nevis®

Nevis for Statutory and Private Health Insurance Providers

Customer identity & access management and strong customer authentication from a single source

Making security an experience.

The Challenges Facing Health Insurance Providers

1

The electronic health record

Health insurance companies have offered the electronic health record (ePA) since 2021. From 2024 onward, health insurance funds must provide policyholders with secure digital access in addition to the electronic health card – which falls within the scope of various laws, such as the GDPR and health insurance legislation.

2

Cybersecurity risks

Health services are exposed to a broad spectrum of threats due to cyberattacks. There is a high risk of privacy breaches since protected health information (PHI) is the most valuable type of data for hackers. As the threat landscape continues to evolve, health insurance providers must constantly update their defensive measures.

3 Complying with legal requirements and privacy

The healthcare sector must comply with numerous legal requirements – including regulations such as the GDPR, German health insurance legislation and the Law on the Digital Modernisation of Healthcare and Nursing Care (DVPMG). These require statutory health insurance funds and private health insurance companies to demonstrably protect personal customer data across all systems used to collect, store and further process this data. These requirements can be extremely complex and dynamic and require constant monitoring and adjustment.

4 Sectoral identity providers

With the introduction of the e-prescription, Gematik relied for the first time on the model of an identity provider service. The new sectoral IDPs to be provided by e-health providers are designed to allow each provider to manage the digital identities and authenticate its customers. It is essential to ensure that the necessary infrastructure and know-how are in place to complete the implementation seamlessly.

This calls for the careful planning and implementation of solutions to meet these requirements.

5 Increased competition

Customers increasingly expect a personalised and seamless customer experience based on the digital technologies that they use daily. Health insurance funds and health insurers 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 funds and insurers.

6 The need for simple and secure authentication solutions

Customer acceptance: 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, e-health providers must ensure that their solutions are sufficiently secure and robust to prevent cyberattacks or misuse.

7 Requirements for DiGA and DiPA

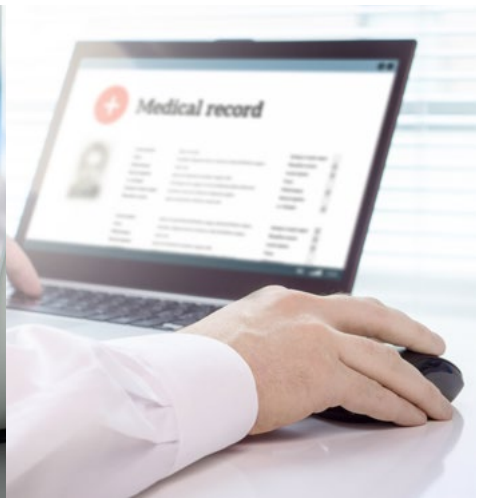
The Federal Institute for Drugs and Medical Devices (BfArM) has published new test criteria for privacy protection requirements for DiGA and DiPA, which will serve as a basis for new certificates in the future. Manufacturers of health and nursing applications must demonstrate that their applications comply with privacy legislation and that only authorised persons have access to patient data. These include the requirements of the European General Data Protection Regulation as well as the broader requirements for DiGA and DiPA.

8 Customer demand for data sovereignty

Customers and patients expect you to treat their data securely and confidentially while at the same time making their data easier to access. Therefore, e-health providers must 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.

How Nevis Supports the Healthcare Sector

From secure onboard to lifelong customer relations



Efficient identity management

Nevis is the beating heart of the security infrastructure for health insurance funds and companies. With Nevis, you can implement the central identity management process efficiently:

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

Streamlined digital access

Nevis ensures that a login process, access to an application or a business process can be assigned to the authorised expert group:

- Doctors, technical experts or nursing staff can log into the e-health portal in seconds
- The users can access patient data conveniently and perform updates or transactions
- Users confirm approvals with fingerprint or FaceID rather than insecure passwords
- Nevis also guarantees availability of the e-health portal around the clock

