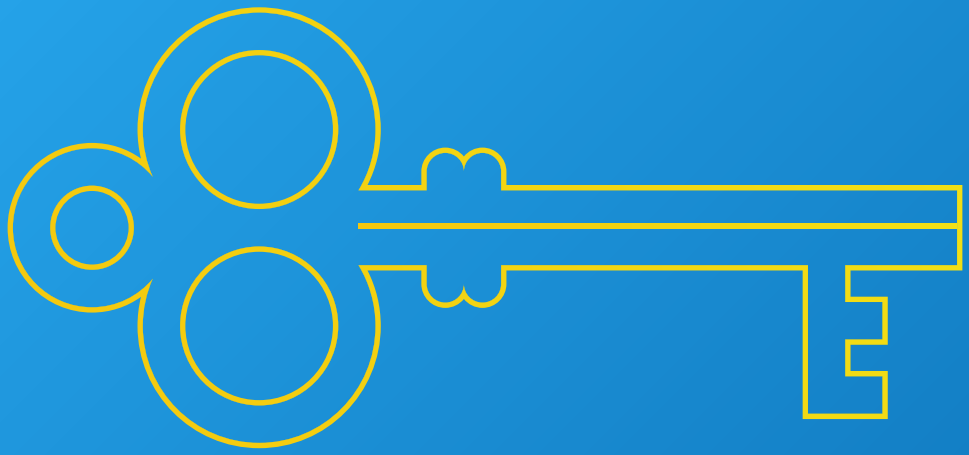
Outbank



About Certificates And Encryptions

A Guide To Secure Online And Mobile Banking

Content

1. Executive Summary

Mobile banking is convenient, fast, efficient, and possible from anywhere. Despite all the simplicity, concerns are increasing as to the security of banking apps, though. According to a test by German consumer organisation Stiftung Warentest in fall 2018, mobile banking is just as secure as online banking. Nevertheless, more than half of German people considers online banking to be insecure, as a survey by German consumer research company GfK stated in the same year. The fear of data breaches and security flaws is huge. A limited amount of information available on how to protect one's personal data reinforces the perceived uncertainty.

In fact, there are numerous security mechanisms and methods that make smartphone banking secure and fully protect banking applications. For example, if you value integrity of your data, you can search for providers that do not use external data storage but store data directly encrypted on your smartphone. If you fear that transactions could be intercepted and diverted, you can stick to banking apps that require continuous validation of the banks' security certificates. If you are concerned that unauthorized persons could make transfers via your smartphone (e.g. in the event of phone loss or theft), you should choose a provider that places importance on local data encryption and uses particularly strong password security measures.

This white paper illustrates what actions Outbank is taking to protect the privacy of its users. It will provide technologies in details and explain how potential hazards can be avoided. A security glossary will help the reader to better understand the security architecture in the banking environment and explain common attack methods. In addition, it should help mobile bankers to find a truly secure application. If you check banking app providers for these conditions, you are on the safe side.

2. How Does Outbank Handle Banking Security?

The financial situation determines how to shape one's life. Money allows you to pay rent, lunch, insurances or to take a trip. That is why all data related to money and finances are not only very personal, but also very sensitive. These data should only be seen by people who are absolutely trusted.

That is why Outbank supports the approach of absolute data privacy and security. Outbank encrypts, stores, and saves the user's sensible data directly on his own device. For this purpose, latest encryption standards are used. To ensure maximum security on the device and during the communication with banks, Outbank has implemented the following security measures:

- **Local Data Storage**

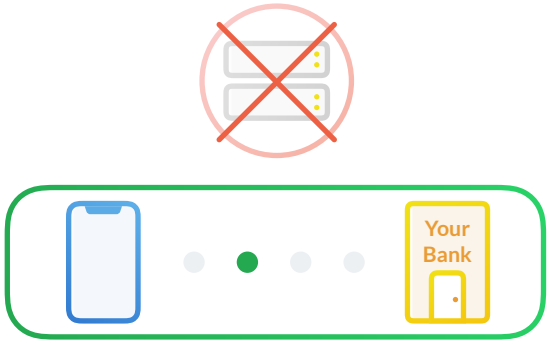
Outbank stores all financial data encrypted on the user's device. The data are only visible to the user but neither to Outbank nor other third parties. The principle underlying is zero knowledge. Even large companies like Apple are increasingly relying on zero-knowledge data security and store the user's data only on his device – without having access to it at all.

