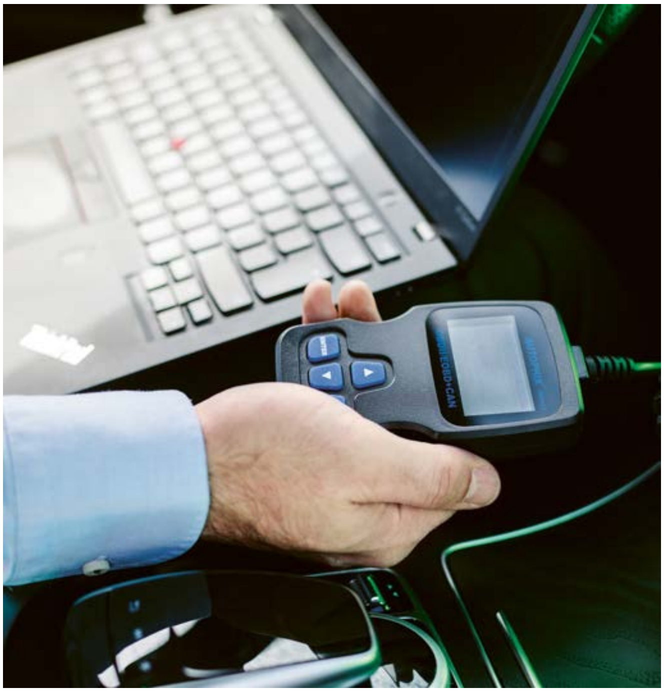
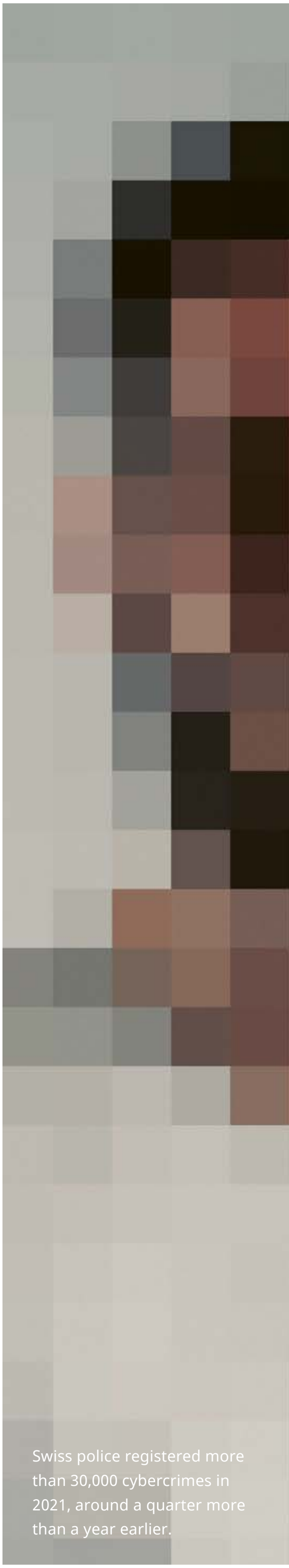
pay

The Payments Professional Magazine from SIX — #6 — 2022

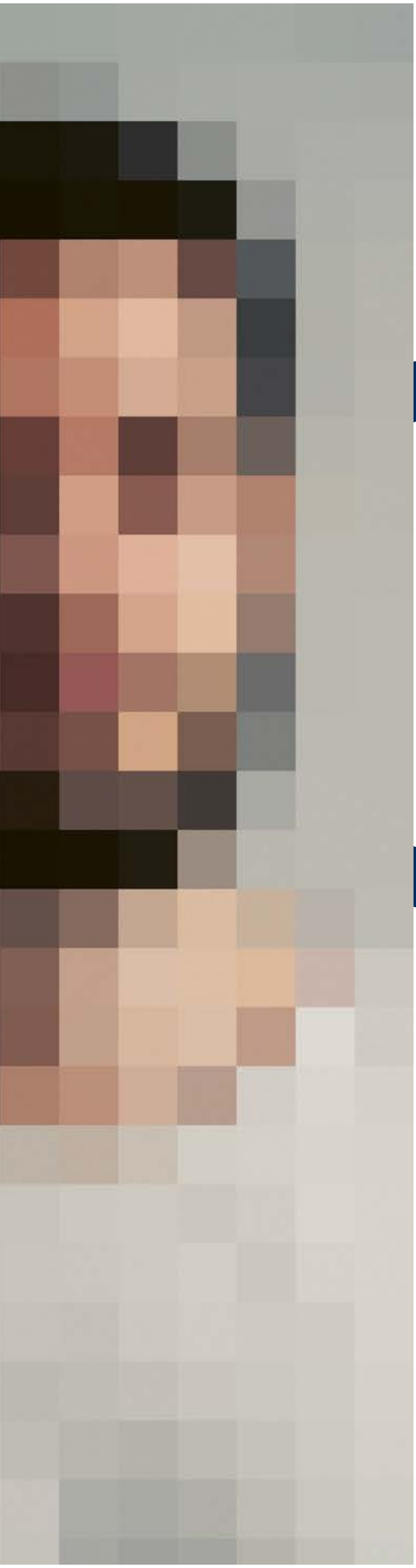
How the Financial Center Is Taking Offensive Action Against Cybercriminals — Future Talk with Hannes Lubich — Hackers and Crackers — Card Amounts at the Checkout — Multibanking Thanks to “Relay”



Publisher SIX Group Ltd, P.O. Box, 8021 Zurich, Switzerland, six-group.com/pay, pay@six-group.com Advisory Board Daniel Berger, SIX; Boris Brunner, Head, SIX; Angelika Christian, SECB; Laura Felber, SNB; Pierre-Michel Gicot, BCV; Susanne Höhener, Liechtenstein Bankers Association; Daniela Hux-Brauss, Credit Suisse (Switzerland) Ltd; Raphael Reinke, SNB; Peter Ruoss, UBS Switzerland AG; Stefan Schneider, PostFinance; Nino Thommen, SIX Editor Gabriel Juri, Editor in Chief, SIX Concept & Design *MADE* Identity AG, Zurich, Switzerland Lithography Marjeta Morinc Printer sprüngli druck ag, Villmergen, Switzerland Translations Mark Rabinowitz, Translation Service Team, SIX (English); Denis Fournier (French) Photo credits Jessica Radanavong (Cover), Vova Krasilnikov (p. 3), Arthur Hidden (p. 4), Jassir Jonis (p. 6), Ornella Cacace (p. 2, 10), Tobias Siebrecht (p. 13) Illustrationen Gregory Gilbert-Lodge (p. 2, 7, 12)



Swiss police registered more than 30,000 cybercrimes in 2021, around a quarter more than a year earlier.



