nevis®

Solution Paper

Nevis ID

Making security an experience.

Content

Introduction

The business world is developing incredibly dynamically. Digitalization is advancing. Nowadays, more and more services are being offered in digital formats. This is having an effect on business processes and models. Everything that could once be purchased in analog in the real world is all of a sudden available online. Though customers are reserved about sharing their own data, when they **trust**[1] your brand they are willing to reveal personal data. It goes without saying that access to your services has to be fast and secure. Your online portal should offer protection against all types of attacks. Both personal data and business applications have to be safe.

Generally speaking, it is essential to protect sensitive information held by companies and public administration against unauthorized access. However, it should simultaneously be possible to process it safely, in compliance with the law, efficiently, cost-effectively, and in a user-friendly manner. Protecting customer identity is an essential part of this guarantee. And security matters more than ever before. It is easy to forget that complicated login processes detract from the desired positive customer experience.

Positive customer experience is key to economic success

Studies show that two-thirds of the competition between companies these days is decided by customer experience. In 2010, it was just 36%[2]. As a result, anyone who wants to survive in this market should not leave any Digital Customer Experience (DCX) demands unsatisfied. Companies have to strike the balance between the best possible user experience and effective data protection.

In order to achieve this goal, companies are turning to high-performance software-based solutions like the ones provided by customer identity and access management systems (CIAM). Not only can they manage several identities or a large number of users, they also help manage centralized and secure access controls. And it's not just customer demands for speed and convenience that are being satisfied, so too is the strict **GDPR compliance** synonymous with and mandatory for CIAM systems when it comes to handling personal and private data.

CIAM systems support the realization of more effective and secure digitalization initiatives. Digital business processes are expedited and optimized through intuitive multi-factor authentication (MFA) based on biometrics. They act as a lever for raising efficiency while simultaneously guaranteeing security, quality, and a good customer experience. Their decisive advantage is that they allow for a consistent and seamless customer experience across all channels – as well as a convenient mobile experience.

CIAM systems offer a clear competitive advantage for all companies committed to first-class customer service and determined to give their customers a secure, comprehensive customer experience.

1: *PwC: Experience is everything: Here's how to get it right*
2: *Superoffice: Customer Experience Statistics*

Customers Want Safe and Easy

Customer Experience and Customer Trust Are the Keys to Success

Customer experience has quickly turned into a top priority for companies. Particularly since the next provider is only a click away. The customer experience has to be a positive one from the first point of contact. Consumer demand for speed and availability of services has increased significantly in the past few years. On top of that, there's a desire for self-service options that empower customers to manage their own data and define their own preferences.

As a provider, you have to ensure that your customers experience better service with you than with the competition. Shifting your focus to the sophisticated, digitally-savvy customers is key. Because when these customers are satisfied and have placed their trust in you, their positive reviews will carry far – as will their negative ones. And this is exactly why investment in this area is a must.

27%

Almost a third of customers believe that their experiences with brands have gotten worse, and not better, over time

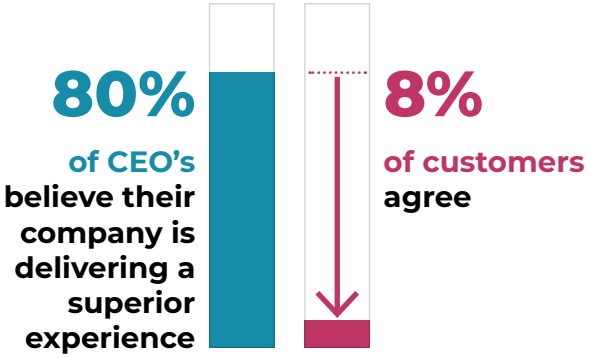
62%

would switch brands if they thought they might have a better experience elsewhere

Source: Experience Gap Report 2018, clearstrategy.com

And yet, many providers across different industries are still unaware of the divide between customer expectations and the actual customer experience.

The Experience Gap



Bain & Company via Craig McVoy, CCXP

But why is it so hard to recognize what customers want or what annoys them? Because in most cases, customers leave without an explanation. Only one in 26 unsatisfied customers actually complains to the provider. This problem is exacerbated by the fact that consumers are generally more likely to share a negative experience than a positive one[1]. That's something all industries have to deal with. A lack of positive customer experience is a threat to business growth.

BRACK.CH

„Nevis combines technical expertise and comprehensive consultation into one attractive package. Their service provider mentality left a lasting impression on us. In addition to their core focus on security, our points of contact always paid attention to key aspects like user experience and business processes.“

Marcel Rassinger
CIO, Competec-Group

A positive customer experience is connected to customer trust. Customer trust is essentially influenced by the services they receive. Trust arises when you understand your customers' needs, respect them, and offer them relevant services. Earning your customers' trust is not only the key to maintaining their loyalty and ensuring they keep coming back, it also guarantees that they encourage their friends to do business with you.

One example of how improved customer experience can lead to customer trust is the elimination of passwords for accessing services.

1: *Superoffice: Customer Experience Statistics*

Passwords are a burden and a source of trouble

When you hear about stolen passwords caused by data leaks, are you relieved that your company isn't affected? Sure. If you can just shrug it off because you know your cybersecurity is state-of-the-art, even better. However, if in both scenarios you still require your users to use passwords, your company is at risk. Because passwords are everything but user-friendly. And that often leads to a large number of users having one and the same password for multiple accounts. If just one of these accounts is affected by a data leak and your user has the same password for an account with your company, you are now vulnerable. Cybercriminals will use stolen passwords wherever they see an opportunity to hijack user accounts. That's because only 28% of users affected by a data leak change their password within three months. And this risky user behavior poses a threat to your company. In Q3 2020 alone there were 770 million attacks on logins using credential stuffing[1]. The industries affected most are retail, e-commerce, gaming, and financial services. According to a statistic from the City of London Police, 16.4 million pounds are lost through online shopping cyber attacks in Great Britain just on Black Friday and Cyber Monday[2].