- **Modern Data Encryption**

If data are encrypted, a reference line like "car insurance" is converted to a long block of encrypted character and number combinations, also called ciphertext. These combinations are unreadable and make no sense to people and computers. Of course, there are big differences in the difficulty of these combinations. Outbank uses the world's most secure encryption standard for sensitive financial data: symmetric AES encryption. This type is also used to secure government documents of highest classification level. To decrypt the data and make them understandable and readable again, a key is required. At Outbank, this key is generated from the user's self-assigned master password. Since only the user knows the password, only he can make his data readable and usable again. No one besides the owner of the master password can access the encrypted content.

- **Direct Bank-Device Communication**

All communication between a bank and the Outbank application is done directly between financial institution and user device. As in the case of local data storage, no servers are interposed for the communication process. Other providers often use proxy servers to communicate with the user's bank. For this, they must know login data unencrypted. Their servers not only know credentials of all their users, but also all financial data sent to users – a very profitable target for



attackers. Outbank eliminates this risk entirely because the app communicates directly with a bank and not via interposed proxy.

- **Secure Bank Certificates**

Each bank holds a security certificate, called TLS or SSL certificate. With this, the bank certifies that the connection to its servers is not compromised but trustworthy. Most banking app providers usually do not validate the certificate explicitly but leave this responsibility to the manufacturer of the operating system. Outbank, however, validates each certificate before establishing a connection. This process is called certificate pinning. In addition, Outbank checks the security of all servers used by providers automatically several times per hour from different locations (different autonomous systems). As soon as an irregularity occurs, Outbank interrupts the connection to the bank immediately. In the event of a cyber attack on the communication with a bank, neither a connection nor a communication between app and bank takes places. Currently, Outbank is one of the very few banking apps that provide this increased security level.

- **Protected Data Synchronization**

Another special feature of Outbank is the secure synchronization of data on all devices during secure sync. For this process, Outbank uses AES encryption. User data are first encrypted and anonymized and only then sent as unreadable cryptograms via an AWS server in Germany. The way through a server is necessary to synchronize the data on all devices. All information on the server are encrypted with the user's individual master password. No one has insight.

In summary, Outbank protects sensitive user data by encrypting all data on the user's device by highest security standards. Even if an user synchronizes his data via the Outbank infrastructure, the data are secure since they are encrypted before being transmitted and only then sent to the server. In addition, Outbank secures communication between app and bank through a continuous validation of the bank's security certificate. How these security technologies actually solve users' problems and fend off cyber threats is shown in Chapter 4.

3. The Transparent Citizen – Also In Mobile Banking?

If I manage my financial data in a banking app, does the company know if my account is in the red? Does it even report that? Do I have to worry about my data being sold to insurance companies or other financial service providers that harass me with offers? And does Outbank not need to know my current financial situation in order to be able to propose changes and savings?

Legitimate questions that Outbank can answer in one word: **no**.

No, Outbank never knows the user's account balance. Whether in debt or billionaire, Outbank has no insight into financial data. They are stored encrypted on the user's device and can only be accessed by the user by entering his master password.

No, no financial data or account balances are passed on to other financial service providers or portals. Since Outbank can not access or view user data, it is impossible to share or sell financial information. In Outbank, only the user and his bank are aware of his financial situation.

No, even with features such as contract switch or contract termination, none of the participating companies gets insight into the user's financial data generally. These companies only receive data that the user enters in the form provided during a switch or termination – no other data like transactions or balances are transmitted. Suggestions for contract changes in the app are based on Outbank's own contract recognition methods. For this purpose, algorithms are used which are executed exclusively on the user's device. Only when the user performs a contract switch or termination, the necessary data will be shared with the companies involved (Verivox or Aboalarm).

