Research brief, July 2021

Navigating the password jungle

Digital user authentication

Serpil Taş
Dr Lukas Wiewiorra
Prof Dr Anna Schneider

HOCHSCHULE FRESENIUS
UNIVERSITY OF APPLIED SCIENCES

wik Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste

Imprint

Authors of the study:

Serpil Taş
Senior Economist | Markets & Perspektives
Contact: *s.tas@wik.org*
+49 (0)2224 92 25 96

Prof Dr Anna Schneider
Professor of Business Psychology
Contact: *anna.schneider@hs-fresenius.de*
+49 (0)221 97 31 99 715

Dr Lukas Wiewiorra
Head of Department | Markets & Perspektives
Contact: *l.wiewiorra@wik.org*
+49 (0)2224 92 25 25

Contact details of the research institutes:

WIK Wissenschaftliches Institut für
Infrastruktur und Kommunikationsdienste GmbH
Rhöndorfer Str. 68, 53604 Bad Honnef, Germany
Tel.: +49 2224 9225-0
Fax: +49 2224 9225-63
eMail: info@wik.org
www.wik.org

Hochschule Fresenius – Fachbereich Wirtschaft & Medien
Business School · Media School · Psychology School
Im Mediapark 4c, 50670 Köln, Germany
www.hs-fresenius.de

General Manager and Direktor: Dr Cara Schwarz-Schiling
Chairwoman of the Supervisory Board: Dr Daniela Brönstrup
Registered: Amtsgericht Siegburg, HRB 7225
Tax No.: 222/5751/0722
VAT No.: DE 123 383 795

General Manager: Prof Dr Tobias Engelsleben, Sascha Kappes, Kai Metzner
Registered: Amtsgericht Wiesbaden HRB 19044

Pictures: Title: claudio-schwarz-purzlbaum - unsplash; p. 4: mohamed Hassan - Pixabay; p. 6/7: Surface - unsplash; p. 8: mindspace-studio - unsplash; p. 10/11: Alexander Shatov - unsplash; p. 12: Thomas Ulrich – Pixabay; p. 15/16: jessie koranteng-unsplash; p. 16 (Fingerabdruck): OpenClipart-Vectors - pixabay, p. 2-15: sabelskay - AdobeStock

Layout: Karin Wagner (WIK)

Foreword

Security is not a priority for all users

Nowadays, internet users are confronted with a multitude of different forms of user registration. An ever-growing number of services require individual registration, while at the same time the number of services being used is constantly increasing. Managing all the login information while navigating the password jungle is a growing challenge.

For this study, WIK took a close look at various registration procedures and technical solutions, as well as the extent to which they are currently being used and their perceived advantages and disadvantages. The results show that internet users in Germany continue to rely on traditional login methods, even though many of them already use a large number of different services that require user registration.

Single Sign-On (SSO) services, which can unify the different combinations of passwords and usernames or email addresses are still not used by many consumers. Nevertheless, this very segment is particularly dominated by large platform providers such as Facebook and Google which are expanding their digital ecosystems with these SSO services. These providers leverage their strong position within their respective digital markets and the associated user base to provide website operators and service providers with a simple login function. However, this function also enables them to gain further insights into the behaviour of their users beyond their own service, thereby increasing their advertising profiles.

Other widespread solutions such as password managers and biometric authentication methods also have their drawbacks, but do not pose the immediate risk that individual usage behaviour can be tracked across different services.

Dr Cara Schwarz-Schilling

Between password and fingerprint

When consumers want to use digital services, they are often faced with the question of how they want to authenticate themselves: should it be “conventional“, for example with their email address and an individual password, or would they rather use SSO solutions from third parties or social networks? Password managers or biometric features, such as fingerprints, can also make it easier to log in to different services. Our data shows that currently, the most common option remains the conventional one.

Security experts recommend using a separate and unique password for each account to reduce the risk in the event of data loss. Despite this, consumers tend to use simpler and thus less secure passwords, and also use similar or even the same passwords for different services.

Introduction

Almost every day, internet users log in to a wide variety of digital services (such as music and video streaming services, marketplaces and social networks) that require the creation of a user account. As the number of services consumers use continues to increase, so does the challenge of adequately managing all accounts and their corresponding credentials.

Although about 50% of internet users claim they forget their passwords at least occasionally, most still rely on memorising their passwords. Users have two basic options for alternative approaches: they can use solutions that make it easier to manage all the login information, or they can use solutions that reduce the number of different login details.

