Deutsche Bank
Global Transaction Banking

Electronic Banking Internet Communication Standard (EBICS)

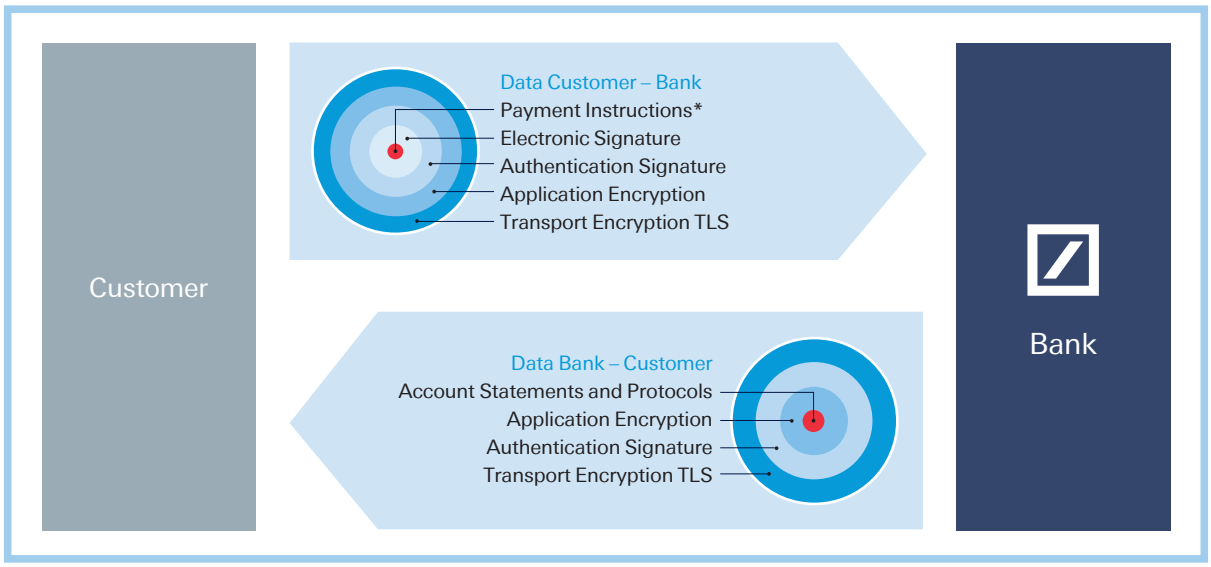
Security recommendations for corporate clients

Effective from September 3, 2018

Contents

1 Introduction

Over the years, the Electronic Banking Internet Communication Standard (EBICS) has proved to be a highly secure, multi-bank-capable system for communication between you and your payment service provider. The EBICS security architecture is based on multiple encryption of banking data, different electronic signatures and comprehensive authorisation management for users (as shown in the following illustration).



* Supports also other instructions and data

The transmission of your payment data to your payment service provider is secured with dual encryption and two signatures. The electronic signature is used to authorise the data content (authorisation), while the authentication signature identifies you as the correct sender (authentication). Your payment data is encrypted with the application encryption function. During transmission, the entire data stream (i.e. including other serial data) is additionally protected by TLS[1] encryption.

In line with advice from the BSI (German Federal Office for Information Security), we specifically recommend the use of TLS 1.2 for EBICS transport encryption with the cipher suites[2] supported and recommended in connection with TLS 1.2.

Your payment service provider sends you data for collection with the same security mechanisms. A bank-generated electronic signature (ES) for this data is technically possible in EBICS but, as this is not universally accepted by the financial authorities, these electronic signatures are currently not yet used.

1 Transport Layer Security

2 Recommendations on EBICS security procedures and key-lengths by the Deutsche Kreditwirtschaft http://www.ebics.de/Spezifikation/

DK (Deutsche Kreditwirtschaft)[3] and the EBICS Company[4] regularly review the security mechanisms and encryption techniques used to ensure they remain up to date and continue to provide this high level of security.

This is extremely important in the light of constantly changing and growing online threats. The rapid growth in malware, the increasingly sophisticated means of attack and the rise in organised crime have made this essential.

To enable the EBICS security mechanisms to provide effective protection of the exchanged data, you will, however, also need to take appropriate technical precautions in your own technical environment. Advice and up-to-date news on basic security are available from www.bsi.bund.de.

