2009 and Ethereum from 2015, which are often devalued as simply "crypto", contain these functions. What has also been overlooked in the reporting on

crypto so far is the fact that these protocols have been running like Swiss clockwork since their introduction. In addition to their functionality, this is precisely where the radical nature of these protocols lies: They function reliably and securely as decentralized systems. These protocols are today's state-of-the-art technology and the "paper" of the future. They are the pioneers for the further development of digital trust, not only in the area of securities, but also for other applications such as certificates, titles to goods, ID cards, etc.

The circle is complete

Thanks to distributed ledger technology, rights can be mobilized digitally and securely with this new legal concept of the ledger-based security. This makes it possible to do digitally what once used to be solely possible through direct physical transfer of a deed or book entry by a licensed intermediary. Issuing, holding, and transferring digital mobilized rights will once again be possible without intermediaries. The circle is complete.

Swiss lawmakers have not been resting on their laurels. They have recognized the potential of distributed ledger technology and, in addition to paper and central databases, have now approved digital functions as an information carrier and form of digital trust for mobilizing a right. Thanks to digital trust and an attentive legislator, the humble paper-based security is experiencing a new lease of life, albeit it in a different format. The way is being paved for a new era of digital mobilization of rights and legally relevant information with a redistribution of some roles among the various market players. New opportunities are opening up to develop products and services for users who are becoming increasingly digital, and whose need for secure and accurate digital information is unbroken. This new era will be able to unfold in an already well-regulated legal environment in Switzerland. Of course, it will still be necessary to make certain adjustments. And these will need to be made carefully and in the right place. ●

Trust is the key to success

Swisscom // Trust plays a key role in our networked and digital world. As an innovative and responsible provider of digital trust products and services, Swisscom is committed to increasing trust in digitalization.

“On the Internet, nobody knows you’re a dog.”

– Peter Steiner

This famous quote by US cartoonist Peter Steiner sums up just how easy it is to hide behind a mask and conceal your true identity in the digital world. The boundaries between digital and physical reality are becoming increasingly blurred. Trust is becoming more and more important in our digital society – it is the basis for working productively together, in both our personal and professional lives. At the same time, the global expansion of networking increases the risk of targeted abuse: Cyber crime, data misuse and identity theft are painful realities that we have to deal with.

Swisscom's Cyber Security Threat Radar 2024 shows that AI-based attacks will speed up this development. The growing danger online is also reflected in the figures from the Swiss National Cyber Security Center (NCSC): The total number of reports received by NCSC in 2023 was 30 % higher than 2022, at almost 50,000.

Identity, integrity and commitment: the pillars of explicit trust

In order to prevent a loss of trust in the digital world, it is essential to establish a trust layer for the internet, along with other security components. The interaction of implicit and explicit trust is key to this. Implicit trust includes cybersecurity measures to protect digital infrastructure and data from threats such as hacking, malware, phishing and theft. Explicit trust refers to actions that are deliberately taken to create and maintain trust, such as the release of verified information by the user or the signing and sealing of documents. In a digital world, transactional trust is vital. This term refers to trust in the context of a digital interaction or transaction between two or more parties. It is made up of the three pillars of identity, integrity and commitment, which are also used offline.

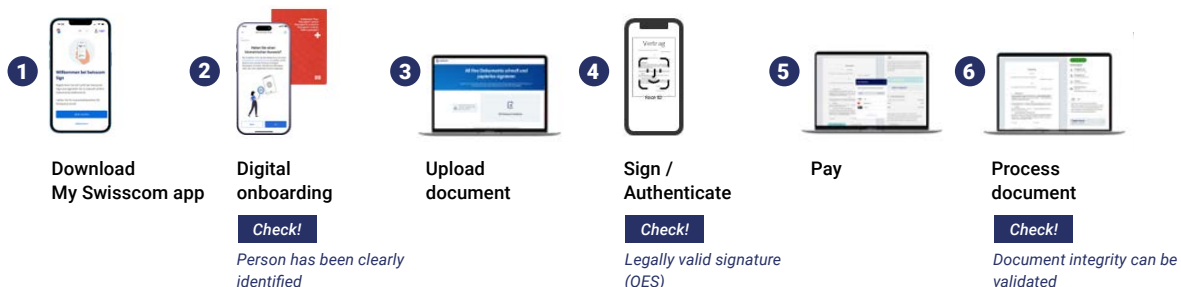

Identity: Who am I dealing with?

Digital identities are the backbone of a healthy digital society and are central to the future. Switzerland does not currently have a clear basis for identification in the digital world. Swisscom therefore wants the Swiss e-ID to be introduced as soon as possible. Swisscom is also running various digital identity projects, in particular the self-sovereign identity (SSI) approach. The aim is to establish comprehensible applications that will add value for our business and private customers and that will allow users to keep control of their data at all times.

Integrity: Is the information being transmitted genuine?

Integrity refers to the stability of information. This is also crucial for trust in digital transactions. Deep fakes

Get started with Swisscom Sign in a few simple steps

Sign anywhere, any time without pen and paper

The QES replaces the handwritten signature and is valid in Switzerland and Europe. Swisscom Sign can be used by private individuals, companies, associations or foundations and is available as an API integration for large organizations and software providers. It allows you to sign documents with other people.

Register free of charge for Swisscom Sign now!
sign.swisscom.ch/sign

Swisscom: the driving force behind digital trust

New technologies such as ChatGPT are now part of society and are speeding up digitalization enormously. At the same time, they also challenge the credibility of information. Digital trust is essential in the networked world, as it is the only way to close the last gap in digital security. Without trust, discontinuities will remain, with negative consequences for customers and providers. Swisscom is trustworthy and secure, and wants to take responsibility in this area, playing a leading role in identifying the best possible way to meet the challenges facing society, the economy and the public sector. As an “innovator of trust”, Swisscom is committed to innovative approaches and uses its expertise to bring integrated solutions to the market, increasing trust. ●

are getting better and better, making it more difficult to recognize false information. Here, too, the decentralized SSI approach plays a key role. This will make it possible to issue digitally verifiable originals of documents such as certificates and testimonials, whose authenticity is assured.

Commitment: Is it formally binding?

Commitment refers to the ability of a digital expression of intent to be reliable and legal binding. Under Swiss and EU law, the qualified electronic signature (QES) is the only digital equivalent to a handwritten signature. Swisscom Sign offers a simple and secure way to use the QES. A QES ensures the integrity of a document by “sealing” it. Any later changes to the document will be identified when the document is checked by a signature validator. As well as saving time and costs, QES has many other advantages. More about Swisscom Sign in the infobox.



Andreas Tölke

Head of FinTech & Digital Trust, Swisscom

Andreas Tölke has worked at Swisscom since 2020, where he is responsible for FinTech & Digital Trust. He previously held various management positions at Credit Suisse. Tölke began his career at the industrial company Georg Fischer in Schaffhausen and is co-founder of a media start-up. He studied business administration at the ZHAW School of Management and Law and holds an Executive MBA from the University of St. Gallen.



“A knowledge-based environment and supporting companies to adapt is decisive for the trust ecosystem”

e-ID // The e-ID is coming in 2026. Private and public stakeholders such as the Digital Identity & Data Sovereignty Association (DIDAS) have been involved in the federal government's consultation meetings and have discussed requirements and design. We spoke to its president, Daniel Säuberli, about the e-ID and the trust architecture it is based on.

Mr. Säuberli, how satisfied are you with the design of the new e-ID?

The introduction of the e-ID is a major step in the digital transformation of Switzerland. It provides a solid basis for the secure, digital verification of identities. As it is such an important building block, it is essential that we work together to identify the requirements, and decide on the details of implementation and any further development. Trusted infrastructures are very complex, so it is important that the team brings a variety of skills together. The project was developed with great foresight by the federal government, under the leadership of the Swiss Federal Office of Justice. Data protection and security concerns were taken very seriously from the outset and taken into account in the design. I am happy with the design and even happier now we have a definitive starting point for the project. The e-ID is a prime example of how we should approach complex federal projects in the future.

Can you see any weaknesses? Are there any aspects you think should have been designed differently?

Although we are now dealing with very advanced issues like cryptography and security, every technological solution is always a compromise between user-friendliness and security requirements. Until now, for example, it has been difficult to balance data-saving sharing of attributes and the need for correlation. There has been progress in this area, which can be taken into account. That's why it is important to keep implementation arrangements flexible, so that we can make continuous and systematic improvements.

“The implementation of the e-ID must remain flexible to enable continuous improvements.”

Some people are concerned about over-identification — consumers will have to prove their identity online for everyday transactions, which is not the case at present. The federal government wants to introduce a blacklist to deal with this. What does that mean?

The ability to share information in a data-minimizing way is an outstanding feature of the future e-ID. It means I will be able to ensure that only the data I actively release as the holder of the e-ID is shared. Trust infrastructure does not prevent users from being completely anonymous or adopting a pseudonym, although attributes or parts of attributes are checked for authenticity. This is not possible with the current physical identity card. When I show it, I disclose all the information it contains. But if a provider in the digital or physical realm submits a proof request seeking information from the e-ID — for example, when verifying the minimum age for a certain service — and the information is not required for the transaction, I can report them. These kinds of self-regulating mechanisms are very important to the ecosystem, and they should be embedded in governance. And so should clear countermeasures in the event of abuse.

Can you explain the vision of the trust architecture behind the new e-ID?

The vision is to create a secure and future-proof digital ecosystem that provides added value to all stakeholders. Thanks to the e-ID, identity can be verified via trust infrastructure, but the infrastructure can also be used to verify various digital credentials and authentic data packages. For example, proof of vaccination, a doctor's prescription, a delivery note or proof of assets from the bank can be made electronically verifiable to automate processes or to protect data. The ecosystem must be developed by fostering innovation and creating a knowledge environment that supports businesses and enables experimentation. We haven't gone far enough yet.

To what extent has the architecture been defined, and to what extent are you as an association involved in the design process?

Like all the other stakeholders, DIDAS is involved in shaping digital trust infrastructure via the federal government's consultation meetings, but as a think tank, it has also established itself as a center of excellence for trust infrastructure. We are closely involved with standardizing the content of level 1 – 3 sectoral ecosystems. To ensure that the needs of all stakeholders are taken into account, we closely monitor how the structures are developed and provide input. ▶

Daniel Säuberli

President of DIDAS

Daniel Säuberli is co-founder and president of the Digital Identity and Data Sovereignty Association (DIDAS) and uses his extensive experience at the interface of business strategy and technology to promote digital identity and data sovereignty. Over a 25-year career, he has worked in various organizations, from start-ups to multinational corporations, including IBM, and sees digital identity as an essential building block for a trusting and automated world where individuals keep control of their data.