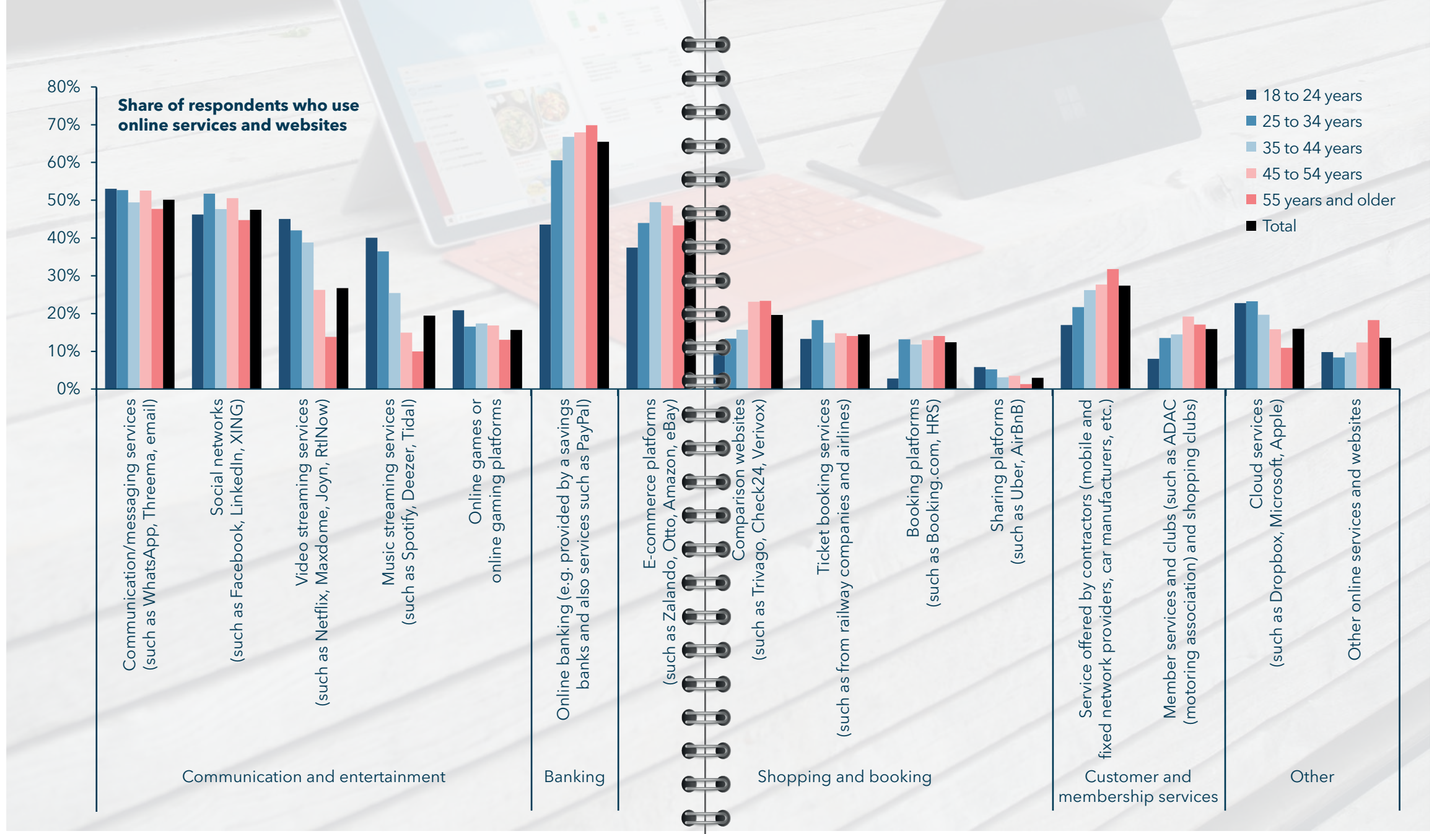
But which authentication methods and solutions do internet users rely on and which are less relevant to them? To answer this question, this study combines results from a quantitative, representative survey with more than 3,000 participants in Germany with the results of an in-depth qualitative survey with 12 consumers.

The daily login routine

Internet users today use a wide range of different digital services, and new ones are added every day.