Popular functions

Identity management solutions for healthcare service providers cover other popular functions in addition to the usual IDM processes. Nevis offers:

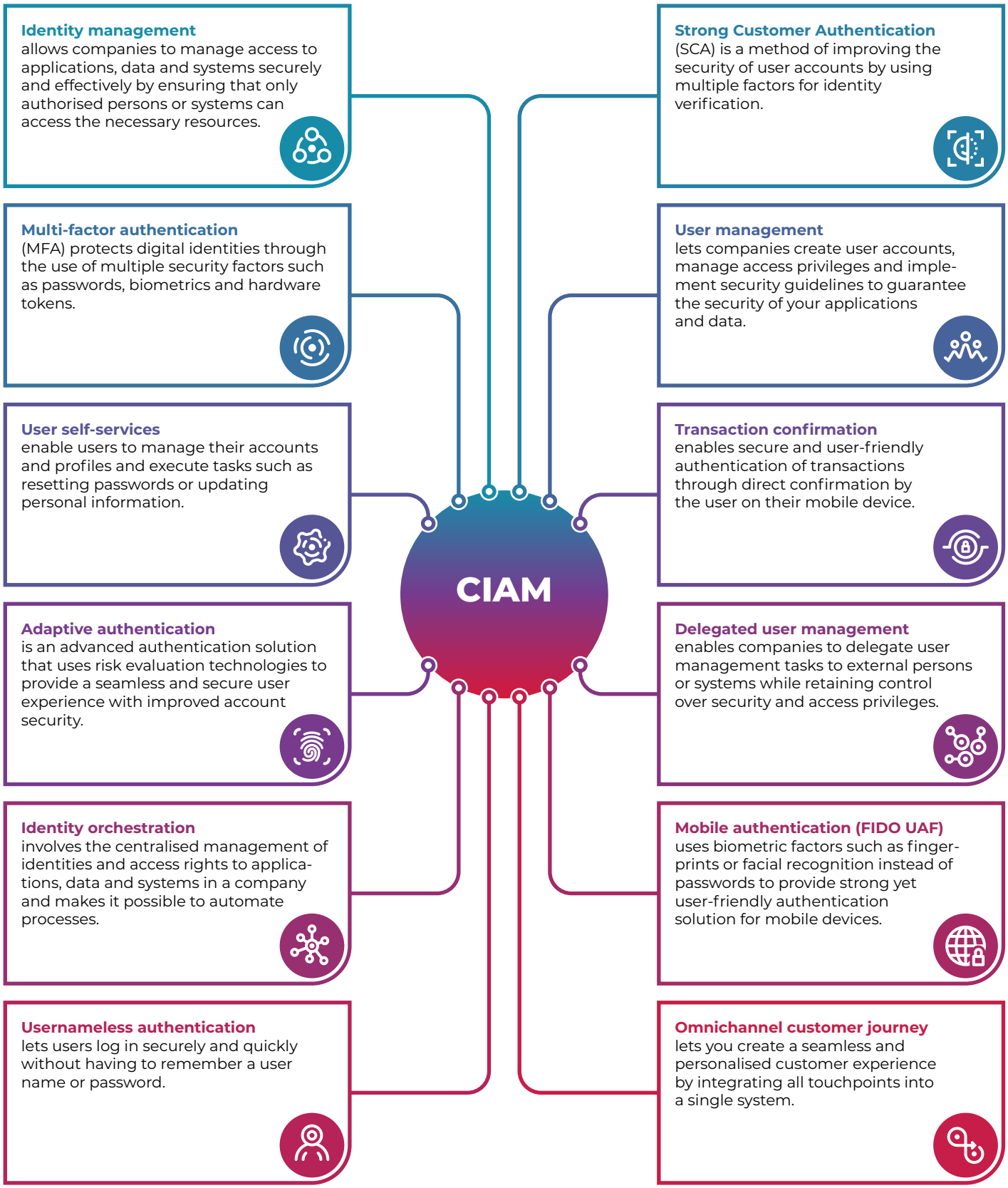
- The ability to exchange master data with the core system
- Provisioning of identity data in different peripheral systems
- Support for different authentication tools: mTAN, SuisseID, HPC Card, Soft Certs, etc.
- Authorisation based on roles and user attributes
- Integration of special client software
- Single sign-on for web applications and other services for secure data exchange