The **Digital Identity & Data Sovereignty Association (DIDAS)** is a Swiss non-profit organization dedicated to promoting secure digital identities and data sovereignty. DIDAS's aim is to create a trustworthy, secure and inclusive digital ecosystem in Switzerland that strengthens control over personal data and promotes the digital autonomy of citizens. The organization helps develop standards and technologies for digital identities and works with a range of stakeholders, including governments, the private sector and civil society groups. DIDAS is actively involved in international discussions and initiatives to promote interoperable, cross-border solutions. The DIDAS platform offers regular workshops and seminars to raise awareness and understanding of digital identity and data protection issues. As a digital bridge builder, DIDAS helps Switzerland lead the way in digital transformation and develop technically advanced and socially responsible solutions. DIDAS is financed exclusively by membership fees.

[didas.swiss](https://www.didas.swiss)

“The e-ID will also make it possible to be anonymous or adopt a pseudonym. In the emerging ecosystem, self-regulating mechanisms are important for governance, and there should be clear countermeasures in the event of abuse.”

How is DIDAS involved with the development of trust architecture?

We are working with various stakeholders to lay the foundations for a digital ecosystem that promotes trust and security in the digital world. Take portability and interoperability, for example: Verifiable credentials such as the e-ID can be used in a decentralized way across different systems and platforms, which makes it easier to integrate them into new and existing systems. This promotes compatibility between the technology used by the federal government and the private sector – and also the “once-only” principle. In other words, the principle of only having to record certain information once, so that it can be shared repeatedly in a verifiable manner and checked by a trusted verifier.

Could e-voting be part of trust architecture at some point?

Like identification, elections and votes need to be easily accessible and barrier-free for all population groups, both digitally and physically. I believe e-voting generally has the potential to simplify and modernize the process. It could lead to higher voter turnout, especially among the younger generation. Trust infrastructure and verifiable credentials could play a role here, for example in verifying identity, votes and voter eligibility.

“The e-ID can be used in a decentralized way via different systems and platforms. This promotes compatibility and flexibility between the technology used by the federal government and the private sector, and helps introduce the ‘once-only’ principle.”

And what about digital signature services? Could these be integrated into e-ID architecture?

Digital signature services are a logical extension of the digital identity infrastructure. It is for the market to decide whether these are delivered by third-party providers or by the federal government. As an active user, what I would like to see is the user-friendly integration of signature services into my business and personal processes.

The e-ID is also likely to be recognized by the EU. How do you see interoperability with other jurisdictions, particularly with regard to the eIDAS Regulation?

Interoperability with the EU and other jurisdictions is crucial to allow the e-ID and other digital credentials to be sustainable in the longer term. For example, eIDAS does not differentiate between the identification of natural persons and legal entities, whereas the e-ID Act only covers natural persons. We need to find ways to ensure that functions and technology are interoperable and meet the high data protection requirements of the Swiss infrastructure. We have good solutions, but they need to be continuously refined.

What about the possibility of obtaining an e-ID without a physical identity check? Are there digital onboarding options?

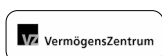
Yes, there are. There will be a digital onboarding process that enables instant comparison of the passport photo details stored by Fedpol with the data collected during e-ID onboarding. The e-ID team has issued a call for tender for this. As far as I know, e-IDs will also be issued by the passport office. The e-ID is always issued to the federal wallet and, if necessary, to other electronic wallets in parallel. ●

We take care of identification. And the rest.



ti&m Online Identification

As experts in online identification, we know identification is only one part of the user journey. That's why our support for our customers goes beyond the seamless implementation of our ti&m Online Identification solution. Working closely with the customers, our UX experts, process consultants and software developers can optimize all parts of the journey and create a unique onboarding experience.



Martin Unterbäumen, Head of Client Engagement, would be happy to advise you:
+41 44 497 75 00 oder ti8m.com/online-id





“Those who are already exploring the e-ID will have a competitive advantage in 2026”

Self-sovereign identity // Identity misuse and theft is a growing threat on the internet. Switzerland and the EU are developing a decentralized digital identity, creating a legal framework and discussing technological issues. We spoke to Désirée Heutschi to find out what actions companies and authorities should take now to prepare for the introduction of secure digital identities.

Désirée Heutschi

Member of the Executive Board
Orell Füssli AG & VR/Co-CEO of
Procivis AG

Désirée Heutschi has been a member of the Orell Füssli AG Executive Board and the Procivis AG Board of Directors since 2020, and Procivis Co-CEO since 2023. She has many years of experience in innovation and the software industry and holds an Executive Master of Business Law (University of St.Gallen).

Ms. Heutschi, according to a German study, one in ten people have experienced identity theft. You are an expert in physical and digital identity solutions. What do you make of this figure?

It does not surprise me. And there has been a legal response: In Switzerland, identity misuse has been a criminal offense since 2023, and the forthcoming e-ID Act will lay the foundations for a secure digital identity issued by the state. At the same time, the EU eIDAS 2.0 regulation requires member states to provide e-ID wallets for their citizens. Both are scheduled to be implemented in 2026.

18 months is not long. How can we prepare?

We need technology solutions that give us security so that we can trust our virtual counterparts. These must comply with both Swiss and European guidelines, as national borders will have little impact when it comes to digital identities and proofs of identity. Over the last year and a half, we have developed a unique product that meets all the requirements for a technology solution and that can be implemented now. Public authorities and businesses should start preparing their systems for the introduction of the e-ID, so that they can take advantage of the benefits immediately.

How will the technological requirements of these directives be implemented?

Using the concept of self-sovereign identity. Digital proofs of identity and verifiable credentials are more than just digital equivalents of physical documents. They contain data known as attributes, which users can share selectively and systematically. They can be used, for example, for secure employee authorization or efficient credit checks. Users keep control over their data and can track which attributes they have shared with whom and when. In contrast to conventional centrally managed systems, information on usage is not passed to third parties.

You are Head of Corporate Development for the Orell Füssli Group and Co-CEO of the subsidiary Procivis, a provider of technology solutions for digital identities and credentials. How do these roles fit together?

One of Orell Füssli's core businesses is security. We have been a trusted partner of governments for many years, helping produce physical trust documents such as banknotes, the Swiss passport and driver's licenses. Procivis adds digital identities and credentials to the portfolio. We have developed a new, forward-looking software solution that can be used to issue, check and store credentials such as an e-ID, a digital driver's license or other digital proofs of identity. We provide this software to public authorities and companies.

Why should public authorities and companies choose the Procivis solution?

Most organizations are not familiar with the technicalities of discussions about protocols, formats and standards. So many of them are waiting for the EU or the federal government to make a decision on these aspects. In Procivis One, we have developed our own pioneering solution that is compatible with multiple protocols, complies with current regulations in Switzerland and the EU, and can adapt to future developments. It complies with SSI requirements and ensures data sovereignty for users. Procivis One is already available and can be operated autonomously by our customers — offering high performance and scalability for millions of users and types of credentials.

What other credentials could become relevant in the coming years?

In Switzerland, there are three different levels of requirement: Level 1 is the digital identity itself, level 2 includes state-regulated credentials such as driver's licenses, criminal record extracts or diplomas, and level 3 covers all other digital credentials such as authorizations and membership cards. The potential uses are practically endless.

What advice would you give our readers?

I am convinced that institutions that are already preparing for the e-ID in Switzerland and eIDAS 2.0 in the European Union will have a competitive advantage. It is a good idea to consider which processes can be made more efficient or redesigned and the impact this will have on existing IT infrastructure. At the same time, it is important to consider the technological aspects in order to simplify future deployment. ●

Orell Füssli is a pioneer in the field of security and education. A leading systems provider for security technologies and identification systems and a long-standing government partner, Orell Füssli sets the technological standard for analog and digital applications. Orell Füssli is active involved with the education sector through its publishing companies and has a stake in Orell Füssli Thalia AG, Switzerland's largest bookseller.
orellfuessli.com

The subsidiary Procivis is an established provider of digital identity technology in Switzerland, and launched its new software solution Procivis One for decentralized digital identities and verifiable digital credentials in 2023.
procivis.ch



Andy Maier

Board of directors, ti&m

As CIO of AXA, Zurich Financial, and the Winterthur Group, Andy Maier has had a lasting impact on the digitalization of the insurance industry. Even after his retirement in September 2023, the InsurTech-expert will continue to work for AXA as a Senior Advisor. He is also a member of the board of directors of SOBRADO AG and Chairman of EcoHub AG and noimos AG. As a member of the board of directors at ti&m, he supports the company with the strategic development of its insurance division.

ti8m.com

What do the two most important stakeholder groups want from an insurance company?

An insurance policy serves to transfer the financial aspects of a risk from a person to an insurance company. It is based on a social principle: That this risk transfer costs the same for everyone when the same risks are selected. If they have to make a claim, customers expect a reliable, quick, and easy service. Investors buy shares in insurance companies because of the long-term, secure dividends. These companies have stable business models, and the returns they generate are very attractive.

The digital challenges for insurance companies

Customer behavior is changing. Young customers are less loyal. Fully digital and flexible products and services are essential. The same goes for omnichannel strategies for advisory services, sales, and other

Why insurance companies need to invest in tech and data now

InsurTech // Insurance companies need to speed up their digitalization – but some lack the skills to do so. Strategic technology partners such as ti&m provide the necessary expertise for tech and data projects so that insurers can successfully tackle the next steps.

services. Insurance companies should interact more frequently with their customers – on easy-to-use digital channels.

The market is putting pressure on prices. New competitors and intermediaries are entering the market. What's more, price transparency is becoming more detailed, which makes it easier for consumers to compare offers. Distribution costs are very high, and exclusive distributors and brokers have to significantly improve their productivity.

Product administration needs to be simpler, more flexible, and more digital

Insurance companies should take proactive steps to reduce claims inflation And they have to make sure that claims handling meets customers' digital requirements. Additionally, the insurance industry is suffering from **the shortage of skilled workers.**

The five investment priorities

Digital transformation is not an end in itself. Insurance companies need to develop digital capabilities that meet customer requirements. A sustainable and strategic approach is crucial here:

Augmented advisory services: Brokers and agencies need digital support for the sales process. The key here is making sure that they can focus on giving advice. Companies should aim to fully automate policy administration and issuing certificates. In addition, they should use Copilot AI and LLM solutions to support their advisors and answer questions about policy terms. Advisors should have a 360-degree view of their customers.

After all, having additional information provides opportunities to give good advice – and opportunities for proactive sales.

