ODDO BHF

Electronic Banking Internet Communication Standard

(EBICS)

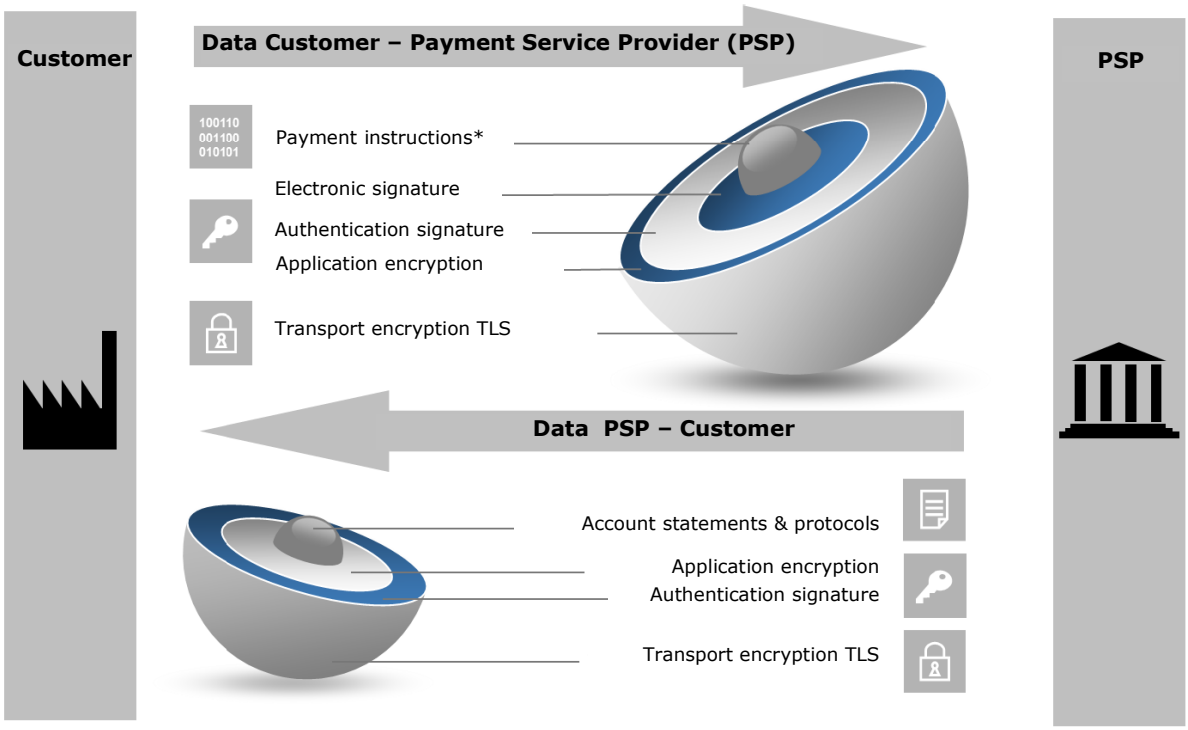
Security Recommendations for Corporate Clients

As of 3 September 2018

Contents

1 Introduction

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



* Other file formats also possible

The transport of your payment data to your payment service provider is secured by means of 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. During transmission, the entire data stream (i.e. including other serial data) is additionally protected by TLS[1] encryption. In accordance with the recommendations of the German Office for Information Security (BSI), we particularly recommend the use of TLS 1.2 for the EBICS transport encryption in conjunction with the "Cipher Suites"[2] supported and recommended in the context of TLS 1.2.

[1] Transport Layer Security
[2] The German Banking Industry Committee's recommendations for EBICS security processes and key lengths

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

DK (Deutsche Kreditwirtschaft – The German Banking Industry Committee)[3] and the EBICS Community[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 particularly important in light of constantly changing and growing online threats. Rapid growth in malware, 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, appropriate technical precautions will, however, also have to be implemented in your own technical environment. Information 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 is not intended to be exhaustive.

Chapter 2 ("General security measures") contains general security recommendations. It includes advice on setting up a security organisation and security management, as well as some tips and recommendations on securing networks.

Chapter 3.1 ("Protecting your electronic signature") examines the risks and threats in key management and, in particular, contains advice on how to store keys securely.

Chapter 3.2 ("Use of portal solutions") considers the specific risks associated with using portal solutions and describes appropriate measures on avoiding such risks.

The increasing use of mobile devices – either for using EBICS apps or as a medium for allocated electronic signatures (AES) – is examined in Chapter 3.3 ("Use of tablets, smartphones and phablets"). This examines, in particular, the specific threats in connection with the use of smartphones and tablets etc., and recommends security measures for these platforms.

