Version October 1st, 2022

Hamburg Commercial Bank

Electronic Banking Internet Communication Standard (EBICS)

Security recommendations for corporate customers

CONTENTS **PAGE**

1 Introduction 03

2 General measures for safeguarding 04

3 Risks and possible threats 05

3.1 Protection for your electronic signature 05
3.1.1 Where are the potential risks? 05
3.1.2 What recommendations for action can be derived from this? 05

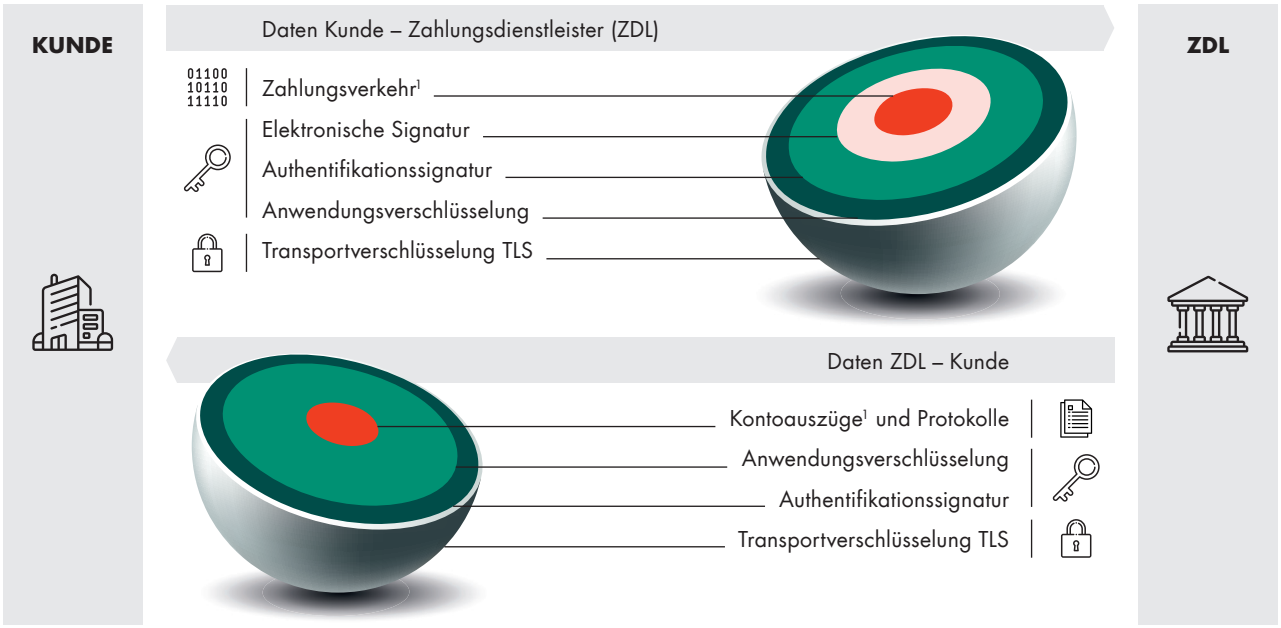
3.2 Use of portal solutions 06
3.2.1 Where are the potential risks? 06
3.2.2 What recommendations for action can be derived from this? 06

3.3 Use of tablets, smartphones and phablets 07
3.3.1 How do you secure your mobile device? 07
3.3.2 How to detect vulnerabilities in software or operating system? 08

3.4 Social engineering 09
3.4.1 How does the attacker proceed and what are his potential targets? 09
3.4.2 What can you do for your safety? 09

1 Introduction

The Electronic Banking Internet Communication Standard (EBICS) has proven itself for years as a multi-bank-capable and highly secure communication procedure between you and your payment service provider. Multiple encryption of banking data, different electronic signatures, as well as a comprehensive authorization management for users form the basis for the EBICS security architecture, which is illustrated by the following figure:



The transport of your payment transaction data to your payment service provider is secured by double encryption and two signatures: The electronic initials/signature releases the technical data (authorization), while the authentication signature ensures that you are the correct sender (authentication). Application encryption encrypts your payment transaction data. During transport, the entire data stream (i.e. including other control data) is additionally protected by TLS[2] encryption. In particular, we advise you to comply with the minimum requirements of the Crypto LifeCycle[3].