Beyond insurance: In the future, insurance companies will be part of various ecosystems. They will be integrated into ecosystems for banking, pensions, home, SMEs, and health. This will provide opportunities to obtain more information about their customers and make sales. In these ecosystems, differentiated partner services such as prevention services will increase customer loyalty.

Zero ops: Insurance companies need to fully automate their operational processes. Manual interventions should be rare. When they are needed, AI should augment them. This means reading documents automatically, identifying requests, and handling them digitally. Digital interactions with customers should take place via a secure messaging board. In addition, insurance companies need to define and automate their oversight and compliance processes.

Digital products for digital natives: Insurers need to create simple, modular products that consumers can combine to suit their needs. Service levels should be clear, and services need to be accessible. Coverage checks and claims handling should be digitalized and mobile-friendly.

Open pensions: Financial transparency in old-age provision is becoming more important: Insurance companies need to identify pension gaps earlier. They should make proposals for ensuring quality of life in old age and communicate them clearly to customers via digital channels.

The twelve capabilities needed to achieve these ambitions

To achieve these five investment priorities, insurance companies need to define their required digital capabilities and determine their current level of maturity:

IT excellence

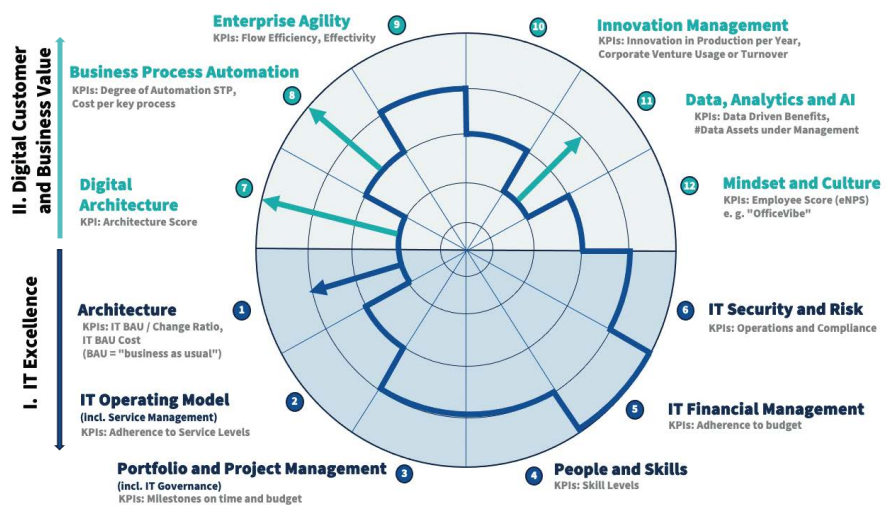
The bottom half of the radar (1 – 6)

shows six fundamental IT capabilities. Logically, companies need to achieve a certain level of maturity with this foundation before they can build on it. IT is primarily responsible for these capabilities.

Digital customer and business value

The top six capabilities (7 – 12)

indirectly generate value for the insurance company's customers and investors. In the digital age, customer benefits and business growth go hand in hand. To develop these capabilities, insurers need to adopt a co-creation approach and involve business and IT sponsors. Insurance companies have recognized that developing digital skills is strategically very relevant and complex. Insurers are already investing more in these capabilities and increasing their efforts to find specialists and expert partners.



ments, and quickly developing an MVP. Working with mobile, UX, and design thinking methods, for example, that open up new perspectives. Integrating security considerations into the design right from the start. And using agile teams to develop products with the insurer and expand its core landscape.

Technological core competencies and on-premises specialists

These four dimensions are the biggest drivers for future value generation: **Digital architecture:** All insurers will invest in developing new cloud-native applications. In addition, they are migrating their core applications to the cloud and modernizing them. This means modularizing and virtualizing applications and automating testing. In the future, insurers will use software to configure their infrastructures and automate application integration and configuration management via scripting. Faster development cycles but also the need for resilience and reversibility will dictate the requirements for this.

Business process automation and augmentation: As described above, insurers will digitalize their current business models over the next ten years. They have to significantly improve the productivity of their consultants and in-house operations through business process automation (BPA). To achieve this, insurers need a taxonomy for

process management, automation frameworks, metrics for performance management, and the technologies to implement them. Using AI analytics to evaluate process data will provide additional information.

Data, analytics, and AI: Data governance, data management, data architecture, master data and metadata management, quality management, data security and privacy management, data leakage and lineage, ethics and compliance – these are all essential for building analytical rules and models. Of course, modern technologies are also needed – and the three major cloud hyperscalers will supply them. On this basis, insurers will be able to develop and test value-enhancing models – and then apply them. The most important areas of application are in Customer 360, risk selection and pricing, claims leakage and fraud prevention, and document intelligence.

Security technologies: Using new technologies also means applying modern and robust security concepts.

Insurers are facing complex business and technology challenges. To tackle them, working with competent IT partners such as ti&m is crucial. Together, they need to analyze their strategic requirements and identify the necessary tech and data capabilities. Their ultimate goal must be to develop software solutions that meet the needs of their customers and employees. ●

Finding the right partner

Insurance companies will not be able to do all this on their own. They will need expert partners who bring technology and business expertise to their projects. ti&m has the essential core competencies as a tech and data partner to support insurance companies in the next steps of their digital transformation.

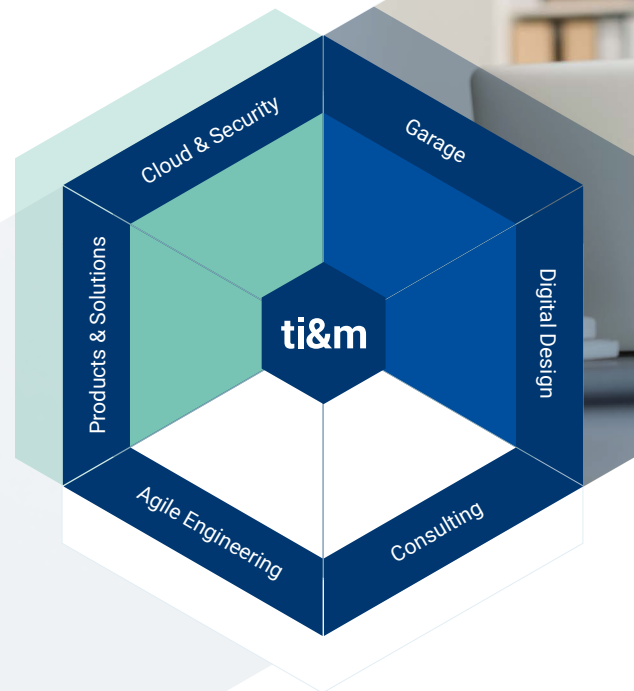
Integrating the entire value chain

What do insurance companies need to look for in a strategic, long-term partner? One of the two most important requirements is the ability to tick all the boxes: developing and evaluating various solutions through consulting, helping shape business require-

We digitalize your company

ti&m stands for technology, innovation and management. We are market leaders in digitalization and security products, as well as innovation projects. Our six offices currently employ over 600 engineers, designers, and consultants. Our growth is based on our strengths and values: the courage to innovate, a passion for what we do, talent, sustainable growth, respect and tolerance, and Swissness.

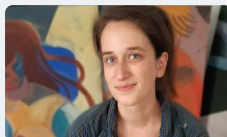
We integrate the entire IT value chain and develop user-centered innovations with unbeatable time to market.



Our engagements



ti8m.com/hack-an-app



ti8m.com/art-at-work

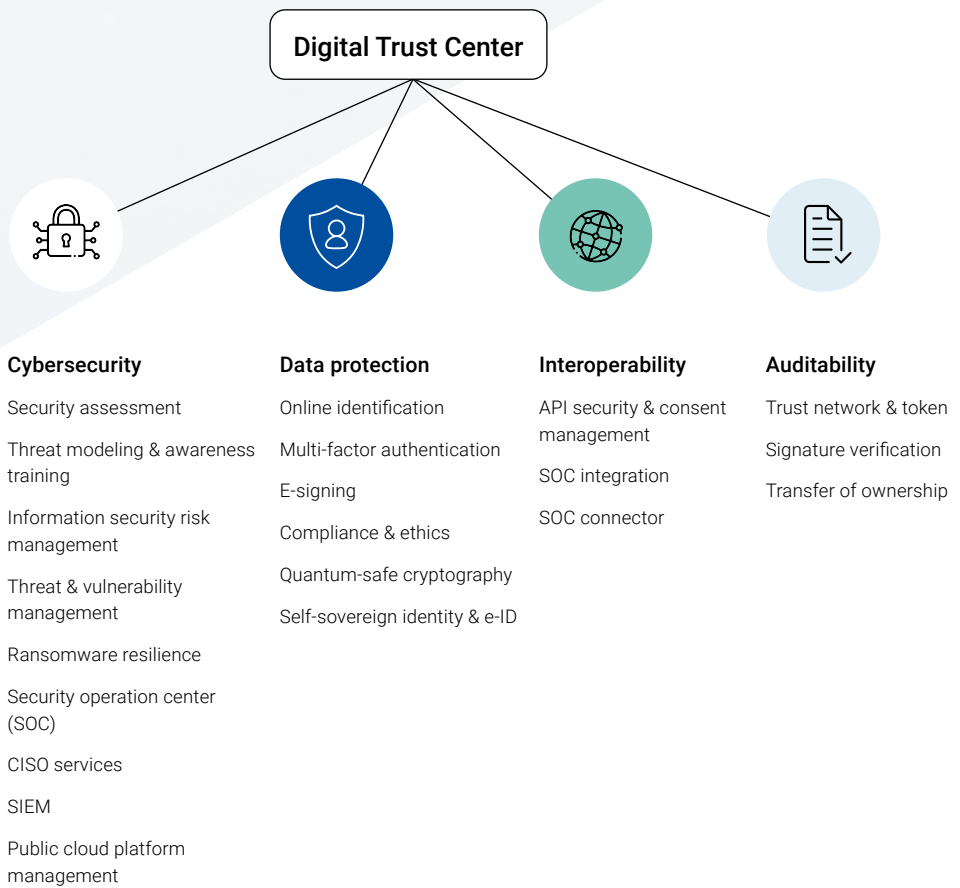


ti8m.com/shake-the-lake

Trust is the basis for every interaction.

With the Digital Trust Center, we at ti&m have established the expertise to holistically integrate all aspects of digital trust into our services, products and software developments.

Our experts support you in creating secure and reliable digital business spaces, minimizing risks, and defending yourself against cyber attacks. So that you can fully realize your digital potential through innovation and new business models.



