



Solution Paper

Nevis Authentication Cloud



Making security an experience.

Content

3 Introduction

- 3 The Digital Revolution

5 Customers Want More Convenience and Security

- 5 Are Customer Experience and IT Security Contradicting Paradigms?
- 7 What Do End Customers Want, How Do Providers Benefit?

9 Authentication

- 9 What Is Multi-Factor Authentication?
- 9 Username and Password – Outdated?
- 10 2FA – 2-Factor Authentication
- 10 2FA Passwordless
- 11 FIDO (Fast Identity Online) – The Standard for Passwordless Authentication

11 What Can the Authentication Cloud Do?

- 11 Nevis Authentication Cloud
- 12 Passwordless Authentication
- 13 Transaction Confirmation
- 14 Branded Access App
- 16 Management Console
- 16 FIDO and Nevis

17 How Nevis Helps Companies

- 17 How Do End Customers Benefit?
- 17 What Is the Advantage for Businesses?
- 18 What is the Advantage for IT?

19 How Do Industries Benefit?

Introduction

The Digital Revolution

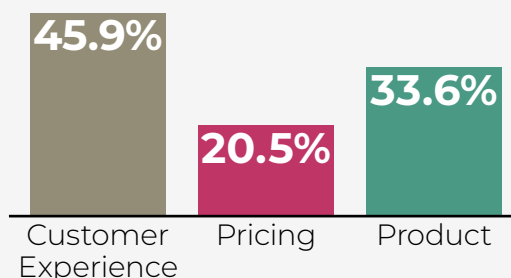
How often do we use digital devices? How much time a day do we spend connected to the online world? Step counters, sleep monitors, online meetings, social media, shopping, banking, household technology. Whatever you want, it's now available online. Digitalization is omnipresent. And that's not all. We're in the midst of a digital revolution. One which will usher in a transformation more massive than the Industrial Revolution. While technological innovations once resulted in disruptive changes to a few industries, digitalization is now changing the world as a whole.

We need to rally customers in this digitalized world and convince them with great services. They are the ones steering the market and making demands. If they're not satisfied, the next provider is only a click away. Providers who don't keep pace, go under. Every day. Never before have Fortune 500 companies disappeared as quickly as they do today. Experts at MIT and Deloitte anticipate that 40% of today's Fortune 500 companies won't exist by 2025 because they won't be able to adapt quickly enough.

But how can you digitally rally potential and existing customers to choose a brand and remain loyal? Having the most innovative product or offering a good service is no longer enough to differentiate your company. It's the customer experience that sets you apart! According to a study by Walker¹, customer service surpassed price and product as the most important key brand differentiator in 2020. That not only sounds plausible, it also

pays off. According to a study by the Temkin Group², 86% of customers who assessed their experiences with a company positively shopped with the company again. By comparison: one in every five consumers avoids a brand after just one negative experience. The key takeaway: access to online services must be designed as conveniently and securely as possible. The digital customer experience (DCX) can't leave anything to be desired. When it comes to security, it's even more clear cut. Customers expect the highest possible level of security whenever personal data is being stored and logins are being managed. The security package is the bare minimum, so to speak, to be in the game. In order to win, it's the customer experience that counts. This is one reason why best-of-breed companies place their strategic focus on this area.

What is the top priority for your business in the next 5 years?¹



¹: Customers 2020: A Progress Report, 2020, Walker
²: ROI of Customer Experience, 2018, Temkin Group

Passwords outdated?

Whether they're online shopping, on social media, or online banking, users have to log in. Over and over. According to a study by Gartner, one person has an average of 130 different user accounts. And most of these accounts are only protected with a username and password.

Passwords are impractical

On average, people have to enter passwords eight times a day for ten different online accounts or apps that they regularly use every week¹. The plethora of passwords, which end users have to remember to access a growing number of online services is overwhelming. Users spend an average of ca. 12 days of their lives just looking for or resetting passwords².

