

Special Terms of Use for mobile payment by wallet with the ZKB Visa Debit Card (February 2024 edition)

1. Use and functions

These Special Terms of Use apply to payments made with a secure token ("token"), e.g. using a digital wallet ("wallet") or another mobile (including electronic) payment solution ("payment solution"). The token is activated using the ZKB Visa Debit Card ("card").

Payment solutions may be made available by providers (e.g. wallet providers) or international card networks ("providers"). The token required for the payment solution is activated by the authorised cardholder on his or her end device (e.g. smartphone, tablet, PC or wearable), and is used for payment at designated acceptance points in Switzerland and abroad.

The token enables the following main functions:

- Authorising transactions carried out online or on-site at an acceptance point.
- Listing of transactions with the token that were authorised and paid (if offered in the payment solution).
- Locking, unlocking or deleting the token as well as other functions according to the payment solution's scope of services or via a secure channel provided by the Bank (e.g. eBanking or Mobile Banking).

These Special Terms of Use supplement the Terms and Conditions for the ZKB Visa debit card ("Card Terms"), and take precedence in the event of any contradictions with the Card Terms. The Card Terms apply to payment solutions even without explicit reference in the individual sections of these Special Terms of Use.

2. Terms and instructions of the provider

The provider provides its services on its own contractual basis with the authorised cardholder, and is responsible for the scope of services and the functionalities of the payment solution. The Bank is not the provider of the payment solution, but simply enables the activation of the token. Thus, the separate terms and instructions for using the payment solution belonging to the relevant provider will apply in addition to the provisions herein. In activating the token and with each use of the payment solution, the authorised cardholder accepts these Special Terms of Use in addition to any terms of the provider.

3. Data processing by service providers and third-party providers

The provisions for the processing of data by service providers and third-party providers in the Card Terms shall apply. In the course of activating the token and using the payment solution, information and data is exchanged between the parties involved, such as the Bank, the provider and the international card network, as well as third-party companies commissioned by them.

The provider collects or receives information and usage data, such as transaction details, as well as data stored on the end device, like data from a SIM or memory card and geodata. The provider processes data independently and autonomously from the Bank for its own purposes in accordance with its own separate terms and privacy policy. This data can be processed both domestically as well as abroad. The provider may engage third-party companies for this purpose. The authorised cardholder acknowledges and accepts that Swiss bank-client confidentiality does not apply to the provider or third-party companies in Switzerland and abroad. In addition, the relevant foreign data protection legislation applies abroad; this may not provide an appropriate level of data protection compared to Switzerland and may lack comparable rights, such as restrictions on access and disclosure. **To this extent, the authorised cardholder expressly releases the Bank from Swiss bank-client confidentiality and Swiss data protection law.**

The Bank is not responsible for the data processing carried out by the provider. The authorised cardholder shall contact the provider directly with any questions or objections regarding data processing.

4. Approved end devices and applications

The provider defines which end devices as well as applications and operating systems are required to use the payment solution. Any questions or objections in case of malfunctions or system failures must be addressed directly to the provider. The Bank shall provide assistance with the activation and use of the token, but not with the installation or maintenance of the end devices, nor of any applications belonging to the provider.

5. Activating, replacing, blocking and deleting the token

The activation of the token is carried out via a process defined by the provider with involvement of the international card network and – if applicable – the Bank. Any such communication is also subject to the provisions on electronic communication channels and notification services in the Card Terms as one of the use cases.

The token can be activated, replaced, blocked, unblocked or deleted in more than one end device without affecting the card status. If the card itself is blocked, unblocked or renewed, the token generally remains active.

6. Activation and legitimisation of transactions

The activation of the token by the provider for the purpose of authorising the use of the payment solution as well as legitimising transactions is carried out using a method provided by the provider (e.g. numeric code, password, biometrics). The method used is part of the provider's terms and conditions, and is agreed between the authorised cardholder and the provider. The Bank is entitled to charge all sums verified in this way to the account and credit them to the acceptance point. This applies even if the transaction is not performed by the actual authorised cardholder. The authorised cardholder is not entitled to revoke submitted transactions vis-à-vis the Bank.

7. Duties of care

In addition to the duties of care stipulated in the Card Terms, the authorised cardholder has additional duties of care. In particular, he/she must store the end devices carefully and protect them from access by third parties using the methods provided by the provider (e.g. numeric code, password, biometrics) as well as other suitable measures. Such measures include in particular the obligations not to carry out any manipulations such as jailbreaking the operating system, to keep the operating system and other applications on the end device up to date, and to take the usual security precautions, e.g. by using an anti-virus programme. Furthermore, passwords, numeric codes etc. may not be stored in an unprotected way on the end device or otherwise recorded, made accessible or shared with third parties. In the event of the end device not being used or being transferred, the authorised cardholder must ensure that the token is deleted and that the payment solution cannot be used to make payments by unauthorised third parties. The authorised cardholder must notify the Bank immediately if he/she suspects unauthorised access or if the end device or the means of identification has been lost.

8. Liability and risk

The service provided by the Bank lies solely in enabling the authorised cardholder to activate the token. The Bank shall not be liable for any damage in connection with the use of the payment solution and is also not responsible for the performance of the provider, nor for the uninterrupted functioning of the payment solution.

By using the payment solution, the authorised cardholder also accepts the following risks: The public and private data transmission networks for the exchange of information as well as the end device are a part of a greater system. They are outside the Bank's control and may become a weak point in the system. In particular, they may be subject to interference by unauthorised third parties. In addition, transmission errors, delays and system interruptions or breakdowns may happen. For example, information transmitted by the provider via text message or e-mail may be misdirected. The Bank shall not be liable to the authorised cardholder in any such case.

In addition to these stipulations, the provisions on assumption of loss in the Card Terms shall apply.

9. Changes to these Terms

The Bank reserves the right to change these Special Terms of Use at any time. The provider generally also reserves the corresponding right with regard to its services, including the types of use and the functions offered.

Changes made by the Bank shall be notified to the authorised cardholder in an appropriate manner, in particular in electronic form in the context of the use of the payment solution. They shall be deemed accepted if the authorised cardholder does not terminate the service within 30 days of notification; or in any event at the latest when the payment solution is next used.

10. Termination and blocking

Either party may terminate the service or block the token at any time and without specifying a reason. On termination, the authorised cardholder shall immediately delete the token from the payment solution. The provider may also be entitled to temporarily suspend or completely terminate its services at any time.

Despite the termination of the service or blocking of the token, the Bank shall remain entitled to debit all amounts from the account which are attributable to the use of the token while it was active, even if the transactions are only received after the termination of the service or blocking of the token (e.g. recurring fees for memberships etc. legitimised by the authorised cardholder).

11. Further Terms and Conditions

The General Conditions of Zürcher Kantonalbank shall apply in addition to the terms and conditions mentioned above. Further information on how the Bank processes data can be found in the data protection declaration at zkb.ch/privacy. All applicable Terms and Conditions are published at zkb.ch/terms.