Leunita Saliji, Head of Cloud & Innovation Hosting, would be happy to advise you: +41 44 497 75 00 or ti8m.com/security



How the Federal Office for Cyber Security is promoting resilience



Cyber resilience //

Cybersecurity is a topic that influences our everyday lives. It is becoming more and more important. This is why the Federal Council turned the National Cyber Security Centre into a Federal Office for Cyber Security (BACS) on January 1, 2024. What does this mean, and what will change as a result?

Cybersecurity has become more and more important at all levels in recent years. It is a key factor for Switzerland's attractiveness as a business location and in its citizens' digital security. It also plays a crucial role in national and international foreign and security policy. Guaranteeing cybersecurity has therefore become a fundamental responsibility for the federal government. The Federal Council has recognized by turning the National Cyber Security Centre into a federal office. However, its core responsibilities remain the same. The Federal Office for Cyber Security (BACS) will continue to be the first point of contact for businesses, public services, educational institutions, and the general public when it comes to cyber issues. It is responsible for coordinating and implementing the national cyber strategy (NCS). Its operational activities help make Switzerland more resilient to cyber attacks.

The cyber threat landscape

The BACS receives reports from the public, businesses, operators of critical infrastructure, and its national and international network of partner organizations. This information gives the BACS a good overview of the current cyber threat landscape. With this overview, it can issue specific briefings and warnings to the relevant target groups.



Florian Schütz

Federal Office for Cyber Security (BACS)

Florian Schütz is Director of the Federal Office for Cyber Security (BACS). He studied at ETH in Zurich and has a Master's in Computer Science and a Master of Advanced Studies in Security Policy and Crisis Management. He has expanded his expertise in IT security in various positions, including at Zalando in Germany.

nsc.admin.ch



Cyber attack on Xplain: the Federal Office for Cyber Security's report on the data analysis
bit.ly/3QLCpmZ

The BACS also uses the findings from its operational activities to raise awareness. These activities are aimed at private individuals, companies, and public bodies. It coordinates these efforts with numerous partners, such as Swiss Crime Prevention (SCP) and the Lucerne University of Applied Sciences and Arts. In addition, the BACS runs nationwide campaigns. Its staff constantly evaluate and review all its efforts to make them more effective.

Protecting critical infrastructure and reducing vulnerabilities

One of the BACS's core tasks is to support operators of critical infrastructure in protecting themselves against cyber threats. To this end, it provides tools and resources that increase the cybersecurity of the infrastructure and its users. This includes providing technical information on IT infrastructures that malicious actors are misusing, for example to distribute malware or operate phishing websites. The BACS's Computer Emergency Response Team (GovCERT) supports operators of critical infrastructure in dealing with cyber incidents. Since the end of September 2021, the BACS has also been the official contact for reporting security vulnerabilities in Switzerland.

MITRE, an international non-profit organization devoted to cybersecurity, has also authorized the BACS to assign CVE numbers. MITRE uses these numbers to identify common vulnerabilities and exposures. As a MITRE partner organization, the BACS is responsible for publishing the reported vulnerabilities in a coordinated manner. It thereby plays a crucial role in minimizing the harm that threat actors can cause due to these vulnerabilities.

Overview of the reports received in 2023

Last year, the BACS – under its former name, the NCSC – received a total of 49,380 reports. That is a significant increase of 30 percent on the previous year. Reports of various forms of fraud topped the list again (around 30,000 reports last year). These forms of attack may include emails that appear to be from the authorities. Scammers often misuse the names of current Federal Councilors in such attacks to make their messages appear more credible. Other examples include bogus messages about undeliverable parcels and investment fraud. The BACS also observed the first attempted attacks using artificial intelligence. In addition, fraudsters occasionally wrote phishing emails in Swiss German, particularly in classified ad fraud.

Ransomware attacks have been a major area of work for the BACS (and its predecessor) for several years. In May 2023, one of the federal administration's IT service providers was the victim of a ransomware attack. The attackers first stole data from the company. They then published the information on the dark web. Data from the federal administration was among the information released. The administration immediately analyzed the leaked data and released a detailed report on it. It also launched an administrative investigation, which concluded at the end of April.

These kinds of attacks on service providers show how important it is to take preventive steps against cyber attacks. With these threats rising, it is essential for national and international agencies to exchange information and communicate after a cyber attack. ●

“There was never any plan to replace today’s cryptographic methods”

Cryptography // Thanks to much higher computing power, quantum computers can solve tasks that today’s computers cannot. The bad news: In the near future, they will be able to crack the encryption methods commonly used today. What will replace the current methods? We spoke to Marc Stöcklin, Head of Security Research at IBM in Rüschlikon, about the upcoming Q-Day.



Dr. Marc Stöcklin

Head of Security Research, IBM Research Europe

Dr. Marc Stöcklin is Principal Research Scientist and Head of Security Research at IBM Research Europe – Zurich and Global Co-Head of Quantum Safe Cryptography at IBM.

research.ibm.com

What encryption methods are there?

There are basically two encryption methods: symmetric and asymmetric. Symmetric encryption uses the same key to encrypt and decrypt, which means that the sender

and the recipient must have the same key. This system has the disadvantage that the shared key must be distributed via a secure channel. To overcome this disadvantage, asymmetric encryption was developed in the 1970s. This uses a key pair consisting of a public key for encrypting and a private key for decrypting. The public key is freely distributed, while the private key remains secret. This enables secure communication without the need to exchange a shared secret key in advance. The asymmetric method created the basis for today’s exchange of information over the Internet, such as online banking, etc. For post-quantum cryptography, only asymmetric cryptography is actually relevant.

How does asymmetric encryption work?

The asymmetric encryption method is based on difficult mathematical problems: in other words, problems that a computer cannot solve quickly, such as factorizing large numbers. Even as humans, we can break down the number 91 into the two prime factors 13 and 7. For a 600-digit number, however, a computer would need millions of years because there is no fast algorithm for this. The security of encryption is based on this one-way function: multiplication is easy, but factorization, i.e. breaking down a

number into its multipliers, is very difficult. Factorizing a large number into prime numbers, which is known as the RSA method, is only one of the possible methods.

Why do quantum computers pose a threat to these encryption methods?

In the 1990s, Peter Shor developed an algorithm enabling a quantum computer to calculate the factorization in just a few hours. Back then, quantum computers were just theory; today, they actually exist. And they are becoming more and more powerful.

So is the encryption in use today still secure?

Yes and no. As things stand today, the RSA method, which has been in use for 50 years, is secure. But with the increase in computing power, quantum computers will in future be able to decode information that is currently protected by these methods.

When will this happen?

There are various estimates, but no one can say for sure. The National Institute of Standards and Technology (NIST) in the USA, for example, assumes that by 2030, there will be cryptographically relevant quantum computers that pose a threat to cryptography. Estimates vary on how many quantum bits, or qubits for short, are needed for a quantum computer to be able to apply Shor’s algorithm or other algorithms that can crack the encryption. Initially, the assumption was that billions of qubits would be needed, but a lot has happened in recent years. Today, the figure is thought to be around 10,000 qubits. Last fall, IBM achieved 1,100 qubits. This number will increase over the next few years, and at some point Q-Day will arrive. Today, we also have the problem that quantum computers and qubits are very error-prone. But again, a lot of progress is being made here to correct or reduce errors more quickly.

What new methods that can withstand a quantum computer are already available as a replacement?

In 2022, NIST selected four quantum-safe algorithms as part of a six-year competition: two CRYSTALS algorithms, CRYSTALS-Kyber and CRYSTALS-Dilithium, as well as FALCON and SPHINCS+. NIST will publish

its new standards this summer. These will be the new standards to secure the digital world for the coming decades. Anyone could take part in the competition, and cryptographers around the world tried to crack the submitted encryption algorithms. Naturally, many were eliminated, and in the end, NIST selected these four algorithms because they are the most secure and also the most practicable. Europe is taking the lead in this area, by the way. All four selected methods were primarily developed by institutes in Europe, and three of the four algorithms were largely developed by us at the IBM research laboratory in Rüschlikon.

In which areas are the algorithms used?

CRYSTALS-Kyber is an algorithm for securely exchanging keys via a public channel. It replaces well-known methods such as the Diffie-Hellman method and, unlike these, is secure against quantum computers. The other three algorithms are methods for digital signatures, to prove the authenticity of certificates, documents, software updates, etc.

When and for whom will the new NIST standard apply?

"Standard" means agreeing on how to encrypt and communicate. The US government is not just doing this for itself, but for the entire ecosystem, including the financial industry and others. It has set out a roadmap defining when and in which applications the new algorithms must be integrated. The NIST standards apply to many areas in the USA, but also have a global impact. Authorities in Europe also cite NIST. Standardization sends out a signal: the encryption of a solution is generally certified. Software manufacturers that supply the US government and the US market must have these certifications. Buyers do not want to implement 20 different algorithms. The private sector will therefore also follow suit, as cryptography is used everywhere and everyone is affected.

Do IBM and the other developers have a patent on their algorithms?

No. One of the requirements of the competition was that the submitted methods must not be patented. All the submitted algorithms are publicly available as open source

and must be free of intellectual property rights. It is important that the algorithms are transparent for all to see and can be checked.

When will the new algorithms replace the current encryption methods?

This process has already started. At IBM, we implemented the algorithms in our mainframes in 2022, before the NIST announcement. Various cloud providers offer the algorithms and they are already integrated in the Google Chrome browser. Apple also announced in its iMessage security update in February that it is now using CRYSTALS-Kyber. The US government, for example, has drawn up a roadmap setting out when the new encryption standards must be implemented in which applications. What is important now is that companies and service providers can prepare for this transition. We don't want a repeat of the Y2K problem. Back then, the transition took place relatively late and it became very expensive. Now we have a little more time, but it will depend on whether we tackle it in time and whether it is planned cleverly.

What difficulties do you see in switching to the new methods? Will it involve a lot of time and expense?

Until now, no one has really given much thought to the cryptographies used. They existed and were used. Nobody has ever recorded which methods are used in today's very complex IT environment and where, as there was never any plan to replace the cryptography. You first need to understand how the relevant data streams are encrypted. IBM supports organizations with the transition: How can you prepare? What should you prioritize? How do you organize and orchestrate the whole thing? And how can you make the switch efficiently over a certain period of time without it costing a lot of money and causing a lot of headaches?