But it's not just users wasting time during registration and authentication processes. Providers across all industries are equally affected, and they're also losing money. That's because forgotten usernames and passwords along with laborious registration processes or insufficient security for various transactions lead to ca. one-third of online processes being aborted³. The following situations can result in added expenses, loss of revenue, and added effort:

- Not checking out a full shopping cart
- A subscription upgrade can't be booked
- E-Banking users reach for the phone instead of looking for information online or resetting their passwords themselves
- Insurance claims are processed on paper instead of electronically and users turn to the competition for supplementary insurance
- More counters have to be staffed than necessary for bureaucratic procedures

66% “A frustrating experience on a website hurts my opinion of the brand overall”

Source: *SilverCloud*

Passwords are insecure

Passwords not only detract from the customer experience, they also cause major security issues. They are often the reason behind data breaches. According to Verizon Data Breach Investigations Report 2019⁴, compromised and weak registration data was the reason for 80% of breaches associated with hacking. And 29% of all breaches, independent of the type of attack, were caused by the use of stolen registration data.

1: *A Large-Scale Study of Web Password Habits*

2: *Openwave Mobility Research*

3: *TNS Research by order of VeriSign, Inc.*

4: *World Economic Forum - Passwordless Authentication: The Next Breakthrough in Secure Digital Transformation, S. 5*

Conventional password practices are little help. On the contrary: users have picked up some bad habits over time. Anyone who's had to enter a complex password on their mobile device knows. It's so tedious that people make risky compromises and use short passwords or the same ones over and over again. Users have become demonstrably more reckless with passwords. The analysis of half a billion cracked accounts showed that few passwords contain more than eight to ten characters. Less than 6% of passwords contain capital letters or symbols¹. That makes them extremely vulnerable to brute force attacks. That's because it's much easier for hackers to simply try out short passwords.

It's easy for criminals to get a hold of usernames and passwords through brute force attacks like phishing and other social hacking techniques. Alarming: a study conducted in early June 2020 revealed that two-thirds of those surveyed who knew that their passwords had been cracked had still not changed them three months later².

In conclusion: it's no longer sustainable for passwords to be the primary authentication solution for end customers. Integrating additional authentication factors or completely foregoing passwords, as Nevis does with its passwordless Mobile Authentication Solution, is advisable. We rely on biometric-based multi-factor authentication (MFA) to optimize security and the customer experience.

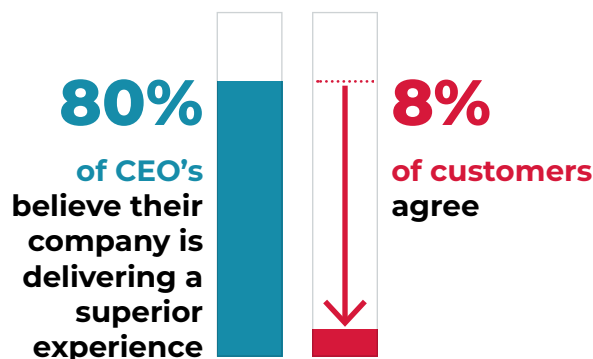
Customers Want More Convenience and Security

Are Customer Experience and IT Security Contradicting Paradigms?

User experience and security are important criteria to counterbalance if you want to attract and retain customers. Unfortunately, the paradigm still holds: increasing security often detracts from the user experience. And vice-versa: an amazing user experience can't be secure. Does user demand for simple, fast, and straightforward online access have to take a back seat to security and compliance?

Providers across a broad range of industries are unaware of the gap between customer expectations and the actual customer experience.

The Experience Gap



Bain & Company via Craig McVoy, CCXP

1: [Duo Labs Security Analysis](#)

2: [Study from the Security and Privacy Institute - Carnegie Mellon University](#)

27%

Nearly a third of consumers believe that their experiences with brands have gotten worse, not better, over time.

Source: Experience Gap Report 2018, clearstrategy.com

Outdated Multi-Factor Authentication (MFA) vs. Biometrics

Security is an ongoing development process, a constant cat and mouse game between attackers and defenders. The attackers are in a position to ascertain, steal, or remove passwords with brute force. As such, the solution should be a combination of multiple factors for identifying the user: multi-factor authentication.

However, studies published over the past few years have highlighted problems with outdated MFA methods¹. They're not user-friendly enough. Examples cited include the manual entry of a dynamic password and the use of additional devices (hardware tokens) to create one-time passwords (OTP). Weak points include: not easy to manage, not easy to integrate into daily life, not mobile. These MFA mechanisms are often used for applications requiring extensive security, like online banking.