Cyberdefense: Switzerland Is Arming Itself

TEXT
THOMAS KOCH
HEAD CORPORATE SECURITY, SIX

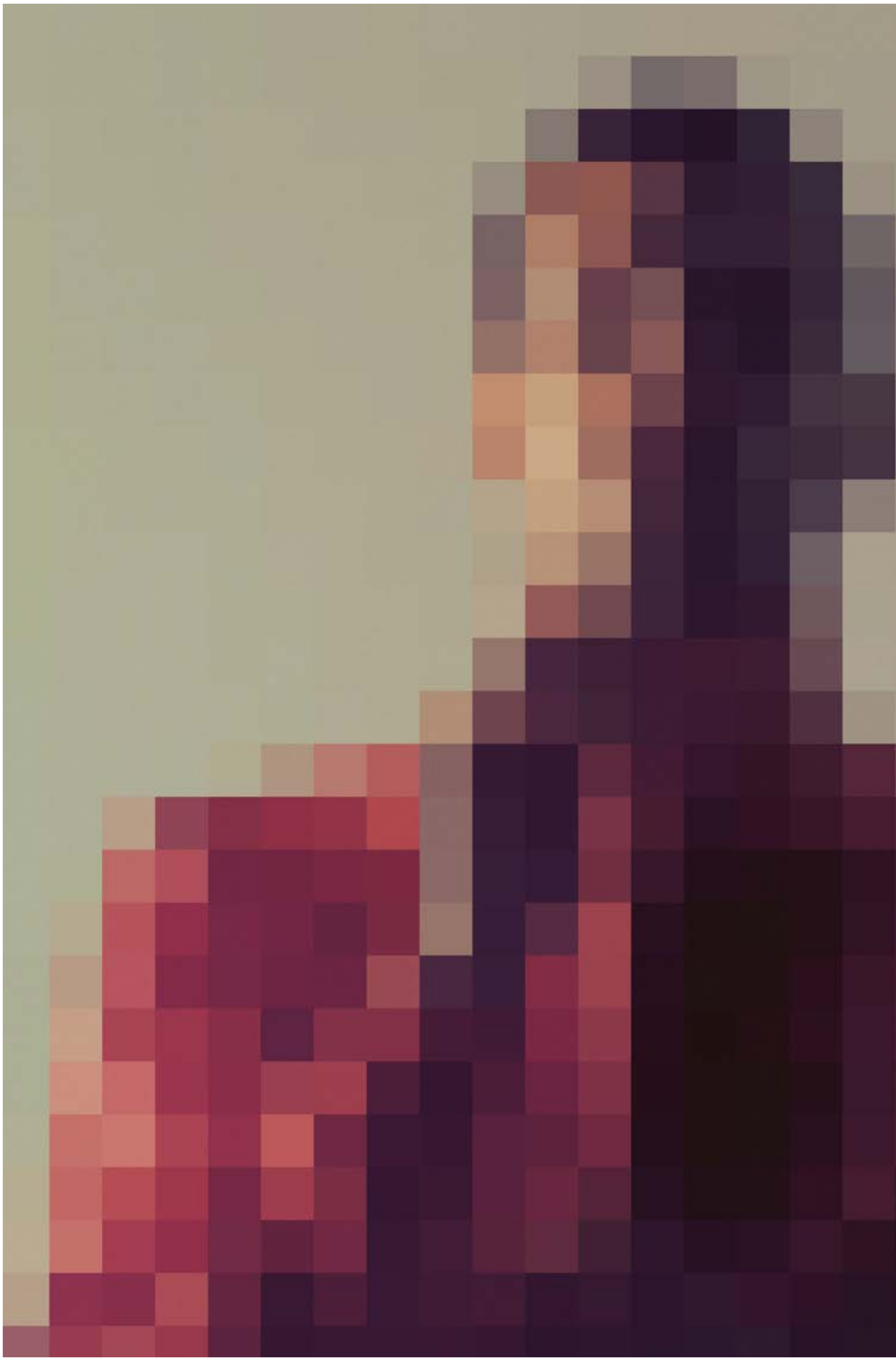
Opportunity makes the thief, in the present day and throughout all of human history. Anything that's not bolted down will get stolen. Thieves in the Middle Ages pilfered bread, poultry, jerkins, candles, and money at market fairs virtually in passing, and cash was also often stolen from churches. The crime sites today are shopping malls, for instance. Or museums, from which paintings, precious gems, or Neanderthal teeth vanish. Or computers, from which data become stolen goods. Larceny and blackmail often go hand in hand. When the loot is from museums, the crime is called "artnapping" when the perpetrators threaten to destroy the stolen art object if a ransom isn't paid. Digital loot also gets held for ransom. In both types of crimes, the criminals largely operate nonviolently. Moreover, the estimated number of unreported cases in the aforementioned crime categories is high, and the victims go to great lengths afterwards to guard and technologically protect their "treasure" better.

Ransomware attacks on businesses are certainly nothing new, but have been increasing exponentially lately. Police crime statistics, in contrast, have registered a significant decline in non-digital theft for years now. Whether this is due merely to a random correlation or causality is anyone's guess. The fact, though, is that increasing digitalization and interconnectedness have enormous impacts on information security and also amplify risks for the financial sector. At the same time, cybercriminals are becoming more and more sophisticated in their misdeeds and have considerable financial resources that are often chipped in by "sponsors." The ranks of the newest generation of cyberassailants with corresponding skills includes state- and corporate-sponsored cybergangs and organized crime outfits. Their motives can go beyond financial interests and may even have political scopes. Alongside ransomware and malware attacks, two other cyberextortion methods stand in the foreground: supply chain attacks aimed at weaker third parties that have access to critical systems, and distributed denial of service (DDoS) attacks aimed at disrupting a service or blocking a certain target group from accessing it.

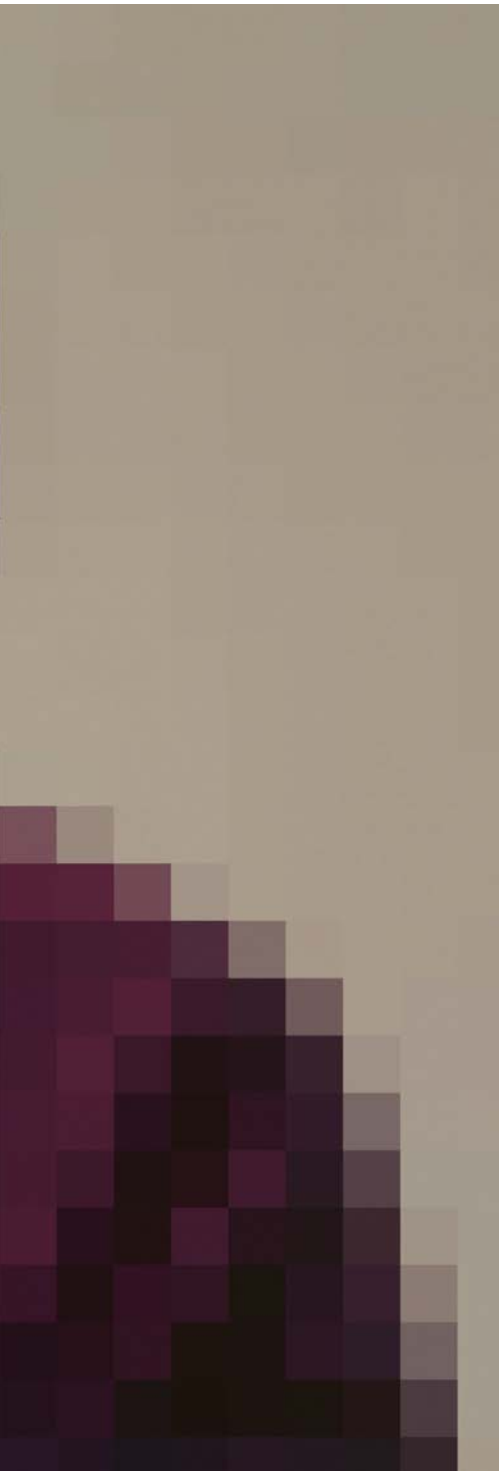
Several financial-sector operators outside Switzerland recently faced attacks of these kinds. New Zealand's stock exchange, for example, saw trading disrupted for

«The more critical the security flaw, the bigger the reward for the ethical hacker.»

Enhancing Security in the SIC System: Endpoint Security and the SSFN The effects of fraudulent payments in large-value payment systems like the SIC system can have far-reaching consequences not just for directly affected participants, but also for the entire payment system. The submission of fraudulent payments as a result of compromised endpoints at SIC participants – i.e., as a result of a breach of devices, applications, or systems that an SIC participant needs to exchange messages with the SIC system – is particularly problematic. The Swiss National Bank will soon establish a binding framework for SIC participants to enhance the protection of their endpoints. The framework will include operational and technical standards to protect endpoints, which are to be implemented by SIC participants or their commissioned service providers by the end of 2024. In addition, at the system level, universal use of the internet-independent Secure Swiss Finance Network (SSFN) to communicate with the SIC system will make a vital contribution to ensuring resilience and failsafety in the SIC system. SIC participants have been able to utilize the SSFN – alongside IPNet and SWIFTNet – as an additional accessway to the SIC system since the start of June this year.



The economic cybercrime (phishing, hacking, malware, DDoS) accounted for nearly 88% of all digital crimes in Switzerland.



two days by DDoS attacks. And a ransomware attack on American Bank Systems led not just to a USD 14 million ransom demand, but also to a data privacy class action lawsuit.

New Organization for the Cyber Resilience of the Swiss Financial Sector

Switzerland appears to be less severely exposed to cybercrime than its neighboring countries are. According to one study conducted by a British maker of security software, last year 0.7% of businesses in Switzerland were hit by ransomware per week. The ransomware attack rates for the countries surrounding Switzerland came in at 1.4% for Austria, 1.6% for Germany, 1.8% for France, and 1.9% for Italy.