Only 28% of users change their password after a data leak.

Article from zdnet.com

Just imagine if your company were to opt for a secure, passwordless login based on biometric authentication e.g. using FaceID or a fingerprint. You'd eliminate the burden of passwords for your customers. No one would have to remember, regularly change, or strengthen a password anymore. You'd substantially improve the customer experience. And you would simultaneously boost trust – that of your customers in your company and of your company in your customers.

Are Customer Experience and IT Security Incompatible Paradigms?

User experience and security are important criteria that need to be balanced out if you want to attract and hold on to customers. However, the paradigm still holds that increased security detracts from the user experience. And, vice-versa: that a great user experience can not be secure. Do user demands for simple, fast, and straightforward online access have to take a back seat to security and regulatory compliance?

1: *Arkose Labs: Q4 2020 Fraud & Abuse Report*
2: *Article from Finance Digest*

The path to a positive and secure mobile customer experience is via modern multi-factor authentication with biometrics. The biometric identification technology built into today's mobile devices facilitate completely new approaches in the realm of authentication. This trend is also being fueled by new standards like e.g. FIDO (Fast IDentity Online). **Gartner recommends that providers make passwordless authentication the highest priority.** Replacing passwords with biometric authentication can improve both user-friendliness and security – an effect not often seen with security and IAM tools[1]. For the first time ever, it's possible for increased security and user-friendliness to go hand-in-hand!

Nevis' customer PostFinance is proof of just how successful this can be:

PostFinance

„Our customers expect passwordless and secure access to their accounts. The number of customer interactions has doubled."

Eric Müller
Lead Solutions Architect
PostFinance

Nowadays, companies have to react more quickly to new demands - be it because of new initiatives or threats. Access to a customer portal or online services has to be easy, safe, and available around-the-clock. You stand to gain when you simplify and expand interactive options with the solutions offered by CIAM systems.

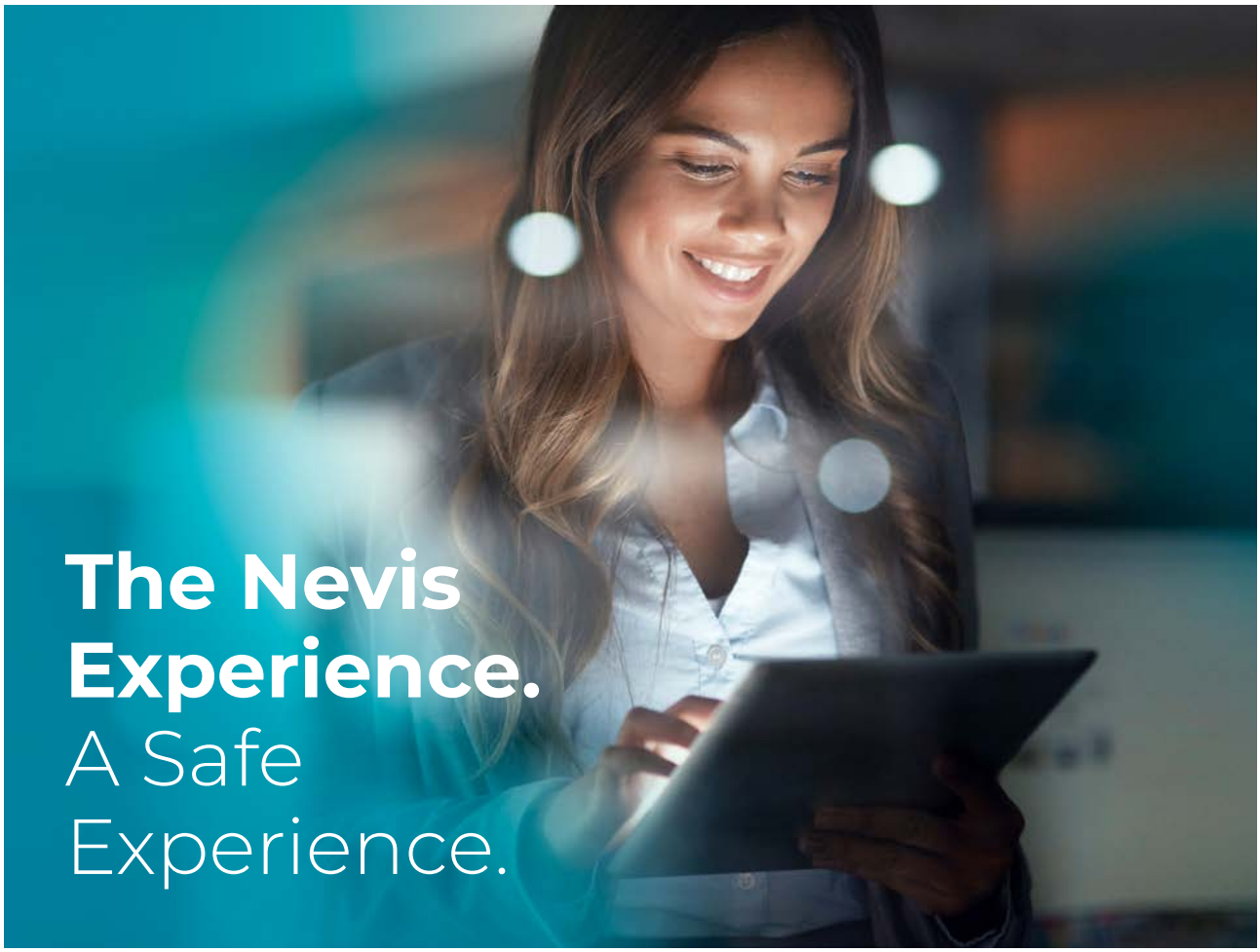
A good CIAM solution serves as a strategic device for customer retention and facilitates a consistently positive experience for end users. Having a pleasant customer experience from the start is crucial.
User identities and access have to be protected and monitored, though not at the expense of the customer experience. According to US analyst Gartner, user-friendliness is a key factor when it comes to choosing CIAM software: "Customer experience is the battlefield"[2]. But customer experience budgets are lagging behind heightened customer demands according to Gartner: "CX budgets are not increasing with increased expectations"[3] and are threatening business success as a result. Because overly-complicated service and a diminished user experience can have a negative impact - like loss of customers and a drop in profits.