4. How To Overcome Banking Risks With Outbank?

Since 2001, Outbank has been monitoring the mobile banking industry and developing the app from categorization to Touch ID in accordance with user needs and industry innovations. At the same time, Outbank is investigating potential threats to mobile banking and how they are raising security concerns. Outbank responds to these potential threats with security technologies developed by the Outbank team over many years and with huge experience.

- **Threat #1: Phone Loss**

What happens to my banking app when I lose my phone? Can the thief or finder steal money from my accounts?

Of course not. Outbank does not store passwords. Therefore, the finder of the smartphone or laptop can not change or reset the password via a reset button or email. If you do not know or forget the master password, the app remains locked.

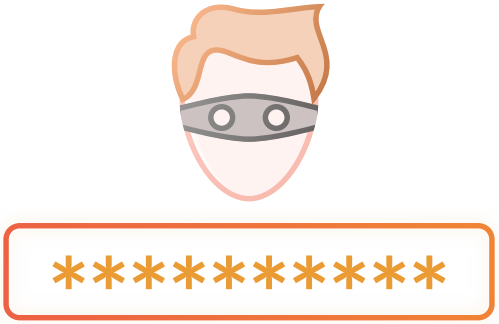
If the finder or thief is in possession of the phone, they can not use the app nor view financial data. They would also have to crack the password. However, this is almost impossible in Outbank, as the next point describes.

- **Threat #2: Password Theft**

Anyone trying to crack the password of an Outbank user bites their teeth. The scammer would have to decipher a highly complex encryption system.

Since Outbank does not centrally store user data or passwords, there are no server databases that could be cracked. Risks due to attacks on password databases are therefore eliminated.

Nowadays, fast computers can calculate so many numbers and character combinations in seconds that even the most complicated passwords can be cracked in no time. Again, Outbank protects every user – no matter how hard or easy he chose his master password. Every single master password is converted into a new, cryptic key of fixed length and thus changed illegible. This conversion happens via the key derivation function PBKDF2. In the past, hashes like MD5 hash



were used. Meanwhile, fast computer systems can easily crack these. The key derivation function PBKDF2 is one of the safest methods for generating cryptographic keys from passwords. Calculation of this key takes a lot of time and immensely increases the effort, an attacker has to raise for guessing the password, for example, with brute force.

- **Threat #3: Bank Hacks**

In recent years, news of cyber attacks on banks have become more frequent, e.g. the British Tesco Bank, the Russian Central Bank, or the Bangladesh Central Bank. Often, man in the middle is mentioned: An attacker interposes between user and bank and thus intercepts the data stream.

Of course, Outbank can not prevent an attack on a bank. However in Outbank, users of every bank are protected in case of an attack: If a bank's security certificate has been compromised or tampered with, Outbank blocks access to the bank. This prevents users from performing transactions in an unsecure banking environment. In addition, Outbank checks every 15 minutes whether the security certificates are intact. This security procedure is also referred to as active certificate pinning.

- **Threat #4: Smartphone Hacks**

Criminals are attacking banks as well as smartphones. They exploit security holes on the device, infiltrate through infected spam emails, or fake WiFi connections. Very often, they then manipulate the TAN generator app or intercept smsTAN so that, for example, they can change the money recipient during a transaction.

Outbank users are protected during a smartphone hack or man-in-the-middle attack on the device as well. The reason for that is once again certificate pinning: An attacker can, for example, still intercept the smsTAN, but he cannot change the recipient or transfer amounts. If he wants to send fake data for the transaction to Outbank, the app detects the manipulation based on the compromised SSL certificate – and terminates the connection immediately.

5. How Can I Protect Myself Better In The Internet?

Security is always a double-edged sword in the Internet, because "security is only as secure as its weakest link". While Outbank takes all necessary steps to ensure nearly 100 % safety of users, the users themselves are responsible as well. Following some tips on how everyone can contribute to greater security in banking:

- **Check Links And Attachments Of Emails**

Viruses often infiltrate PCs or smartphones through infected email attachments or links. Therefore, users should not open attachments from senders they do not know.

By now, spoofing emails are well-engineered. They adapt to an user and pretend to be a person or institution the user is often in contact with. If you are unsure about an email, a Google search with the email's subject might help. If it is an infected spam email, usually the first search results indicate it.

