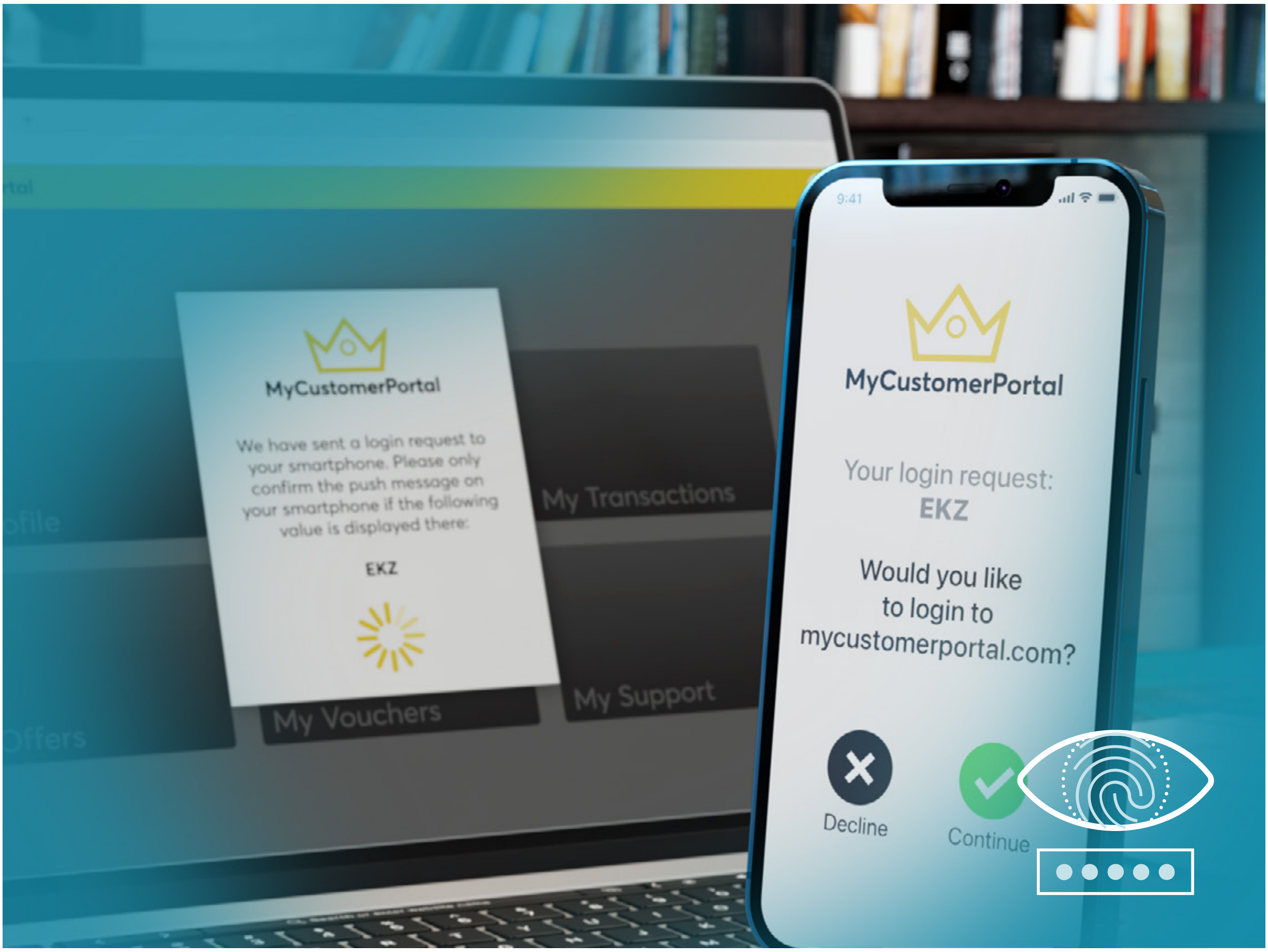
Making security an experience

White Paper

Decisive factor for more security: Multi-factor authentication

How multi-factor authentication in CIAM solutions enhances the customer experience



MyCustomerPortal

We have sent a login request to your smartphone. Please only confirm the push message on your smartphone if the following value is displayed there:

EKZ

Your login request:
EKZ

Would you like to login to mycustomerportal.com?

The majority of customers are very concerned about the security of their data on the Internet. A simple but very efficient measure for more data protection is multi-factor authentication. But what exactly is behind it? And how can increased security through multi-factor authentication be perfectly harmonised with user convenience for a good customer experience? You will find the answers to these questions in this white paper.

