nevis®

Nevis for Insurance Companies

Digital security infrastructure for insurance portals

Making security an experience.

The Challenges for Insurance Companies

1

Credential stuffing is a genuine threat

The sensitive information processed by insurance companies is of particular interest to cybercriminals and can be easily stolen if not adequately protected. A privacy breach can have catastrophic consequences not just for the customers affected but also for the company.

2

Technically challenging

Insurance portals must coordinate the needs of different groups – private customers, business customers, brokers and insurance consultants as well as business partners and internal employees – within a uniform security infrastructure. At the same time, insurance companies have very specific security requirements and must protect customer data as well as online price calculators against industrial espionage.

3 Guaranteeing compliance

Insurance information is highly sensitive and must be handled confidentially and securely in accordance with the applicable privacy and security regulations – such as the GDPR, the German Federal Data Protection Act or the Swiss Federal Act on Data Protection – in the relevant country. There are several challenges when it comes to implementing a CIAM solution that complies with these regulations.

4 Customer journey

Insurance providers meet a range of requirements, such as questions about insurance services, contract amendments, reporting claims and agreeing new contracts. It all begins with the onboarding process, which is tailored to the specific needs of the user. However, all it takes is a complicated portal access to reduce the customer's purchase incentive and cause them to seek offers from a competitor.

5 Increased competition

Customers increasingly expect a personalised and seamless customer experience based on the digital technologies that they use daily. Insurance companies must be able to keep pace with customer expectations and adapt quickly to these trends if they want to remain competitive. Negative user experiences will simply encourage policyholders to switch to other providers.

6 The need for simple and secure authentication solutions

New authentication solutions can be bewildering for customers, leading to frustration or rejection. In addition to informing their customers about the new solutions and supporting them during the rollout, insurers must ensure that their solutions are sufficiently secure and robust to prevent cyberattacks or misuse.

7 Customer demand for data sovereignty

Customers and partners expect you to treat their data securely and confidentially, while at the same time making their data easier to access. Insurers must therefore find ways of giving customers control of their data by implementing transparent data protection practices and informing customers how their data is collected, stored and used.

8 Personalisation

Offering a seamless experience when customers register and request quotes is a major challenge. Collect data securely to keep track of important customer milestones such as weddings or births and identify opportunities for new insurance needs.

How Nevis Supports the Insurance Sector

From secure onboard to lifelong customer relations

Detect fraud quickly and reliably

Use a certified identity management tool to guarantee secure access to user accounts. Prevent unauthorised persons gaining access to customer data under false pretences.

- Account activation/self-regulation
- Ordering new services and authorisations
- Linking identities and credentials
- Delegated administration: authorisation management by customers

Ensure increased privacy and guaranteed compliance

Show that you protect all personal customer data that you collect, store and process in all the systems you use and keep your company safe from reputational damage and sanctions.

- Clear and instant customer identification with ID verification
- Instant logins with MFA and biometrics
- The login replaces insecure, difficult-to-remember username and password combinations.
- Know your customer (KYC) identification check

Create connections using identity federation

Incorporate different insurance brokers by means of identity federation and link an identity across multiple identity providers (e.g. IG B2B in Switzerland, EasyLogin in Germany).