Similarly, phishing emails attempt to lure users to infected websites. Often disguised as a well-known company, phishing emails contain infected links. In some cases, attackers pretend to be a person in the recipient's company to strengthen their trust (CEO fraud). If there was no contact with the company or person in the last two or three weeks, these emails should be deleted directly. If you want to assure yourself and open the email, you should not click directly on the link provided. The link address can usually be displayed by mouse-over. If this address does not lead to the company's website, it might redirect to an infected website.

- **Use Official App Stores**

If you do not download apps from Google's or Apple's official app stores, you risk infecting your device with viruses.

Especially for very popular or highly anticipated apps, there is a risk that other websites will offer downloads of these versions. Since these websites are not subject to the security regulations of the official app stores, their apps are often infected with Trojans.

Users should therefore download apps only from the official Apple App Store or Google Play Store. All apps listed there are checked by the platforms in advance. They can usually be downloaded without hesitation.

- **Authenticate With 2 Devices**

In fall 2016, a security hole in the photoTAN process caused a stir throughout Germany. The reason for the vulnerability was that TAN authentication was done through one device only.

Typically, two independent devices are used for a secure TAN process (two-factor authentication). As a result, only the one who has both devices can perform an operation. In the photoTAN process, however, the TAN is not generated on a second device. Attackers have an easy job: They settle into a gap on the smartphone and hack the TAN generator app. In this way, they can manipulate, record, intercept, or change the money transfer to transfer it to another account.

Therefore, users should always use two different devices for TAN operations. When transferring money, for example, it makes sense to receive a mobile TAN for the transaction on the smartphone and perform the operation on the Mac or PC. This ensures that both generation and application of a TAN are safe.

- **Avoid Websites Without A Lock**

If a website has a valid security certificate, it will immediately be displayed to every user by a small lock icon in the URL bar of the browser. The TLS or SSL certificate encrypts data streams. Any website that queries or stores user data should therefore have a certificate. If it is not available, the data can be displayed freely and provide a simple target for attackers. Users should always take a quick look at the URL bar before registering on a website. Does a lock appear? If so, basic security is created.

- **Avoid Banking In Public Networks**

In contrast to private Wi-Fi at home, public Wi-Fi connections are rarely encrypted. Anyone who connects here runs risk of having their data intercepted or manipulated. In some cases, criminals even set up their own “free Wi-Fi“ connections, in order to hack attached devices and read the data. It would be almost negligent to perform online banking in public, free networks.

Therefore, users in a public Wi-Fi should not retrieve personal or confidential information or even do mobile banking. If you use external computers for surfing or banking often, you should always clear the cache of the browser afterwards. In the cache, browsers store the data of the last connections. If this information is not deleted, criminals can later read and abuse it. Users should therefore refrain entirely from using third-party computers for their banking business.

6. Glossary

AES Encryption

Advanced Encryption Standard (AES) is the most secure form of data encryption up to now. This method creates a hieroglyphic ciphertext of a certain length (128 bits or a number with 39 digits) from a plaintext such as the **master password**. The conversion from plaintext to ciphertext is secured by another key. This has a length of 128, 192, or 256 bits, which corresponds to a number with 39, 58, or 78 digits each. When the key is entered, the conversion is undone and the plaintext (the master password) becomes readable. If encryption and decryption key are the same, it is called symmetric encryption.

Autonomous System

An Autonomous System (AS) is a cluster of networks that communicates through a protocol. Every major Internet Service Provider such as Telekom or Vodafone has its own AS. All AS are interconnected and together they form the Internet. At **certificate pinning**, Outbank uses various AS to validate the **security certificates** of the banks. If the certificates of a bank differ in each AS, a manipulation is indicated. Since Outbank queries the certificates in different AS, it will detect this manipulation immediately and therefore can protect its users from this threat.

Brute Force

In information technology, the Brute-Force search is a method where all possible solutions are tried until the right one is found. Criminals use this method, for example, if they want to guess passwords. In Outbank, users are protected through cryptographic keys that are generated from the **master password** using **key derivation function PBKDF2**.