Your payment service provider supplies you with data for collection using the same security mechanisms. A bank-side electronic signature (EU) for this data is technically possible in EBICS, but not yet universally recognized by the financial authorities. Therefore, this EU is currently still waived.

The German Banking Industry[4] as well as the EBICS company[5] regularly check the security mechanisms and encryption techniques used for up-to-dateness in order to maintain this high level of security.

This is particularly essential due to the permanently changing and intensifying threat situation on the Internet. The rapidly increasing number of malware and ever more sophisticated attack techniques as well as the rise in organized crime make this necessary.

However, in order for the security procedures contained in EBICS to be fully effective in protecting the exchanged data, appropriate precautions must also be taken in your technical environment. Information and, in particular, current messages on basic security can be found at www.bsi.bund.de.

This document is aimed at all customers who use EBICS, in particular corporate customers and their IT departments, security officers and system administrators. It describes threats that are present in specific implementation variants and provides recommendations on how to counter them.

The document is intended as a recommendation and does not claim to be complete.

[1] Auch andere Dateiformate möglich
[2] Transport Layer Security
[3] https://www.ebics.de/de/ebics-standard/krypto-lifecycle
[4] The German Banking Industry (DK for short) is the association of the Federal Association of German Cooperative Banks, the Federal Association of German Banks, the Association of German Public Sector Banks, the German Savings Banks and Giro Association and the Association of German Pfandbrief Banks that represents the interests of the leading associations in the banking industry.
[5] Members of the EBICS Society are the banking industries of Germany, France, Switzerland and Austria.

In Chapter 2 ("General measures for securing"), this document provides general security recommendations. This section contains information on setting up a security organization and security management, as well as a few tips on securing networks.

In Chapter 3.1 ("Protecting your electronic signature"), this document discusses risks and threats in key management and, in particular, provides information on how to protect your electronic signature.

Chapter 3.2 ("Use of portal solutions") then looks at the specific risks involved in using portal solutions and presents appropriate measures for avoiding these risks.

Chapter 3.3 ("Use of tablets, smartphones and phablets") takes account of the increasing use of mobile devices – either for the use of EBICS apps or as a medium in the context of distributed electronic signatures (VEU). Here, particular attention is paid to the special threats associated with the use of smartphones and tablets, etc., and recommendations are made for security measures for these platforms.

Since social engineering attacks are playing an increasingly important role as a growing element in a wide variety of types of identity theft – also due to the ever-increasing use of social networks and the accompanying disclosure of personal and official information – a separate chapter is devoted to this topic in this document (Chapter 3.4).

2 General measures for safeguarding

The "Terms and conditions for remote data transmission (DFÜ)" (in short: DFÜ customer terms and conditions), which you have received from your payment service provider or which are published on their website, represent a minimum requirement. However, you can optimize your security even further.

Take information security measures at the organizational, technical and personnel levels. These include access protection, installation of firewalls, authorization management, and monitoring and logging. Protection against malware is indispensable in today's world.

In addition, you should have a regulated process for installing software and precautions to protect the corporate network, such as:

– Software should be installed and maintained exclusively as part of a regulated process (e.g. temporary assignment of administrator rights and documentation). Particularly in the case of installation of the EBICS software by third-party service providers, special technical accesses should be used for the installation, which should be deactivated again after the installation. These technical accesses should be approved in advance by the person responsible for IT in your company. To increase security, the approval and execution of the installation should be carried out in a dual control process and logged. Workstations and access paths required for installation and maintenance (e.g., for remote maintenance software) should be defined and approved in advance.