In Switzerland, the National Cyber Security Center (NCSC) is the first contact point for businesses, public administration, educational institutions, and the general public seeking help or information on cyber issues. Operators of critical infrastructures especially receive support pertaining to protection against cyber risks as well. In addition, an association called the Swiss Financial Sector Cybersecurity Center (Swiss FS-CSC) was founded under its leadership in April 2022. It aims in particular to facilitate the exchange of information between financial market players and to improve cooperation with regard to sector-wide preventive measures and the management of systemic crises.

Such crises are systemically relevant when they affect payment and securities settlement systems. SIX, as the operator of these financial market infrastructures in Switzerland, naturally has an extraordinary interest in such cooperation and is actively engaged as a founding member. The Swiss FS-CSC's membership roster currently includes over 100 Swiss banks, insurance companies, and financial organizations operating under the watchful eye of the Swiss Financial Market Supervisory Authority (FINMA). FINMA is also on board as an affiliate. The association's organizational pillars consist of a steering board, an expert group, and an operational cybersecurity cell (OCS). In the event of a systemic cyber incident, the steering board coordinates the actions necessary to overcome the crisis and takes charge of communication within and outside the association.

The association's internal expert group runs projects aimed at strengthening cyber resilience and organizes strategic and operational cyber exercises for Swiss FS-CSC members.

Finally, the OCS monitors the situation in the financial market, shares information on relevant proceedings, writes sector-specific reports, and helps association members resolve crises. The intention is that there will be cooperation on this task with one of the service providers with international experience in this area.

Offensive Cybersecurity

SIX, as the backbone of systemically vital financial market infrastructures, plays a prominent role in safeguarding the stability and security of the Swiss financial center. SIX maintains a structured, constantly updated risk registry that includes information security risks. The range of reactions to threats in recent years have included technical measures to support basic security, a buildup of capabilities and simulations, and organizational measures. The updated information security strategy also includes new initiatives such as improved vulnerability management response times, expanded protection against ransomware attacks, and the continual improvement and expansion of the SIX Security Operations Center (SOC).

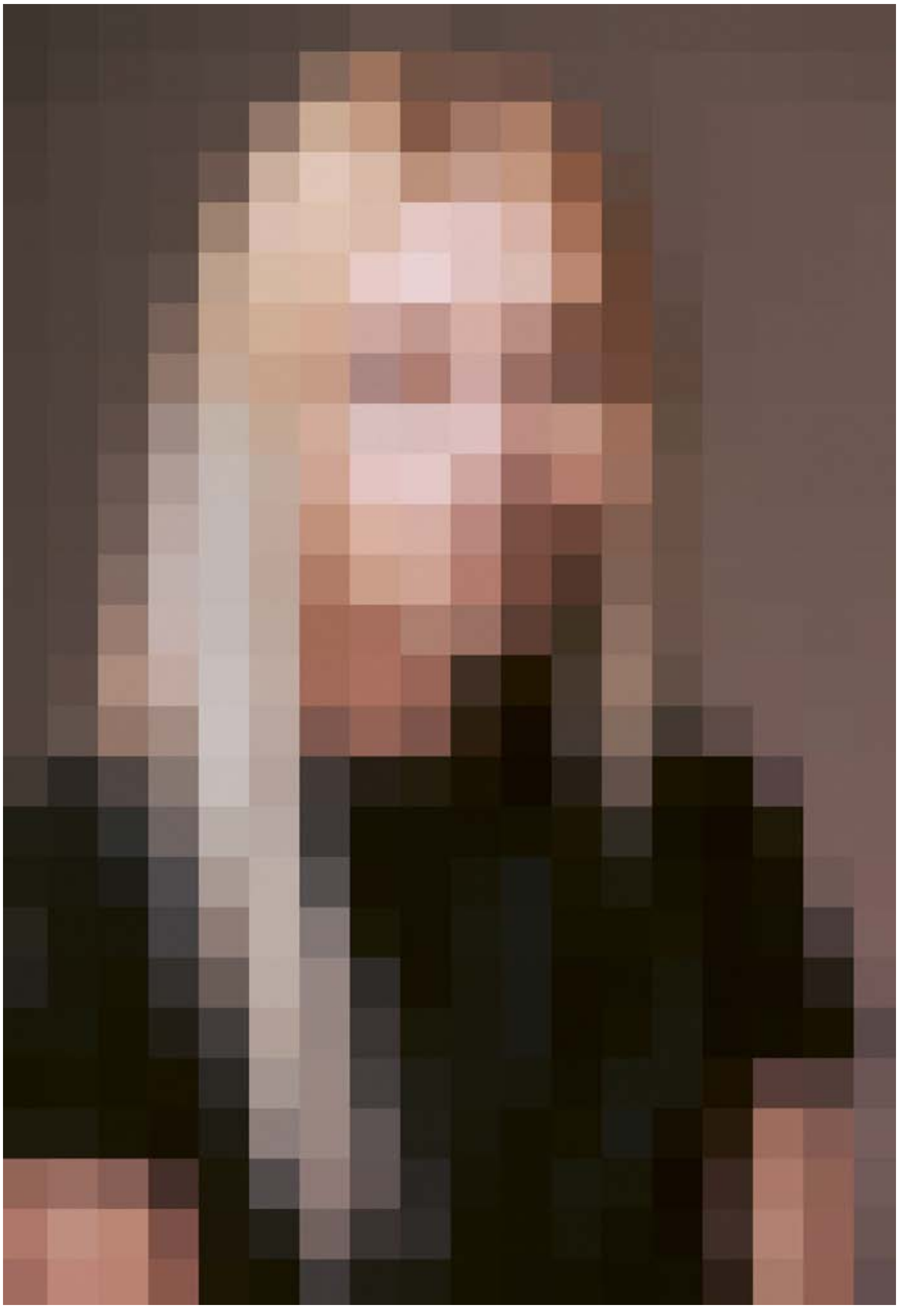
One team is now also using an approach called offensive cybersecurity. It appropriates scenarios, attack techniques, and methods employed by real-world hackers and mimics them in a controlled environment. The team's arsenal includes penetration testing, adversary emulation, and a vulnerability disclosure program. The aim of penetration testing is to systematically infiltrate applications and systems to sniff out security vulnerabilities and report them to application developers and system operators. Adversary emulations serve to test the fail-safety of a network against sophisticated attackers or threats with or without advance warning and to integrate the knowledge gained from that into defensive cybersecurity training.

The vulnerability disclosure program (called also a bug bounty program) is the latest trend in offensive cybersecurity. It allows systems to be deliberately attacked by a select group of ethical hackers, who get financially rewarded for their work. All of them can proactively report an incident or a suspected information security vulnerability online to SIX from anywhere around the world.

In early April 2022, SIX developed a bug bounty program initially focused on systems connected to the internet. At a later point, SIX also plans to allow internal systems and cloud services to be hacked ethically. The bug bounty program offers many advantages. For one thing, there are thousands of hackers around the world with a vast array of creative ideas that a single team alone would never be able to muster. Moreover, every technology has its own specialists that SIX can pick out specifically. Furthermore, bug bounty programs run for a long time, sometimes even for years, whereas classic penetration tests usually run for just a few weeks. Compensation for the bounty hunters is based not on their invested time, but on the vulnerabilities discovered. The more critical the security flaw, the bigger the reward for the ethical hacker.

Be it under the framework of the Swiss FS-CSC or in dialogue with ethical hackers, cooperation will help to stem the risk of cyberattacks on the financial industry. Financial center players are expected to secure their applications and systems like a fortress as much and as quickly as possible so that cybercriminals have less of an opportunity to steal their property or the property of third parties.

The Swiss economic cybercrime statistics recorded the largest percentage increase in the two components of phishing (by 88%), and of ransomware (by 53%) in 2021 compared to 2020.



«Cybersecurity governance cannot be delegated.»

HANNES LUBICH,
EMERITUS UNIVERSITY PROFESSOR AND STRATEGY CONSULTANT FOR IT SYSTEMS, NETWORKS AND IT SECURITY

TEXT
GABRIEL JURI

The cybersecurity threat in Switzerland does not seem to be as great as in other countries. Why is that? We have been an attractive target for a long time and, especially in regulated sectors, have waged a long defensive battle and learned our lessons. In addition, local companies can afford elaborate security measures better than those in economically weak regions.