CEO Fraud

CEO Fraud is often used in **phishing emails**. This scam aims to get users to transfer money. An attacker fakes emails, which he sends, for example, on behalf of a CEO or another person in the receiver's company. In it he asks the user to transfer money.

Certificate Pinning

Like any trusted website, every bank has a **security certificate**. This confirms the bank's identity and promises a non-manipulated connection. In a cyberattack on a bank, for example through **man in the middle**, the security certificate could be **compromised** and therefore no longer trustworthy. The attacker could thus manipulate the connection between bank and user. Outbank protects its users against it by checking each security certificate every 15 minutes using certificate pinning. If Outbank detects that a certificate is invalid, the connection is blocked in advance.

Compromising

When a system is Compromised, the safety of data is no longer guaranteed. Attackers could invade, display, or manipulate data. Often attackers compromise the connection between bank and user to intercept data (**man-in-the-middle attack**). Procedures such as **certificate pinning** protect users in Outbank from effects of compromised connections.

End-To-End Encryption

End-To-End Encryption ensures that data are constantly encrypted and protected as they are being transmitted. In Outbank, this encryption method is used in combination with the **zero-knowledge principle** for secure data transmission (**secure sync**). There, the data are first encrypted by highest standards (**AES encryption**) on the user's device. Only then do they leave the device in direction of the cloud storage. The data can not be viewed by any of the participating companies at any time. Only the user can decrypt the data with his **master password**.

Key Derivation Function PBKDF2

To convert a password into a cryptic key, Key Derivation Functions are used. A certain function is applied to the same password several times. These iterations ensure that the original password can no longer be guessed. This makes it even more difficult for attackers to guess passwords, for example using the **brute-force method**. Outbank uses the standard PBKDF2: Password-Based Key Derivation Function 2.

MD5 Hash

The Message Digest Algorithm 5 (MD5) is a function that converts text into a 32-character string, no matter how long or short the text is. If only one letter in the text changes, a completely different string is created. Only if the strings (hashes) of two data packets match, integrity of the data is confirmed. This procedure facilitates the comparison of data. Previously, MD5 hashes were used so that passwords did not have to be transferred or stored in plaintext. Nowadays, fast computer systems can easily crack MD5 hashes. Therefore, this method is no longer secure enough to generate cryptographic keys. Outbank therefore uses **key derivation function PBKDF2**.

Man In The Middle

In a Man-In-The-Middle (MITM) Attack, an attacker places himself between two systems, e.g. the user and his bank. The attacker can thus intercept, control, and manipulate the data exchange between the two. Outbank users are repeatedly protected against MITM attacks, for example by continuously checking the security certificate (**certificate pinning**).

Master Password

The Master Password is a user-assigned password that the user creates when first setting up Outbank. With this password, the user unlocks the Outbank app. To decrypt the data after synchronization via **secure sync**, the user must enter his master password as well. The password is not stored and therefore can not be reset. If you do not know the master password, the app will remain closed. Not saving passwords increases security: If no passwords are stored, they can not be stolen. If an user forgets his password, he must reset Outbank and all data stored in the app will be lost.

Phishing Emails

Phishing Emails aim to intercept the user's banking credentials. They disguise themselves usually as a known sender, such as major banks, payment systems, online-shopping companies, logistic service providers, or packing stations. In doing so, they redirect the user to a malicious website that is similar to the layout of the sender's company. For example, the user is prompted to log in to pay outstanding amounts or to have vouchers transmitted. The website records the user's login and password entries. The attacker can then use the login data for his own benefit. Well-known phishing methods include **CEO fraud** and **email spoofing**.

Secure Sync

In Outbank, the Secure Sync is the secure data transfer across multiple devices. When an user uses secure sync, his data are automatically updated on multiple devices. Numerous security technologies protect data transmission, including **AES encryption**, **end-to-end encryption**, **key derivation function PBKDF2**, and **certificate pinning**. Before the data are sent, they are encrypted on the user's device. Neither Outbank nor the cloud provider Amazon can view the data before, during, or after the transfer. The data remain fully encrypted throughout the whole process. Only when the user enters his **master password**, the data are readable again. Currently, secure data transfer is available for iOS and macOS devices.