This document is intended for all customers that use EBICS, in particular corporate clients and their IT departments, security experts and system administrators. It describes threats encountered in specific implementation forms and recommends countermeasures.

Please note that this document merely contains recommendations and does not claim to be complete or exhaustive.

Section 2 ("General security measures") contains general security recommendations. It includes advice on setting up a security organisation and a security management system as well as some tips and recommendations on making networks secure.

Section 3.1 ("Protecting your electronic signature") examines the risks and threats in the management of keys and contains particular advice on storing your keys securely.

Section 3.2 ("Use of portal solutions") considers the specific risks involved in using portal solutions and describes appropriate measures for avoiding such risks.

The increasing use of mobile devices – either for using EBICS apps or as devices for distributed electronic signatures (German: VEU) – is examined in Section 3.3 ("Use of tablets, smartphones and phablets"). The specific threats in connection with the use of smartphones and tablets, etc. are examined here and recommended security measures are proposed for these platforms.

As social engineering attacks are an increasingly common element in many different forms of identity theft – due in part to the ever increasing popularity of social networks and the associated exposure of personal and professional data – an entire section has been dedicated to this topic (Section 3.4).

3 Deutsche Kreditwirtschaft (German Banking Industry Committee, DK) is the voice of the leading German banking-sector associations. These are the National Association of German Cooperative Banks (BVR), the Association of German Banks (BdB), the Association of German Public Banks (VÖB), the German Savings Banks Association (DSGV), and the Association of German Pfandbrief Banks (vdp). The DK superseded the Zentraler Kreditausschuss (ZKA) in August 2011 and carries its work forward.

4 The members of the EBICS Company are the umbrella organisations of the credit sectors of Germany, France and Switzerland.

2 General security measures

The Terms and Conditions for Electronic Data Transmission (EDT), which you received from your payment service provider, represent the minimum requirements. But you can do more to increase your security.

You should take steps to improve information security at the organisational, technical and staff level. These include access protection, the installation of firewalls, authorisation management as well as monitoring and logging. Protection against malware is also indispensable in today's world.

In addition, you should have a regulated process in place for installing software and take measures to protect your corporate network, for example:

- Software should only be installed or updated as part of a regulated process (e.g. temporary assignment of administrator rights and documentation). In particular if EBICS software is installed by external service providers, special technical access rights should be used and then deactivated after the installation is complete.

Such technical access rights should be approved in advance by the responsible IT manager at your company. To increase security, the installation should be approved, executed and documented by two different people. The workstations and access routes required for installation and maintenance (e.g. for remote support software) should be defined and approved in advance.

- In keeping with standard practice, the EBICS user profiles should also be checked regularly and kept up to date (e.g. by deleting profiles for employees who have left, amending signing authorisations, etc.).

- If you feel that a particularly high level of protection is required for the EBICS client, operations should be performed on a dedicated, secured, stationary device. You can achieve this, for example, by ensuring that only a limited number of people have access to the EBICS client.

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

- The use of antivirus software is indispensable. This software should also be updated regularly. As a rule, antivirus software contains an automatic protection function so that it is permanently running in the background and is updated as soon as the computer is restarted. If there is no automatic protection function, the antivirus software should be updated manually every time the computer is restarted and before the EBICS system is started. The antivirus software should perform a full scan of the computer at regular intervals.

- As a general rule, passwords should be sufficiently long and should contain a mixture of capitals and lower-case letters, numbers and special characters. It is recommended that passwords are changed regularly. The same password should not be used to access different programs or websites.

- To protect passwords, these should not be stored in the system in plain text (e.g. in a file). Instead, a commercially available key management program could be used; these generally include a function for generating secure passwords. In addition, you may wish to use a program which allows passwords to be entered without using the keyboard. This prevents any unauthorised individuals from logging passwords entered via the keyboard (using a keylogger[5]) and misusing them.

- In general, EB products (EBICS clients and portals) display the last login or login attempts; this should always be checked and you should pay particular attention to any failed login attempts.

- A secure internet connection should be used for EBICS communication. We strongly advise against using unsecured or unknown WiFi connections (e.g. in an internet cafe).

5 A keylogger is a hardware or software program that logs, monitors or reconstructs a user's keystrokes on a computer. Keyloggers can be used, for example, to pick up passwords entered by a user and make them available to an attacker unbeknown to the user.