62%

would switch brands if they felt that they would have a better experience elsewhere.

Since customers leave the necessary additional device at home for safekeeping, the ability to use it anytime and anywhere is significantly restricted. This, in turn, limits the opportunities to interact with the bank.

Modern multi-factor authentication uses biometrics. Biometric identification technologies built into today's mobile devices facilitate completely new approaches to authentication. This trend is also being fueled by new standards like, e.g., FIDO (Fast IDentity Online). **Gartner recommends providers make the issue of passwordless authentication a top priority.** Replacing passwords with biometric authentication can improve user friendliness as well as security – an effect not often observed with security and IAM tools². For the first time ever, it's possible for security and user friendliness to go hand in hand!

Just how successful this can be is evidenced by long-time Nevis client PostFinance:



PostFinance

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

Eric Müller
Lead Solutions Architect
PostFinance

1: World Economic Forum - Passwordless Authentication: *The Next Breakthrough in Secure Digital Transformation*, S. 5

2: Gartner: 2020 Planning Guide for Identity and Access Management

What Do End Customers Want, How Do Providers Benefit?

End customer trust in digital channels should be consistently reinforced. It is especially important to provide added protection for “everything associated with money, high value, the health sector, and privacy¹”.

Whether an end customer logs in via a browser or a smartphone or a digital kiosk² registration should be easy and also – regardless of the end device selected – facilitate transactions that are as streamlined and seamless as possible.

Nowadays, providers are focused on new customer expectations when it comes to authentication: fast, straightforward, accessible from everywhere, accomplished without the annoyance of typing in passwords, possible without additional devices, always available.

Nothing is better equipped for the task than a smartphone. There are an estimated 3.5 billion smartphones worldwide (more than

toothbrushes). Users spend an average of nearly three hours a day on their smartphones and have more than 2600 interactions (typing, swiping, pushing). **The smartphone is an integral part of our lives**, a device that we always have with us, wherever we are, always at hand, easy to use, and very personal.

These mobile devices have separate, closed, protected areas: security chips. They are physically detached from the main chip and contain cryptographic material (so-called private keys³). The cryptographic material can only be obtained by using biometrics to access it. So even when a device is lost, its security chip is protected against manipulation and the private keys cannot be stolen.

The smartphone has secure biometric input options, which are ideal for replacing passwords. The biometric information never leaves the device. This makes it possible for us to use the security chip as the perfect tool for authenticating customers online both securely and safely.

1: *Prof. Christoph Meinel, Director of the Hasso-Plattner-Institut (HPI)*

2: *The digital kiosk, or thin client, is e.g. a workstation for inputting medical data, a check-in counter, a self-service station, or an information terminal with public access.*

3: *A private key lets its holder decrypt data encrypted with the public key, generate digital signatures, or authenticate him or herself.*

1. Users have grown accustomed to biometric input on smartphones and tablets. Over 80% already use their finger or face to unlock their devices¹. Furthermore, the technology has since become ubiquitous and is available on most devices. Studies show that users also desire this positive, simple alternative for authentication.
2. Users don't want to enter passwords on their mobile phones. We all know how inconvenient it is to type a long message on-the-go, for example on the way home after a long day at work. Numerous studies show how bad passwords are. A study by the University of Munich investigated how we use passwords on our smartphones. It determined that users opt for even shorter and easier passwords than on their desktop computers². That means that passwords created on smartphones are even easier to crack.
3. Nowadays, additional devices or processes, like RSA tokens, smartcard readers, USB keys, SMS or the like, are used for secure transactions, especially in banking or healthcare. However, these can rarely if ever be combined on a smartphone – and SMS is no longer recommended for security reasons. A study also indicates that one-third of participants do not have their hardware token available when needed.
4. Users have to be offered a passwordless experience for the “mobile first” world in which we're currently operating. A study conducted by Mastercard reveals that almost every second person in Germany will abort a process if their password isn't readily available³.