The transition is very complex because there are many dependencies in today's IT landscape. A company obtains most of its software, or at least components of it, from various providers or directly from the cloud. This means that the transition has many dependencies, as the systems must continue to be compatible with each other. For example,

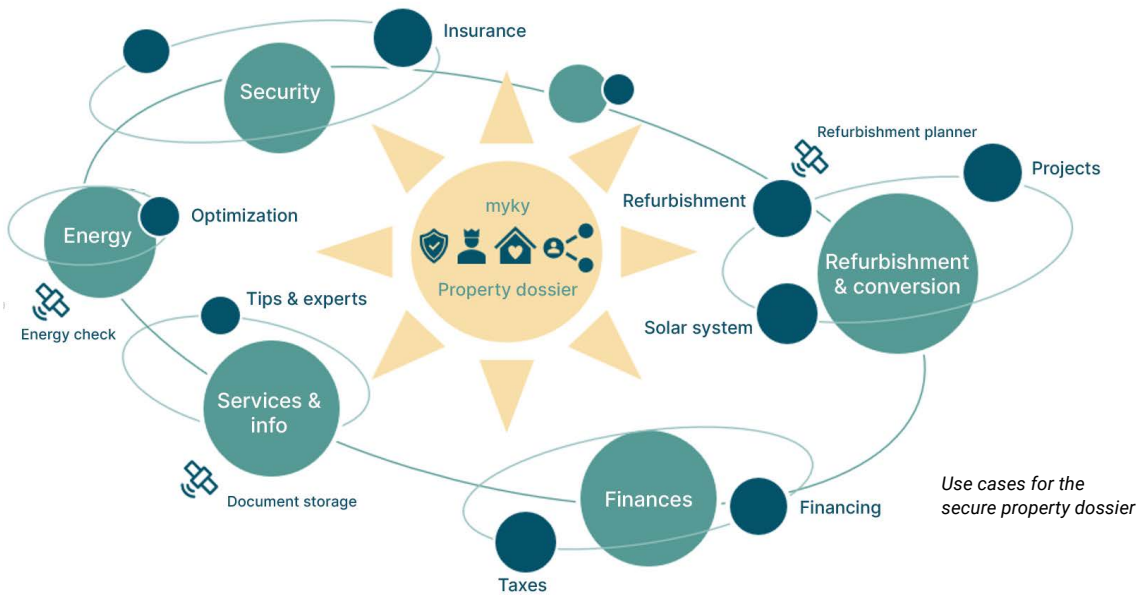
a bank must ensure that the transition not only takes place in the backend of its online banking system, but that all its customers, i.e. the browsers they use, are also able to make the change. In today's initiatives, where workloads are moved to clouds or containers in clusters, the quantum-safe issue should be integrated from the outset. Making this change retrospectively is much more complex and expensive. This is where the concept of crypto-agility comes in, where cryptography does not have to be deeply embedded in the code, but is externalized in the form of Cryptography as a Service. This means that cryptography can be managed and used more easily and effectively. Germany's Federal Office for Information Security (BSI) recently published a recommendation on crypto-agility that serves as a guide for companies. ●



In the second part of the interview, Marc Stöcklin explains whether we are ready for Q-Day and which other areas of cryptography IBM is researching.



Continue reading online now:
ti8m.com/cryptography



Digital trust and data exchange in the housing ecosystem

Digital ecosystems // A key challenge for the development of cross-company customer journeys is reliable data that is well protected at all times and can be shared as easily as possible between companies and customers in a controlled manner. This article provides insights into the topic using the example of the start-up myky. myky is the secure, personal and digital property dossier for property owners and their key to tools, tips and a network for managing their home sustainably.

Housing is a fundamental human need. In all aspects of housing and real estate there are countless use cases where companies and private individuals need and process data. myky has increasingly focused on the sustainable refurbishment of residential buildings in recent months, which is why we are using this example for this article. The real estate sector is a key factor for Switzerland in achieving its CO₂ targets. According to the Federal Office for the Environment, real estate is responsible for almost a quarter of today's greenhouse gas emissions and offers great potential for improvement. Customer surveys conducted by myky show that refurbishment is a complex task for owners that they will only tackle if it is economically and ecologically sustainable for them. Key challenges include a lack of data on the current condition, the ideal approach, and reliable projections of realistic funding, as well as the costs of refurbishment.

The challenge of data quality

There are many sources of data associated with real estate. In addition to public data sources, which are being continually expanded, specialized data providers offer information on all properties in Switzerland. Other possible sources include data from companies that work with real estate data for their products and services, such as banks for granting mortgages, insurance companies for buildings insurance or household contents insurance, energy suppliers, as well as tradesmen, building contractors, and architects. These stakeholders have an isolated view of the property, which is often based on the time of the last transaction/interaction with the homeowners and



Tiziano Lenoci

CEO myky AG

Tiziano Lenoci has an MSc in business administration and was a member of the Group Management of the GVB Group before founding myky AG. He was CEO of GVB Services AG and, among other things, responsible for group-wide marketing & sales and start-up investments.

myky.ch



Stefan Reitbauer

CEO NNH Holding AG

Stefan Reitbauer is a business informatics scientist and already addressed the topic of corporate networks in his doctoral thesis at the University of St. Gallen. Before becoming CEO of NNH at the end of 2022, he held various positions at Swisscom, including Field CTO for Banking and Insurance.

usually only includes “reliable” data for their respective topics. As soon as these companies start working on new, “broader” use cases, they often lack a reliable data basis. For example, information required for sustainable refurbishment – such as on the heating system, building volume or location – is often outdated, incomplete, and not centrally available or usable.

myky as the key to a sustainable home – smart and secure

Homeowners usually have the best, most comprehensive access to the “right” information about a property. In practice, this information is often filed away physically in conventional folders at present. myky’s vision is to provide homeowners with a platform for them to store information about their property digitally and securely, which they can then use to help with specific applications such as refurbishment. With the myky property dossier, the idea is that an “intelligent assistant” gives owners valuable information and shows them opportunities and risks associated with their property.

Sharing data

In today’s networked world, it is essential that data platforms do not operate in isolation, but can interact seamlessly with other systems and partners. An important pillar of myky’s property dossier is that data relating to the property is shared – under the homeowner’s control and only with the homeowner’s consent. This means that not only does the homeowner share data about their property as required, but also that the companies the homeowner interacts with pro-

vide data for the property dossier. In the context of sustainable refurbishment, homeowners can share information on the current condition of the building (heating, insulation, etc.) and their refurbishment plans with banks, tradespeople, building experts, or their buildings insurance company. In return, the companies can share information with homeowners about their mortgage, the value of their property, their insurance cover, or even specific offers for their home ideas. Ideally, for example, tradespeople would work interactively with homeowners directly in separate project areas of the myky property dossier to develop a suitable, financially optimized refurbishment project.

Google-based platform as the technical basis

In an era where data is at the heart of so many organizations, security and trust in the management of that data are critical. This applies in particular to private information that owners collect about their home. Homeowners and companies alike are faced with the challenge of comprehensively protecting this information, while at the same time taking advantage of the opportunities offered by modern technologies and making well-founded, data-based decisions. To achieve this, myky uses a platform set up by NNH Holding. This platform was implemented on behalf of 19 cantonal banks together with ti&m as general contractor and implementation and operating partner. NNH’s vision is that many companies like myky will be able to use the NNH platform to efficiently and securely implement cross-company customer journeys involving housing. The NNH platform is based on powerful standard services from the Google Cloud Platform (GCP) for central components such as data processing and analysis (including BigQuery), system integration (including Apigee) and security. Important design criteria of the platform include:

- *Using open standards and established products*
- *Benefiting from the innovative power and functional scope of a leading cloud solution through the consistent use of Google products*
- *Implementing best practices such as data storage in Switzerland, customer-managed encryption and zero trust, including between the platform components*
- *Defining API-based data products instead of a rigid real estate reference data model*

Our next use cases also focus on advanced functions for controlled data sharing, enabling data-based decisions, and flexible and secure interactions between companies and private individuals. For a sustainable home and thus a contribution to achieving CO₂ targets. ●

Digital trust at ti&m: a holistic approach

ti&m Digital Trust Center // Data breaches, cyber attacks, corporate misconduct: Almost every day we read about incidents that shake our confidence in the digital world. Traditional security measures and compliance standards alone are not enough to meet today's complex requirements. With our Digital Trust Center, we pursue a holistic approach that aligns trust, security, and technology.

Our private and business spheres are shifting more and more into the digital world. We carry out our transactions (almost) exclusively online, and store our personal information – from tax returns to children's photos – somewhere in a cloud. And so it goes without saying that the same principle applies to digitalization as to a bank: Trust is the highest good. Digital trust is becoming a decisive competitive factor. To meet the demands and challenges in the long term, it is crucial to view the issue from all perspectives.

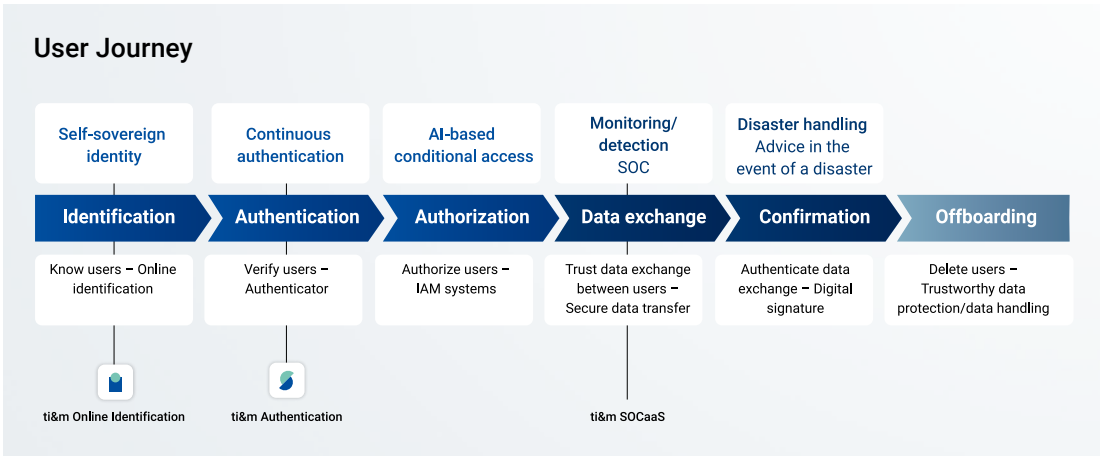
Blockchain, AI and co. – technology takes center stage

Technology plays a key role in digital trust. But this role is quite ambivalent. Innovations such as blockchain, artificial intelligence and IoT certainly offer new opportunities to strengthen digital trust. However, they also pose new dangers that threaten to shake trust, whether intentionally through the activities of cyber criminals or unintentionally through an incorrect response from an intelligent chatbot due to bias. Our Digital Trust Center seamlessly integrates these technologies into existing infrastructures and processes. This enables companies to minimize risks and strengthen trust in the stakeholders through automated compliance checks, continuous security analysis, and tailored training.