1: Gartner: 2020 Planning Guide for Identity and Access Management
2: Gartner Customer Experience Summit, 2019
3: Gartner Customer Experience Survey, 2018

A modern CIAM system is not only necessary from a security perspective. It is also the most important digitalization tool. It facilitates unlimited mobility, reduces frictional loss, and improves the customer experience as a result. It increases operational efficiency and makes it possible to respond more quickly to changes and improve your services. Furthermore, it ensures compliance with complex regulations and provisions like the GDPR.

Use the Nevis ID platform to provide your users secure access to information and applications, increase the level of security where necessary, and securely and effectively manage identities and everything that this entails.

We help you competently perform all those tasks, which are not part of your core business. And remember: if you ignore your customers' demands for convenience and security, you'll lose them to the competition and won't attract new ones.



CIAM

Download White Paper **What is CIAM?**

A successful customer experience largely depends on striking a balance between security and user-friendliness. Personal data is essential to a personalized and relevant user experience. However, customers have to trust you before you gain access to this personal data. You establish this trust with an exceptional user experience. It doesn't make sense to sacrifice security for usability, or vice-versa. At first, this seems like an irreconcilable problem. However, companies can tackle it by integrating CIAM.

We refer to the customer identity and access management functions as the three "Cs": connect, collect, and convert. CIAM is a solution for managing digital identities (users and the information connected to these users) and user access controls to data collected and stored by a company (or outsourced cloud provider). Thanks to these digital identities, customers have both convenient and secure access to their users accounts and data. This makes it easy for companies to lay the groundwork for unique and personalized user experiences.

Unlike identity and access management (IAM), CIAM is a customer-oriented solution, which places a large number of decisions regarding data storage and access rights in the hands of users themselves. By opting in or out of access and security protocols, configuring their own privacy settings, and determining what data they want to share and what information they want to see, users can shape their own experience with a brand or service provider.

With CIAM, you offer your customers simplified digital access without having to make any security compromises. The best systems include functions like passwordless login, extensive self-service options, and biometric identification. They also guarantee compliance with legal regulations like the General Data Protection Regulation (GDPR). This lets companies define their individual security levels – depending on how sensitive the data and information to be accessed are. For example, less confidential information can be protected through social login (i.e. login via a social media account), while more sensitive data can potentially require additional authentication – like distinct biometric features – before access is granted in order to verify the identity of the user.

A good CIAM system like the Nevis ID platform helps you tackle challenges in the following areas:

- digital identities
- single sign-on (SSO)/social login
- passwordless access
- behavior analysis
- multi-factor authentication (MFA)

Technical aspects of CIAM

The following standards have now become commonplace in modern CIAM systems:

- FIDO for authentication needs (creating a secure connection)
- OAuth 2.0 for authorization
- OpenID Connect and SAML for the Federation (identity federation)

FIDO (Fast Identity Online) is the world's largest ecosystem for standard-based, interoperable authentication with the goal of resolving the world's password problem. The FIDO standard is an open industry standard for secure, fast, and simple authentication on the Internet. It makes it possible for companies to deploy hardware-based authentication, like fingerprint and facial recognition, in their products. Product users can then simply register with online services without having to remember a complicated password.

The **OAuth 2.0-Framework**[1] is a set of defined process flows for delegated authorization. It improves automated access to applications that belong neither to the user nor to the service provider, but rather to a third party. Service providers and other dependent parties can carry out actions on behalf of the end user and access resources without end users having to reveal their registration data.

OpenID Connect (OIDC) is an authentication protocol that facilitates the exchange of credentials and basic end user profile information between identity providers and service providers. OpenID Connect is a series of defined process flows for federation authentication, which uses OAuth 2.0 as its basis and builds on it[2]. These processes add an identity layer in order to facilitate a federated authentication[3]. OpenID Connect works for both web and mobile applications. OIDC lets relying parties (RPs) authenticate users across websites and apps without having to own and manage password files. Thanks to OIDC, the relying party is always aware of the identity of the person currently using the browser or native app, without having to manage the identity of the user itself[4].

Security Assertion Markup Language (SAML) is an authentication protocol that lets identity providers (IdP) relay authorization data to service providers (SP). SAML establishes the connection between the authentication of a user's identity and authorization for the usage of a service. SAML contains a set of defined process flows for federated authentication, which is wholly independent from OAuth 2.0. In contrast to OpenID Connect, which is used for CIAM scenarios, SAML is predominantly used in workforce IAM cases.

1: *Definition from TechTarget*
2: *openid.net*
3: *hackernoon.com*
4: *OpenID FAQ*

What Can the Nevis ID Platform Do?

The Nevis ID platform is a modern solution for effective identity and access management. Thanks to its modular construction and open interfaces, it can be flexibly adapted to a broad range of requirements. Nevis is installed upstream of the existing infrastructure and adds another layer of security by controlling all user access to customer gateways and portals.