A modern authentication system is not only necessary for security reasons, it is also the most important tool for digitalization. It facilitates unlimited mobility, reduces frictional losses, and improves the customer experience. It increases operational efficiency and guarantees improved compliance with regulations. We help you accomplish all these tasks outside of your core business scope as efficiently as possible. Because if you ignore your customers' need for convenience and security, you'll lose them to the competition and fail to attract new ones.

.....
1: *Google survey of 1'000 customers*

2: *Manuel von Zezschwitz, Alexander De Luca and Heinrich Hussmann: „2014. Honey, I shrunk the keys...”*

3: *Mastercard-Study*
.....

Authentication

What Is Multi-Factor Authentication?

Multi-factor authentication (MFA) is a security mechanism, which authenticates people based on more than one required security and validation process. The most important means of identification are based on the principles of knowing, having, and being. Beyond that, both location and time serve as verification attributes and can be consulted as additional factors.

The combination of these identification factors reliably ensures that the person who wants to access confidential data is really the person he/she claims to be:

- **have** – possession of a device (mobile phone, debit card etc.)
- **know** – a password, security question, PIN
- **be** – biometric features (fingerprint, face ID, iris pattern)

Additional factors used to verify identity and uncover fraud attempts (adaptive MFA), especially in the finance sector, are:

- **location** – specific IP address
- **time** – compared to the previous or usual sessions

Two-factor authentication (2FA) is familiar to most users as a version of MFA, even if the term is not that common. For years we've been using 2FA to withdraw money at ATMs: only when our debit card is used (something we possess) and the correct pin code is entered (something we know) can the transaction be completed.

The market offers a number of different alternatives for authentication. And depending on the application case, the second factor selected can be quite different. There are countless devices and solutions that can be used for two-factor authentication: from tokens to one-time passwords (OTP) via SMS and RFID cards to smartphone apps or mobile IDs.

However, most of these methods have their disadvantages:

- media interruption
- additional hardware
- delayed delivery / emails not trustworthy (spam)
- no direct connection to the company
→ loss of trust
- cost factors

Username and Password – Outdated?

Whether for online shopping, social media channels, or online banking, usernames and passwords are frequently used to legitimize, i.e., verify identity. Though this so-called one-factor authentication is based on a combination of two features – 1. username and 2. password – both features belong to the same factor – the knowledge factor.

Simple implementation and affordability are the most important reasons why passwords are still the most common form of one-factor authentication. However, this doesn't justify them. Should a password fall into the wrong hands, it can have serious consequences. Cybercriminals can purchase goods, prey on online accounts, and use fake identities to abuse chats for their personal gain. Consequently, those who simply entrust system access to a username and password are not especially secure. Nowadays, even a carefully selected password alone can no longer be classified as secure.

On top of that is the fact that one factor is no longer compliant with regulatory demands depending on the industry or business process in question. Two features based on knowledge (username and password) are not enough. Multi-factor authentication is urgently needed. This plays an especially decisive role when it comes to protecting social data and monetary transactions.

2FA – 2-Factor Authentication

The authentication process for 2-factor authentication generally starts with the entering of a secure password – the first factor. Should the system confirm that the password submitted is correct, the user is not directed to the desired content but rather to an additional security gate – the second factor. This helps prevent someone with unauthorized access to the password from gaining access to data or other functions. However, 2FA also works without a password.

2FA Passwordless

As mentioned above, the second factor may require an additional device (possession). However, unlike a smartphone, this device might not always be available. Alternatively, passwordless authentication with a biometric feature (be) offers a simple and secure form of identification and uses this second factor to answer the question: "Who are you?". Passwordless authentication is geared towards collecting biometric data (a set of fingerprints, a face, or an iris pattern), which can be used to clearly and unequivocally identify a person. During the authentication process, these biometric features are captured with the help of biometric sensors and then compared to the data already stored on the device. Should the scanned data match the stored data, it is authenticated.

Attracting and retaining customers through an optimized combination of user friendliness and security is contingent on the development of a long-term security strategy. Saying goodbye to purely knowledge-based authentication for this process is long overdue.