According to experts, criminals are always one step ahead. Is cyber protection really almost impossible or are companies simply not up to date? Today, criminals can spend considerable resources on ever new forms of attack and the necessary know-how and infrastructure – in some countries with the approval or cooperation of state authorities. Effective defense against targeted attacks with a substantial use of resources is therefore indeed difficult. However, criminals in particular must keep their costs under control. If an attack becomes too expensive, they switch to the next target. It is important for companies to design their cyber protection as well as feasible, possibly using external expertise.

Who benefits more from artificial intelligence (AI)? Chief Information Security Officers or cybercriminals? At the moment, "targeted" AI is more likely to be used in the professional criminal field – but security systems are also increasingly relying on it. However, these systems are often "closed" and are only used indirectly as an integral part of a service (e.g., threat detection and analysis). In addition, not every rule-based system is an "artificial intelligence" – a lot of marketing is involved here.

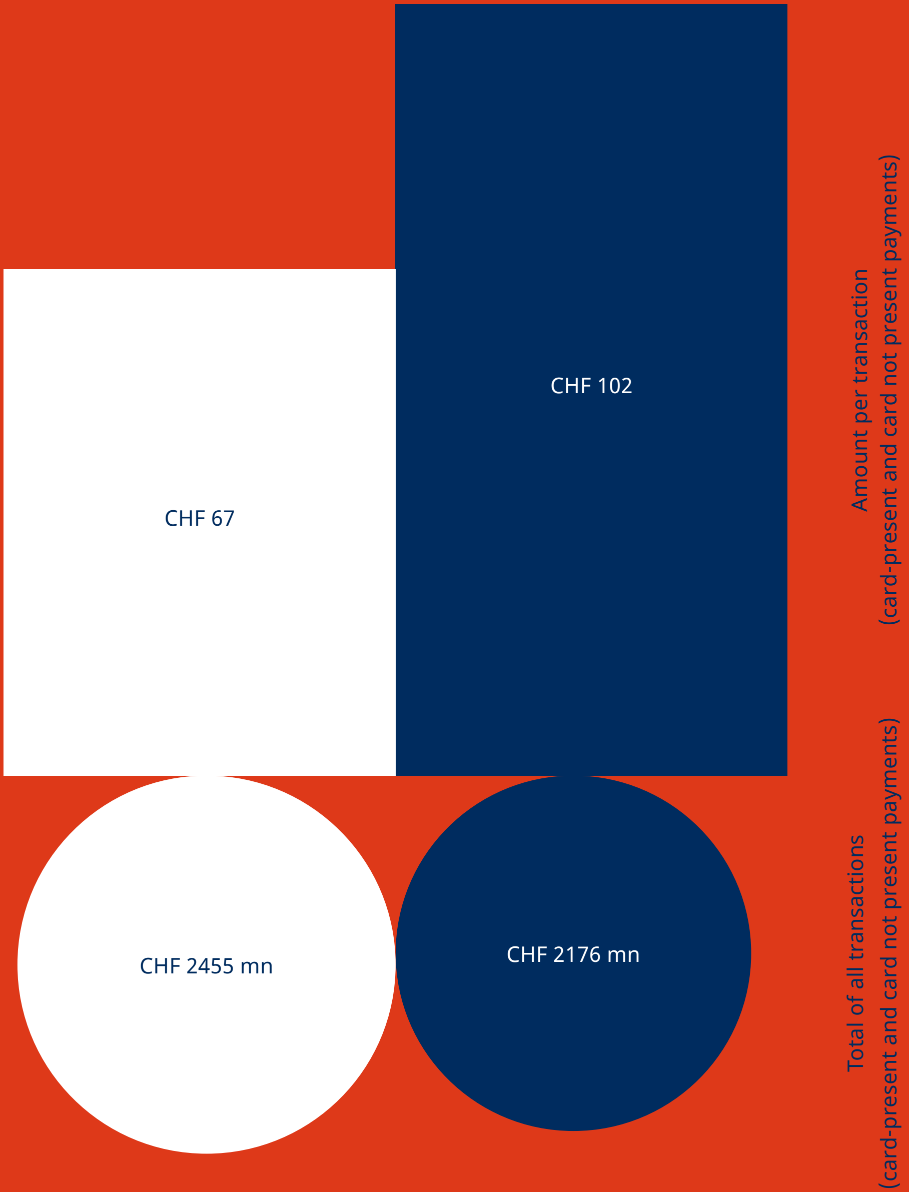
Who is least prepared for ransomware attacks at the customer-bank interface? Above all, asset managers or trustees without a banking license, who are therefore neither heavily regulated nor monitored. But even market participants who only offer electronic financial services do not always have the necessary practical experience. They often believe that they can outsource cybersecurity along with the rest of IT to external service providers. However, the related "governance" cannot be delegated.

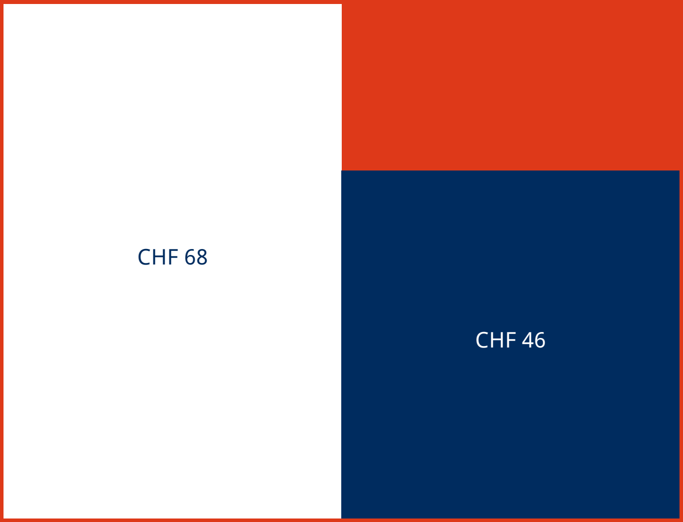
To what extent are legal foundations for cybersecurity effective? Legal requirements create the necessary pressure to act in order to establish cybersecurity even where persuasion fails. The financial sector is already very well covered here. Companies in the manufacturing industry are often not sufficiently sensitized. They run the risk of losing intellectual property, sales or their reputation with partners and customers. Laws can have a very positive effect here, as long as they do not overregulate and do not bring new risks and inequalities of opportunity in the market.

The average amounts of domestic and foreign cards in and outside Switzerland differ noticeably – exemplified by the month of June 2022.

The average amount of transactions with Swiss credit cards is higher abroad than domestically. One reason may be that larger purchases occur abroad (e.g., weekly shopping or overnight stays in hotels), while everyday small purchases prevail at home.

- ○ Domestic credit cards in Switzerland
- ● Domestic credit cards abroad





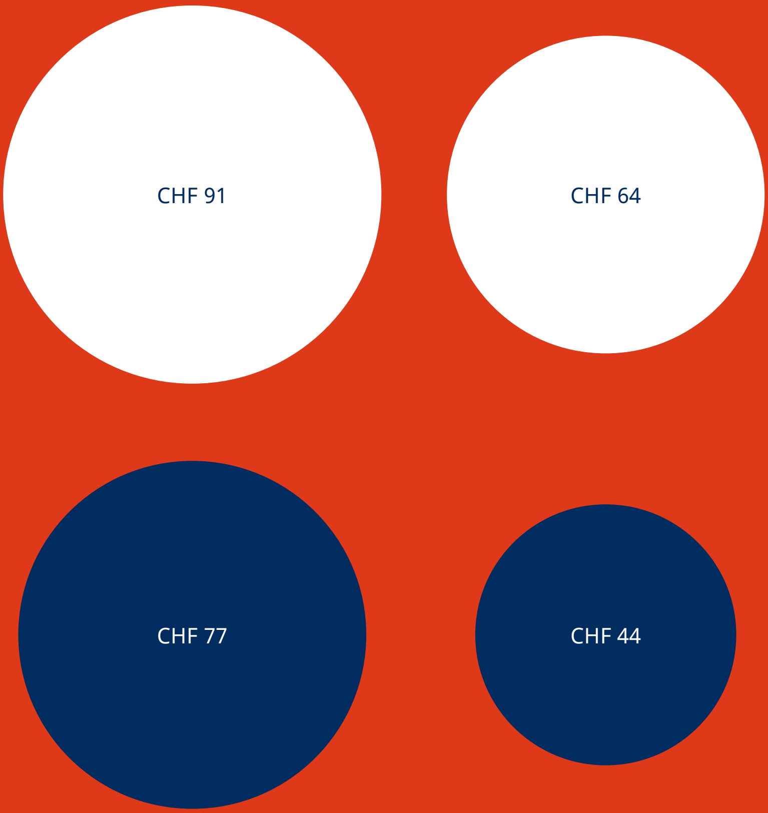
Debit card amounts per transaction

People with foreign debit cards (such as tourists or cross-border commuters) spend less money per payment in this country than Mr and Mrs Swiss abroad.