As social engineering attacks are becoming 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 disclosure of personal and professional data – an entire chapter has been dedicated to this topic (Chapter 3.4, "Social engineering").

[3] The German Banking Industry Committee (Deutsche Kreditwirtschaft, DK) is, as an alliance of the National Association of German Cooperative Banks (Bundesverband der Deutschen Volksbanken und Raiffeisenbanken), Association of German Banks (Bundesverband deutscher Banken, BVR), Association of German Public Banks (Bundesverband Öffentlicher Banken Deutschlands, VÖB), Deutsche Sparkassen- und Giroverband (DSGV) and the German Pfandbrief Banks (Verband deutscher Pfandbriefbanken, VDP), the lobby group for the German credit industry's umbrella organisations. In August 2011, it became the successor of the German Central Credit Committee (Zentraler Kreditausschuss, ZKA) whose work it continues.

[4] The EBICS community consists of the German, French and Swiss credit industries.

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 application- and data-access protection, the installation of firewalls, authorisation management as well as monitoring and logging. Protection against malware is indispensable in today's world.

In addition, you should have a regulated process in place for installing software and should 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, where 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 beforehand by the responsible IT manager at your company. To further improve security, the installation should be approved, implemented and documented using the dual-control principle. The workstations and access routes required for installation and maintenance (e.g. for remote maintenance software) should be defined and approved in advance.

- In keeping with standard practice, the EBICS user profiles should also be checked on a regular basis to ensure they are up to date (e.g. by deleting profiles for employees who have left, updating signing authorisations, etc.).

- If you believe that a particularly high level of protection is required for the EBICS client, it should be run on a dedicated, secured, stationary device. This can be achieved, for example, by ensuring that only a limited circle of persons has 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 should contain an automatic protection function so that it is permanently running in the background and updating itself as soon as the computer is booted. In the absence of such automated mechanisms, the antivirus software should be updated manually each time the computer is booted and before the EBICS system is started. The antivirus software should perform a full scan of the computer at regular intervals.

- In general, passwords should be sufficiently long and contain a mixture of upper- and lower-case letters, numbers and special characters. It is recommended that passwords be changed regularly. Identical passwords should not be used for different purposes or logins.

- To protect passwords from being compromised, they 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 – which generally include a function for generating secure passwords. In addition, you might also wish to use a program that al-

lows password entry without using the keyboard. This prevents unauthorised parties from logging passwords entered at the keyboard (using a keylogger[5]) and misusing them.

- In general, electronic banking products (EBICS clients and portals) display the last login or login attempts; you should always check this and pay particular attention to any failed login attempts.
- A secure internet connection should always be used for EBICS communication. We strongly advise against using unsecured or unknown WiFi connections (e.g. in an internet café).

[5] A keylogger is hardware or a software program that logs, monitors or reconstructs a user's keystrokes on a computer. Keyloggers can be used, for example, to eavesdrop passwords that a user enters via the keyboard, which can then be covertly accessed by a hacker.

3 Risks and potential threats

3.1 Protecting your electronic signature

3.1.1 What are the potential risks?

The security procedures defined in EBICS for the authentication, encryption and authorisation of payment orders (electronic signature) offer 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 so-called asymmetric encryption, which uses private keys to generate signatures for authenticating EBICS users and for authorising payment orders. Public keys are used to check the signatures and encrypt the data. It is therefore vital that the private and public keys be stored securely and protected against unauthorised access and (undetected) alteration. Unauthorised persons in possession of a copy of the key 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 (chipcards) in the framework of a remote signature procedure, or saved as software keys in files. Payment service providers tend to offer their clients chipcards as these offer greater security. The keys are additionally protected with a personal identification number (PIN). For security reasons, we recommend that you store keys on chipcards as these cannot be copied or removed without detection, nor can they be used without knowledge of the PIN.

Should you, nevertheless, chose to use key files[6], you should take great care to ensure that these are securely stored and saved, and protected against unauthorised access.

You should be particularly wary 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 that contain key files could be accidentally left lying around or remain plugged into the computer.

3.1.2 What measures are recommended?

Secure storage of software keys

Key files can be copied covertly and, in this way, fall into the hands of unauthorised individuals. Consequently, 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 medium (e.g. USB flash drive) on which the software keys are stored must be protected against fraudulent use and theft. This means that it must be

[6] Where a hardware device (e.g. a chipcard) is not used, the keys are stored in key files which are known as software keys.

kept securely, e.g. by locking it away. We additionally recommend that you also restrict access to the security device. For example, by using a special USB flash drive with a numerical keypad and encryption hardware.