Passwordless authentication offers four different advantages compared to traditional knowledge-based authentication:

- **efficiency:** it increases revenue and sinks costs (e.g., no more SMS fees)
- **improved user experience:** secure login and shopping without obstacles
- **strategic competitive advantage:** increased interoperability thanks to FIDO standard
- **optimized security¹**

FIDO (Fast Identity Online) – The Standard for Passwordless Authentication

FIDO is the largest global ecosystem for standard-based, interoperable authentication with the goal of solving the world's password problem. The FIDO standard is an open industry standard for secure, fast, and simple authentication online. It gives companies an opportunity to install hardware-supported authentication like fingerprint or facial recognition in their products. This allows product users to register for online services with ease and without having to remember complicated passwords.

What Can the Authentication Cloud Do?

Nevis Authentication Cloud

Authentication indicates that the digital identity of a user has been detected, and it has been verified that the person actually is who he/she claims to be. In the context of online services, Nevis can use this authentication to guarantee that the person who logs on is also the person who created the online account – and not, for example, a bot using a brute force attack (by attempting innumerable passwords) to attempt to penetrate an account.

It's common for a user to choose a password when first registering an account. Alternatively, the Nevis Access App can be used for authentication when setting up an account. Users fill out the standard registration form, but the account is connected to the Nevis Access App in the process (e.g., by scanning a QR code). With biometrics, the system accesses the security chip on the smartphone and creates a link to the account. At this point, the user can completely forego passwords.

The Nevis Authentication Cloud...

...expands your infrastructure with passwordless authentication and transaction signatures as a service. Our FIDO-certified solution offers the authentication experience today's end customers expect. Your customers can log in without a password. And since they only need their mobile phone with its security chip, the process is more convenient and reliable. This multi-factor method is far more secure than

¹: World Economic Forum - Passwordless Authentication: *The next breakthrough in secure digital transformation*, S. 13

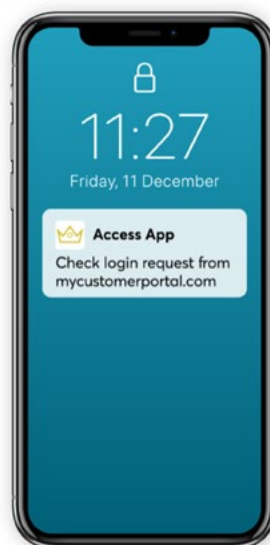
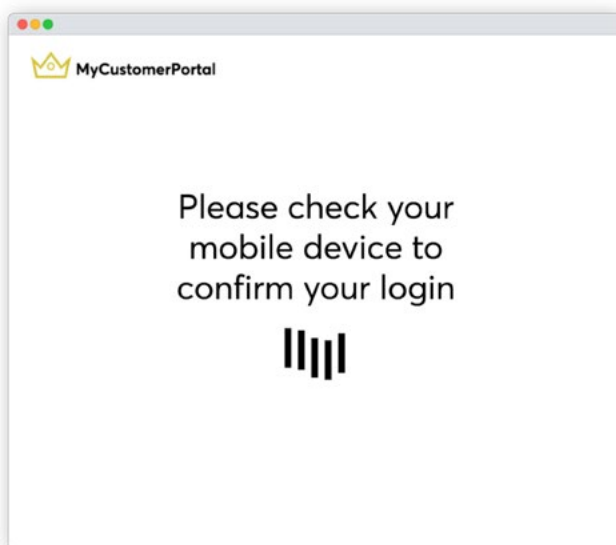
old password-based solutions. With the most modern server technology, the system can also be used for particularly sensitive transaction confirmation applications.

Nevis offers a passwordless login experience, which relies on the biometric authentication options of modern smartphones. The underlying technology based on the established FIDO standard guarantees interoperability and long-term investment protection. As a member of the FIDO Alliance, Nevis is strongly committed to supporting current and future FIDO standards. With its certified FIDO implementation, Nevis guarantees compliance with the demanding security and interoperability demands of FIDO security standards. Nevis' mobile authentication solution is available as an SaaS (Software-as-a-Service) offer or on-premise.

Passwordless Authentication

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.

This future scenario is characterized by maximum user friendliness: your customers enter their username on a registration page and click on the "sign in" button on their mobile device. The Nevis Authentication Cloud entity sends a push message (a deep link for mobile first) to the user's mobile phone. After opening the message, the user can authenticate him/herself with the selected biometric method. Once the process is complete, the Nevis Access App confirms the user's identity, and the authentication is successful. The user is logged in automatically.