Content

Foreword

Shopping, transferring money, taking out insurance and so on and so forth – nowadays we all do countless things online. This usually calls for an online account and log-in information. And for the same reason, sensitive data is stored on countless servers. In view of the renewed **dramatic increase in cyberattacks in Europe**, it is not surprising that users are increasingly concerned about their data.

Phishing or brute force attacks are just some of the tricks that criminals use to try to compromise user accounts. Multi-factor authentication (MFA) offers an additional layer of protection against this. But as with any measure you take to increase the security of your customers' data, you shouldn't forget about MFA: Better protection must not come at the expense of the customer experience. After all, customers are not employees who are obliged to accept additional security measures. If they feel that their user experience is suffering as a result, they are sure to switch to another provider offering a higher level of convenience.

That makes it important to implement MFA in a way that balances data security and user-friendliness. In modern customer identity and access management solutions, the use of MFA as a security layer is taken as read. At the same time, it is possible to combine MFA with passwordless identification measures, which not only offers another layer of security is added but also streamlines the login process. On the following pages, we will explain in detail how MFA works and how it can be perfectly adapted to the requirements of your users within your CIAM – ensuring the very best customer experience and a loyal clientele.

We hope you'll find it an informative read.

Stephan Schweizer
CEO, Nevis Security AG

Introduction

In this white paper, we explain in detail why MFA should be an indispensable part of security measures for companies today and how this actually works. We also show how you can combine your MFA measures with passwordless authentication within the framework of CIAM. In this way, your customers' desire for high security with maximum login convenience can be fulfilled with bespoke perfection.

Why should companies rely on MFA?

The answer is simple: Because passwords alone are not secure and compromised user accounts are still one of the biggest threats to data security.

Although many customers are concerned about the security of their data, they themselves do not always exercise the greatest caution. For example, easy-to-crack numerical sequences such as '123456' or simple word-number combinations such as 'hello123' are still very popular password choices. Also, 44 percent of 1,000 consumers surveyed in our study for the **Nevis Security Barometer 2021** said they use the same password for multiple accounts.

Passwords as a risk factor

Of the consumers surveyed,

44.3%

use the **same password** for **multiple accounts**.

Source: Nevis Security Barometer 2021

By behaving in this way, they are playing into the hands of cyber criminals and their most common attack methods. According to the 500 IT decision-makers surveyed for the Nevis Security Barometer, these include brute force attacks (around 27 percent) and credential stuffing attacks (around 23 percent).

Brute force attacks

Brute force attacks involve hackers using sheer might. Using a list of valid user names, a bot tries to find out the corresponding passwords through automated trial and error.

Phishing attacks

Phishing is at the forefront of social engineering attacks that make use of human weaknesses to illegally obtain login data. Phishing emails – supposedly from trustworthy senders – are intended to trick recipients into revealing sensitive login data on fake pages, for example.

Credential stuffing

Hackers also take advantage of the fact that a frighteningly large number of users use the same usernames and passwords with different providers. If criminals have already captured user data through brute force or phishing, they may try to log in to other websites in the next step through credential stuffing – with fatal consequences for users.

One against all

All of these attack methods have one thing in common: MFA can put an effective stop to what criminals are doing. Simply because multi-factor authentication requires at least a second identification factor in addition to the password. With single-factor authentication – which is unfortunately still widely used – hackers have an easy task once they know the password. But if another factor is required within the framework of MFA to establish user identity – such as verification of biometric data in an access app on the smartphone – online criminals are locked out.

Security vulnerabilities can cause costly reputational damage

If data or services cannot be accessed as a result of a hack, this means enormous losses in turnover for online trade, for example. It is estimated that **cybercrime will cost companies around the world USD 10.5 trillion per year by 2025**. In 2015, it was 'only' USD 3 trillion.

Not to mention the consequences of damage to your company's image if security breaches become known on a large scale – and customers abandon ship.

What is more, organisations now face significant fines for breaching legal data protection requirements due to poor security. **According to the latest annual report by law firm DLA Piper**, fines of almost EUR 1.1 billion (USD 1.2 billion) were imposed on companies for breaches of the European Union's General Data Protection Regulation (GDPR) last year. This is a new record high.

How does MFA work?

With MFA, users are authenticated by at least two different security and validation procedures. Basically, there are four types of authentication technologies. They are based on the factors knowledge, possession, biometric characteristics and location. If only two different variants are used, this is called two-factor authentication (2FA).

The four categories of MFA

→ Knowing

This is something that only the user knows. These include passwords, PINs, answers to security questions or the user ID. The transaction number (TAN) or one-time password (OTP) also fall into this category. Today, TAN generators or authenticator apps are usually used for this. They always generate new passwords based on time and events. The TAN procedure becomes even more secure if the account number and the amount are also included in the process.