Expertise throughout the entire user journey

By integrating technology, compliance, governance, and a trusting corporate culture, companies can create a foundation for digital trust that equips them for the challenges of the future. ti&m offers a comprehensive range of coordinated services and products that help companies build and maintain digital trust. Based on our many years of expertise and innovative strength, our Digital Trust Center advises our customers on implementing secure trust concepts and develops tailor-made solutions that address the specific requirements and challenges of our customers throughout the entire user journey.

To protect our customers against the constantly growing number of cyber threats and attacks, we work with them to develop proactive and effective security strategies. We develop and implement secure digital platforms and infrastructures for our customers, helping them to build resilience against future threats. With ti&m Online Identification, ti&m Authentication, and SOCaaS (Security Operations Center as a Service), we offer proven security and authentication products that can be seamlessly integrated into existing solutions. By combining our products and services, we create a robust security environment that ensures digital trust and enables companies to design their digital business processes securely and efficiently. We pay particular attention to continuously improving our solutions and adapting them to the changing threat situation.



Our expertise and our commitment to digital security enable companies not only to meet their current security needs, but also to act in a forward-looking and resilient way. We thus play a key role in ensuring that our customers can operate successfully and confidently in the digital age. We provide companies with comprehensive support in successfully shaping their digital transformation and help to build trust among their customers, partners, and employees.

Global perspective and cultural change

The World Economic Forum has developed a framework that offers a comprehensive guide for companies to understand and implement digital trust on a global level. It includes guidelines on cybersecurity, privacy, transparency, redressability, auditability, fairness, interoperability, and safety, and shows how digital trust can be strengthened throughout the economy through collaborative approaches.

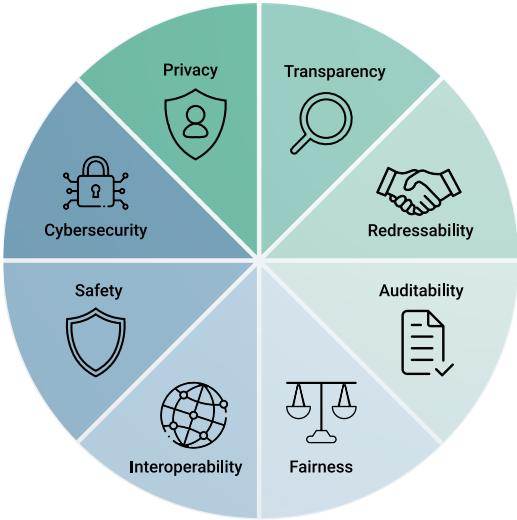


Leunita Saliji

**Head of Cloud & Innovation Hosting,
Member of the Executive Board**

Leunita Saliji has been working at ti&m for over six years and has been responsible for Cloud & Innovation Hosting at ti&m since December 2023. Prior to this, she held various management positions at ti&m as Head of Application Management and Head of Operations & Services Management. She has a Master's degree in Business Information Technology and teaches at the Swiss Distance University of Applied Sciences.

ti8m.com



However, anchoring digital trust in an organization in the long term requires more than just innovation, technological expertise, and the right measures in terms of cybersecurity, data protection, and interoperability. Digital trust, transparency, ethics, and respect must be embedded in the corporate culture, and the management must model these values on a daily basis. Without this, even the most well-thought-out measures will not have the desired effect. A successful change in culture is the only way to strengthen employees' and customers' trust in the long term. ●



How ti&m creates digital trust

Authentication & identification //
 With our products and services, we support our customers along the entire IT value chain in creating secure and trustworthy digital business environments.

Cyber attacks have not only increased significantly in Switzerland. They are also causing billions of dollars in damage worldwide. The widespread phishing method is still an effective way for cyber criminals to obtain sensitive information. Adequate protection therefore forms the basis for the success and well-being of individuals, companies and societies. The threats are continually increasing. Comprehensive security of sensitive data and adequate protection of complex systems, open platforms and innovative solutions are therefore essential, and are fundamental pillars of digital trust.

Passwords that do not exist cannot be stolen or guessed

One of the key measures to improve digital security is passwordless authentication. This offers a future-proof alternative to conventional passwords. Password systems are known to be vulnerable. This is why the FIDO Alliance (Fast Identity Online) – a cross-industry association of organizations and companies – has developed and promoted global standards to reduce the use of

passwords and support secure and user-friendly solutions. With passkeys, an extension of the FIDO2 standard, an innovative option has been created that replaces passwords with cryptographic key pairs. Unlike passwords, these private keys are never exchanged over the network and so never leave the device (smartphone or other hardware token) or the device manufacturer's ecosystem. Therefore, in contrast to passwords, they cannot be intercepted or stolen.

Future-proof product with the “key” to success

ti&m embraced the paradigm shift in secure authentication as long ago as 2013 and offered its customers a passwordless and phishing-resistant alternative. With ti&m Authentication, we have developed a user-friendly authentication platform that meets the highest security standards and is based on the same technology as passkeys. We recognized the added value and potential of this technology early on and used our extensive digitalization experience to simplify the main authentication hurdles without compromising security. Seamless and simple integration into customer-specific environments offers the necessary flexibility of a local Swiss product, whether in traditional corporate networks, cloud infrastructures or mobile applications. A trailblazer in the development of more secure, user-friendly and adaptive authentication solutions in a world that has to adapt to ever-changing requirements.

The growing trend towards passwordless authentication and its advantages in terms of security and user-friendliness are clear. Nevertheless, it will probably be



some time yet before the new technology is fully established and accepted in our everyday lives. As experts in cybersecurity and authentication technologies, we can provide comprehensive advice for our customers and implement customized security solutions that offer the perfect balance between user-friendliness and the highest security standards.



Philip Dieringer

Head of the Bern office, ti&m

Your expert for secure authentication.



ti&m Online Identification

Every customer relationship begins with secure identification of the new customer. Everyday life is complicated enough, and customers don't have the time (or simply don't want) to physically stand in line at a branch or struggle through an unintuitive identification app online just to open a new account.

It is frequently pointed out that digitalization is more than just transferring analog processes to the digital world. It's about rethinking entire processes and mapping them in a digital solution that helps users to obtain services more quickly and easily and frees companies from tedious and cost-intensive administrative tasks. With ti&m Online Identification, we offer our business customers exactly that: A fully automated solution that allows new customers to identify themselves and open an account at any time and from anywhere in the world.

More than just identification

As experts in online identification, we know identification is only one part of the user journey and the processes that take place in the background. That's why we not only support our customers in seamlessly implementing ti&m Online Identification as a white label solution. We also optimize all parts of the existing or newly created user journey and thus increase the customer onboarding conversion rate. For us, thinking complete processes through to the end also means linking identification with CRM or other applications and integrating downstream services such as digital signatures. For its new signature process "Swisscom Sign", Swisscom uses ti&m Online Identification to identify customers in a legally valid way and to issue qualified electronic signatures that can be used repeatedly to conclude contracts and transactions in Switzerland and the EU. Software development kits

(SDKs) for web and mobile platforms (iOS and Android) enable seamless integration into different environments, and the identification service can be used either on-premises or as a service from ti&m.

Highest safety standards

Secure authentication like in ti&m Authentication or identification solutions such as ti&m Online Identification are important digital trust elements. They allow users to authenticate themselves at any time to access data and services, or to open a new account around the clock to enter into a new business relationship and use electronic signature services. The award-winning ti&m Online Identification is FINMA-compliant and meets all Swiss and European security standards such as ETSI and eIDAS. Our document verification system recognizes identity cards and passports from over 40 countries and is able to read the document used for identification through both the machine-readable zone (MRZ) and the visual inspection zone (VIZ).

Identification is often the first contact a new customer has with an organization's digital services. User-friendly identification and onboarding processes are therefore important for creating positive customer journeys. Because, as is so often the case on a journey, the first step is the most important. And for new customers it has to be simple, secure and fast.



Martin Unterbäumen

Head of Client Engagement, ti&m

Your expert for online identification.

AI – a matter of trust?

Artificial Intelligence // The extent to which we can trust AI is increasingly becoming the crucial question of the 21st century.

Almost all of us have questioned whether we can trust the answers provided by generative AI. On one hand, it's unclear whether the data used for training, such as newspaper articles and blog posts, is factually correct. On the other hand, there is the question of how much bias is embedded in large language models. Clearly, none of us want bias in our answers. But what is bias? Who actually determines what bias is? Prejudices shape us as individuals and as a society and are simply a part of reality. An example: More men than women work in leadership positions. We all probably agree that this isn't good. But it is the reality. Should generative AI reflect the world as it is, or as it ideally should be? And what does such an ideal world look like? Is the notion that there should be an equal number of men and women in leadership positions not also a bias – albeit a positive one? There are various initiatives, such as AI alignment, to integrate societal values into large language models. This also enables organizations to ensure that the AI tools they use comply with internal business rules and compliance requirements. However, training large language models entirely without bias will hardly be possible. Because just like with humans, learning inherently involves bias.

Although all major language models have ethical safeguards, the media regularly reports on so-called jailbreaks. Jailbreaking involves circumventing content moderation guidelines (e.g., on topics like racism and sexism) through specific text prompts. In the best case, the responses provoked by

jailbreaking are simply amusing; in the worst case, the incorrect (pricing information, binding commitments) and damaging (sexism, racism) responses can have legal and financial consequences for companies. Guardrails are used to try to limit usage to intended areas and prevent the chatbot from being “tricked”. Content filters for questions and answers can ensure that no undesirable topics are discussed. Additionally, it may be useful for large language models to always include a disclaimer in their responses, indicating that the answers should be verified by the user.



The problem of so-called hallucinations, that is, generating false or invented information due to data gaps, has also not yet been satisfactorily resolved. Data gaps arise, for example, because the datasets used for training are outdated. If an organization uses an AI chatbot linked to a large language model, the data used may be months or even years old. New and specific information about products and services is missing, leading to incorrect answers that undermine the trust of customers and employees in the technology and ultimately in the organization. This problem can be addressed with Retrieval Augmented Generation (RAG): RAG includes current information or other

additional knowledge sources such as internal company data without the need to train large language models with the new datasets. One wants to utilize the diverse capabilities of large language models, but not rely on their “knowledge”. Since many organizations still distrust AI-generated responses, a “human in the loop” is often embedded in the processes.