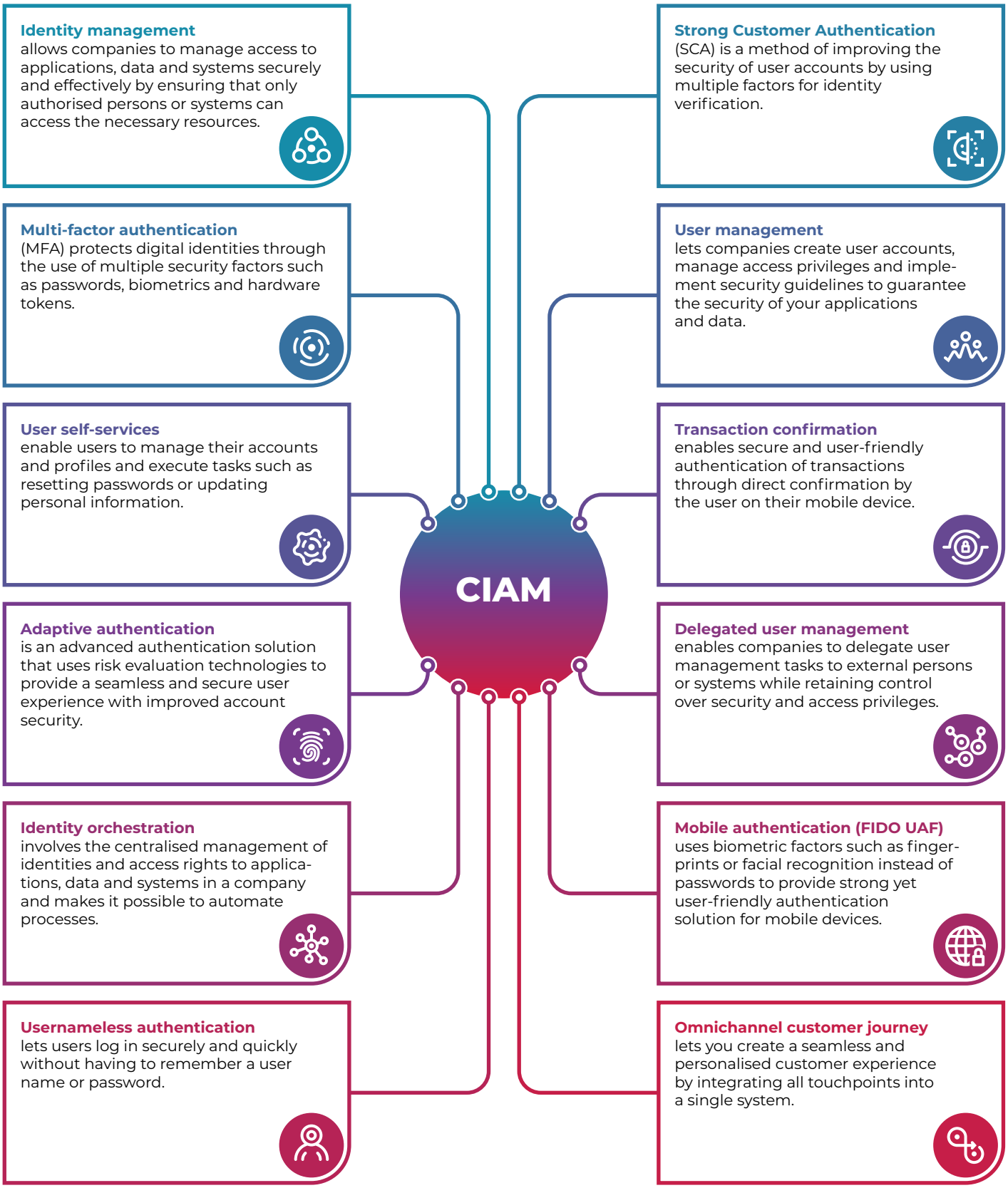
- Efficient management of customer accounts thanks to comprehensive self-service with the option of social logins (Facebook, Google, etc.)
- Support for multiple authentication tools and authentication strengths
- Quick and automated provision of the best possible security infrastructure

Guarantee rapid access to revisions, updates and offer overviews in the online sales channel. Whereas customer data and consultations were previously most commonly documented in person, by phone or by post – most customers today prefer to take out their insurance policies online. Customers also expect the process to be seamless with their data being processed securely.

Customer identity and access management (CIAM) offers precisely that and helps build customer loyalty. With the help of CIAM, insurers can record and organise customer identity and profile data. They can also manage customer access to applications, services and online profiles.

CIAM combines security and customer experience into a perfect solution for data and access management.

Key CIAM Functions for Insurance Companies



Identity management
allows companies to manage access to applications, data and systems securely and effectively by ensuring that only authorised persons or systems can access the necessary resources.

Multi-factor authentication
(MFA) protects digital identities through the use of multiple security factors such as passwords, biometrics and hardware tokens.

User self-services
enable users to manage their accounts and profiles and execute tasks such as resetting passwords or updating personal information.

Adaptive authentication
is an advanced authentication solution that uses risk evaluation technologies to provide a seamless and secure user experience with improved account security.

Identity orchestration
involves the centralised management of identities and access rights to applications, data and systems in a company and makes it possible to automate processes.

Usernameless authentication
lets users log in securely and quickly without having to remember a user name or password.

Strong Customer Authentication
(SCA) is a method of improving the security of user accounts by using multiple factors for identity verification.

User management
lets companies create user accounts, manage access privileges and implement security guidelines to guarantee the security of your applications and data.

Transaction confirmation
enables secure and user-friendly authentication of transactions through direct confirmation by the user on their mobile device.