3 Risks and potential threats

3.1 Protecting your electronic signature

3.1.1 What are the potential risks?

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

All of these mechanisms are based on asymmetric encryption, which uses private keys to generate signatures for authenticating EBICS users and for authorising orders. Public keys are then used to check the signatures and encrypt the data. So it is extremely important that the private and public keys are securely stored and protected against unauthorised access and any (undetected) changes. Unauthorised persons in possession of a copy of the keys and the corresponding password or PIN can submit orders and authorise them under a false identity and possibly gain access to account information and manipulate orders.

The keys can be stored either on special hardware (chip cards), as part of a remote signature process or as software keys in files. Payment service providers generally offer their clients chip cards, which provide greater security. The keys are additionally protected with a personal identification number (PIN). For security reasons, we recommend that you store keys on chip cards as these cannot be copied or removed without detection, nor can they be used by anyone who does not know the PIN.

However, if you do choose to use key files[6], you should take great care to ensure that these are securely saved and stored and protected against unauthorised access.

You should be particularly aware of the following risks when using key files:

- Hackers may use malware to obtain key files and passwords undetected.
- Other people (e.g. system administrators) may have access to key files stored on a central storage device.
- Removable devices containing key files may be accidentally left lying around or plugged into the computer.

3.1.2 What recommended measures can be derived from this?

Secure storage of software keys

Key files can be covertly copied and, in this way, fall into the hands of unauthorised individuals. So software keys should not be saved on stationary data storage devices (e.g. local drives or network drives); instead they should at least be saved on removable data storage devices, which must be stored securely when not in use.

The security device (a USB drive, for example) that the software keys are stored on must be protected against theft and improper use. This means that it must be stored securely, e.g. by locking it away. Furthermore, we recommend that you also restrict access to the security device. For example, by using a special USB drive with a numerical keypad and encryption hardware.

Immediate cancellation if misuse or theft is suspected

If you suspect that any keys have been misused or the key storage device has been stolen or lost, you should inform your payment service provider immediately and cancel the EDT access of the users concerned via EBICS (order type SPR).

Clear allocation of security devices on which software keys are stored

Each employee who uses the EBICS client system as an EBICS user must be allocated his/her own security device (e.g. USB drive) and assume responsibility for it. The user must use this device exclusively for storing the key files for the EBICS system.

Changing the key files regularly

When using key files, we recommend that you change the keys regularly at specific intervals. The rules for changing the keys should be part of your company's internal security policy.

The EBICS standard or EBICS client software provides appropriate functions for updating the used key files.

6 Unless a hardware device, such as a chip card, is used, the keys are stored in key files which are then known as software keys.

Use of suitable security devices to store key files and appropriate passwords for accessing the software keys

Security devices for storing key files should be used only for this purpose and not be used to store any other data. Access to both the device and the software keys stored on it must be secured by means of a password. As a rule, the EBICS software allows the user to access the keys only if he/she enters the correct password. Your company's internal security policy should include rules for creating and changing passwords. The Federal Office for Information Security (BSI) provides advice on creating secure passwords at www.bsi.bund.de.

If any security devices are no longer required, they should be securely disposed of or destroyed.

Multiple signatures provide greater security

From a legal point of view, it is possible to authorise banking transactions with a single signature, however, to increase security the DK recommends joint signing. In this case, you agree with the payment service provider that two signatures are required for full authorisation.

3.2 Use of portal solutions

3.2.1 What are the potential risks?

Unlike an EBICS system operated on a local computer, with a portal solution the system is centrally operated by the payment service provider or other service provider for a number of customers.

The portal solution is accessed via a browser which displays all the features of the EBICS system. None of the data – except for the secret key if using key files – are stored locally at your company. Specifically, the EBICS keys for authentication and encryption and all banking data (payment orders, statements, etc.) are stored in the operator's portal environment.

In addition to entering a user ID and a password, it may be necessary to enter another code that the portal operator sends by text message to a pre-arranged mobile telephone number.

In particular, the risks identified in Section 3.1 "Protecting your electronic signature" apply to the use of keys. It is essential that you follow the recommendations for minimising risks provided in that section.

Particular attention should be paid to the following risks when using portal solutions:

- The use of a browser means that portal solutions may be targeted by malware. In certain circumstances, malware may manipulate payment data or provide access to sensitive data (such as account information).

- If a browser is hacked, the portal access data may fall into the hands of third parties.

3.2.2 What recommended measures can be derived from this?

Use of authorised browsers

Only use browsers that have been approved by your payment service provider and promptly carry out the security updates made available by the browser provider. Refrain from using any add-on programs in the browser if these are not required.