– As is generally the case, authorization profiles for EBICS should also be regularly checked and adjusted to ensure that they are up to date (e.g. deletion of employees who have left, changes to signing authorizations, etc.).

– If you consider a particularly high level of protection to be necessary for the EBICS client, it should be operated on a dedicated, secured, stationary end device to ensure security. You can achieve this, for example, by only granting access to the EBICS client to a restricted group of people.

– The operating system and other installed software should be updated regularly (installation of patches).

– The use of antivirus software is essential. This software must also be updated regularly. As a rule, the antivirus software has an automatic mechanism so that it runs permanently in the background and ensures an update immediately after the computer is started. If such an automatism is missing, then the antivirus software should be updated in principle after each start of the computer and before the start of the EBICS system manually. At regular intervals, the computer should be subjected to a complete scan by the antivirus software.

– In general, passwords should be sufficiently long and contain upper/lower case letters, numbers and special characters. Changing passwords on a regular basis is recommended. Identical passwords should not be used for different purposes or accesses.

– To prevent passwords from being spied out, they must not be stored in plain text on the system (e.g. in a file). Instead, a key management program available on the market could be used, which usually also allows secure passwords to be generated. In addition, a program for secure password entry could also be used that allows password entry by bypassing the keyboard. In this way, passwords entered via the keyboard can be prevented from being recorded by unauthorized persons (using so-called keyloggers[6]) and misused.
– As a rule, electronic banking products (EBICS clients and portals) display the last login or login attempts. This should always be checked. Pay attention to incorrect login attempts.
– The Internet connection required for EBICS communication should always be established via a secure Internet access. The use of unsecured or unknown WLAN access (e.g. Internet café) is strongly discouraged.

3 Risks and possible threats

3.1 THE PROTECTION FOR YOUR ELECTRONIC SIGNATURE

3.1.1 WHERE ARE THE POTENTIAL RISKS?

The security procedures defined in EBICS for the authentication, encryption and authorization of payment orders (electronic signature) offer a very high level of protection against fraudulent manipulation and unauthorized access to confidential data in electronic banking.

All these procedures are based on so-called asymmetric encryption procedures, in which signatures are created in each case with a private key for the authentication of EBICS users and for the authorization of orders. Conversely, public keys are used to verify signatures and encrypt data. It is therefore of particular importance that the private and public keys are stored securely and protected against unauthorized access and (unnoticed) changes. Unauthorized persons in possession of a copy of the keys and the associated password or PIN can submit and authorize orders under false identities, possibly gain access to account information, and manipulate orders.

The keys can either be stored on special hardware (chip card with signature function), as part of a remote signature procedure, or as software keys in files. As a rule, payment service providers offer their customers chip cards that provide enhanced security. Here, the keys are additionally protected with a PIN, a personal identification number. For security reasons, we recommend the use of chip cards, as they can neither be copied or stolen unnoticed nor used without knowledge of the PIN.

Should you nevertheless use key files[7], it is essential to ensure that they are stored and saved securely and protected from unauthorized access.

In particular, you should be aware of the following risks when using key files:

– The key files can be routed to an attacker unnoticed by malware along with the passwords.
– In the case of key files that are stored on a central storage medium, other people may have access (e.g. system administrators).
– Removable media containing key files can be accidentally left open or accidentally get stuck in the PC.

3.1.2 WHAT RECOMMENDATIONS FOR ACTION CAN BE DERIVED FROM THIS?

Secure storage of software keys

Key files can be copied unnoticed and thus fall into unauthorized hands. You should therefore not store software keys on stationary data carriers (local drive, network drive), but at least on removable data carriers that must be stored securely after use.

The security medium (e.g. USB stick) on which the software keys are stored must be protected against misuse and theft. This requires secure storage, e.g. by locking it up. Furthermore, we recommend that you additionally secure access to the security medium. This can be done, for example, by using a special USB stick with numeric keypad and encryption hardware.