Security Certificate (SSL, TLS)

A Security Certificate confirms that a website transmits data securely and encrypted. Especially for websites that provide personal and sensitive user data, the certificates are absolutely essential. They are transmitted via the Transport Layer Security (TLS) Protocol, which is why they are also known as **TLS certificates**. Previously, they have been transmitted via the Secure Sockets Layer (SSL) Protocol and are therefore referred to as **SSL certificates**. The certificates are issued by certification authorities such as Comodo, VeriSign or Symantec. Those check whether the applicant (for example the operator of a website or a bank) is entitled to receive a certificate for a specific Internet address. Depending on the level of security, the applicant must meet requirements of varying complexity.

Spam Email

Spam means unwanted, often virus-infected emails. Every trusted email provider today has a spam folder integrated. Using intelligent algorithms, suspicious emails are sorted out and automatically stored in the spam folder. The user can then decide if these emails should be opened or deleted.

Spoofing Email / Email Spoofing

In Email Spoofing, attackers fake their identity. For example, a name known to the email recipient is displayed as sender. The actual email address, however, is fake. As with other **phishing emails**, email spoofing is about receiving secret user data or persuading the user to transfer money.

TAN Procedure

A **Transaction Number (TAN)** can be used to authorize certain transactions, such as mobile and online banking transfers. To generate this one-time password, various methods are used.

Tan/iTAN
A TAN list is the initial version of all TAN procedures. The printed list contains a certain number of TAN codes that can be used in any order. If the list is used up, the user receives a new one. By now, this procedure is no longer in use because it is too unsafe. In the Indexed TAN list (iTAN), each TAN is assigned a certain number. For a transaction, the bank asks for a specific number from the list. This procedure will also be discontinued in September 2019 due to security issues.

smsTAN (mobileTAN, mTAN)
In the smsTAN procedure, the TAN is sent by the bank via SMS to a stored mobile phone number of the user.

optical chipTAN
For the optical chipTAN process, an user receives a TAN generator from his bank. In order to perform a transaction, he puts the bank card in the generator. On the screen of his device (PC or smartphone), five flickering bars appear. To generate a TAN, the user needs to hold the generator within the specified range of the flicker code. Subsequently, the TAN is generated and appears in the display of the generator.

manual chipTAN
In the manual chipTAN process, an user also receives a TAN generator with card slot. Before a transaction is triggered, a start code appears on his device's screen. The user has to enter this code in the TAN generator. Then he types in the account number of the recipient and transfer amount. From this information, the TAN is generated eventually.

photoTAN
A photoTAN process is performed by a single device. The data of each transaction are displayed as a colorful pixel graphic. To decrypt and generate a TAN, the user needs an app from the bank or a photoTAN reader. If only one device is used in this procedure, it is considered unsafe. Therefore, in Outbank this process is currently only possible with an additional device.

pushTAN
In the pushTAN process, the user also requires a separate app. Before he can authorize a transaction, he receives a notification in the pushTAN app. After verifying and confirming the information contained, the TAN is generated.

Two-Factor Authentication / Two-Device Authentication

Two-Factor Authentication (2FA) is designed to protect users from theft of digital identity. For this, an user must confirm his identity through two independent factors. This happens, for example, via a password and additional information that are sent by SMS when logging in. Attackers can only pretend to be the user if they have both factors – in this case, password and mobile phone.

In the context of TAN procedures, this technique is also referred to as **two-device authentication**. One device is used for TAN generation and one for execution. With **smsTAN** for example, an user prepares a transfer on his PC or Mac and requests the TAN in the TAN window. The TAN will then be sent to him via SMS on his smartphone. He enters the code into the window on his PC or Mac and sends the transfer order.

Zero-Knowledge Principle

The term Zero Knowledge was coined by Edward Snowden. The zero-knowledge principle aims to ensure that personal data are constantly protected even when transmitted via cloud providers. Therefore, the data are transmitted encrypted. Thus, neither the data processing company nor the data-transfer or cloud-storage provider can view personal user data. Outbank uses zero knowledge in combination with **end-to-end encryption** for **secure sync**.