→ Having

For this, the user must be in possession of a certain object. This can typically be a smartphone, chip card, USB token or TAN generator. The hardware token is used to generate a one-time password or a one-time passcode (OTP). Today, the use of a separate hardware token is often replaced by the smartphone because many people always carry it with them. An authentication app that the user has installed beforehand then provides the OTP. Separate additional devices such as a USB token or a TAN generator are no longer up to date. They are usually kept at home, which imposes time and geographical restrictions on the user – for example when carrying out banking transactions.

→ Being

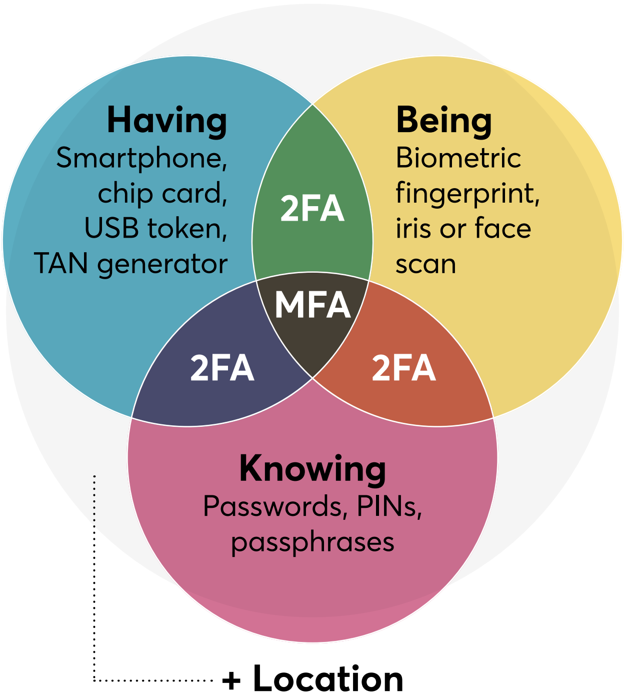
Something that the user is. In other words, the user's unique biometric features are used for identification purposes. These can include a fingerprint, iris or face. Once these factors have been scanned and stored, the user can only be identified by a sign of life. For this, users must be on site and identify themselves with their biometric features in real time. The system cannot be fooled by a photo, for example. Biometric authentication usually requires modern mobile devices that have the necessary technologies.

→ Location

Particularly in the financial industry, factors such as IP address, location using GPS data if possible – and in some cases time of use compared to previous online sessions – are also used to verify identity.

Interaction of multiple factors

In the actual MFA process, the provider now combines two or more factors, for example, as follows: When it comes to using a credit card, its possession is just as necessary as the knowledge of the PIN, the validity and the verification number. As an additional security barrier, users are often requested for a TAN number (knowledge), which is generated by means of a TAN generator (possession). The more factors that interact, the better the protection against data misuse.


Having
Smartphone, chip card, USB token, TAN generator
Being
Biometric fingerprint, iris or face scan
Knowing
Passwords, PINs, passphrases
2FA
2FA
2FA
MFA
+ Location

IP address, GPS data
(can be matched as an additional factor in the background)

Basic considerations for the use of the MFA

Companies from various industries can benefit from the advantages of MFA. These include providers of financial services and banking, public authorities, insurance companies, engineering manufacturers as well as players in online retail, healthcare or online casinos.

Regardless of the industry, when introducing the extra layer of protection provided by MFA, they need to ensure that they strike a balance between security and convenience for customers. For this to succeed, careful planning is required. The following points should therefore be determined in advance.

Obligatory or optional?

Since MFA always involves a certain amount of additional effort for your customers, it is important to decide how protection and user convenience are optimally weighted in individual use cases. To get started, companies need to think about how they will introduce MFA for their customers: Should this technology be mandatory or optional?

After all, there are numerous use cases in which MFA can theoretically be used. But where does it make sense? To avoid unnecessarily complicating user identification – potentially resulting in a poor customer experience – careful consideration should be given to when MFA is really necessary and when it is not.

Even in the financial industry, where most transactions are high-risk, MFA need not be the tool of choice everywhere. It is advisable to always offer different options. For example, you could give customers the option to choose the type of second factor themselves. Then consumers decide for themselves whether they receive an SMS message – though this is less secure – or whether they prefer to receive push notifications via their mobile app for authentication.

Of course, companies need to consider the security implications of giving their customers a choice between different MFA routes and communicate potential security risks clearly.