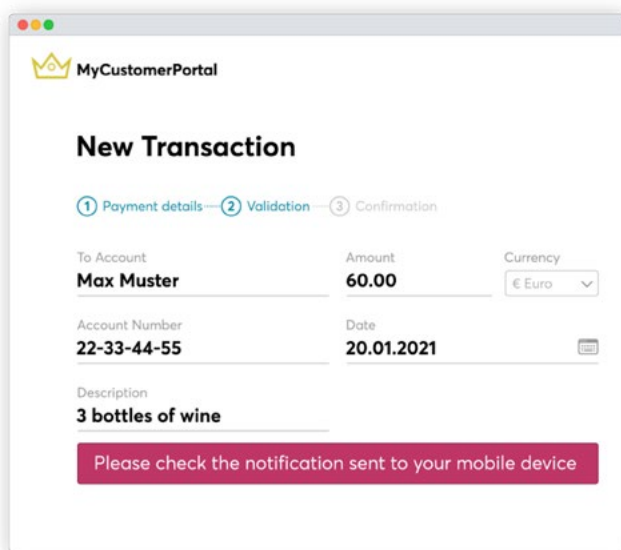
Transaction Confirmation

The transaction confirmation is an additional security measure required for financial transactions and information updates. It is used when the user has to review and confirm certain information in addition to authentication. The transaction confirmation makes it possible to unequivocally and securely confirm both financial and operational transactions with just one click.

A push message informs the user of the pending transaction. Subsequently, all the necessary transaction details are displayed so that the customer can look through the details and make any necessary corrections before approving the transaction. After reviewing the data, the transaction can either be confirmed or aborted by a simple fingerprint or facial scan or entering a PIN.

Transaction confirmation not only increases protection against potential fraudulent attacks, it also prevents human error and typos.

In addition to added customer security, transaction confirmation also offers companies significant advantages. All transactions, confirmed or aborted, are logged and archived. When in doubt, this makes it possible to prove whether and when a transaction was approved or rejected. This is especially practical when it comes to adhering to compliance and auditing guidelines.



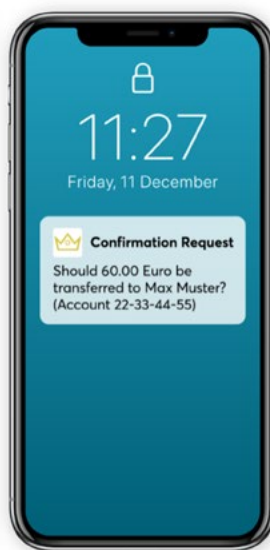
The screenshot shows a web browser window with the title 'MyCustomerPortal'. The main heading is 'New Transaction'. Below it, there are three steps: '1 Payment details', '2 Validation', and '3 Confirmation'. The 'Payment details' step is active. The form contains the following fields:

To Account	Amount	Currency
Max Muster	60.00	€ Euro

Account Number	Date
22-33-44-55	20.01.2021

Description
3 bottles of wine

Please check the notification sent to your mobile device



Transaction confirmation also prevents so-called friendly fraud, when customers falsely submit refund requests. Furthermore, customers are protected against phishing, social engineering, and data-switching attacks. And well-known security problems facing SMS/OTP providers (e.g., intercepting SMS or SIM swapping) do not pose a problem for mobile transaction confirmation.

The only question remaining is how to prove that the person who initiated the transaction is the correct person. This problem can also be resolved through biometric verification of the user, much like login authentication. The transaction signature function not only deploys the “What you see is what you sign” principle, it also guarantees the non-repudiation of confirmed transactions. The potential application cases are nearly endless:

- payment confirmation
- e-Commerce transactions
- granting of GDPR¹ consent
- Confirmation of ZertES-compliant document signature processes and much more

Branded Access App

Building a successful brand can take years. The goal is to achieve the desired brand perception from customers, create trust and loyalty, generate positive emotions, and simultaneously distinguish yourself from the competition. That includes appealing to customers with consistent brand performance regardless of channel or end device. Both the core message as well as visual brand identity elements should always be visible to customers in one form or another.