○ Domestic debit cards abroad

● Foreign debit cards in Switzerland

Source Swiss National Bank data portal, Payments and cash withdrawals.
The data are taken from a partial survey. More information: Financial Market (data.snb.ch)



Amounts per credit card transaction (card-present payments only)

Amounts per debit card transaction (card-present payments only)

Even focussing just on card-present payments*, it turns out that the average amounts spent with foreign cards in Switzerland differ considerably from those with domestic cards abroad – this applies to both debit and credit cards.

* Card-present payments refer to payments made at the point of sale.

○ Domestic cards abroad

● Foreign cards in Switzerland

Combating Hacking of Cars and Medical Devices with Ethics

TEXT
SIMON BRUNNER

On-site visit in Zurich-Altstetten. The address leads to a gray office building. An anonymous door on the third floor opens. A bare corridor leads to an austerely furnished meeting room. We're on a visit to a cybersecurity firm. Or, to put it more precisely, we're dropping in on a former hacker who helps businesses find vulnerabilities in their own security setups. His name is Marc Ruef.

But first, let's get the clichés out of the way. A hacker runs around in a grungy hoodie? Ruef sports a full beard and wears a suit and a tailored shirt. Hackers are criminals? "Never in my life have I been interested in stealing something or harming anyone," the 41-year-old says. Hackers operate in a legal gray zone? Ruef teaches at the Swiss Federal Institute of Technology and several universities of applied sciences.

The native of Aargau came into contact with computers at an early age. When he was 12, he was given permission to practice programming on his father's PC, but only for a few hours a week. He quickly figured out how to unlock the computer himself. Since he feared that his activities wouldn't go undetected, he consulted a library and learned how to manipulate the time stamp. At the same time, he came across literature on computer viruses. From then on there was no holding him back.

Hackers and Crackers

It was the 1990s. The moniker "hacker" in those days was still an honorable appellation. The bad guys – the criminals – were called "crackers." Today the term "hacker" carries a positive connotation only if it is combined with ethics. Specialists like Ruef who make computer systems more secure are thus known as "ethical hackers."

But back to Ruef in his teenage years. To him it was all about tackling the toughest intellectual challenge. The tinkerer wanted to demonstrate that no IT system is truly secure. The hacker scene was still young in those days, and Ruef quickly became a full-fledged member of the family. When he became one of the first to share his knowledge with the public, Ruef was ostracized from the scene, which doesn't want security vulnerabilities to get publicized and fixed. Ruef launched a pathbreaking security portal on the internet at the age of 16, he penned first

Company cars are particularly vulnerable to hacker attacks. Marc Ruef in action.

book when he was 18, and at the age of 22 he authored his "magnum opus," as he calls it: The Art of Penetration Testing. It's a hefty 900-plus-page tome that describes how to systematically scan one's own network for vulnerabilities and security holes. The book sold out in a flash.

After a basic business education, Ruef turned his hobby into a profession, working initially for an IT security firm. Then in 2002, he and two partners founded scip AG. His enterprise, which now has 50 employees, advises midsize and larger companies on how to better protect themselves against cyberattacks.

Cars as Drivable Datacenters

Since founding his company, Ruef himself has specialized in out-of-the-ordinary cybersecurity use cases such as car hacking, where an attacker infiltrates a vehicle's electronics and hijacks key functions such as starting or stopping the engine or unlocking the doors. "Modern cars are drivable datacenters," Ruef says. "Loads of electronics are installed in them." But it's engineers – not cyberspecialists – who design cars, he adds. "So, there are big security holes as a result," Ruef explains.

Another pet issue for scip is medical devices. Ruef and his team have proven that automated drug delivery appliances and vital-sign monitors in hospitals can be manipulated via the IT network. A malicious attacker could overdose a patient without the devices signaling an anomaly or sounding an alarm. "The hospital that uses this equipment was very concerned," Ruef says, "but – as so often happens – the manufacturer didn't want to patch the security hole on the grounds of it being too expensive." The vulnerability didn't get fixed until the US Food and Drug Administration got involved.

Other modern forms of cybercrime that scip is addressing include deepfakes – i.e., authentic-looking or -sounding fake photos, audio clips or videos –, cheating in the billion-dollar e-sports business, and sextortion, a technique that uses compromising content to blackmail victims.

Ruef is also dealing extensively with the interface between society and technology, addressing issues concerning data protection, societal vulnerability, and human interaction with artificial intelligence systems. In addition, Ruef helped develop a system that predicts cyberattacks worldwide and forecasts which cybercrime gang will be particularly active in the near future.

Hacking as a University Subject?

"The demand for cybersecurity has exploded over the last ten years," Ruef says. This pleases him on one hand because his enterprise is profiting from the boom, but he is also disillusioned: "Many companies are too reckless. They build complex IT systems but lack the resources to comprehend and manage them." Ruef often gets ridiculed for his mantra exhorting businesses to "build your computer systems as simply as possible," but he nonetheless preaches it tenaciously.

Ruef was a self-taught hacking pioneer. What does the scene look like nowadays? Most of the job applicants at his firm hold a university degree in informatics, for example, with a major in security or cybersecurity, Ruef says. They are often well-educated, he attests, "but creativity falls a little by the wayside. Hacking is not something you can learn at university."

In the end we talk about artificial intelligence. Does Ruef fear that computers will rule us one day? He laughs and points to a poster hanging on the wall. It displays the results of an IQ test that Ruef and his team developed for digital assistants: Siri scored the highest, followed by Alexa, Cortana, and Google. "I also took the test," Ruef says, "and was happy to beat the devices by a mile."

CBDCs Are Taking Off

According to the consulting firm PwC, by mid-2021, almost 70% of central banks had developed concepts or prototypes for central bank digital currencies (CBDCs). The Bahamas were the first to introduce their Sand Dollar. A year later, the "PwC Global CBDC Index" mentions 80% of central banks. And three others have launched their CBDCs as legal tender: Nigeria, Jamaica and the seven member countries of the Organisation of Eastern Caribbean States. If you would like to find out more about the rapid global development of this topic, you can consult the interactive tracker from the US think tank Atlantic Council.