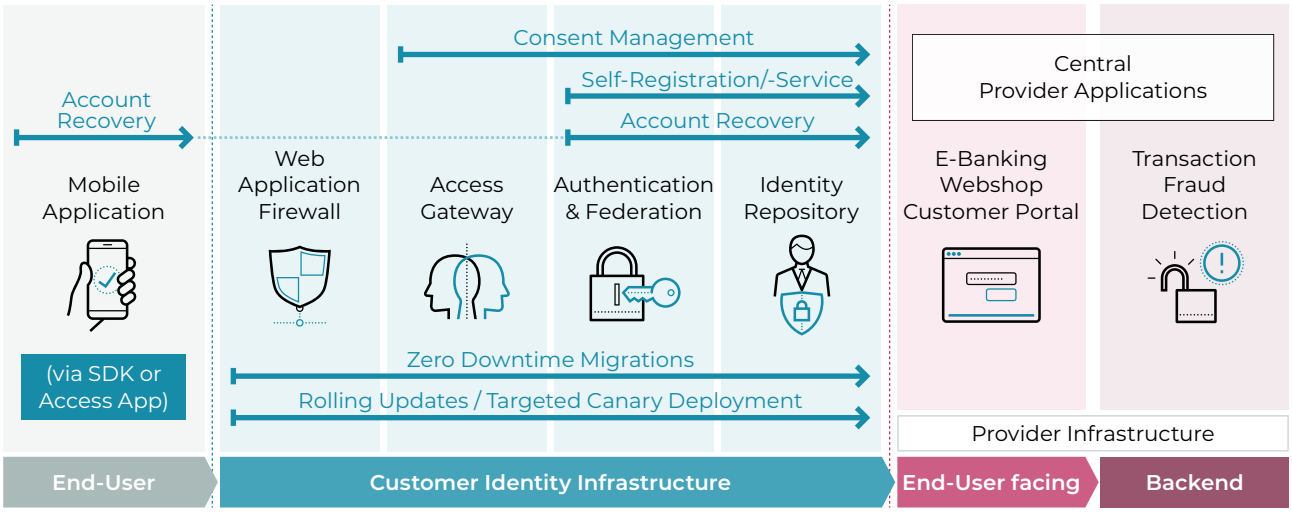
Authentication and authorization are at the heart of successful customer identity and access management. Nevis consists of a secure entry gateway combined with a web application firewall, an authentication service, and identity management.

However, the Nevis CIAM software includes additional functionalities to make the entire authentication and authorization process flow more effective. You can learn more about these and other functionalities below.

The Nevis ID platform encompasses sophisticated, tried-and-tested, product components for customer identity and access management and offers functions like:

- web access management and federation
- entry gateway and web application firewall (WAF)
- strong two-factor authentication (2FA)
- adaptive authentication
- support for social login/social identities
- mobile authentication in compliance with FIDO standard with our access app and SDK
- User management with self-registration for users and their devices

An overview of the Nevis ecosystem functionalities:



The Nevis System serves as an intermediary and enables secure and verified access by proxy to data, applications, and company domains not directly accessible to the user.

The Nevis solution is scalable and can be expanded with additional functional components at any time. Nevis' modularity and expandability guarantee maximum protection of your investment.

Identity Management

Identity management (IDM) is concerned with the identification of individuals in a system providing resources. It controls the desired level of access to resources by reconciling defined identities with user permissions and restrictions and creating different users roles, groups, and guidelines. For example, if users want to access resources to which they have no access rights according to the guidelines, access is denied. Occurrences such as these are logged and available as a report.

Identity management helps determine

- what a user may do
- what devices a user can access certain resource with
- under what circumstances a user is granted access

Guidelines determining what users can do depending on factors like their device or location are key to identity management systems. As such, the system delivers reports and security warnings and handles other operational and management requirements.

The technical architecture of Nevis Identity Management components facilitates the following functionalities

User Management – Comprises the global management of all users and their permissions. Nevis centrally manages the identities, credentials, roles, and attributes of users and makes these applications, services, and systems available through a secure communication infrastructure. Furthermore, user accounts and rights are automatically allocated in accordance with a rule and role model. Self-administration, delegated administration, and identity management workflows facilitate effective user management.

User Self-Service – User self-registration is one of the most established mechanisms on online portals. Users are permitted to initiate the process of creating an account and to provide identity data. It is possible to provide template (with options for customization) registration processes and to generate your own registration processes.

Delegated Administration – Users do not register themselves, rather this is done by a delegate. Nevis offers administrative interfaces, which let delegates like e.g. account managers set up, manage, and delete user accounts and passwords on behalf of customers. Delegated administration can also prevent e.g. unauthorized minors from accessing user accounts. In this case, rules are defined so that only parents can manage their children's accounts.

Extensible Data Model – Nevis Identity Management is delivered with a core data model. The data model consists of fixed entities (core entities) like e.g. user, departments/units, applications, and roles as well as attributes. There are also flexible, customizable properties. The data model also encompasses the relationships between these entities. The fixed identities (user, units, etc.) and their attributes (general properties or features of the entities) are prescribed. The selection of attributes is based on our customers' best practices.
However, there are always business requirements and use cases that are highly specific and perhaps not addressed by the pre-defined data model. For these cases, the data model also contains so-called "properties".
A property is comparable to an attribute of an entity e.g. the attribute "first name" of the entity "user". Thanks to the use of properties, the data model can easily be customized and adapted to very specific demands.

History-Aware Data Model – The history viewer shows how data changes over time and consolidates events. Nevis stores events like insertion, update, and deletion in version tables along with the timestamp and the event actor (i.e. the user who carried out the action).

Multi-Tenant Support – Makes it possible to serve multiple clients without letting them see each other's data, user administration, and the like.

Real-Time Provisioning – The provisioning module is responsible for distributing information about changes to Nevis identity management. These changes might be e.g. the creation of a new user or allocation of a role. Provisioning events triggered by such changes are written to message queues and can be consumed by other systems. One example would be initiating a new customer entry in Salesforce after registering on the company portal for the first time.

Web-based Interface – Nevis' web user interface (web GUI) offers an administration interface for identity management. You can manage the following items using the web GUI:

- users
- organizational units
- applications
- user credentials (authentication information)
- roles and properties (permissions information)
- company roles
- clients
- permission guidelines and email templates

Access to these items is managed through administration roles. The web GUI can be customized by changing the log color or placement to match the organization's corporate design.