Immediate blocking of keys on suspicion of misuse or theft

In the event of suspected misuse or theft, you are advised to immediately inform your payment service providers of the misuse of the keys or the loss/theft and to block the dial-up access of your affected users using EBICS means (administrative order type SPR).

[6] A keylogger is hardware or software that logs, monitors or reconstructs a user's keystrokes on a computer.
Keyloggers can be used, for example, to read passwords that a user enters on the keyboard and make them available to an attacker unnoticed.
[7] If no hardware medium is used, e.g. smart card, the keys are stored in key files and are then called software keys.

Unique assignment of the security media on which the software keys are stored

Each employee who uses the EBICS customer system as an EBICS participant must be assigned his own security medium (e.g. USB stick), for which he must take care. The participant should use this medium exclusively for storing the key files for the EBICS procedure.

Regularly change the keys used

If you use key files, we recommend that you change the keys at regular intervals. Requirements for changing keys should be part of your company's internal security policy.

The EBICS standard or the EBICS client software offers corresponding functionalities for updating the keys used.

Use of appropriate security media to store key files and use of appropriate passwords to access the software keys

Security media for storing keys should only be used for this purpose and should not be used to store other data. Access to both the medium and the software keys stored there must be secured by a password. As a rule, the EBICS software used already allows access to the keys only by entering an appropriate password. Rules for creating and changing passwords should be part of your company's internal security policy. The German Federal Office for Information Security (BSI) provides tips for secure passwords at www.bsi.bund.de.

After the last use, the safety media should be safely disposed of or destroyed.

Increased security through multiple-eye principle

From a legal point of view, it is possible to sign the bank signature individually; to increase security, the German banking industry recommends joint signing. In this case, you agree with the payment service provider that two signatures are required for complete authorization.

3.2 USE OF PORTAL SOLUTIONS

3.2.1 WHERE ARE THE POTENTIAL RISKS?

In contrast to an EBICS system operated on a local computer, a portal solution is an offering that is operated centrally by the payment service provider or a service provider for a large number of customers.

The portal solution is accessed via a browser, with all functionalities of the EBICS system being displayed in this browser. All data – with the exception of the secret key when key files are used – is not located locally on your premises. Specifically, the EBICS keys for authentication and encryption as well as all banking data (payment orders, account statements, etc.) are stored in the environment of the operator of the portal solution.

In addition to entering the user ID and password, it may also be necessary to enter a further identifier, which the portal operator sends by SMS to a previously defined mobile phone number.

The risks described in Chapter 3.1 "Protecting your electronic signature" also apply in particular to the use of keys. It is essential that you follow the measures recommended there to minimize the risks.

The following risks must be considered when using portal solutions:

– The use of a browser means that portal solutions are always the focus of malware. Under certain circumstances, this can manipulate payment transaction data or gain access to sensitive data (e.g., account information).

– Due to an attacked browser, the required access data to the portal could fall into the hands of third parties.

3.2.2 WHAT RECOMMENDATIONS FOR ACTION CAN BE DERIVED FROM THIS?

Using shared browsers

Use only a browser approved by the payment service provider and carry out the security updates provided by the manufacturer for this purpose in a timely manner. You should refrain from using additional programs in the browser unless they are required. This applies in particular to Java applications provided by additional plug-ins[8]. Additional programs in the browser should only be activated for trustworthy websites. If mechanisms for phishing and malware protection are integrated in the browser to be used, these should also be used. The BSI provides tips for secure web browsers at https://www.bsi.bund.de.

[8] A plug-in (also software extension or add-on module) is an optional software component that extends or modifies existing software.

Use of antivirus software

Make sure that the antivirus software you use protects the browser you use. To protect yourself, you must always keep the software up to date, include updates or install newer program versions.