Further details
www.pwc.com
www.atlanticcouncil.org/cbdctracker

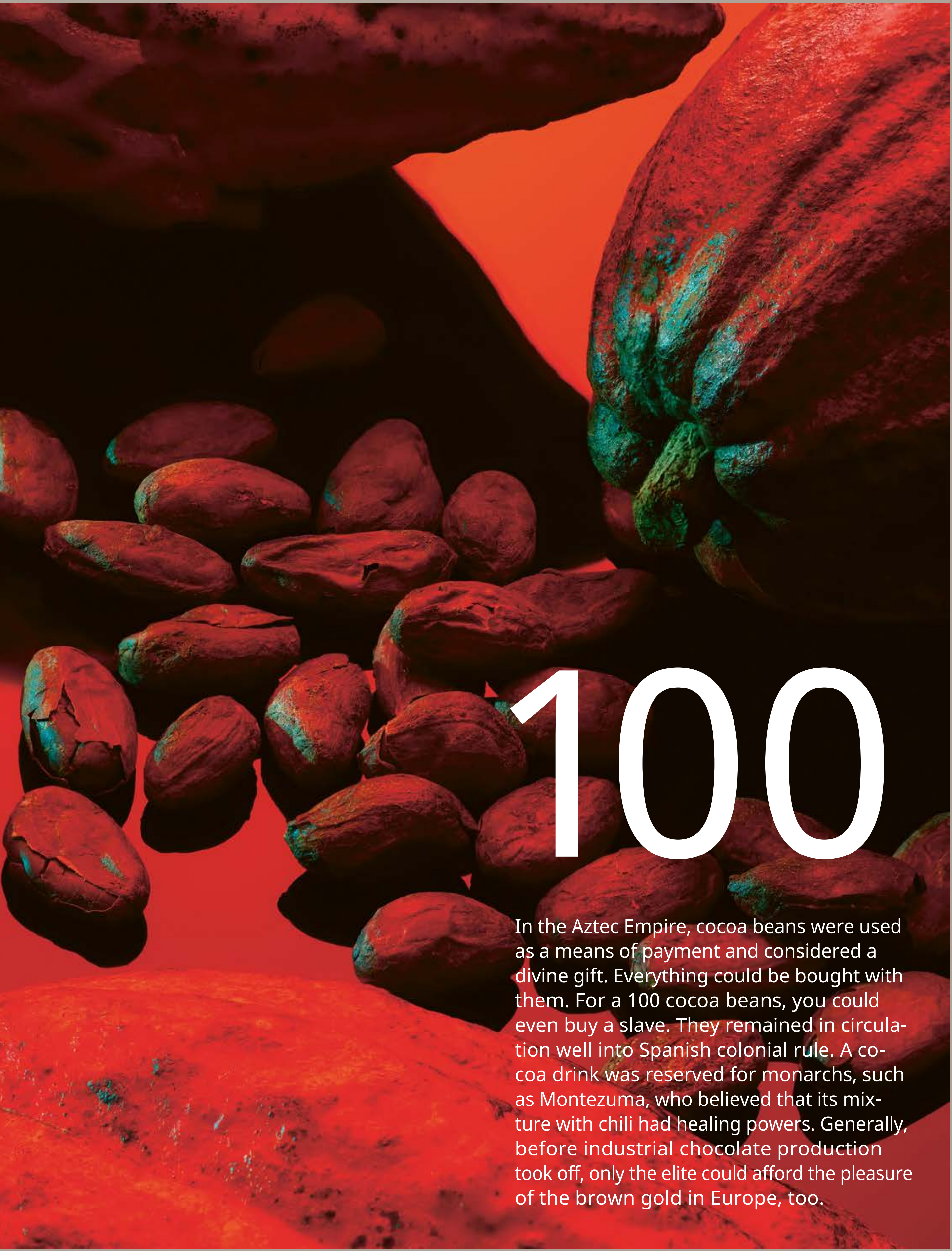
A World Without Cash?

Is it conceivable that in Germany, too, the number of cash transactions could one day be below 15% or even lower – as in Scandinavia, Iceland and the United Kingdom? These and other exciting questions related to developments in payment transactions are the subject of the new expert report "World without cash – changes in conventional banking and payment systems," which has been submitted to the German Bundestag.

Further details

Since 26 August, the Swiss Finance Museum has been presenting the special exhibition "Banks in transition: from counters to apps." It offers a look back at the history of payment slips.

Further details
finanzmuseum.ch



100

In the Aztec Empire, cocoa beans were used as a means of payment and considered a divine gift. Everything could be bought with them. For a 100 cocoa beans, you could even buy a slave. They remained in circulation well into Spanish colonial rule. A cocoa drink was reserved for monarchs, such as Montezuma, who believed that its mixture with chili had healing powers. Generally, before industrial chocolate production took off, only the elite could afford the pleasure of the brown gold in Europe, too.

Things Are Getting Serious with Structured Addresses

Required knowledge

— Knowledge of the ISO 20022 standard
— Prior knowledge of address data storage

It has been clear for some time that SWIFT will enable structured addresses in accordance with the ISO 20022 standard for cross-border payment transactions in November this year and will make them mandatory in November 2025. The fact that the Swiss financial center is adapting to the international framework and will also introduce the obligation to use structured addresses as of November 2025 has also been known for a long time. Now things are getting more specific for the first time. While it has been possible to use the structured address in Switzerland since the switch to ISO 20022, this is now also possible for cross-border payments with the migration in the SWIFT network from the previous MT messages to the new MX messages. In two cases, the use of the structured addresses is even mandatory, namely when using the elements “Ultimate Debtor” and “Ultimate Creditor.”

However, this is only possible if the sending bank has switched to MX. Banks worldwide have until 2025 to do this, so in this migration phase it is essential for customers to check with their principal bank whether the ultimate debtor or ultimate creditor or the other new capabilities of MX messages can already be used. Under certain circumstances, this may also differ according to currencies or payment methods. In order to ensure end-to-end transfer of data, not only the sending bank must have switched to MX, but also the recipient bank and, if necessary, the intermediary institutions. SWIFT is planning to provide some assistance in this regard in its network over time. The internationally phased conversion over the next three years with several thousand SWIFT participants is therefore complex. Due to this progressive conversion, the Payment Market Practice Group (PMPG) recommends using the new elements, such as the ultimate debtor or ultimate creditor, only from November 2023. In contrast, the Swiss interbank community, with around 320 participating institutions, finds it easier to introduce the new message version or any new rules. SIC and euroSIC will support the new elements from November 2022, both for domestic payments and for the transmission of cross-border payment orders. In Switzerland, moreover, it does not make a difference whether the new message versions based on Swiss Payment Standards (SPS) 2022 or those from SPS 2021 are being used in the customer-bank interface. This is because the current messages according to SPS 2021 already allow the use of structured addresses. Even though they allow fewer address elements, most use cases are sufficiently covered, as the new message versions do not have different, but just additional elements that mainly affect other addressing systems. Conversely, this means that even with today’s SPS version, an ultimate debtor or ultimate creditor can be provided with structured addresses if these orders are to be forwarded as cross-border payments via the SWIFT network with MX messages. From 2025, when the general use of structured addresses becomes mandatory worldwide, everything should be much simpler and clearer.

MARTIN WALDER,
HEAD BILLING & PAYMENTS STANDARDS, SIX

SEPA adopts structured address
With the new SEPA 2023 rulebook, structured addresses will also be introduced as an option in the SEPA zone. This enables uniform processing, regardless of whether a payment is routed via SIC, euroSIC, a SEPA provider or SWIFT. And as for the change after next in 2025, the mandatory use of structured addresses is also planned. The exact rules will be published as part of SPS 2023 in February 2023.

Structured data

```
<Dbtr>
   <Nm>JOHN SMITH[1]</Nm>
   <PstlAdr>
     <StrtNm>HOOGSTRAAT[2]</StrtNm>
     <BldgNb>6[3]</BldgNb>
     <BldgNm>PREMIUM TOWER[4]</BldNm>
     <PstlCd>1000[6]</PstlCd>
     <TwnNm>BRUSSELS[7]</TwnNm>
     <Ctry>BE[8]</Ctry>
   </PstlAdr>
   <ID>
     <OrgId>
          <LEI>HB7FFAZI00MZ8PP80E26[5]
          </LEI>
     <OrgID>
   </ID>
</Dbtr>
```

[1] Name
[2] Street Name
[3] Building Number
[4] Building Name
[5] LEI (Legal Entity Identifier)
[6] Postal Code
[7] Town Name
[8] ISO Country Code

Graph 1: Example of a structured address in pacs.008

ISO 20022 Multibanking Thanks to SWIFT's "Relay" Scenario

Required knowledge
— In-depth knowledge of pain message types

Although customer-bank messages are generally excluded from the ISO 20022 migration in SWIFT, there is one exception: in what is called the "relay" scenario. This occurs when a financial institution offers its corporate customers account concentration, also known as multibanking. With just one technical bank connection, the corporate customer can instruct other banks worldwide and receive account statements. Without multibanking, a company with, for example, five banking relationships must also main tain five technical connections to the banks. With multibanking (Figure 2), only a single connection is required – which saves the customer time and money.