According to our survey, around 48% of internet users in Germany use 4 to 12 services every week. Furthermore, 12% of respondents use up to 30 services from a variety of categories every week.

Digital services for communication and entertainment have the highest number of users. These include social networks, communication services such as email, WhatsApp and Threema, streaming services for music and video, and online games.



Data based on WIK's annual online survey. Data in body text: N=3,016.
Data for figure: N=2,344. Analysis excludes "no answer"/"don't know" responses.

Online banking, services for online purchases and bookings, and online customer and membership services are also used by many internet users. In contrast to the communication and entertainment category, however, services in these categories are used less by young internet users than by older users.

For many of the digital services used, creating a user account is a basic requirement to enable the service to be used to its full extent.

Overall, 42% of internet users use digital services that require a login almost every day.

Although logins are now an integral part of everyday life, they do not affect all internet users equally and with the same intensity.

Common but complicated

The most common and widely adopted method of authentication is a combination of a username or email address and a password.

Around 86% of internet users in Germany rely on this method. However, this method becomes increasingly complicated as the number of different services increases, especially if users employ different login credentials for each of the services and even change them on a regular basis.

Data based on WIK's annual online survey: N=2,287.
Analysis excludes "no answer"/"don't know" responses.

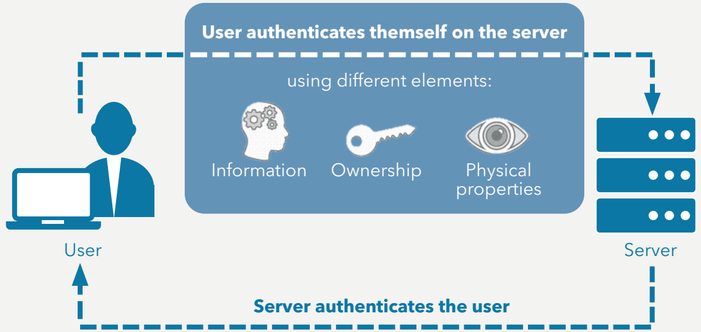
Simple but uncommon

Technical solutions such as password managers and SSO services can help users to deal with the overload of passwords and thereby reduce the security risk that arises from the use of identical passwords for different services.

Password managers allow convenient administration and central storage of the login data.

SSO solutions replace different individual logins with a central login service and are therefore designed to reduce the number of different login requirements.

However, at least one of these two solutions is currently used by only **32%** of respondents.



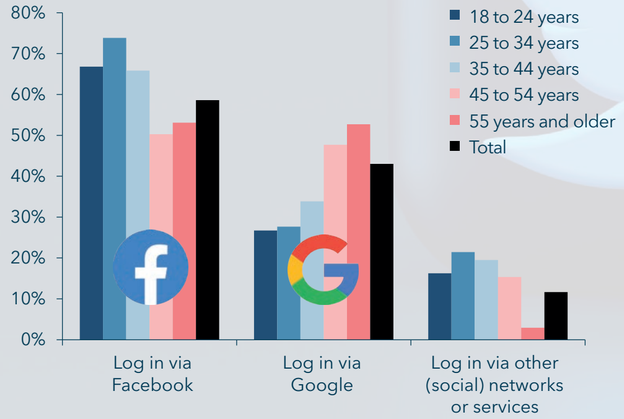
Data based on WIK's annual online survey. N=2,287.
Analysis excludes "no answer"/"don't know" responses.
Source of figure: https://www.tuv.com/germany/de/authentifizierung.html

Social logins

Digital platform providers' SSO services (aka social logins) are used most frequently. In particular, users who value a simplified and convenient login process consider this option to be advantageous.

Overall, the use of social logins in Germany is still fairly unpopular, with uptake at **around 13%** of internet users. Facebook holds the largest market share of existing social login solutions, followed by Google, LinkedIn, Yahoo and Twitter.