Another challenge is the granular authorization of users. Not all employees or customers should have access to the same, often highly sensitive data. Ways must be found to embed sensitive internal company data in such a way that employees and customers only receive answers to their prompts that are intended for them.

We at ti&m are convinced: AI can only realize its potential if secure, trustworthy, and ethical solutions are created. Because AI without digital trust is worthless. ●



Lisa Kondratieva

Head of AI & Digital Solutions,
ti&m

Your expert for Artificial
Intelligence and digital solutions.

Improving the resilience of IT services with SBOMs

Software Bill of Materials // A SBOM is a list of all the software components, dependencies and metadata that are linked to an application. Automating the creation and maintenance of a precise list of software “ingredients” helps protect applications better.



Stephan Sutter

CTO Bern, ti&m

Stephan Sutter is the CTO at our office in Bern. He has been working as an IT architect for around 23 years and as an ICT management consultant for banks, insurance companies, and administrative bodies for 16 years. Stephan Sutter studied industrial electronics at the Higher Technical Institute for Electrical Engineering and obtained a Master of Science in telematics (ICT) management.

To help an organization better understand the impacts of software vulnerabilities, an exercise can be carried out with a Red Team competing against a Blue Team. Unlike penetration testing, in this approach the attacking Red Team attempts to exploit gaps, while the Blue Team defends against the attack with countermeasures and security services. The major challenge here is that one exploitable vulnerability is enough for the Red Team to succeed, but the Blue Team has to protect all vulnerabilities.

As part of a study, an AI research team investigated the impacts of several large language models (LLMs) and open source vulnerability scanners as attackers in sandbox environments. The outcome — GPT-4 was able to exploit 87 percent of the vulnerabilities, while the other LLMs and the vulnerability scanners exploited 0 percent. If the vulnerability was not mentioned in a CVE Description (Common Vulnerabilities and Exposures), the level fell from 87 to 7 percent. The study shows how important it is to support the Blue Team in defending against such attacks. One option is to identify and eliminate vulnerabilities as quickly as possible using SBOMs.

NIST defines the minimum standards for SBOMs for the first time

At a three-day workshop attended by 1,400 people, the US National Institute of Standards and Technology (NIST) made the use of SBOMs mandatory. The intention is to achieve the following objectives:

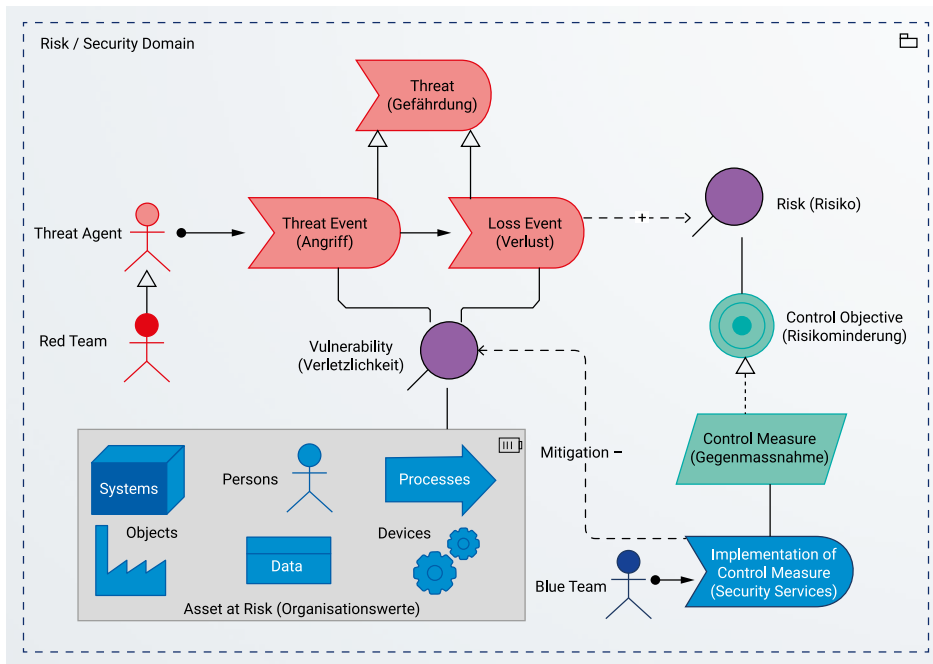
All parties involved in the software supply chain develop a common understanding of the challenges posed by software weaknesses in terms of semantic interoperability.

Automating tools and processes can make it easier and faster to identify software with weaknesses.

With a higher degree of automation, the frequency of scans can be increased and/or adapted to the risk. Software that is available directly from the internet is checked more frequently than software that a team uses on the intranet.

Vulnerability management checks software with vulnerabilities for exploitability and replaces it with corrected versions or protects it using other measures.





You can also read all the articles online in our blog: ti8m.com/blog

Simple version of the risk and security archimate metamodel.

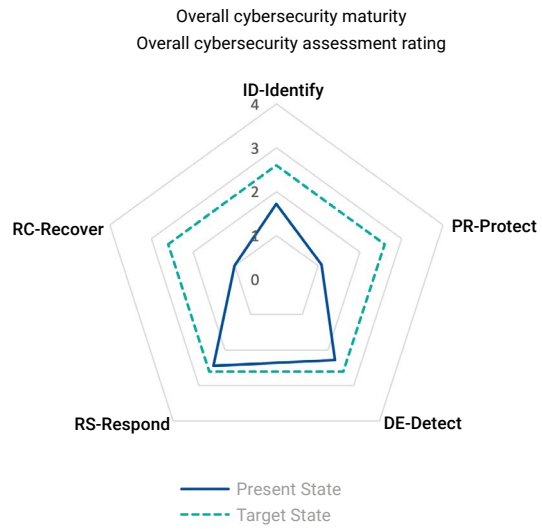
more quickly, and collaboration with partners along the supply chain is intensified so that vulnerabilities can be resolved before the Red Team can exploit them.

And in Switzerland?

The Federal Office for National Economic Supply recommends measures to improve ICT (information and communication technology) resilience in the ICT Minimum Standard 2023 and offers an assessment tool for businesses and organizations to measure their own resilience. The decision to introduce SBOM-based processes brings improvements in the following areas:

- Identify (ID)**
- Detect (DE)**
- Respond (RS)**

The diagram illustrates the outcome of such an assessment. We have expanded the assessment tool to make the effects of introducing an SBOM clearly visible – without an SBOM, the maturity is 1 (partial), but with an SBOM it is 3 (repeatable). An organization that has automated its SBOM processing maturity is close to the recommended ICT Minimum Standard for the Detect and Respond functions. It also improves the Identify function, while Protect and Recover must be addressed with other measures.



The assessment tool of the Federal Office for National Economic Supply shows how SBOM improves security maturity.

A tool like SBOM can significantly strengthen an organization's ICT resilience. SBOM standardization and implementation in the tools along the software supply chain supports the Blue Team in eliminating vulnerabilities. Existing tools can automatically process standardized SBOMs from all suppliers, reducing manual tasks and giving the Blue Team time to increase the maturity of other processes that improve resilience.

“SBOMs are essential for effectively managing the software supply chain”

The Information Service Center EAER ISCeco develops, integrates and operates specialist applications in the Federal Department of Economic Affairs, Education and Research (EAER) and has recently started using SBOMs. We spoke to Manuel Gysin, Software Engineering Team Leader, about introducing SBOMs and their benefits.

What are the biggest challenges in managing IT security, and how can SBOMs make a difference?

Modern software is very complex, often comprising hundreds of third-party components. These components can be embedded both in the runtime environment and directly in the software. Without a precise overview, it is difficult to react to CVEs, as these are either unknown or it takes too long to analyze each individual CVE. We need to understand which components are actually being used, as well as requiring a fast and automatic response to newly discovered CVEs, and we also need to integrate security awareness into the development process. A modern, tool-chain-based DevSecOps approach enables software to be checked automatically with every commit.

Why did you get involved with SBOMs?

The impetus came from discussions about their importance and the increasing call for transparency in software development. In its guidelines, the US government requires its suppliers to use SBOMs. This reinforced our decision to work with SBOMs too. Shortly after the decision from the US, we began to implement SBOMs in all our internal development projects and to require our external suppliers to use them as well.

Which specific processes do SBOMs support?

Today, SBOMs are a central trigger for our security incident response process. Interestingly, the need for a dedicated security team arose precisely because of the introduction of SBOMs, as we were initially unable to deal effectively with the reports. This shows how SBOMs contribute to raising awareness and further developing the organization's security culture.

Will SBOMs soon be the standard here too?

In my view, SBOMs are indispensable. The length of time between a vulnerability being discovered and it being exploited is now extremely short. Reactive monitoring of software for security vulnerabilities is no longer up to date. An SBOM lists all the software's "ingredients", including the runtime environment, and gives a complete overview of how secure it is. Future developments will make SBOMs even more comprehensive and service-oriented, from network devices to software packages.

What are the success factors for introducing SBOMs?

Key success factors include clear guidelines and standards, integration into existing processes, the use of automation tools, comprehensive training, data security and compliance, active supplier management, regular updates, and continuous improvement through feedback.

Is effective supply chain management possible at all without an SBOM?

In the context of security, supply chain management is critical when it comes to minimizing risk, ensuring compliance, increasing transparency, improving incident response, fostering collaboration and developing sustainable security practices. SBOMs play a central role in this, as they provide transparency and detailed information that is essential for effective software supply chain management. ●



Manuel Gysin

Software Engineering Team Leader at ISCeco

Manuel Gysin has worked in the IT industry for over 20 years, including as a system and DevOps engineer and software developer. He leads the engineering team for system and application development at ISCeco and also acts as scrum master. His expertise spans cloud-native solutions, CI/CD processes, open source technologies and security solutions.

isceco.admin.ch

Confidential notarial services in the digital age

Notarial services // Secure technological solutions are the basis for moving trust-based sectors such as notarial services into the digital world. Against the backdrop of the Swiss Federal Act on Digitalization in the Notarial Profession (DNG), significant steps have already been taken to improve accessibility, efficiency, and legal certainty.



Pascal Wild
Head of Consulting
and Member of the
Executive Board, ti&m

After studying business informatics at the University of Zurich, Pascal Wild worked in various positions in the IT and financial sector, most recently as a member of the Executive Board at Inventx, where he was responsible for the Banking division. He has been head of consulting at ti&m as of this year.
[ti8m.com](https://www.ti8m.com)

Important functions performed by notary's offices include safeguarding deeds such as declarations of intent in a correct, forgery-proof and long-term way, securely storing documents, and correctly entering them in the relevant registers. The digitalization of the notarial system is advancing worldwide, and Switzerland is making every effort not to be left behind. An overview of the current situation in Switzerland and the most important legal issues:

The technological foundations

Digitalization in the notarial sector is based on several key technologies that are integral to the transformation from analogue to digital processes:

Qualified electronic signatures (QES) are essential for the authenticity of digitally created documents and allow electronic documents to be signed with legal validity.