Immediate blocking of keys where misuse or theft is suspected

If you suspect that key has been misused or stolen, you should inform your payment service provider immediately about the misuse or loss/theft of the key and lock the EDT access of the users concerned via EBICS (order type: SPR).

Unambiguous allocation of each security medium 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 medium (e.g. USB flash drive) and be responsible for it. The user must use this device exclusively for storing the key files for the EBICS system.

Changing the key files regularly

If key files are used, we recommend that you change the keys regularly at specific intervals. Key-change requirements 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.

Use of a suitable security medium to store key files and suitable passwords for accessing the software keys

A security medium for storing key files should only be used for this purpose, and not to store any other data. Access to both the device and to the software keys stored on it must be password-protected. In general, the EBICS software only allows the user to access the keys if the correct password is entered. Your company's internal security policy should include rules for creating and changing passwords. The German Office for Information Security (BSI) has advice on creating secure passwords at www.bsi.bund.de.

Security devices which are no longer used should be securely disposed of or destroyed.

Multiple signatures provide greater security

From a legal perspective, while it is possible to authorise the banking data with a single signature, multiple signing is recommended to increase security. In this case, you agree with the payment service provider that two signatures are needed for full authorisation.

3.2 Use of portal solutions

3.2.1 What are the potential risks?

In contrast to an EBICS system running on a local computer, a portal solution is a system that a payment service provider or a service provider operates centrally for many clients.

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 when using key files – are stored locally at your company. Specifically, the EBICS keys for authentication and encryption and all banking data (payment orders and account statements etc.) are stored in the environment of the operator's portal solution.

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

In particular, the risks set out in Chapter 3.1 "Protecting your electronic signature" apply to the use of keys. It is essential that you observe the recommendations for minimising risks provided in that chapter.

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

- The use of a browser means that portal solutions are commonly targeted by malware. In certain circumstances, malware may manipulate payment data or access sensitive data (e.g. account information).
- If a browser is hacked, the data needed to access the portal could fall into the hands of third parties.

3.2.2 What steps are recommended?

Use of approved browsers

Only use browsers that have been approved by your payment service provider and install the vendor's published security updates at short notice. Refrain from using browser add-ons if these are not absolutely needed. This applies in particular to Java applications which are made available via additional plug-ins[7]. Browser add-ons should only be enabled for trusted websites. Any phishing- and malware-protection mechanisms integrated in the browser should also be used. The BSI offers tips for secure Web browsers at https://www.bsi.bund.de.

Use of antivirus software

Ensure that the antivirus software used also protects the browser. To protect yourself, you must always ensure that the software status is kept up to date, and load available updates and install newer program versions.

Secure access to the portal solution

When you use a portal solution, your data (e.g. an input payment) are transmitted between the browser on your computer and the portal. These data should be transferred in encrypted form only. In doing so, the operator of the portal solution must use the TLS protocol for encryption to ensure that a secure network connection is established between the browser and portal.

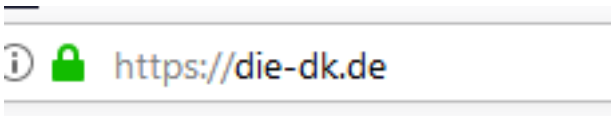
The TLS protocol ensures that data cannot be viewed or manipulated during transmission.

[7] A **plug-in** (also known as a **software add-on** or **add-on module**) is an optional software component that enhances or changes an exiting software program.

In order to establish a secure connection, the portal solution must have an URL that starts with the abbreviation **https** (as opposed to 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 portal solution operator. 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's status bar.

There should be no certification issue flagged up when you attempt to access the site via its internet address. If a problem arises, the browser issues a warning, indicating that there is a problem with the security certificate and/or informs you that the connection cannot be trusted. If this happen, 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 for accessing the portal solution should also be used.

3.3 Use of tablets, smartphones and phablets

New vulnerabilities in software and operating systems are discovered every day. These can be exploited by hackers and pose a risk for your tablets or smartphone. To protect yourself, you must ensure that the operating system and applications are always up to date, software updates are activated, and new program versions are installed. Keeping abreast of developments may often seem challenging. The same rules that apply to your PC principally also apply to your mobile device.

3.3.1 How do you secure your mobile device?

Password

The greatest potential risk is the loss of your smartphone! For this reason, you should set a password-protected screen timeout, or use additional security measures. This prevents unauthorised persons from accessing your applications and data.