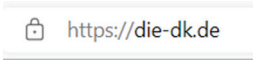
Secure access to the portal solution

When using a portal solution, your data (e.g. a captured payment) is transferred between the browser on your computer and the portal. This data should only be transmitted in encrypted form. The operator of a portal solution must use the TLS protocol for encryption so that a secure network connection is established between the browser and the portal.

The TLS protocol ensures that data cannot be viewed or manipulated during transmission.

To establish an encrypted connection, the portal solution must have a URL that begins with the abbreviation **https** (and not http).

Most browsers help you here by displaying a "lock icon" in the browser, for example. Never enter confidential data (especially your PIN code and password) without first checking the address!



Notes on security settings for various browsers can be found at www.bsi.bund.de.

Certificate verification

The certificate must be issued for the operator of the portal solution. It is signed by a trusted certification authority.

To make sure that you are actually connected to the desired address, you have the option to check the server certificate. To do this, double-click the "lock icon" in the browser status bar.

There must be no certification problems when calling the Internet address. In these cases, the browser warns and indicates a problem with the security certificate, or gives the indication that this connection is not trusted. In this case, please close the application immediately and report the error to the customer service of the portal solution operator.

3.3 USE OF TABLETS, SMARTPHONES AND PHABLETS

New vulnerabilities in software and operating systems are discovered every day. These can be exploited by attackers and thus pose a threat to your tablet, smartphone or phablet. To protect yourself, you must always keep the operating system and applications up to date, include updates or install newer program versions. Keeping track of this is often a challenge. Basically, the same rules apply to your mobile device as to your computers.

3.3.1 HOW DO YOU SECURE YOUR MOBILE DEVICE?

Password

The biggest security risk is the loss of your mobile device! Therefore, assign a password for a screen lock or use additional security mechanisms. This prevents unauthorized persons from accessing your applications and data.

If you lose your mobile device, it is best to change all passwords and use a security program to remotely delete your data from the mobile device.

Use in public

Never leave your mobile device unattended when you have your EBICS application open. Also make sure that no one is looking over your shoulder when you enter sensitive data. Only use your mobile device for your banking transactions in trusted WLAN environments or via your mobile data connection.

Trusted sources

Download apps only from trusted sources (i.e. official app stores). Nevertheless, check the privacy settings, access rights and, if necessary, other external ratings for the apps downloaded there.

If smartphones are used as business cell phones in the company, then a usage agreement should be concluded. An important aspect of this usage agreement is which apps are permitted or prohibited on the devices. It has long been impossible to keep track of the number of apps available. A **blacklist** of banned apps is therefore difficult to keep up to date. A **whitelist** with **trustworthy apps** is therefore recommended. However, the question arises here as to how trustworthiness can be determined. The Privacy-Grade project of Carnegie Mellon University offers a clue for the trustworthiness of apps. There, Android apps are rated from A+ to D according to the American grading system. The evaluation criterion is the comparison between the users' expectations of the apps' curiosity and the actual access rights.

Narrow your security policy to the current framework.

Trusted links

Be wary of links you receive via SMS, email, or messaging apps. This also applies to links hidden behind QR barcodes. Only follow links that come from trusted sources.

Deactivation of unneeded services

Disable Internet access, Bluetooth, WLAN and NFC[9] when you are not using them. This makes it more difficult for criminals to access your data via WLAN hotspots and Bluetooth. It is best to encrypt your data and also deactivate the device identification via Bluetooth.

Antivirus programs

Use an antivirus program. You can find apps for this in your store (some of them are even free).

Back up data, delete data

Back up your data regularly to a secured, stationary device. If you sell, give away or dispose of your mobile device, delete the data beforehand.

Maintain the operating system of your device

Every manufacturer offers regular service and security updates for their operating systems. Check the websites of your manufacturer for more information.

3.3.2 HOW TO DETECT VULNERABILITIES IN SOFTWARE OR OPERATING SYSTEM?

There is software available to detect vulnerabilities and the current software status of your applications as well as your operating system. We recommend that you use them.