This applies above all to Java applications which are made available via additional plug-ins[7]. Any add-on programs in the browser should only be activated for trusted websites. Any phishing and malware protection mechanisms integrated in the browser should also be used. The BSI provides advice on secure web browsers at www.bsi.bund.de.

Use of antivirus software

Ensure that the antivirus software used also protects the deployed browser. To protect yourself, you must ensure that the software is always up to date, carry out any updates or install newer program versions.

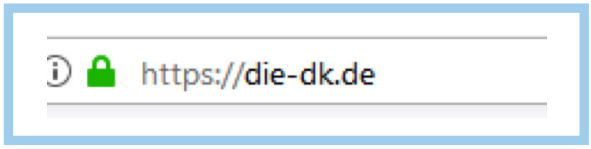
Secure access to the portal solution

When you use a portal solution, your data (e.g. an entered payment) is transferred between the browser on your computer and the portal. This data should be transferred in encrypted form only. In this context, the portal solution operator must apply the TLS protocol for encryption to ensure 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 transfer.

7 A plugin (also software extension or add-on) is an optional software component that extends or modifies the existing software.

To indicate a secure connection, the URL of the portal solution must start with the abbreviation https (not http).



Most browsers help you with this, e.g. by displaying a "lock symbol" in the browser's status bar. Never enter confidential data (especially your PIN and password) without first checking the address!

Information on security settings can be found at www.bsi.bund.de.

Checking certificates

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

To ensure that you are actually connected to the desired address, you can check the server certificate. To do so, double-click on the lock symbol in the browser status bar.

There should be no certification issue flagged up when you attempt to access the site via its internet address. If there is a problem, the browser issues a warning and indicates that there is an issue with the security certificate and/or informs you that the connection cannot be trusted. If this occurs, close the application immediately and report the error to the portal operator's customer service.

Additional security functions for the portal solution

Any additional security functions (e.g. two-factor authentication[8]) that are provided to access the portal solution should also be used.

3.3 Use of tablets, smartphones and phablets

New weak points in software and operating systems come to light every day. These can be exploited by hackers and pose a risk for your tablet, smartphone or phablet. To protect yourself, you must ensure that the operating system and applications are always up to date, software updates are carried out or newer program versions are installed. Keeping abreast of developments may often seem challenging. In principle, the same rules apply to your mobile device as to your PC.

3.3.1 How do you make your mobile device secure?

Password

The greatest security risk is posed by the loss of your mobile device. For this reason, set a password to lock your screen or employ additional security measures. This prevents unauthorised individuals from accessing your applications and data.

Should you lose your mobile device, it is best to change all of your passwords and to use a remote-access security program to delete the data stored on your device.

Using mobile devices in public

Never leave your mobile device unattended while your EBICS application is open. Ensure that no one is looking over your shoulder when you enter sensitive data. Only use your mobile device to carry out banking transactions in secure WiFi environments or via your mobile data connection.

Trusted sources

Apps should only be downloaded from trustworthy sources. Even then, check the privacy settings, access rights and, where applicable, external reviews for apps downloaded from these sources.

If smartphones are used as business phones within your company, employees should sign a Usage Agreement. One important aspect of this agreement relates to the apps that are allowed or prohibited on the devices. It is becoming ever more difficult to maintain an overview of all the available apps. So keeping a blacklist of prohibited apps up to date is not easy. It is consequently advisable to maintain a whitelist of

8 The purpose of two-factor authentication (2FA) is to identify users by means of two independent components. For example, 2FA can involve the combination of a component that the user "knows" (e.g. a password) and a component that the user "possesses" (e.g. a chip card).

trusted apps. This poses the question, however, of how trustworthiness can be determined. The PrivacyGrade project of Carnegie Mellon University provides a basis for determining app trustworthiness. Android apps are graded in terms of privacy there by the US academic grading system, which ranges from A+ down to D. The evaluation criterion is the comparison between people's expectations regarding the information needs of the apps with the actual access rights.

Determine the restrictions in your security policy to cope with the current security-related conditions.

Text messages, emails or QR codes

Treat any links you receive via text message or email with caution. The same applies to links that are concealed behind QR codes. Only follow links that come from reliable sources.

Deactivate any unnecessary services

Deactivate internet access, Bluetooth, infra-red as well as WiFi and NFC[9] when you are not using them. This will make it difficult for criminals to access your data through WiFi hotspots and Bluetooth. It is best to encrypt your data and to deactivate Bluetooth device identification.