Artificial intelligence increases efficiency and accuracy in the automatic processing and analysis of documents.

Platform ecosystems and chatbots support digital communication and interaction, leading to better customer relationships and more efficient processes.

Implementations and developments in Switzerland

Various Swiss cantons and parties are taking different approaches to digitalization:

The canton of St.Gallen is working on introducing electronic land register transactions and has proposed an interim solution with mixed submissions of electronic data and paper documents. This solution is designed to take advantage of the benefits of digitalization while maintaining legal security.

The canton of Valais has introduced a platform that allows land register data to be transferred directly and digitally between notaries and land registries.

SIX Terravis is a platform that plays a key role in the digitalization of the land register system in Switzerland. It enables electronic access to land register data, which speeds up and simplifies the processing of property transactions. The system supports notaries, authorities, mortgage banks, and other parties involved with efficient digital services that make transactions secure and transparent.

Global perspectives and role models

Countries such as France and Austria have already fully digitalized their notarial systems and offer valuable insights into the implementation and benefits of such measures. These countries use advanced AI applications and electronic document management systems to make notarial services more efficient and secure.

Future developments and challenges

Despite the clear benefits of digitalization, there are still challenges: Full digitalization requires not only the implementation of secure technologies, but also compliance with strict data protection laws and the adaptation of existing regulatory frameworks.

Vision for the digital notary's office

"We will digitalize business transactions in the notarial sector by 2027, allowing us to work with our business partners securely and without media disruptions." This is the vision of the Swiss Association of Notaries in May 2023. The future of the notarial profession involves a comprehensive digital environment in which all processes and transactions are handled digitally. The focus here is on land register transactions, commercial register transactions, property and inheritance law transactions, and other notarial services.

The bottom line: Digitalization in the notarial profession offers many advantages such as greater efficiency, improved legal certainty, and easier accessibility. Despite existing challenges, progress in Switzerland and other countries is promising. The continuous development and adaptation of technologies and legal frameworks will be crucial in order to fully exploit the full range of benefits of digitalization in the notarial profession.

Lawyer Cornelia Stengel on the opportunities and limits of digitalization.

“Digital registers promote innovation – both in the technical solutions and in the business models they enable”

From 2027, it will be possible to create and archive documents electronically in Switzerland. Is there still a need for action from a legal perspective?

The Swiss Federal Act on Digitalization in the Notarial Profession (DNG) lays the foundations for public deeds to be drawn up in electronic form and stored in a central digital register of deeds maintained by the Confederation. This infrastructure update is an important step towards fully digitalized business transactions without media disruptions. I am pleased that the final version of the law formulates the basic requirements in a technology-neutral way and that the detailed implementation provisions are regulated at ordinance level. This allows flexibility in the development of technical solutions (perhaps even based on DLT?) and makes it easier to continuously take into account the current state of the art. However, there is still work to be done before fully digitalized business transactions are possible. For example, remote authentication remains difficult, as there is currently no reliable digital proof of identity in Switzerland. Until an electronic ID is available, notaries must find alternatives to verify the identity of the parties involved, e.g. certified ID copies or ID copies signed and delivered live using QES.

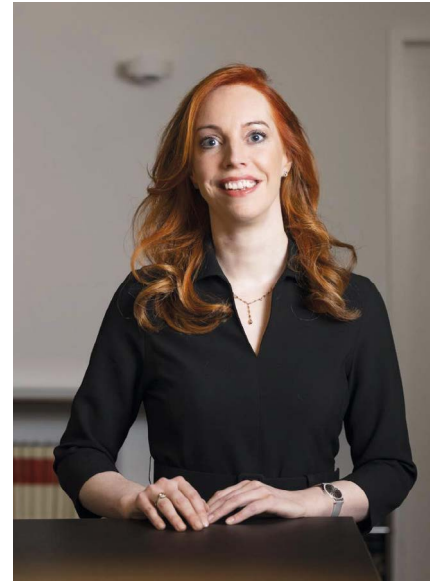
Distributed ledger technologies such as blockchains appear to be the ideal solution for taking over the work of notary's offices. Will notary's offices be one of the first areas to be fully automated and digitalized?

DLT would definitely lend itself to the secure, transparent, and cost-effective creation and storage of digital documents. However, just as we still have to write or at least create

prompts for emails despite the Internet, the use of this technology for the creation and storage of documents in no way replaces the work of notaries. In addition to the mere creation and storage of documents, they are responsible for a variety of tasks that make an important contribution to legal certainty and legal peace. For example, the content of sales contracts or marriage and inheritance contracts must still be drafted and/or checked for compliance with the law in each individual case. It is also the responsibility of the notary to ensure that the parties involved are aware of the content and obligations and the scope of the respective transaction when concluding important legal transactions such as the purchase of real estate or inheritance contracts. A digital register cannot perform these important functions.

The digital land register has been online in the canton of Zurich since last summer – and in the canton of Bern since mid-2020. Are there any other digital registers?

Based on a motion by member of the Council of States Beat Rieder, efforts are currently underway in Parliament to modernize the retention of title register. At present, the retention of title must be entered in a non-digital register at the debt enforcement office at the debtor's place of residence or registered office. In the event of a change of residence or registered office, the entry must be updated in the register of the new responsible debt enforcement office in order to remain valid. It is clear that a revision is necessary. However, as Managing Director of the Swiss Leasing Association, I am advocating a more comprehensive revision of chattel mortgage law and the creation of a



Prof. Dr. Cornelia Stengel

Lawyer for financial market and data protection law, Kellerhals Carrard

Cornelia Stengel is a partner at Kellerhals Carrard and visiting professor and head of the interdisciplinary #FinTank at the University of Applied Sciences and Arts Northwestern Switzerland. She is a member of the Executive Board of Swiss Fintech Innovations (SFTI), Managing Director of the Swiss Leasing Association (SLV) and a guest of the Expert Commission on Digitalization of the Swiss Bankers Association (SBA) and a member of the Board of Directors of the St.Galler Kantonalbank. [kellerhals-carrard.ch](https://www.kellerhals-carrard.ch)

national digital chattel register¹. Instead of land, which is entered in the land register, rights to property, e.g. ownership or liens, could be entered in the chattels register if required. This would create additional opportunities for securing ownership and make access to financing easier or more favorable for SMEs. ●

Shaping the future in the SOC:

Transforming job profiles through infrastructure as code and AI



In an age where digital threats are as dynamic as the technologies that combat them, the Security Operations Center (SOC) is the first line of defense against cyber attacks. The SOC is more than just a monitoring center; it is the strategic nerve center for security intelligence and response. With the help of security information and event management (SIEM) systems, these teams can aggregate a wide range of security data from various sources, giving them a 360-degree view of potential threats.

From a reactive to a proactive approach

Security Operations Center // Infrastructure as Code (IaC) and Artificial Intelligence (AI) are powerful weapons against cyber threats. Using these approaches changes the profile of the employees in Security Operations Centers (SOC).

These critical security functions have undergone enormous change in the last decade. While SOC/SIEM specialists once focused primarily on detecting and reporting security breaches, the emphasis has now shifted to a proactive and preventative approach. Technologies such as machine learning and Infrastructure as Code (IaC) have come to the fore and are placing new demands on job profiles. This technological revolution means that today's security experts need more than just comprehensive IT security skills; they also need to be able to understand and adapt complex algorithms, develop their own security tools and design infrastructures that automatically adapt to the ever-changing threat landscape.



Ralph Keller

Head of SOC/SIEM, ti&m

Building on his roots as a computer scientist, Ralph Keller has over 20 years' experience in the IT industry, primarily working with IT service providers and managed service providers. He took on the role of Head of SOC/SIEM at ti&m last year and is responsible for establishing these with our customers and partners. He is also privately involved in the start-up scene and contributes his expertise as a lecturer at various educational institutions.

ti8m.com

How automation is changing the nature of the SOC

Using IaC to automate security measures makes it possible to define security settings and policies as code, which speeds up the implementation of security standards and incident responses. This development changes the nature of the SOC by combining responsiveness with precision and creates a need for skilled workers who are just as confident at programming as they are at security analysis.

SOAR intermeshes security, development and operation

With the ongoing integration of SOAR (Security Orchestration, Automation and Response), incident response processes can be further optimized. Designing playbooks that define automated workflows for common threat scenarios requires a deeper understanding of the entire cyber attack lifecycle. At the same time, the DevSecOps approach requires even closer intermeshing of security, development and operation, which means that security experts are more and more involved in development processes. Looking to the future, we can expect a further increase in the use of AI in the SOC/SIEM environment. AI algorithms that can learn from data and act independently will radically change the way security alerts are analyzed and handled. They enable the rapid identification of complex attack patterns and ensure an adaptive response to the constantly changing tactics of attackers. But it's not just about defense — attackers

are also upgrading their set-ups and using AI to orchestrate sophisticated cyber attacks. This is leading to an arms race in the cyber world, meaning that security experts must constantly adapt their strategies and develop their skills to keep pace.

Further training for security teams — a critical success factor

To be successful in this highly dynamic environment, companies need to invest in further training for their security teams, especially in the areas of AI and machine learning. This will equip these experts not only to act in response to security incidents, but also to develop preventative measures that can anticipate new attack vectors. CI/CD pipelines (Continuous Integration/Continuous Deployment) and automating processes help to increase quality and efficiency, and speed up responsiveness. It is important to use open and flexible SIEM systems that offer scope for customization and extensions, as is the case with open source solutions such as Elastic.

The new generation of SOC/SIEM specialists must therefore have a wide range of skills and knowledge. From programming and system administration, to data analysis and science, to the ethical use of technology — all of these are now key components of effective security work. Armed with this knowledge, security teams can not only respond to threats, but also anticipate them and take preventative action to ensure the security and resilience of their organization in an unsafe digital world. ●

Swiss Security Software. One you can trust.



ti&m Authentication

Swiss security and authentication software: From multi-factor authentication to security consulting, we offer products with the perfect balance between the highest security standards and user-friendliness. Our many years of experience in developing and applying security solutions make us the ideal partner in all aspects of cybersecurity.



Philip Dieringer, Head of the Bern office, would be happy to advise you:
+41 31 960 15 55 oder ti8m.com/2fa

ti&m