Customer communication using SMS, email, and letters – Nevis' output management supports multilingual templates and all standard channels of customer communication. In addition to password reset emails or SMS notifications, Nevis also creates direct PDF files to e.g. deliver registration codes to customers by post.

Not all of these features are directly visible to end users. However, they are all important for effective and compliant identity management.

Access Management

Access management (AM) is an information security and data management process and secures the implementation of security guidelines in access control systems. If access management is effective, applications are protected. AM controls user access to digital data, services, and applications on the basis of the rules established in the identity management (IDM). In order to gain access, users have to authenticate themselves and be authorized by the IT system. The AM guarantees that the roles and guidelines defined in the IDM are observed and uses them as the foundation for processing access requests.

Nevis offers strong user and system authentication (strong customer authentication, SCA) in combination with identity and access management. Nevis thus covers the entire identification, authentication, and authorization process. Entry gateways and web application firewalls (WAF) are added components. While these additional applications filter content from user requests to protect your company's online applications from internal and external threats, Nevis' authentication processes are focused on user identity. The most important task is to check whether users are who they claim to be in order to prevent unauthorized users from accessing your applications.

Nevis Identity and Access Management simplifies on and offboarding processes, pools the management of team permission, and facilitates hierarchical access. These and other functions increase company security and productivity. At the same time, they result in reduced internal expenses and security overhead.

Secure authentication is guaranteed by a variety of authentication backends as well as additional functions like multi-factor authentication, strong customer authentication (SCA), identity federation, and API authorizations. Find more details below.

Federation

Federation combines electronic identities and attributes of an individual across different identity management systems. This makes it possible to outsource identity management processes.

Federation standards like SAML 1 and 2, OpenID Connect, Web Services Federation (WS Federation), and OAuth 2 are based on a trust in the connected identity providers (IdP) and are secured using digital signatures and encryption. In addition to these standards for federated identities, Nevis Identity Management can also be used as a local authentication backend.

The Nevis ID platform supports identity federation with external networks or security domains. Single sign-on and social logins are also possible.

Single Sign-on

Many companies integrate single sign-on (SSO) to make sign-up and login for all their online services easier for their customers.

Thanks to SSO, one central sign-on and login are sufficient. There's no need to sign on and log in all the time and separately to various company services.

Single sign-on for users means that all subsequent logins to access multiple web applications on the backend are automatic after a single, central login.

Nevis offers:

- consolidation into one central identity for users
- identity mapping
- minimal application adjustments
- centralized IAM processes

Benefits:

- improved usability
- improved business flexibility
- increased application protection

Social Login

The social login (a form of SSO and Federation) lets users register via a website or app belonging to a social network provider. Social login is a form of single sign-on for multiple systems. Available information from social networks is used to sign on to a third-party website. The social login simplifies the sign-up process, reduces frictional loss, ensures more precise and validated data, and offers end users convenience.

Bring Your Own Identity (BYOI)

Solutions with approved electronic identities, for example SwissID in Switzerland or Verimi in Germany, work similarly to social logins. Customers use their personal, verified, and approved electronic identity.

Companies wanting to reap the benefits have to integrate "bring your own identity" (BYOI). Doing so helps increase trust in customer identities. Gartner recommends: "Implement 'bring your own identity' (BYOI), but make sure that the level of trust provided by the identity provider matches the level of risk"[1].

Multi-Factor-Authentication

Multi-factor authentication (MFA) is a security mechanism, which authenticates individuals using more than one required security and validation process. Because authentication based merely on a username and password as a means of identification is not secure and is also vulnerable to hacker attacks.

The primary means of identification are based on the principles of knowing, having, and being. Both location as well as time can also serve as verification features and can be consulted as additional factors.

The combination of these identification factors is a reliable way to ensure that those attempting to access confidential data are indeed who they claim to be:

- **Having** – possession of a device (mobile phone, bank card etc.)
- **Knowing** – a password, security question, PIN
- **Being** – biometric features (fingerprint, face ID, iris pattern)

Additional factors used to verify identity, which are especially common in the financial sector for detecting intent to defraud (adaptive MFA):

- **Location** – specific IP address
- **Time** – compared to the previous or usual sessions

1: Gartner Innovation Insight for Bring Your Own Identity, 2018

The more sophisticated the MFA configuration, the safer the system. However, sacrificing user-friendliness is not an option. Not every online process requires the same measure of security. That's why Nevis can be configured so that the system chooses the strength of authentication processes based on the risk, thus guaranteeing maximum user-friendliness at all times.

Multi-factor authentication makes maximum user-friendliness possible because biometric procedures like facial recognition and user keystroke dynamics take neither time nor effort. At the same time, they increase protection against unauthorized access since users like to circumvent more complex manual security measures. The combination of multiple identity factors is therefore very effective at hampering identity theft. This is particularly important when it comes to sensitive processes like payments and access to documents worth safeguarding.

The benefits of MFA

- improved security thanks to a combination of different authentication processes
- increased user-friendliness with biometric procedures
- hampers identity theft
- more flexibility when protecting resources

Passwordless

Passwordless authentication verifies whether users are who they claim to be. Unlike traditional systems, the user does not have to manually enter a string of characters (password). Instead of the password, other authentication processes are used. Nevis uses biometric procedures like facial recognition (e.g. FaceID from Apple) or a fingerprint for passwordless authentication. This increases both security and user-friendliness.

The special thing about this solution is the **combination of maximum safety and user-friendliness**: your customers provide their usernames on the login page and tap the "login" button on their mobile phone. Nevis sends a push notification (a deep link for Mobile First) to the user's mobile phone. Once the message has been opened, the user can use the chosen biometric method for authentication. Once the process is complete, the Nevis Access App confirms the identity and the authentication is successful. The user is automatically logged in.

Passwordless authentication is a matter of a few seconds with most of that time needed to enter a username or email address. This occurs even faster if the browser completes the email address during the second registration.