Share of respondents who use social login services



Log in	Twitter	Google	Linkedin	Yahoo
First Name	First Name	First Name	First Name	First Name
Last Name	Last Name	Last Name	Last Name	Last Name
Nickname	Nickname	Nickname	Nickname	Nickname
Email Address	Country	Email Address	Email Address	Email Address
Birthday	Profile Photo	Age	State	Age
Gender	Location	Birthday	Country	Birthday
City	Follower Info	Gender	Profile Photo	Gender
State		City	Interests	Country
Country		Profile Photo	Languages	Profile Photo
Location		Education	Address	Interests
Profile Photo		Work History	Phone	Contacs
Likes		Locale	Education	Friends
Languages		Friend Info	Honors	
Education		Contacts	Publications	
Work History			Certifications	
Religion			Bio	
Political View			Industry	
Relationships			Work History	
Friends			Skills	
Friend Info			Favorites	
			Connections	

Pro and Cons

From the point of view of a service provider, the installation of social logins on its own website or app is advantageous. Service providers expect a higher conversion of visitors to registered customers due to the implementation of social logins.

In addition, certain attributes and information of the user profile stored with the social network can simply be transferred by the service provider. This drastically simplifies the login and registration process for new services and thus reduces the barrier to entry for new users.

At the same time, however, this means that user behaviour can be tracked across different services and data from different sources can be combined.

Data based on WIK's annual online survey. Data in body text: N=2,287.
Data in figure: N=304. Analysis excludes "no answer"/"don't know" responses.

Figure source: Gigya, Inc. (2015): Social Login 101: Everything You Need to Know About Social Login and the Future of Customer Identity. White Paper.

Security and reliability or convenience?

Very few of those internet users who place a stronger focus on security compared to aspects such as speed or simplicity use a social login.

Many express doubts about the security of these procedures, as well as data protection concerns. There is also a low level of trust in social login providers such as Facebook or Google.

Users of social logins are convinced of the convenient nature of the solution. Logging in and registering with digital services is generally more convenient, easier and faster using social logins and makes memorising new passwords obsolete.

"The question is how responsible they will handle the data. Because theoretically they now have your Facebook login." (Willi, 19)

"I mean, you feel like you're spinning this cobweb of information. And somehow I don't feel like I want to do that." (Nils, 23)

"People don't give it much thought, they just take the (...) path of least resistance and simply use Facebook, because it's more convenient for them, because it's quicker." (Anna, 25)

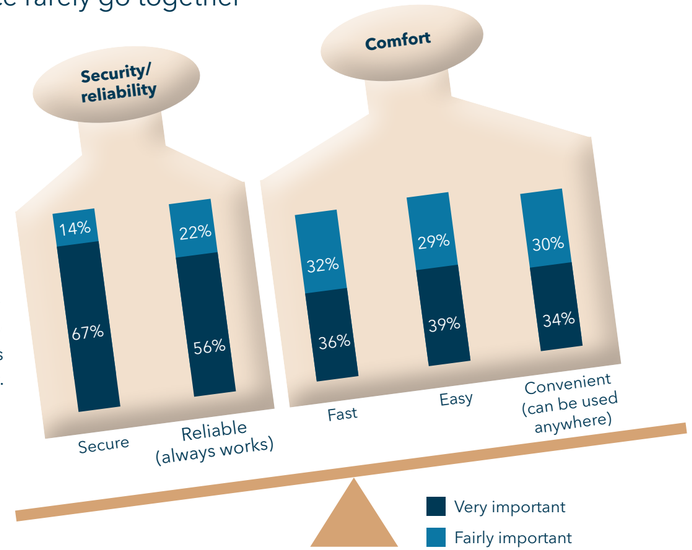
"Because it has often been made public that Facebook passes on data to third-party providers." (Maximilian, 30)

"Because it's much, much easier to register. I don't have to go to the trouble of writing my name and last name. It's a very quick process." (Sinem, 23)

Security and convenience rarely go together

Additional security often comes at the expense of usability and increases complexity for users, while very convenient systems usually require users to be willing to compromise on security.

Although internet users attach more importance to security and reliability than speed, simplicity and convenience, the latter elements are nevertheless key features of authentication systems for more than 60% of internet users.



Data based on WIK's annual online survey. N=3,016.
Analysis excludes "no answer"/"don't know" responses.