Abort after entering the PIN

Communication between your mobile device and your payment service provider is extremely stable. System crashes or similar are very rare.

Therefore, be suspicious if your mobile device behaves unusually. In particular, if there are aborts or error messages after entering a PIN. If in doubt, contact your payment service provider.

[9] Near field communication (NFC) is an international transmission standard based on RFID technology for the contactless exchange of data by electromagnetic induction using loosely coupled coils over short distances of a few centimeters and a maximum data transmission rate of 424 kbps. To date, this technology has been used primarily in micropayments – cashless payments of small amounts. Other applications include the transmission of Bluetooth or WLAN authentication data to establish communication, or calling up web links if a URL in the appropriate format has been stored in the NFC chip.

3.4 SOCIAL ENGINEERING

Social engineering is the term used when an attacker exploits human characteristics to obtain confidential information. Many people think of cybercriminals as technically skilled geniuses who program complex computer codes in order to penetrate other people's computer networks. However, this often does not correspond to reality. In addition to classic "hacking", i.e. penetration by technical means such as computer viruses, there is also an easier way for criminals to obtain the desired information.

Why not just ask nicely? Hard to believe, but the method of "social engineering" promises great success for the attacker, especially in companies with above-average IT security precautions.

To this end, attackers exploit human characteristics of employees, such as good faith, helpfulness, pride, conflict avoidance or respect for authority, in order to use psychological tricks to obtain the desired information. A social engineering attack usually begins with the acquisition of general information about the company that is to be attacked or spied upon.

Social engineering is a popular way for cybercriminals to gain unauthorized access to sensitive information: It costs nothing and overcomes even the best security technology barriers.

3.4.1 HOW DOES THE ATTACKER PROCEED AND WHAT ARE HIS POTENTIAL TARGETS?

Even an organizational chart and the telephone list can be enough for a savvy attacker. Knowing the prevailing hierarchical structures, the attacker calls the company. He pretends to have a false identity in order to slowly gain access to the target information by asking clever questions and using psychological means. Often, the perpetrator slips into the role of a person of authority or trust. In doing so, he collects pieces of the information puzzle that make him appear trustworthy elsewhere.

Social engineers particularly often target passwords, such as bank account credentials. For example, the attacker feigns a problem that needs an immediate solution, e.g., a hacker attack that requires immediate access to your account. Because he appears determined and authoritarian, has selected his victim beforehand from a psychological point of view, and additionally confronts him with stress, the victim often willingly gives him the access data.

Social networks on the Internet provide a good starting point for social engineering. A wide range of background information about people can be found via these platforms. The information they reveal about their profile can be collected and used as a basis for further information gathering.

3.4.2 WHAT CAN YOU DO FOR YOUR SAFETY?

Be cautious about giving out information.

Social engineers pretend to be someone they are not in reality and thus feign an identity. Therefore, do not provide any information that you have not been expressly authorized to provide. This applies to work and company organization, responsibilities, personal information of colleagues or even user data. Only disclose as much information as necessary and question unusual concerns of a caller.

Let safety prevail over politeness.

Reckless decisions regarding safety are made especially in stressful situations or out of politeness. When in doubt, safety comes before politeness. You should agree with your supervisor that you will not suffer any disadvantages if they reassure themselves in case of uncertainty and the management board or an important customer has to wait a while for the desired document.

Protect sensitive information.

Never keep written notes and correspondence on your desk, but protect this information from the eyes of third parties. Always store sensitive documents encrypted on your PC. Even from seemingly unimportant information, important conclusions can be drawn in interaction with others. Avoid talking about sensitive company internals in public places such as a train compartment or a café.

Do not follow references to sensitive content.

Be especially careful if you are asked to access sensitive data under an urgent or rewarding pretext. For example, attackers like to impersonate your boss or your payment service provider to obtain sensitive information.