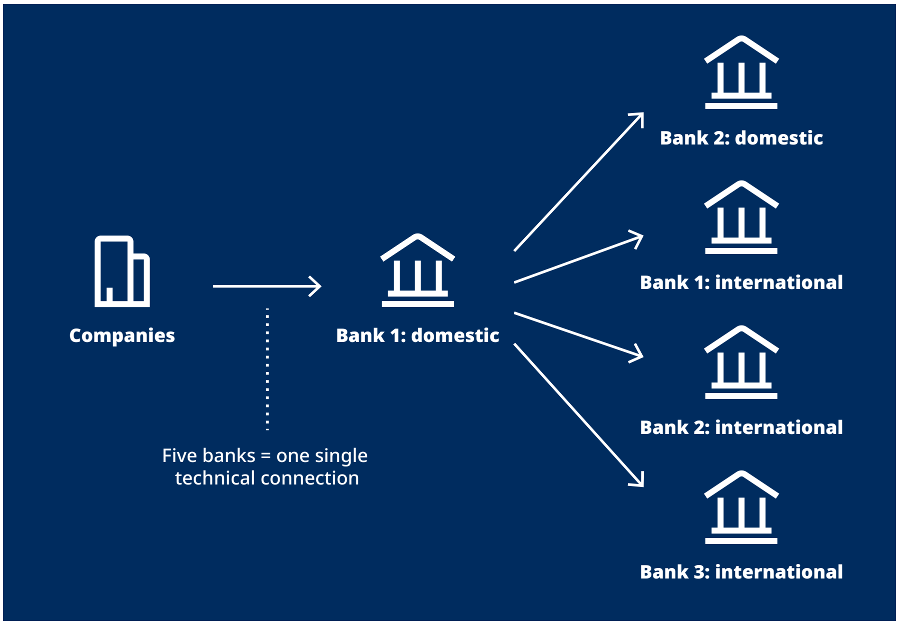


Figure 2: Message flow over the SWIFT network for the relay scenario

Time Saving and Efficiency Gain

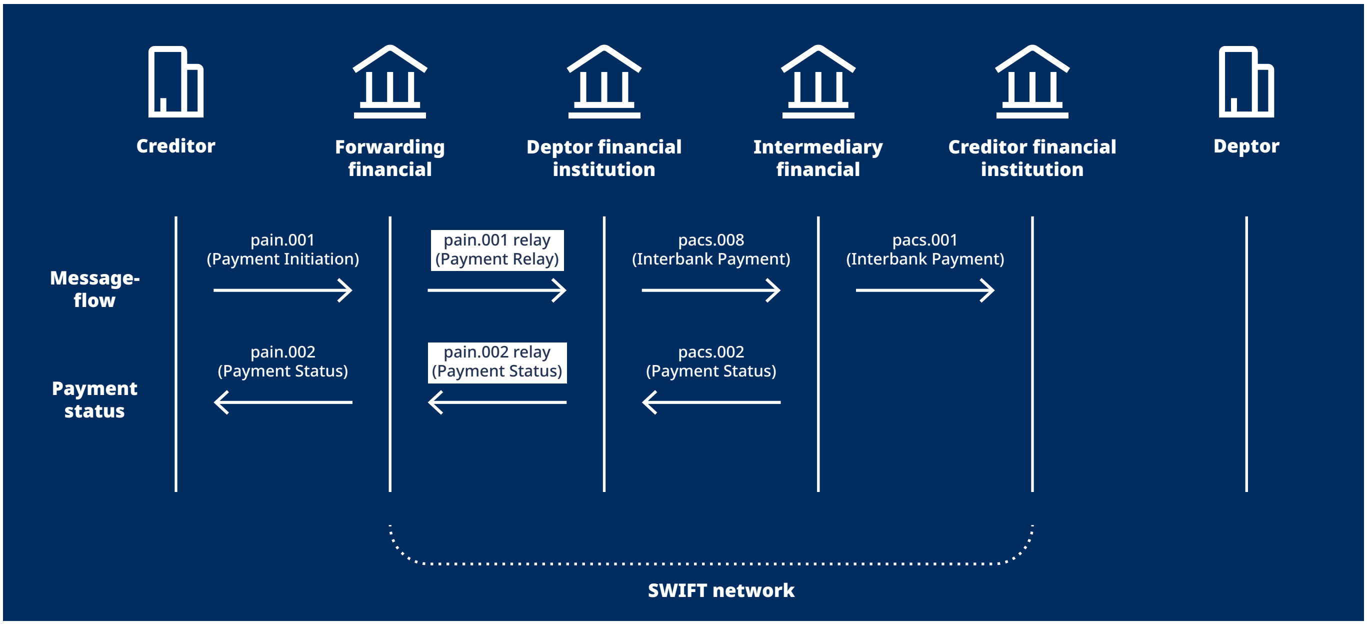
Multibanking is suitable for all companies with multiple account numbers. In Switzerland, for example, 70% of SMEs have more than one banking relationship. With multibanking, accounts from third-party banks can be managed domestically and, thanks to the SWIFT "relay" scenario, also worldwide via a single bank connection. On the one hand, payments can be made from a third-party bank account abroad to local suppliers via a single bank connection. On the other hand, thanks to electronic account statements, the customer receives full transparency about all accounts, including those with third-party banks. This significantly increases the time saved and the gain in efficiency.

The Promoters

The Cross-Border Payments and Reporting Plus (CBPR+) working group has been defining the usage guidelines for the relay scenario in close cooperation with the Common Global Implementation (CGI) working group. They cover the interbank scenarios "Payment Initiation" (pain.001) and "Payment Status Report" (pain.002).

CGI, which represents both the financial (banking) and corporate worlds, is supported by SWIFT to promote the adoption of the ISO 20022 standards for financial

Figure 3: Bank orders with multibanking account service


Creditor
Forwarding financial
Deptor financial institution
Intermediary financial
Creditor financial institution
Deptor
Message-flow
Payment status
pain.001 (Payment Initiation)
pain.001 relay (Payment Relay)
pacs.008 (Interbank Payment)
pacs.001 (Interbank Payment)
pain.002 (Payment Status)
pain.002 relay (Payment Status)
pacs.002 (Payment Status)
SWIFT network

messages and to facilitate the transition to these ISO 20022 messages.

The Two ISO 20022 Messages in the Relay Scenario

Payment Initiation

In this relay scenario, the initiating party sends the "Customer Credit Transfer Initiation" (pain.001) interbank message to the forwarding financial institution or the debtor's financial institution to request the movement of funds from the debtor's account to a creditor. The forwarding institution acts as the concentrating financial institution that forwards the pain.001 message to the debtor's financial institution (see message flow in Figure 3).

Payment Status Report

In this relay scenario, the entrusted financial institution sends the "Customer Payment Status Report" (pain.002) interbank message to the previous party in the payment chain to inform it of the positive or negative status of an instruction. The pain.002 message is also used to notify the payment recipient of an outstanding transfer order (see Payment status in Figure 3).

The SWIFT Roadmap

In November 2022, financial institutions will start migrating to ISO 20022 (MX) for cross-border payments and reporting, with a parallel phase of MT messages until November 2025. This roadmap is also groundbreaking for the relay scenario. Banks that support multibanking must therefore switch to the ISO 20022 relay scenario by 2025 at the latest.

PETER RUOSS,
PRODUCT OWNER PAYMENT SOFTWARE
PARTNERSHIPS, UBS SWITZERLAND AG

Through the Thicket of Digital Certificates

Required knowledge

— Basic knowledge of cryptographic procedures

Digital certificates are indispensable. Their TLS, HTTPS, CA, ECC and RSA forms not only sound "cryptic" – they are, according to the original meaning of the word, "hidden." Hidden and ubiquitous behind the internet connections they secure by encrypting the data. This means that unauthorized third parties cannot read or manipulate the data traffic between the browser, the visited website and the website server.

A digital certificate – also known as a public key certificate or identity certificate – is nothing more than a cryptographic key. Issued by a trusted certification authority, the certificate attests to the authenticity of a person's online credentials and identity. It's like a security badge that assures both the person entering the data and the data recipient that the data is being transmitted to a trusted source.

Transport Layer Security (TLS)

TLS is the successor to the now-obsolete Secure Sockets Layer (SSL) protocol. In practice, it serves as the standard method for securing machine-to-machine communication, in the form of digital certificates.

TLS certificates are most commonly used on websites. Only they can ensure that a website is encrypted as HTTPS (marked by a lock icon in the address bar) and data can be transmitted securely between websites, browsers and web servers without being intercepted or altered. This makes it possible to authenticate the identity of a website operator.