Passwordless authentication improves the customer experience and boosts approval for mobile solutions. You significantly increase authentication security, reduce cases of fraud by up to 99%, cut costs thanks to fewer support requests, and reduce the burden of maintaining passwords on IT employees. The Nevis passwordless solution also comes without expensive SMS transaction fees.

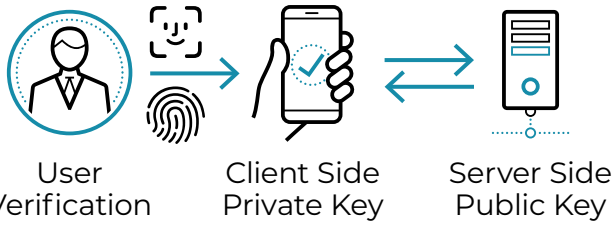
- faster, more practical, and safer than a password
- improved customer experience
- more approval for mobile solutions
- up to 99% fewer cases of fraud
- cut costs thanks to fewer support requests
- less burden on IT employees to maintain passwords
- no SMS transaction fees

Biometric Procedures

Thanks to a combination of possession ("something I have": smartphone) and biometrics ("something I am": face or fingerprint), biometric procedures meet the demands for strong 2-factor authentication. The level of security is similar to a password plus a second factor.

Added security with 2-factor authentication

Strong authentication uses at least two of three possible identification categories.



For biometric authentication, the interaction between biometrics, device, and server infrastructure works as follows: first, the user installs a so-called **access app** via the app store. Then the user connects his/her device to the account. This generates a **key pair**. The **private key** always remains on the smartphone and is stored in a specially designated chip set (**secure enclave** or **trusted execution environment**). These types of chip sets have long been in use (initially with e.g. Apple iPhone 5S or Samsung Galaxy S5).

Every time there is an authentication or transaction confirmation, a signature operation is performed on the smartphone using the private key. Biometrics are only used to unlock the private key, which is why the biometric information never leaves the smartphone.
The exchange of the key (device registration) as well as the use cases login, transaction confirmation, and device deregistration are performed in accordance with the standardized FIDO-UAF protocol.
The solution is easy to expand on: if smartphones offer additional biometric methods in the future, these can be integrated by updating the app without any major changes on the server side or to the processes.

Mobile Authentication

Mobile authentication is secure and seamless and is accomplished by having users verify their identities with the help of their mobile phones. Mobile authentication lets end users verify their identity and confirm transactions with a number of identification factors. Each factor is based on something the end user knows, has, or is: a secret, a specific device, or a fingerprint.

The combination of strong cryptography and standardized authentication schemes makes mobile authentication easy and secure for users. Protected credentials are only stored on the user's device. This protects both user privacy and companies from potential business threats like security breaches during login.

Mobile devices are increasingly becoming the primary or even sole channel for contacting companies.

Nevis provides customers with user-friendly, strong authentication on their mobile devices using a fingerprint or facial recognition as well as a PIN. This process is based on the FIDO standard.

There is a separate, secure chip on mobile devices for this purpose. It operates completely independently of the main chip on the device and is used exclusively to store and process biometric and cryptographic data and authentication requests. The data never leaves the device, cannot be manipulated, and is not even accessible to the authentication application (e.g. the access app). As such, users retain sole control over their biometric features.

During the registration of the mobile device as an authentication factor, the system generates a key pair consisting of a private and a public key. The private key components – protected with biometrics or a PIN – are stored in the aforementioned secure chip on the mobile device. The public key components are sent to Nevis. When the user logs in or is authenticated, Nevis can use the public key component to check whether the response to the authentication request was actually signed using the private key, which is only accessible to the authorized user.

Depending on the application, the authentication request for passwordless access is sent to the mobile device via a QR code, a deep link, or a push notification.

Nevis stores the user identity in compliance with GDPR during mobile authentication.

Transaction Confirmation

Transaction confirmation is an additional security measure, which is required for certain financial transactions and other especially sensitive activities. It is deployed when the user has to verify and confirm specific information in addition to authentication. Transaction confirmation makes it possible to securely and unequivocally confirm financial as well as operational transactions with just one click.

A push notification informs the user of a pending transaction. Then, all the necessary particulars about the transaction are displayed so the customer can review the details and make corrections if necessary before approval. Once the data has been verified, the transaction can be confirmed or rejected simply by scanning a fingerprint or face, or entering a PIN.

Transaction confirmation not only minimizes the risk of fraud, it also prevents human errors and typos.

So-called **friendly fraud**, where customers make unwarranted refund claims, is also prevented by transaction confirmation. Customers are also protected against phishing, social-engineering, and data-switching attacks. Common security problems, which SMS OTP providers have to contend with (e.g. SMS interception or SIM swapping), also pose no problems for mobile transaction confirmation.

In addition to increased customer security, adopting transaction confirmation also has significant **advantages for companies:** all transactions, whether confirmed or declined, are logged and archived in the background. When in doubt, this makes it possible to prove whether and when a transaction was approved or declined. This is especially practical with regard to compliance and auditing guidelines.

There is still the question of how to prove that the person who initiated the transaction is the right person. This problem can be solved either through biometric verification of the user or with a PIN, similar to authentication at login. As such, transaction confirmation functionality not only implements the “what you see is what you sign” principle, but also guarantees non-repudiation of confirmed transactions. The possible use cases are manifold:

- payment confirmation
- e-Commerce transactions
- granting GDPR consent[1]

1: The European Union (EU) General Data Protection Regulation has been in force since 25 May 2018.

Consent and Privacy Management

Consumers have become more sensitive when it comes to data protection. That's why more regulations on the protection of user data online have now been implemented around the world. The EU General Data Protection Regulation (GDPR) stipulates that consent for data usage (like with cookies) has to be obtained, documented, and managed. In addition, users should be clearly informed about what data is collected and how it is processed. **Companies have to adhere to the local guidelines on data storage and data retention.** That's why security functions have to be implemented, which guarantee the protection of user data.

