


Klevio's Digital Security


Secure **technology** // Impossible to hack

Klevio has been built to the same security standards as digital banking services, ensuring it is **completely secure and can't be hacked.**

	SECURE SERVERS	Microservices separated by concerns. Passwords hashed with a secure password hashing algorithm. Automatic data backups. Network layer protection and application layer rate limiting to mitigate DoS attacks.
	ENCRYPTED COMMUNICATION	All communications use secure network protocols, messages between services, devices and apps additionally signed using asymmetric cryptographic signatures.


Secure **architecture** // Impossible to seize

Your data is stored in secure cloud-based servers so only you ever have full access and control of your entry system. Your entry system and data are **impenetrable from any attack.**

	CLOUD SERVER ARCHITECTURE	Devices need to receive a cryptographically signed message from two separate services to run any action on your locks. These services are hosted on a secure server in the cloud.
---	----------------------------------	---

Secure **data** // Impossible to trace

The physical locations of locks are never tracked. There are no property addresses in the system. Simply put, **a hacker would not know what digital key unlocks what door.**

	NO ADDRESS DATA	Locks and keys in the main services are represented by abstract non sequential ids.
---	------------------------	---