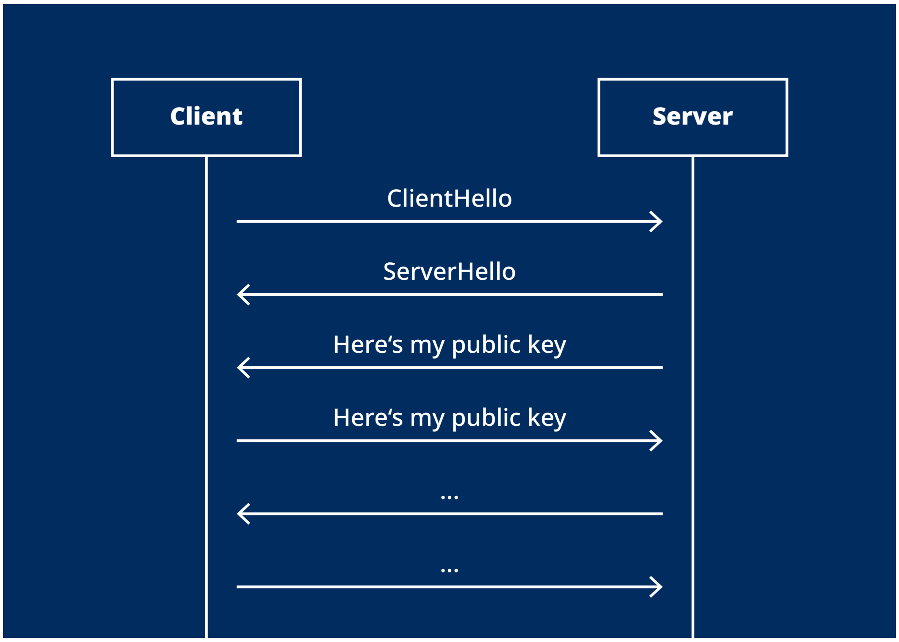
How the TLS Certificate Works

The TLS certificate establishes an encrypted connection between a website or a server and a browser without the person visiting the website noticing anything.

First the authentication takes place. With each new session the person starts, their browser and the website operator's server exchange and mutually validate their TLS certificates. Then the key exchange takes place.

The server shares its public key with the browser, which the browser then uses to create a passepartout key (pre-master key). Finally, the server decrypts this passepartout key with its private key and establishes a secure, encrypted connection for the duration of the session.

Figure 4: Key exchange with TLS



What Are the Three Types of Cryptography?

Cryptography deals in general with the topic of information security and in particular with the encryption and decryption of information. An algorithm is used that encrypts the plain text and thus makes it unreadable. It is used for data encryption, authentication and digital signatures.

Symmetric encryption falls into the first cryptographic category. Here, the sender and receiver share a single key, with the former using it to encrypt the plain text and thus transmit it to the receiver. The receiver then uses the same key to decrypt the encrypted text or to recover the plain text of the sender.

The second category includes public key encryption or asymmetric encryption. There are two interconnected keys: public and private. While the public key can be freely distributed, the corresponding private key must remain secret. The public key is used to encrypt the data that a person wants to send. The private key used to decrypt the data is usually kept by the creator of the key pair. The most commonly used algorithms here are RSA (Rivest–Shamir–Adleman) and ECC (elliptic curve cryptography), with TLS certificates often using RSA. The recommended size of these keys is constantly increasing (e.g., from 1024 to 2048 bits) so that they remain highly effective. ECC is just as effective in cryptographic terms as RSA. However, its key size is considerably smaller, which on the one hand reduces the computing and storage effort, and on the other hand results in higher speed and security. The downside is that not all ECC-based applications are interoperable with TLS certificates.

The hash function represents the third cryptographic category. This algorithm does not use a key but numerically compresses the plain text using fixed lengths so that the plain text content can no longer be recovered. Hash functions are commonly used by computer systems to encrypt passwords.

What is the Purpose of a Digital Signature?

A digital signature, issued by trust service providers such as SwissSign, is a signature certificate that is cryptographically bound to a document by a public key infrastructure (PKI). Digital signatures validate and authenticate the identity of the signer and the integrity of the document. They offer a high degree of certainty that the signer actually drew up the document and ensure that no changes have been made to the document. Digital signatures are sometimes suitable for securing access to confidential databases or in the eGovernment environment, such as for applying for passports online.

**PETER RUOSS,
PRODUCT OWNER, PAYMENT SOFTWARE
PARTNERSHIPS, UBS SWITZERLAND AG**

Phygital Banking Using the Example of Payment Cards

The physical and digital worlds are increasingly merging. Combined, they can lead to new, exciting customer experiences. Digitalizing physical processes, supplementing the virtual world with physical services – that is the quintessence of "phygital."

Today, individuals expect personalized, convenient and secure payment options that can be easily integrated into their physical and digital lives. Traditional cash counters are being transformed into digital self-service areas, which at the same time enable personal consulting.

Payment cards are a good example of phygital banking. After opening an account, issuing a card is the next important interaction between the bank and its customers. To bridge the time until the physical card arrives, the bank offers an immediately available virtual card that enables customers to shop online. The bank then sends updates on the physical card (e.g., about the postal delivery status), which customers can view at any time on their mobile phones. Physical cards can be backed up in a mobile app and then combined with digital tools for carbon tracking and offsetting.

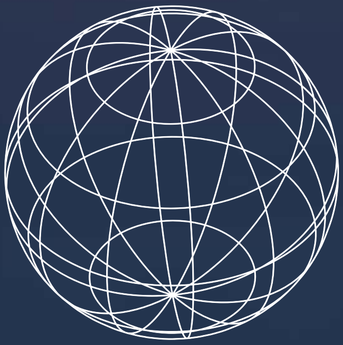
Brand Experience

The card's physical carrier letter can also be phygital: customized with content and QR codes that turn the arrival of a new card into a brand experience for customers. And the card itself, personalized with images chosen by customers. Or it is provided by kiosks that can authenticate a card holder and issue a new card in a matter of minutes. Mobile apps can also support activation of the card so that there is no need to visit a bank branch.

The technology group Giesecke+Devrient has recently examined what this means for banks and financial service providers and looked into the enormous opportunities for innovation it presents in its "Opportunities in the phygital landscape" study. The survey of financial service providers in 15 countries showed how relevant physical payment cards will remain as an important link between banks and customers. Cards act as a unique branding element and serve as a physical anchor for digital services. Phygital offerings help banks stay relevant in the face of innovative user experiences at neobanks and big tech companies.

**GABRIELLE BUGAT,
MEMBER OF THE MANAGEMENT BOARD OF GIESECKE+DEVRIENT AND RESPONSIBLE FOR THE CARD & DIGITAL PAYMENT DIVISION**

FURTHER INFORMATION



SWIFT Go: A New Standard in Low-Value International Payments

Sending money around the world should be simple. Simple for small businesses buying supplies abroad. And simple for families sending money to loved ones overseas.

The introduction of SWIFT gpi transformed high-value international payments forever – making them quicker, more transparent and predictable. With that positive experience on their side, SWIFT is making the same thing possible for low-value payments too.

The low-value payments market is skyrocketing, with research from McKinsey predicting 10% market growth between 2018 and 2023. With this in mind, SWIFT is laying the foundations for a smarter solution, and providing banks with all the tools they need to revolutionize their low-value payment offerings.

As the market continues to grow, so too do customer expectations. With services throughout daily life becoming quicker and more intuitive, customers expect the same in more complex areas as well – like payments. Financial institutions must innovate to keep up with these expectations.

Building on Solid Foundations

The idea behind SWIFT Go is simple – enable banks to offer their customers a quick, easy and predictable way of sending money around the world, directly from their bank accounts. SWIFT's service level agreements lie at the heart of this solution and enable exactly that.

When a bank signs up to SWIFT Go, they work out all fees with their counterparties. This ensures that payments are competitively priced and lets customers see exactly how much their transfer will cost before it begins its journey. The solution uses MT103 messages and is transparent too, allowing sending banks to integrate tracking information directly into their front end for added predictability.

Banks also agree to process payments in a maximum of four hours and promise not to apply any extra deductions. This keeps money moving fast and gives customers peace of mind that their payment will arrive at its destination on time.

SWIFT Go payments travel over the same infrastructure and network as SWIFT gpi, meaning banks and their customers benefit from the same security and service availability level. So, wherever a payment is heading, every cent is safe and sound.

A Fast-Growing Community

SWIFT enables instant and frictionless transactions across its network of more than 11,000 institutions – connecting four billion accounts in 200 countries. And SWIFT Go is a crucial part of this, enabling greater financial inclusivity for SMEs and consumers in developing and emerging economies.

Several large correspondent banks across Switzerland's important trading partner countries have already signed up, including the UK, US, China, United Arab Emirates and India. In total, over 250 banks in 90 countries have joined the community.

ROGER INDERBITZIN, HEAD OF SWIFT SWITZERLAND & LIECHTENSTEIN

FURTHER INFORMATION

Price is what you pay,
value is what you get.

Warren Buffett (1930)