Consent and privacy management help companies comply with these provisions and acquire user consent. Communication preferences and consent to legally binding agreements can be revised at any time.

Nevis offers an out-of-the-box and quick-to-integrate solution that lets users accept or decline the relevant terms and conditions by simply clicking a button. During this process, the system stores and verifies when the user has accepted which version. In addition, newsletter, marketing campaign, sales and product update emails, etc. preferences can be managed.

User Behaviour Analytics (Adaptive Authentication): Fraud and Suspicious Activity Recognition

User behavior analytics can be used to detect anomalies in user behavior in order to prevent and fend off unauthorized data access. It is possible to detect certain patterns in user behavior that indicate either normal or strange behavior.

User data must be tracked, collected, and evaluated in order to analyze user behavior. This data is generated when digital services are used and it can be processed by monitoring systems.

Information like location, device details, and the current time can be captured and analyzed as can typical user mannerisms like keystroke dynamics, taps, and mouse movements. These dynamic user identity aspects can be compared against earlier interactions in order to assess a risk. The effectiveness of these components is based on the fact that the correlation of multiple attributes, like behavior biometrics, geolocation, and device information, generate very distinct digital user footprints. Analysis already starts on the login page and continues until the end of the session.

Abnormal user behavior may indicate an attack. In response, security teams receive the information they need to act, if necessary. First, a risk threshold value based on the abnormal behavior is sent to the risk management system. The system can then prevent the suspicious transaction or verify its legitimacy through additional authentication (step-up).

Nevis lets you combine leading anomaly detection technologies on a single platform and deploy them as a centralized service for all applications.

Administrations Console/Management Console

Nevis provides a configuration, deployment, and monitoring solution that supports modern DevOps practices. As a result, organizations can deploy new capabilities faster while satisfying higher security requirements. Reusable configuration templates include best practices for common use cases. This reduces costs and improves productivity. Comprehensive validation of configuration modifications also facilitates continuous compliance with your organization's security policies and procedures.

The platform was developed with scalability and security for companies in mind. The modular architecture supports various deployment processes in order to meet the requirements of demanding IT environments. The access control functions include finely graduated permissions for projects and users.

Nevis thereby provides a "configuration generation engine" that validates and deploys configurations without human interaction.

Companies with unique infrastructures and integration challenges can expand on the basic templates to satisfy all business demands. This minimizes complexity and covers common application cases, which can also be easily adjusted.

Benefits:

- quickly configure and implement security best practices using reusable configuration templates
- test new configurations and infrastructure options separately thanks to the complete separation of configuration and infrastructure data
- revise, share, and review declarative configuration files with support for the "git version control system"
- validate configuration changes and review deployment plans prior to deployment to avoid unpleasant surprises in production
- accommodate your company's modus operandi
- flexible deployment processes thanks to the modular architecture
- integrate tools already in use through the "configuration generation engine"

How Nevis Helps Companies

Customer identity and access management with Nevis guarantees the level of security desired and increases your competitive advantage. Both browser-based and app-based login processes are supported. This lets you offer your customers the same level of convenience with maximum security on any device.

→ Modular, flexible, stable, secure.

What's the Advantage for End Customers?

Customers want to access online offers with minimal effort and maximum security. They expect innovative and exceptional experiences when it comes to customer identity, but also the highest standards for security, data protection, and compliance. Customers expect...

- a seamless experience across all channels
- intuitive, user-friendly, and secure digital access
- identity theft protection
- passwordless, split-second sign-up, as simple as unlocking a smartphone
- no additional devices or processes
- convenient transaction confirmation

How Do Companies Profit?

Companies have to earn customer trust and loyalty in order to tap new opportunities for growth and competitive advantage. It is crucial to assume a leading role in the digital ecosystem and meet today's demands for digital transformation. New offers have to be available quickly, and the costs should be kept to a minimum. Nevis ID gives you a number of advantages. Some highlights:

- significantly better usability thanks to the elimination of unnecessary steps
  - increased customer loyalty
  - increased willingness to pay premium prices
- available as an app with user-defined branding
- seamlessly integrates into existing infrastructures and is future-proof
- reduced market entry time for digital offers
- no ongoing SMS transaction fees thanks to passwordless access
- fewer aborted conversion processes with securer and simpler transaction confirmation (FIDO)
- comprehensive identity and access management helps you learn more about your customers while simultaneously supporting the implementation of regulatory demands for sensitive user data (GDPR, PSD2, GKV-SV (National Association of Statutory Health Insurance Funds) etc.)
- the combination of high-end security and ample user friendliness will contribute to an increase in customer interactions while fulfilling all regulatory requirements

What's the Advantage for the IT Department?

Without IT, digitalization innovation is hardly feasible. However, the requirements are manifold: a coherent security infrastructure must provide easy and secure access to online services, conform with legal directives and compliance, and generate as little maintenance and help desk effort as possible. Nevis ID offers maximum support for achieving these goals. It saves costs while simultaneously offering legal security:

- integrated into your IT environment in just a few steps
- out-of-the-box integration for Azure AD B2C and big e-commerce shops
- automated standard processes reduce help desk expenses
- available as an app with individualized branding and as a software development kit (SDK)
- data center either in the EU or Switzerland
- complies with all regulations regarding data protection, consent, and deletion like GDPR, PSD2, GKV-SV etc.
- FIDO-certification guarantees compliance with demanding security and interoperability requirements
- investment protection: the FIDO-based implementation facilitates rapid modification for future mobile device capabilities
- open architecture supports a broad range of standards
- Nevis grows with you, whether you need to handle larger volumes or incorporate new technologies

How Do Different Industries Benefit?

Companies across all industries have to face the challenge of their customers being online and mobile more and more frequently and for longer periods of time. If companies don't offer customers convenient and secure online access to their services, they will quickly switch to the competition.