Providers of digital services in the healthcare sector are aware of their duty to protect extremely sensitive patient data. Health services are also under pressure to operate very efficiently. Service providers such as general practitioners and consultants, hospitals, radiology institutions and laboratories, but also health insurance providers and public authorities should therefore collaborate with the help of an efficiently digitalised process chain. Since highly sensitive information is transmitted, a robust infrastructure is the prerequisite for participation in integrated healthcare delivery.

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

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

The Most Important CIAM Functions for the Healthcare Sector



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.

Protected by Compliance

Under the terms of the GDPR, the healthcare and life sciences sector in general is under an obligation to demonstrably protect personal customer data across all systems used to collect, store and further process this data. With Nevis, healthcare facilities can be sure that their IT systems comply with the applicable regulations and laws. With Nevis, you are automatically compliant with legislation such as the GDPR, HIPAA, HITECH, Electronic Prescription of Controlled Substances (EPCS) – and can avoid unnecessary and costly sanctions that will harm your company and its reputation.

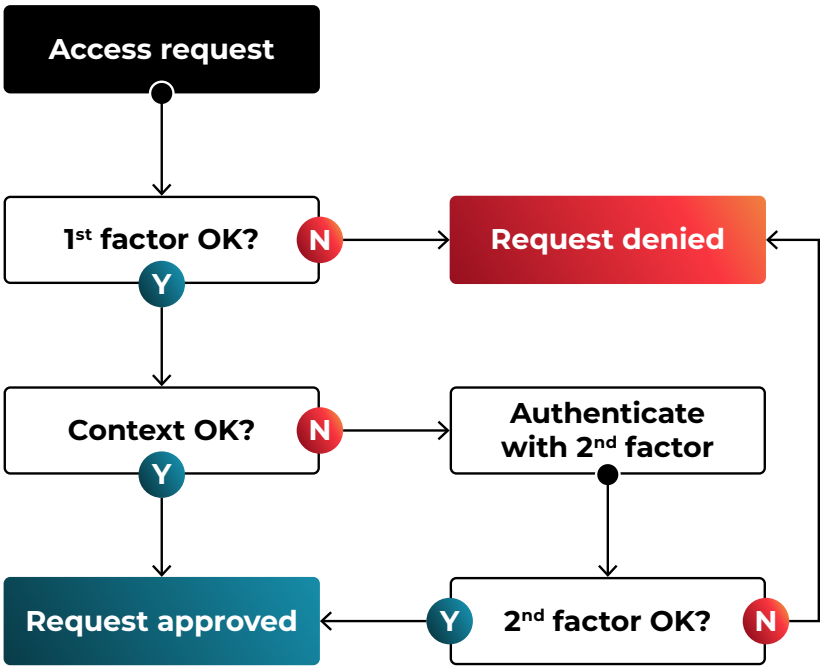
Convenient Login With No Loss of Security

Today's users of e-health 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 healthcare facilities to adapt the authentication strength to the level of risk, thereby guaranteeing a secure environment for patient 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 patient data based on the risk assessment and the strength of the authentication.

The Healthcare Sector Trusts Nevis

«The HIN platform is being continuously expanded in close consultation with Nevis. Our joint goal is to push ahead with the digitisation of the Swiss healthcare system and the associated advantages in terms of user convenience and efficiency.»

Aaron Akeret
Solution Engineer & Enterprise Architect
Health Info Net AG

Success stories

MediData

MediData –
Protected Health Data

HIN –
IAM for Health Info Network

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