Adaptive MFA based on context and risk

The good thing is that modern MFA offers the possibility to increase authentication requirements based on context and risk.

For instance, if a user attempts to authenticate from a device they have used many times before, immediate access can be granted. If the authentication attempt is via a new device, authorisation from a known trusted device can be requested.

With MFA based on context and risk, organisations can achieve flexibility across different use cases to help ensure that customers see their security and user experience needs best met.

Improving the customer experience with MFA in modern CIAM solutions

Modern CIAM solutions such as the Nevis Authentication Cloud naturally include MFA as an additional security barrier for the greatest possible security in the collection and management of customer identity data. In doing so, it fulfils the following important requirements that are generally necessary when MFA is used for customers.

Mobile first

Today, many people almost always have their mobile phones with them. It therefore makes the most sense to use an application on the mobile phone for MFA. Then there is virtually no danger that users will not have an external additional device with them when they need it. Moreover, your customers' acceptance of the MFA increases if they can use it on their smartphone, which is always within reach anyway.

Convenient management of all functions

With the Management Console included in the Nevis Authentication Cloud, your organisation has a convenient tool to manage all integrated apps including MFA. After all, it makes no sense to leave the MFA implementation to individual app development teams who do not have the necessary experience in terms of data security. The Management Console has features that let you manage users and devices and remove inactive users or devices that are no longer in use from the system. It also allows administration of access tokens – such as those used by applications for login authorisation.

Preserve your branding

Building a successful brand takes years. Every MFA tool your customers use, such as your Access app, should therefore be branded to your specifications. Solutions from vendors that cannot be adapted to your corporate identity inevitably dilute the customer experience with your brand. Also, users might have doubts about whether a nameless, unfamiliar app is really related to your brand and your company. That's why the Access app included in the Nevis Authentication Cloud is designed for your customers to carry your logo, colours and the font of your choice without the need for major programming. In addition, the Nevis Access app is hardened, end-to-end encrypted and FIDO-certified. It can be integrated in no time using a software development kit (SDK).

Passwordless, biometric authentication

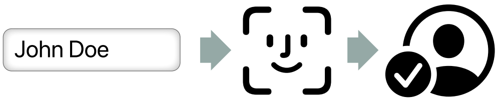
With the option of passwordless, biometrics-based MFA, the Authentication Cloud offers optimum security and convenience.

The most commonly used method is out-of-band authentication. This is a specific form of MFA or two-factor authentication (2FA). To obtain the second authentication factor, the use of a separate communication channel is required. For example, after entering a user name and password on a trusted device, the user receives a push message or has to identify themselves using their fingerprint.

As a particularly convenient form of user identification, the Nevis Authentication Cloud offers the possibility of passwordless authentication and transaction signing. The need for an insecure password is completely eliminated.

The passwordless authentication process takes a matter of seconds for the user. Customers enter their username on the login page and tap the 'Sign In' button on their smartphone. The Nevis Authentication Cloud instance sends a push notification to the user's mobile phone ('Having' factor). When they open it, they can authenticate themselves with the biometric method they have chosen ('Being' factor). If the authentication is successful, the Nevis Access app confirms this and the user is automatically logged in.

Passwordless authentication using biometric features in the Access app

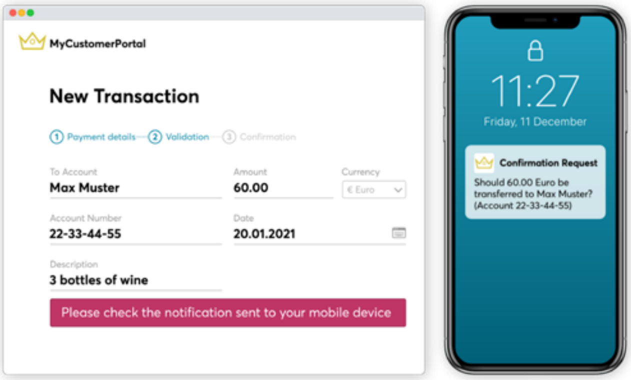


- True passwordless alternative and protects the account against credential stuffing and account take over attacks.
- It's just a matter of entering a username and authenticating.

Transaction confirmation

For transactions with a particularly high level of security – such as financial transactions or information updates – a transaction confirmation should also be the norm for added security. Here, too, MFA plays an important role. As with the login using MFA, a push notification informs the user about the upcoming transaction and about important details such as the amount of money or the account number of the recipient. This gives the customer the opportunity to take corrective action before confirming the transaction with their chosen biometric authentication. Another advantage of the transaction confirmation: It not only enhances security – it also protects against incorrect entries and thus ensures a positive customer experience.