Convergence

"Well, I always try to change my [personal data] a little bit, if that's possible (...). In terms of age (...) sometimes you just swipe. Then I just stop at some point." (Katharina, 23)

"I don't really use Facebook actively. Simply because I have a lot of work colleagues there and I think that there is a greater sense of inhibition and you want to make a professional impression. Therefore, I would say that my account is cleaner. I don't share anything, I don't post anything. Instagram is a bit more personal. That's where I share my opinion, because I have a certain overview of who sees the things I post." (Eva, 23)

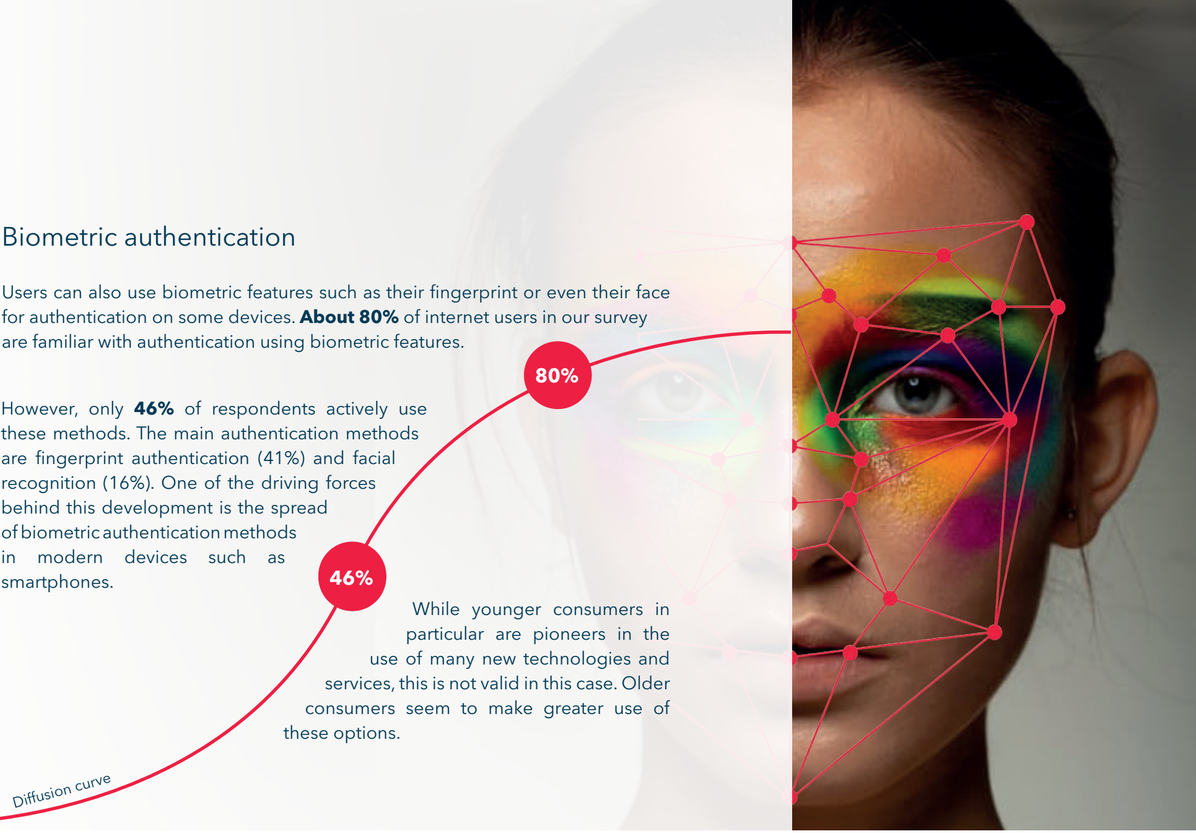
Digital identities created on various internet-based services do not necessarily correspond to the real identity of the user. It is common for users to use different digital identities that each represent only a subset of their real identity or even include false information. This may be the case if users want to remain anonymous or if they are concerned that their digital identity or the information they provide could be misused. Depending on the particular context, users present different facets of their identity while other elements are concealed.

However, the aggregation of different digital identities can create an image that is closer to the real identity of the user. New biometric methods are occasionally discussed very critically, as they enable the user to be clearly identified.

Biometric authentication

Users can also use biometric features such as their fingerprint or even their face for authentication on some devices. **About 80%** of internet users in our survey are familiar with authentication using biometric features.

However, only **46%** of respondents actively use these methods. The main authentication methods are fingerprint authentication (41%) and facial recognition (16%). One of the driving forces behind this development is the spread of biometric authentication methods in modern devices such as smartphones.



While younger consumers in particular are pioneers in the use of many new technologies and services, this is not valid in this case. Older consumers seem to make greater use of these options.