Antivirus software

Use antivirus software. The relevant apps can be found in your app store (some may even be free of charge).

Saving and deleting data

Save your data regularly on a secure, stationary device. Delete all data before you sell, give away or dispose of your mobile device.

Maintaining your device's operating system

All manufacturers issue regular service and security updates for their operating systems. See your device manufacturer's website for details.

3.3.2 How can you identify weak points in software and in the operating system?

There is software available to identify weak points and to find the current version of the software for your applications and operating system. We recommend that you use such software.

Interruption after entering a PIN

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

For this reason, you should be suspicious if your mobile device behaves abnormally, especially if the system crashes or you receive error messages after entering a PIN. If in doubt, contact your payment service provider.

3.4 Social Engineering

Social engineering is the term used to describe the methods hackers use to exploit human nature to obtain confidential information. Many people imagine cyber criminals are technological geniuses who program complex computer codes in order to infiltrate computer networks. Often, however, this is not the case in reality. Apart from conventional "hacking", that is by infiltrating computer networks by technological means such as computer viruses, there is another easier way for criminals to obtain the information they are looking for.

Why not just ask for it politely? It may be hard to believe, but "social engineering" methods have huge potential for hackers to achieve their aims, especially in companies with above-average IT security arrangements.

Hackers use psychological tricks to exploit human qualities such as good faith, helpfulness, pride, a desire to avoid conflict or respect for authority in order to obtain the desired information. A social engineering attack usually starts by obtaining general information on the company that is to be targeted or spied on.

Social engineering is a popular method used by cyber criminals to gain unauthorised access to sensitive information: it doesn't cost anything and helps them overcome even the best technological security barriers.

9 Near-field communication (NFC) is a set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within 4 cm (1.6 in) of each other. NFC devices are used in contactless payment systems, similar to those used in credit cards and electronic ticket smartcards and allow mobile payment to replace/supplement these systems. This is sometimes referred to as NFC/CTLS (Contactless) or CTLS NFC. Further applications include the transmission of Bluetooth or WiFi authentication data for establishing communication, or opening web links if a URL has been stored in the NFC chip in the appropriate format.

3.4.1 How do hackers go about this and what do they hope to achieve?

An organisation chart and list of telephone numbers is often enough for a practised hacker. Armed with knowledge of the company's hierarchical structures, the hacker then phones the company. Using a fake identity, they employ skilful questioning and psychological methods to cautiously and slowly work their way towards the desired information. The perpetrator frequently assumes the role of a person in a position of authority or trust. They puzzle together pieces of information that make them appear trustworthy in another setting.

Perpetrators of social engineering frequently target passwords, such as access data for banking information. For example, they feign a problem requiring an immediate solution, such as a hacker attack, supposedly necessitating immediate access to your bank account. Because the hacker comes across as determined and authoritative and uses psychological criteria to choose their victim as well as placing them in a stressful situation, the victim is often prepared to disclose the access data.

Online social networks provide a convenient starting point for social engineering. Criminals can find a great deal of background information about individuals on these platforms. The details that people disclose via their profile can be collected and used as a basis to procure further pieces of information.

3.4.2 What can you do to safeguard your security?

Be reticent with information

Perpetrators of social engineering pretend to be someone that they are not, and in doing so, fake their identity. For this reason, do not give out any information that you have not been expressly authorised to disclose. This includes details regarding work processes and company organisation, roles and responsibilities, colleagues' personal data or even user data. Only provide as much information as is necessary and question any unusual inquiries by callers.

Prioritise caution over courtesy

Imprudent decisions regarding security are made especially in stressful situations or out of politeness. If in doubt, caution should outrank courtesy. You should clarify with your line manager that you would not be penalised if you performed a double check in case of doubt and the Management Board or a key client had to wait some time for a requested document.

Safeguard sensitive information

Never keep written notes and correspondence on your desk – prevent this information from being seen by any unauthorised individuals. Always store sensitive documents in encrypted form on your PC. Key conclusions can be drawn from even the most trivial details when combined with other information. Avoid speaking about internal company matters in public places, such as on a train or in cafés.

Do not follow links to sensitive content

You should be particularly cautious if you are asked to access sensitive data on an urgent or prospectively rewarding pretext. Attackers like to pass themselves off as your boss or your payment service provider in order to obtain access to sensitive information.