Delegated user management
enables companies to delegate user management tasks to external persons or systems while retaining control over security and access privileges.

Mobile authentication (FIDO UAF)
uses biometric factors such as fingerprints or facial recognition instead of passwords to provide strong yet user-friendly authentication solution for mobile devices.

Omnichannel customer journey
lets you create a seamless and personalised customer experience by integrating all touchpoints into a single system.

Nevis – Your Partner for Security and Compliance

Nevis offers you the solution: Your customers receive passwordless and secure access to their accounts so they can manage all their insurance affairs in seconds – with total convenience and security.

Convenient Login With No Loss of Security

Today's users of insurance services not only have high expectations in terms of user-friendliness but also attach greater importance than ever to the adequate protection of their data. Restricting user-friendliness for the sake of security – or vice versa – is therefore not an option. The online portal must therefore enable and expand the use of a new login process.

Adaptive Authentication

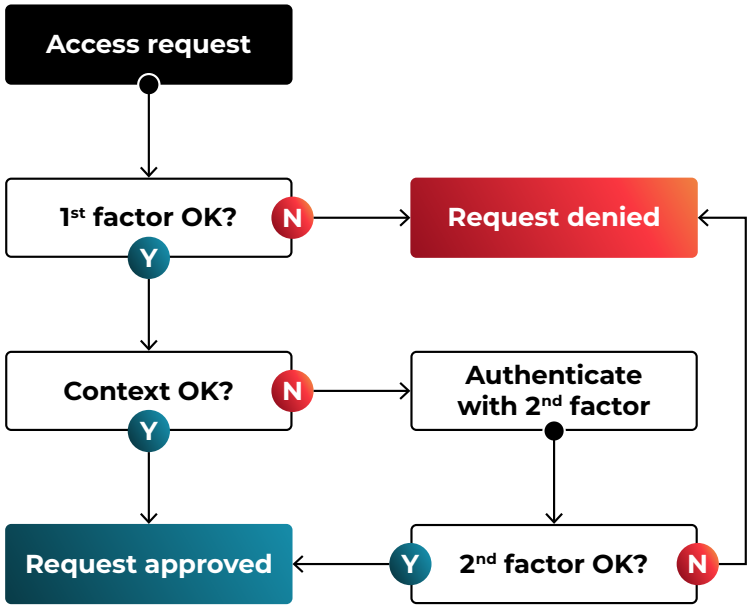
Adaptive authentication allows insurance companies to adapt the authentication strength to the level of risk, thereby guaranteeing a secure environment for customer data.

How it works:

Risk assessment: If a user wishes to access patient data, the system evaluates the risk associated with the request based on criteria such as the user's location, the device and the time of access.

Authentication strength: Based on the risk assessment, the system determines the authentication strength required. If the assessment returns a high level of risk, additional authentication measures are requested.

Access control: Once the user has provided the necessary authentication, the system either grants or denies access to the policyholder's data based on the risk assessment and the strength of the authentication.



The Insurance Sector Trusts Nevis

«The fact that Nevis always welcomed our feedback while developing the solution – and implemented our wishes directly following appropriate analysis – was a real plus for us.»

Kenneth Nydegger
Product Owner of all Gateway Services
die Mobiliar

Success stories

GENERALI

Generali – IAM for Secure Digital Business Processes

die Mobiliar

Die Mobiliar – Access Infrastructure

helvetia

Helvetia Insurance – Web Application Firewall

Contact us to arrange a consultation.

Switzerland (HQ)	+41 43 508 06 81
Germany	+49 89 3803 8684
UK	+44 20 4579 0404

or via contact form:

nevis®

Making security an experience.

About Nevis

Nevis Security AG is a pioneer in digital security and a strong advocate for the use of passwordless, user-friendly access solutions worldwide. As the market leader in Switzerland in the area of customer identity and access management (CIAM), Nevis provides organisations in the financial, insurance and iGaming sectors with the highest level of data protection and seamless authentication procedures. Nevis technology secures over 80 per cent of online banking transactions in Switzerland – demonstrating the company's expertise and commitment to innovation. Headquartered in Zurich/Switzerland with offices across Europe, Nevis is constantly expanding its global presence through a rapidly expanding partner network, emphasising its role as a key player in the digital ecosystem. Nevis aims to strengthen its position as a leading authority in digital identity security worldwide and to provide scalable, forward-looking solutions that meet the growing needs of its customers.

www.nevis.net