[8] The purpose of two-factor authentication (2FA) is to identify users by means of a combination of two independent attributes. An example of a 2FA could thus be the combination of one component that the user knows (e.g. a password) and one that he/she possesses (e.g. a chipcard).

Should you lose your mobile device, you should optimally change all your passwords and use a remote-access security program to delete the data stored on your mobile 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 input sensitive data. Only use your mobile device to effect banking transactions in secure WiFi environments or via your mobile data connection.

Trusted sources

You should only download apps from reliable sources. Even so, you should still check the data privacy settings, access rights and where applicable, other external ratings for apps downloaded from these sources.

Where companies use smartphones as business mobile phones, a usage agreement should be concluded. An important aspect of this usage agreement should: which apps are allowed, and which ones are forbidden on the devices. The number of available apps meanwhile makes it impossible to keep track of them. It is therefore difficult to keep a **blacklist** of forbidden apps up to date. It is therefore recommended that a **whitelist** with **trusted apps** be maintained. But here the question arises as to how to determine the trustworthiness of the app. The PrivacyGrade project of Carnegie Mellon University – which rates Android apps using the US grading system from A+ to D – gives one indication of the trustworthiness of the apps. The rating criterion is the comparison of users' expectations regarding the information needs of the app 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 the links behind QR codes. Only follow links that originate from reliable sources.

Deactivate any unnecessary services

You should deactivate internet access, Bluetooth, infra-red, as well as WIFI and NFC[9] when you are not using them. This makes it difficult for criminals to access your data via WiFi hotspots and Bluetooth. Optimally, you should also encrypt your data and disable device identification via Bluetooth.

Antivirus software

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

[9] Near Field Communication (NFC) is an international transmission standard based on RFID technology for the contactless exchange of data via electromagnetic induction by means of loosely coupled inductors over short distances of just a few centimetres and with a maximum data transfer rate of 424 Kbit/s. Up to now, this technology has mainly been used in the area of micropayments – low-value non-cash payments. Other applications include the transfer of Bluetooth or WiFi authentication data for establishing a communication link, or for calling up web links if a URL is saved in the NFC chip in a suitable format.

Saving and deleting data

Back up 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?

Software is available to detect vulnerabilities and to find the current software version for your applications and operating system. We recommend that you use such software.

Glitches after entering a PIN

The communication between your mobile device and your payment service provider is extremely stable. System crashes and similar incidents are very rare.

You should therefore 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 acquire confidential information. Many people imagine cyber criminals to be technological geniuses who program complex computer codes in order to infiltrate computer networks. In reality, however, this is often not the case. Apart from conventional "hacking", in other words, 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's hard to believe, but social engineering techniques 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.

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

An organisational chart and telephone directory is often enough for a practised hacker. Armed with knowledge of the company's predominant hierarchical structures, the hacker then phones the company. Using fake identities, they use skilful questioning and psycho-

logical techniques to cautiously and gradually work their way towards the desired information.

The perpetrators frequently assume the role of someone in a position of authority or trust. In doing so, they piece together slivers of information which they later use to make them appear trustworthy in another setting.

Social engineers frequently target passwords, e.g. log-in data for banking information. They might feign a problem requiring an immediate solution, e.g. a hacker attack necessitating immediate access to a bank account. Because they comes across as assertive and authoritative, used psychological criteria to vet their victims beforehand, and also put pressure on their victims, these are often willing to disclose the log-in data.

Social networks in the internet offer a good starting point for social engineering. A large amount of personal background information can be found on these platforms. The information which is disclosed via their profiles can be gathered and used as the basis for further information acquisition.

3.4.2 What can you do to protect your security?

Be reticent with information

Social engineers feign to be someone that they are not and, in doing so, fake their identities. For this reason, do not disclose any information for which you have not been expressly authorised. This includes details regarding work processes and company organisation, roles and responsibilities, colleagues' personal information and, in particular, 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, prioritise caution over courtesy. You should clarify with your supervisor that you will not be penalised if the Management Board or a key client has to wait for their requested document while you double check the request.

Safeguard sensitive information

Never keep written notes or correspondence on your desk – you should protect this information from being seen by unauthorised individuals. Always store sensitive documents in encrypted form on your PC. Important conclusions can be drawn even from ostensibly trivial information when combined with other data. Avoid discussing internal company matters in public places, e.g. on the train or in cafés.

Ignore orders to access sensitive content

You should be particularly wary if are asked to access sensitive data on an urgent or prospectively beneficial pretext. Attackers like to masquerade as your boss or payment service provider in order to obtain access to sensitive information.