Transaction confirmation with the Nevis Authentication Cloud



New Transaction

To Account: Max Muster
Amount: 60.00
Currency: € Euro
Account Number: 22-33-44-55
Date: 20.01.2021
Description: 3 bottles of wine

Please check the notification sent to your mobile device

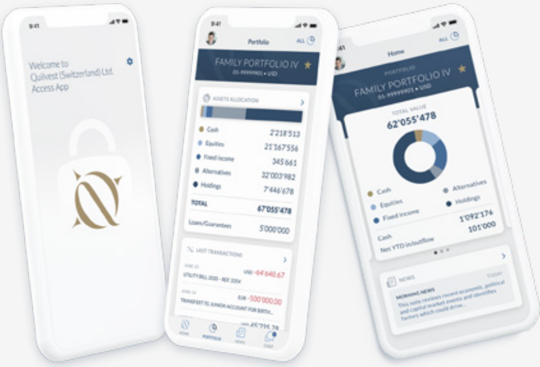
11:27
Friday, 11 December

Confirmation Request
Should 60.00 Euro be transferred to Max Muster? (Account 22-33-44-55)

Success story

Secure authentication in e-banking with the Nevis Authentication Cloud

QUILVEST
SWITZERLAND



Particularly in the financial industry, digitalisation is associated with special requirements. Quilvest (Switzerland) Ltd., a renowned independent asset manager, has developed a new platform in which secure communication is also possible with the help of a chat function. This fulfilled user wishes to get in touch with their advisors quickly and without complication – and in a legally secure form, which could not be guaranteed by external messenger services. At the same time, the need for a new authentication option including a firewall for the establishment of e-banking was taken into account. Nevis won over Quilvest with usability, security, stable availability of the Authentication Cloud and the option of branding the app.

Secure, flexible and user-friendly

Nevis supports Quilvest with a combined solution of proxy server, IDM, WebAuth firewall infrastructure and Access app with cloud solution. The Nevis Authentication Cloud is used for authentication. Identification is done with username and password, fingerprint/ face ID or PIN. There are two options for authentication: Clients can log into the web portal and enter their contract number and password. A push authentication is then sent to them in the app. To verify their identity, they use a PIN or fingerprint/face ID.

Alternatively, clients can open the mobile banking app. In the app, they enter their contract number and receive a push notification that they must confirm – also using a PIN or fingerprint/face ID. After successful authentication, users are automatically redirected back to the banking app via automatic 'app-to-app switching'. Transactions to new recipients and amounts above a certain level are also additionally authorised via the Access app.

The result: Users are more open to e-banking and mobile banking because it is no longer as complex as it used to be. Mobile and e-banking can also be used in a single app – thereby simplifying handling.

MFA – scoring points with convenient safety

With the number of cyberattacks continuing to rise, the importance of security cannot be neglected – especially in the login process and online transactions with an increased level of protection. This is why companies can no longer avoid using MFA. However, since this entails a certain amount of additional work for users – depending on the type of implementation – you should proceed carefully when choosing your MFA solution. Fiddling with different devices and awkwardly typing in codes or passwords can cause frustration among users. Not only does this lead to a poor customer experience – it might also drive users to less secure identification methods.

One solution to this challenge involves MFA systems that use biometrics to combine maximum security and the highest level of user convenience.

Secure for specific target groups

Of course, when using 2FA/MFA concepts, you should keep the requirements of your target group in mind and consider the following:

- Not all customers have the very latest smartphone models, so they may not be able to use biometric authentication
- Entering complicated passwords, PINs and TANs on your mobile phone is cumbersome

Nevertheless, the advantages of MFA outweigh the disadvantages. The latter can be effectively offset by a carefully considered choice of user-friendly procedures – focusing on biometrics – and through context-based and risk-based use. With CIAM solutions such as the Nevis Authentication Cloud, you not only succeed in implementing MFA close to the target group. Among other advantages, you benefit from features such as an app that can be fully customised to your design or the possibility of transaction confirmations. This makes it simple and straightforward to strike the right balance between data security and usability.

nevis®

Making security an experience

About Nevis

Nevis develops security solutions for the digital world of tomorrow. Our portfolio includes passwordless logins, which are intuitive to use and offer optimal protection of user data. Nevis is the market leader for Identity and Access Management in Switzerland, and it protects over 80 percent of all e-banking transactions. Government authorities and leading service providers and industrial companies across the globe rely on Nevis solutions. The specialist in authentication operates offices in Switzerland, Germany, the United Kingdom, and Hungary.

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.

Follow us

www.nevis.net