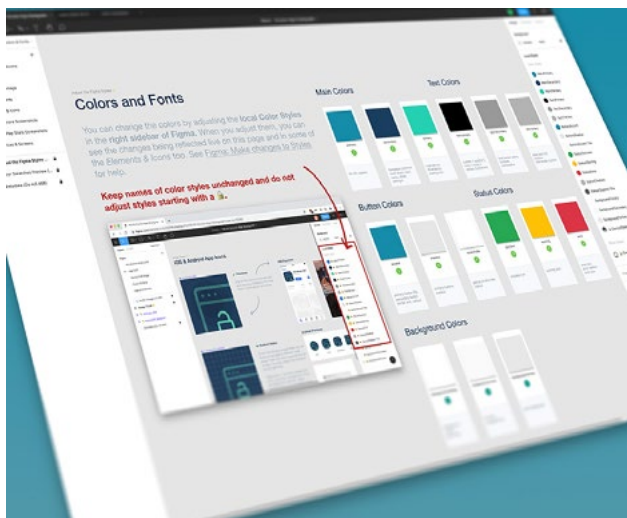
Your brand has to convey trust. The trust you earn from your customers. That is why we have branded our Access App according to your specifications. With no programming effort, it can be customized with your logo, your colors, and the font of your choice. This uniform appearance helps you gain the trust you desire from your customers. The app's security features will help you solidify this trust.

What's more is that you significantly distinguish yourself from the competition if the Access App communicates your corporate identity and is branded with your design. This gives your users the certainty they need that their data and accounts are safe in your hands. After all, who would want to authenticate themselves using a nameless, unfamiliar app that is not clearly associated with the brand in question or the affiliated company?

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

Since you don't have to make any compromises when it comes to your brand identity or the customer experience and security, you can design our Access App completely in line with your visual and communications requirements: our app is completely "brandable". But what does that mean exactly?

"Completely brandable" means that every detail of the app can be flexibly adjusted to your preferences and corporate design: colors, fonts, text, images, icons, and background. You can even choose the language used to display messages and content in the app.



Isn't it amazing to have so many options for individually branding and designing the Access App? However, unlimited design freedom often means investing a lot of time configuring before you have any initial results to show for it. That's why we created a Figma template of the app for you, which lets you adjust the app screen with just a few clicks. With the helpful preview function, you can

put each individual app screen through its paces before releasing your app in the Apple app store or on Google Play.

There is also the added option to upload user-defined icons, create app backgrounds, and freely determine what texts and messages are displayed in the app for companies with very demanding CI/CD requirements. The only thing you can't change in the Nevis Access App is the layout and the shape of the individual fields as well as the number of screens in the app.

The most important features of the Nevis Access App:

- White label mobile app, completely brandable
- Mobile SDK (integrated into the existing business application)
- Complies with industry standards and is FIDO-certified
- Conforms with GDPR, SCA¹, PSD2², and other regulations
- Passwordless (implied MFA)
- Biometric authentication
- The application is hardened and end-to-end encrypted

1: Strong Customer Authentication (SCA) offers an additional level of security when customers perform online transactions.

2: The second payment service directive from 2015 (Payment Services Directive, PSD2) regulates EU payment services.

In addition to a brandable white label Access App, we offer you the option to integrate our Authentication Cloud into your native mobile app using a software development kit (SDK) certified according to FIDO UAF 1.1. The SDK is especially useful for companies that already have a native mobile app for their customers or are in the process of developing one.

Whether you incorporate our brandable white label Access App or the Authentication Cloud SDK in your native App plays no role for your customers. Both options signal that security and convenience are your top priority and that you make no compromises when it comes to either.

Management Console

The Nevis Authentication Cloud Management Console gives system administrators all the necessary tools to manage your integrated apps and customize branding of the white label app. It also lets you view, modify, or delete all user accounts.

The console affords comfortable options for integrating new web applications – both for tailored applications and existing Nevis Security Suite entities. You can also use the console to manage access tokens, which the applications use for login approvals and transaction signatures.