Benefit from the Nevis ID platform. That way your customers can easily and safely conduct their online business with you around-the-clock and on-the-go. The Nevis ID platform offers your customers:

- around-the-clock access
- on-the-go access
- passwordless access
- secure access

The broad range of functions and the scalability of the Nevis ID platform facilitate the execution of a broad variety of demands. For example, all industries benefit from identity and access management solutions for their portals and the manifold self-service processes.

Every industry is unique and has its own challenges. The Nevis ID platform offers solutions for your industry's specific issues and will distinguish you from the competition.

Industry	Problem	Solution	Benefit
Financial Services and Banking	complicated account access via external tool	passwordless login app	increased user interactions
	identity theft	approve transactions biometrically	maintain customer trust good reputation
	regulatory compliance	2FA with passwordless transaction confirmation (FIDO standard)	PSD2 and GDPR compliant
	fraud prevention and detection are not user-friendly complex and costly	ongoing, risk-based user authentication using a combination of anomaly detection technologies	more customer-friendly since additional authentication (step-up) is only required when necessary reduced manual effort for fraud department lower costs and losses
	complex account administration	extensive self-services	customers are able to reset passwords themselves, helpdesk is relieved
	complex administration for business clients	delegated identity administration for business clients	business clients are empowered to perform recurring operations independently less idle time and support effort

Industry	Problem	Solution	Benefit
Government	over-the-counter business is time consuming	online businesses secured via transaction confirmation, also for document confirmation 2FA for all businesses	faster processes secured transactions time, effort, and cost savings increased customer-friendliness and reputational gains
	traditional document signature cannot be uniquely assigned to a single person	only biometrically authenticated transactions are executed	secured transactions time, effort, and cost savings increased customer-friendliness and reputational gains
	documents have to be sent by registered mail or delivered in person	integration of SwissID or other recognized electronic identities for authentication purposes	documents can be transmitted online, encrypted and legally valid time and money savings for citizens and authorities environmentally friendly
	conducting interagency business is complicated	multi-tenant security platform for national-level operations	secure exchange of information across agencies and agency levels
	complex administration for business clients	delegated identity administration for business clients e-government services in company environment	business clients are empowered to perform recurring operations independently less idle time and support effort
	risk that normal safety measures are not sufficient	high-security IAM solutions for applications with increased security requirements (e.g. judicial and police systems)	significantly reduced cyber-security risk at the technical level

Industry	Problem	Solution	Benefit
Insurance	complicated access to insurance portal	passwordless authentication	increased user interactions
	management of customer accounts is complex	effective management of customer accounts thanks to extensive self-services as well as optional social logins (Facebook, Google etc.)	lower helpdesk and supports costs increased customer satisfactions thanks to an improved user experience
	uploading sensitive information is tricky	passwordless, biometric 2FA	compliance/data security
	risk that normal safety measures are not sufficient	adaptive protective mechanisms for applications and price calculator	significantly reduced cyber-security risk at the technical level improved user experience since additional authentication (step-up) is only required when necessary
	communication and data exchange with insurance brokers is complicated and not secure	integration of insurance brokers via identity federation (e.g. IG B2B in Switzerland, EasyLogin in Germany)	increased efficiency, security, and user experience when dealing with insurance brokers
	complex administration for business clients	delegated identity administration for business clients	business clients are empowered to perform recurring operations independently less idle time and support effort

Industry	Problem	Solution	Benefit
ICM and Engineering	access to industry portal is insecure and complicated	passwordless, biometric 2FA	protection of intellectual property, time-saver for partners, retailers etc. no more SMS fees
	complex account administration	self-services for end users (e.g. self-registration, "forgot password" function)	customers are able to reset passwords themselves, helpdesk is relieved
	risk that normal safety measures are not sufficient and additional measures detract from the customer experience	support for various authentication mechanisms tailored to security requirements	tailored security and maximum customer experience since additional authentication (step-up) is only required when necessary
	complex administration for business partners and specialist departments	delegated user administration for business partners and specialist departments	business partners and specialist departments are empowered to perform recurring operations independently less idle time and support effort
	different data silos complicate reconciliation and authorization management	connection to the ERP system, bi-directional reconciliation of master data and authorization information	effective reconciliation of master data and authorization information
	customers and employees waste time with separate logins for different systems	cross-organizational single sign-on across different applications and shop systems using identity federation	once logged in, customers and employees have access to all applications and systems effective implementation of the solution
	order processes are not sufficiently automated	integration of special devices (e.g. barcode scanners) for automatic ordering processes	more effective ordering processes with reduced costs
	IoT can not be well integrated	IoT integration	easy IoT integration

Industry	Problem	Solution	Benefit
Healthcare	access to e-health portal is complicated	passwordless, biometric 2FA	time-saver for customers no more SMS fees
	no control over who gains access to personal data	confirmation of access for third parties transaction confirmation as needed	control for patients lower support effort and costs for providers shorter paths, quicker decisions added trust
	security level of authentication with a username and password is insufficient	support for various authentication tools: mTAN, SuisseID, HPC Card, Soft Certs, etc.	sensitive data is better protected easy integration of different authentication tools into the existing system
	patients, customers, and employees waste time with separate logins for different systems	single sign-on for web applications and additional services for secure data exchange	once logged in, customers and employees have access to all applications and systems
E-Commerce	shop login is complicated i.e. username and password are often not readily available	passwordless login	fewer aborted transactions and higher turnover
	SMS messages incur costs	passwordless confirmation	no more SMS transaction costs
	integration of security mechanisms is complicated	use shopware plugin[1]	quick integration of convenient improved security
Gambling operators	family members with login data can access player's account	biometric, passwordless authentication	compliance: access is protected and only available to authorized players
	stakes not secured	transaction confirmation	sensitive transactions are secure player is safeguarded

1: Only works with "shopware" systems.

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

Your Nevis partner: