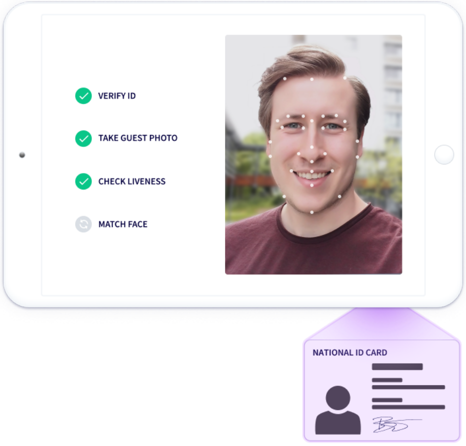
ZIPKEY



Security at every level

WHITE PAPER

Key Takeaways

- ZipKey was designed around the principle that visitor management should comply with the highest security standards without compromising on the user experience
- Fraud-proof security mechanisms have been built into every layer: the product itself, the infrastructure, and our data protection mechanisms
- Automation makes visitor management more secure and customized at the same time

January 2019

»Security at every level« has been the guiding principle of ZipKey's development process since day one

Author
Christian Böhlke, CTO ZipKey

Zipkey ensures the security of your business without paralyzing employees and guests with inflexible processes. I wanted to take the chance to share some details into how we designed our product to protect high-security buildings and offer an exceptional user experience at the same time.

Customers trust us with managing the security-critical visitor management process for them. To provide them with the high-security product they need, our development efforts are always guided by the principle **»Security at every level«**. Below, I will provide details into the mechanisms built into these different levels, namely, our product (1), our infrastructure (2), and our data protection protocols (3).

We employ product security measures that are based on intelligence agency recommendations

Let me start by describing how the product[1] itself contributes to a highly secure visitor management process in our customers' buildings. Three components are critical here: First, the authentication process, second, the user rights management, and third, the password policy.

[1] In the context of this white paper, the term »product« refers to our ZipKey Enterprise product

Our authentication process ensures that only unambiguously identified and authorized individuals are being granted access to buildings. The process starts with the host creating an invite for their guest(s) in the ZipKey dashboard. Guests receive this invite via email. ZipKey creates a digital ID of the guests based on the information the host provides. Complementary information can be added by guests during pre-registration. A QR code is connected to the guests' ID which can be used as a first identifier. To make the QR code fraud-proof, it changes every 30 seconds; this way a stolen picture of the code will not work to identify as that guest.

To enter the building, guests must prove their identity using multi-factor authentication: To begin with, guests scan their ID card or QR code at the ZipKey terminal (depending on system settings and whether the guest has used ZipKey before). Next, ZipKey scans their face using a biometric face recognition camera, which checks the liveness of the individual and matches the biometric information with the ID card photo.

ZipKey's authentication process follows the same logic as modern airport border control processes. The way we designed the product enhances both the security of the buildings and the user experience. An unauthorized guest will not be able to supply all factors (possession and biometrics factors) required for access. If at least one of the authentication factors is missing or supplied incorrectly, ZipKey will not recognize the identity of the guest as being established with sufficient certainty. As a result, the guest will not be granted access to the building. Furthermore, the authentication process is quick (it only takes 20 seconds), provides a seamless user experience, and is immune to human error (ie. our ID scanner immediately recognizes fake IDs, while the human eye can only spot parts of the ID watermarks).

> “ *The authentication process is quick, provides a seamless user experience and is immune to human error*

ZipKey's user role rights management ensures that the different user groups can only see and edit information according to their role. The hierarchy follows this structure: Super Admin > Local Admin > Receptionist > Employee > Guest. The roles are provided with cumulative rights. This means that an Admin can see everything a Receptionist sees and more and a Super Admin can see everything an Admin sees and more. The consistent rights management makes sure

that only users with high privileges have access to security-critical information.
The privileges of the individual user roles can be found in our user guide.

Our password policy ensures that user passwords are safe and user accounts are protected from unauthorized access. When a user sets a password, ZipKey checks whether the password meets our security standards and will reject a password when it does not. We then show the user recommendations how he or she can improve the password strength while still keeping it manageable. The user is then asked to add security features to the password such as special characters, a combination of upper- and lower- case characters, etc. This protects user passwords from being easily hacked by password bots.

Additional security features that are not discussed in this white paper include NDA signing or security training. They further enhance the security of the building and protect sensitive company information of our customers.

Our infrastructure meets the highest security and reliability requirements

Apart from the product itself, infrastructure plays a critical role in ensuring the security of ZipKey. To maximize the security of our infrastructure, we use encryption protocols, exclusively work with highly trusted partners, restrict access to our servers, and employ reliable backup mechanisms.

> “ *All our databases are encrypted with AES-256, which protects the data from unauthorized access.*

ZipKey encrypts all data both »in transit« (during data transfer) and »at rest« (while the data remains stored). We employ strong cryptographic methods, for which no attacks are currently known. HTTPS is used to connect the user's browser to the ZipKey servers. The specific version of the protocol and the type of encryption depends on the browser. However, ZipKey servers only accept common and secure protocols. This ensures that an attacker who manages to secretly relay and possibly alter the Internet connection of a ZipKey guest is not able to read passwords or other access information. Even if an attacker knows all the traffic, he cannot gain unauthorized access to a building.

For the storage of data, we only use the services provided and maintained by Google Cloud. These services are all configured by Google experts, which ensures an extremely high level of security and minimizes the risk of configuration errors. The software used by Google is strongly protected against attacks, and companies such as SAP, HSBC bank, and Bloomberg also entrust their data to Google in this way. We require connections to our databases to be encrypted. This protects customer data and passwords from being accessed by an attacker who would succeed in recording the communication between our servers and the databases. In addition, a connection to our databases is only possible from our servers. Therefore, in a hypothetical scenario, even if a hacker would have taken possession of the address of the database and its keys, he would not be able to access the databases and read data from them. All our databases are completely encrypted with AES-256, which protects the data from unauthorized access. AES-256 is a highy secure encryption algorithm approved by the American NSA (National Security Agency) for the encryption of top-secret documents. To store the keys of our encrypted databases, we use Google's Key Management Service. This protects the keys on special Hardware Security Modules (HSMs). The keys do not leave these hardware modules and access to them is fully logged. This guarantees that it is not possible to steal our keys and protects our keys with Google's highly recognized technology. Furthermore, all our data is stored in Germany which ensures that strictest regulations are being met.

> “ *Our multi-layer backup process ensures that customer data is always available and can only be accessed by authorized systems.*

Only our administrators have access to the servers with the customer data. Our developers only have access to the test systems where they can test new features. Only successfully tested new features are transferred from an admin to the servers running ZipKey. This ensures that no developer can jeopardize the correct operation of our servers through errors or inattention.

A reliable backup process is paramount to the security of our product. Therefore, we decided to partner with a cloud provider employing a rigorous backup mechanism. Google Cloud uses data redundancy so that data processed by our system is always stored in several locations. In addition, Google uses object versioning which means that the replacement or deletion of a file is logged and the old file is not lost but remains stored. Lastly, a daily backup of our entire database is created and AES-256 encryption of all backups protects them from unauthorized access. This multi-layer backup process ensures that customer data is always available and can only be accessed by authorized systems.

We believe that a strong product reputation depends on rigorous data protection and security protocols

Our data protection and security protocols act as a shield for user data. In order to ensure data integrity, we have established strict codes of conduct for ourselves, work with EU based services, and only store data necessary to offer a seamless user experience.

Our internal rules and procedures require each new member of our team to undergo a training process that establishes awareness of the cyber attack gateways and gives clear codes on how to deter attacks. Our internal IT security policies are aimed at preventing malware infection as well as mitigating damage and responding correctly to incidents.

> “ *Our internal IT security policies are aimed at preventing malware infection as well as mitigating damage and responding correctly to incidents.*

Just as we protect our customers' data from loss and unauthorized access, we also have **strict policies regarding the extent to which we disclose this data to third parties**. This categorically only happens to providers of IT services that play an important in the reliable functioning of the product, such as real-time notification services or cloud providers. For a detailed list of what types of customer information we share with which companies, please see our Data Processing Agreement. In principle, we only use and store data that our users have consciously and voluntarily provided to us. If a customer leaves us, we warrant that we delete all customer data within the agreed period.

We store user data only for the necessary duration and maintain a **uniform deletion concept**. Here we distinguish between three different types of data: First, master data of guests who have registered via ZipKey. Second, personal transaction data, such as the timestamp of a visit. Third, aggregated transaction data that can no longer be mapped to individuals. Data in the first category is being deleted after three years of inactivity by the user. Data in the second category is stored for three years and then deleted by default. During the three years, the customer is free to download an export of the data or to extend the deadline. Data in the third category, which are not personal and are used for administrative purposes, will not be deleted.