The console also offers a simple to operate interface for user and device administration. Admins have the option to search by user and device in order to remove inactive users and outdated authenticators (i.e., old phones) from the system.

Furthermore, companies can use the console to brand and customize their white label app. As a result, the app can subsequently be released in the Apple and Google app stores without any programming hassle.

FIDO and Nevis



Mobile devices are increasingly becoming the primary and even only channel for contacting companies. Nevis gives customers user-friendly and strong authentication on their mobile devices with fingerprint and facial recognition and in accordance with FIDO standards.

For this purpose, mobile devices have a separate and secure chip, which operates completely independently of other device components. It is exclusively used to store and process biometric data and authentication requests. The data never leaves the device, can not be manipulated, and is not even accessible to authentication apps (i.e., your Access App). Users maintain sole control over their biometric features.

During the registration process, the information flow extends in the background to the Nevis Authentication Cloud entity, where the user identity is stored in a GDPR-compliant manner and a user-specific QR code or deep link is generated. The Nevis Access Application reads this code and subsequently authenticates the user using his/her stored biometric features. In this way, private cryptographic keys on the device's security chip are paired with the public key on the server to facilitate passwordless registration.

How Nevis Helps Companies

How Do End Customers Benefit?

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 registration, as simple as unlocking a smartphone
- no additional devices or processes
- convenient transaction confirmation

What Is the Advantage for Businesses?

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. You gain all these advantages with the Authentication Cloud. Some highlights:

- Significantly better usability thanks to the elimination of unnecessary steps
 - increases customer loyalty
 - increases willingness to pay premium prices
- Lower TCO (total cost of ownership) since it can be integrated into your IT environment in just a few steps
- Available as an app with user-defined branding or integratable in existing app with SDK
- Combination of high-end security and ample user friendliness will contribute to an increase in customer interactions while fulfilling all regulatory requirements
- Reduced market entry time for digital offers
- More customer interactions without added SMS expenses
- Fewer aborted conversion processes with secure and simple transaction confirmation (FIDO)
- Secure and intuitive online business thanks to PSD2, SCA, and GDPR-compliant transaction signature
- Investment protection: the FIDO-based implementation facilitates rapid modification to future mobile device capabilities
- FIDO certification guarantees compliance with demanding security and interoperability requirements.

What is the Advantage for IT?

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. The Authentication Cloud 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 with no additional infrastructure investment
- Out-of-the-box integration for Azure AD B2C
- Quick integration using widget in e-Commerce shops, portals etc.
- 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 (National Association of Statutory Health Insurance Funds), etc.
- FIDO-certification guarantees compliance with demanding security and interoperability requirements

How Do 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.

Apply the Nevis Authentication Cloud. That way your customers can easily and safely conduct their online business with you around-the-clock and on-the-go. The Nevis Authentication Cloud offers your customers:

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

A good customer experience will increase interactions. Since the Authentication Cloud works without SMS, your return on investment (ROI) is often already achieved after just one month.

Every industry is unique and has its own challenges. The Nevis Authentication Cloud offers the solutions for your industry's specific issues and will improve your competitive edge:

Industry	Problem	Solution	Advantage
Financial Services and Banking	complicated account access via external tool	passwordless login app	increased user interactions
	identity theft	passwordless login app: approve transactions biometrically	maintain customer trust good reputation
	regulatory compliance	2FA with passwordless transaction confirmation (FIDO standard)	PSD2 and GDPR compliant
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
Insurance	complicated access to insurance portal	passwordless login app	increased user interactions
	email communication with customers is inconvenient	push notifications via login app	increased user interactions
	uploading sensitive information is delicate	passwordless, biometric 2FA	compliance/data security
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
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 processes, quicker decisions added trust

Industry	Problem	Solution	Advantage
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.



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

© 2024 Nevis Security AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of Nevis Security AG. The information contained herein may be changed without prior notice. Some software products marketed by Nevis Security AG contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by Nevis Security AG for informational purposes only, without representation or warranty of any kind, and Nevis Security AG shall not be liable for errors or omissions with respect to the materials. The only warranties for Nevis Security AG products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, Nevis Security AG has no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein.

This document, or any related presentation, and strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by Nevis Security AG at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.