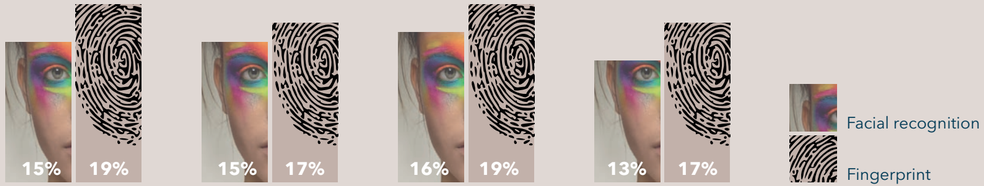
Data based on WIK's annual online survey. N=3,016.
Analysis excludes "no answer"/"don't know" responses

Today and tomorrow

Consumers use biometric methods such as facial recognition and fingerprints mainly to unlock their devices such as computers, laptops and smartphones. However, some consumers also rely on biometrics for authentication when using certain apps or logging in to online banking.

In the future, consumers can also imagine using their face or fingerprint as an authentication method to access medical information, for communication with authorities, and for smart home applications

Possible future use cases from the consumers' point of view[1]



Data based on WIK's annual online survey: N=3,016.
Analysis excludes "no answer"/"don't know" responses.
1) Respondents who are aware of biometric authentication procedures.

Outlook

Although SSO solutions simplify the administration of login information and make signing in to digital services more convenient, consumers are reluctant to use them. Consumers are particularly concerned about the security and reliability of social logins. Furthermore, the idea of making additional data available to the large platform operators by using social logins has frequently been cited as a reason for refusing to use them. From the perspective of website operators and digital services providers, social logins are an equally ambiguous tool. On the one hand, they allow users to log in more easily and quickly, and enable operators to access existing user information. On the other hand, extensive integration of this technology into the digital ecosystems of large platform providers and the information that can be collected using it may work to the advantage of the platform providers for advertising on the integrated websites and services.

The use of biometric features for authentication appears to be gaining momentum in Germany. So far, biometric features such as facial or fingerprint recognition are mainly used for unlocking digital devices, but in the future, consumers can imagine using biometric features in other areas as well.

The implementation of biometric authentication methods is currently being pushed in a number of other domains. In early 2021, for example, Flywallet introduced "Keyble", a wearable device with biometric authentication capabilities that allows users to make contactless payments and manage digital tickets, access cards, keys and signatures.[1] Amazon also started rolling out „Amazon One" in its bricks-and-mortar stores in autumn 2020. Amazon One allows customers in Amazon Go stores to authorise payments using only the palm of their hand. For this purpose, Amazon One's system creates a scan of the palm print, which is stored in the cloud in an encrypted manner and linked to a stored credit card.[2] Privacy experts have criticised Amazon One's implementation, which, unlike Apple's, is based on processing biometric information in the cloud.[3] Particular consideration must be given to the fact that a user's biometric characteristics are unique and immutable, and therefore, unlike a compromised password, cannot be easily changed.

1) See https://www.techradar.com & https://www.flywalletpay.com. Another example is the Bracelet by Deed, which can identify users via gesture recognition (see https://www.infineon.com).
2) See https://techcrunch.com.
3) https://mashable.com.

About this study:
The online survey for this study was conducted with 3,016 consumers in the last quarter of 2019 by the international market research institute YouGov. The results were weighted to draw representative conclusions for the German population (age 18+). In addition, a total of 12 qualitative interviews were conducted in November and December 2020. The full results of the survey are published in WIK Discussion Paper No. 462, available electronically at www.wik.org/en/.

About WIK:
Founded in 1982, WIK (Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste) in Bad Honnef, Germany offers consultancy for public and private clients around the world. Its focus is on the telecommunication, Internet, post and energy sectors giving advice on policy, regulatory and strategic issues. More information is available at www.wik.org/en/.

About Hochschule Fresenius University of Applied Sciences:
With more than 17,000 students across numerous national and international locations, Hochschule Fresenius University of Applied Sciences is one of the largest and most renowned private universities in Germany. Practical, innovative study, training content focused on the requirements of the labour market, small study groups and well-known cooperation partners are just some of the many advantages of Hochschule Fresenius. With its headquarters in Idstein near Wiesbaden, Hochschule Fresenius can look back on almost 170 years of tradition. More information is available at www.hs-fresenius.de/en/.

HOCHSCHULE FRESENIUS
UNIVERSITY OF APPLIED SCIENCES

wik Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste