

We offer you **security, privacy**
and **anonymity** in your
communications.

Introduction

In this whitepaper, we will explore in detail how Enigm ensures the protection of user information, the confidentiality of conversations, and anonymity within the platform. You'll discover how Enigm is redefining the norms of digital communication by providing an environment where users can connect without fear of intrusion or unwanted surveillance.

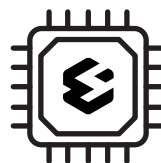
Our solution is based on four essential components:



App



Servers



eSIM



Network



App

Features

All Enigm features are designed to ensure that your communications are secure, private and anonymous. With a focus on innovation and protection, our messaging app offers you a comprehensive tool to protect your privacy and maintain full control over your data.

The app allows you to send text and multimedia messages, such as photos, videos and documents, all protected with end-to-end encryption, ensuring that only you and the recipient can access them. Additionally, you can define the lifetime of messages, allowing them to self-destruct after a specific period, eliminating any trace of the conversation. You can also securely attach files, knowing they are protected by the same robust encryption that secures your messages. To protect your identity, the audios sent may be modulated, so that your voice is not recognized. The application includes an anti-screenshot system, which detects and prevents any capture attempt to protect the confidentiality of your messages.

As for calls and video calls, you can make them with the certainty that they are end-to-end encrypted, ensuring that your communications are completely private. Additionally, during calls and video calls, you can modulate your voice to protect your identity. We implement a system that prevents the recording of conversations and the capture of video calls, guaranteeing the total privacy of your interactions.

The app also allows the creation of work groups, where communications are encrypted, and user anonymity is rigorously protected. In these groups, users cannot see or interact privately with other members they do not have as contacts, thus maintaining anonymity. The group creator can define strict permission controls, such as who can send messages, delete messages, forward messages, and more, ensuring that the group operates under a governance regime.



Anti-screenshots



Destruction of messages



Voice modulator



Recording inhibitor



Permission management



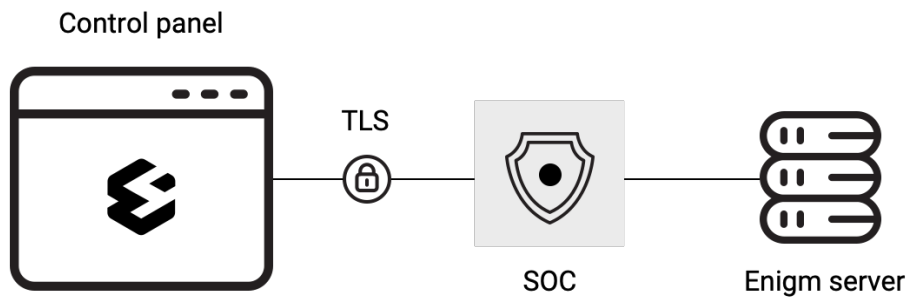
User privacy

FEATURED FEATURES

“ Enigm does **not store any messages on the phone**, not even in cache. What prevents data recovery with forensic techniques. ”

Control panel

On our platform, security and full control over your account and devices are fundamental aspects. Therefore, we have developed an intuitive and powerful web control panel that allows you to manage all aspects of your account safely and easily. From controlling connected devices to fully managing your account, our web control panel provides you with all the tools necessary to ensure your privacy and security.



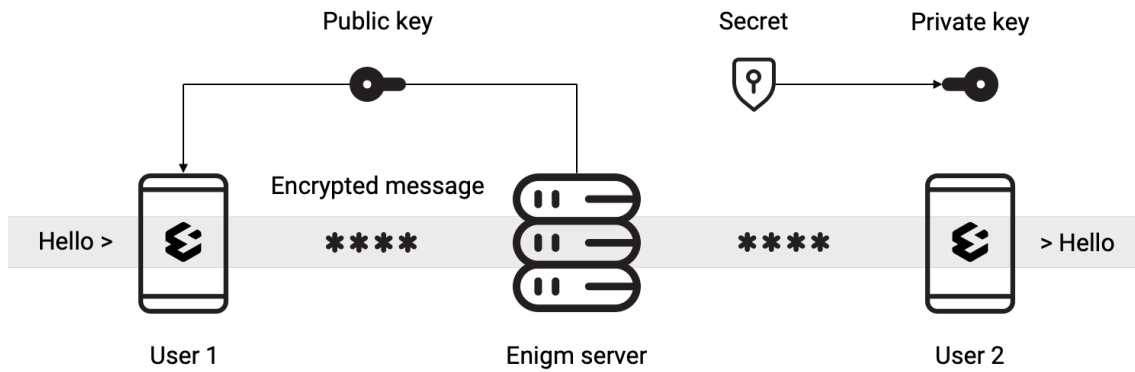
Our web control panel allows you to have comprehensive control over the devices connected to your account. You can see all the devices that have access and, if necessary, remotely log out of any of them, ensuring that only authorized devices have access to your account. Additionally, you can turn push notifications on or off based on your preferences and privacy needs, ensuring you only receive alerts on the devices you want.

Managing your account is also simple and secure through the web control panel. You can decide whether your account is visible on the public server or if you prefer it to only be accessible on private servers, thus controlling who can find and communicate with you. If you ever need to recover your password, you can do so using the passphrase generated during registration, allowing you to quickly and securely restore your access. You also have the option to change your PIN code and password at any time to maintain the security of your account, adapting them to your needs.

Additionally, the panel gives you the ability to delete all data associated with your account, including messages and media files, leaving only your profile and contact list if you wish. And if you decide that you no longer want to be on our platform, you can permanently delete your account, disappearing completely and without leaving any trace, as if you had never existed.

Encryption

We integrate the most advanced encryption and security technology to protect the confidentiality of your conversations. From AES-256 encryption to the use of post-quantum algorithms and digital signatures, our focus is on ensuring that your messages always remain secure and private.



In our messaging system, encryption is the cornerstone of data security. We use AES-256 encryption to ensure every message sent is protected end-to-end. AES-256 is an encryption algorithm widely recognized for its robustness and security, using a 256-bit key to effectively protect data.

In addition to AES-256 encryption, we implement post-quantum technology to further strengthen our security. We use the Kyber algorithm to generate and manage encryption keys. Kyber is a cryptographic scheme specifically designed to resist attacks from quantum computers, ensuring the longevity and security of our keys in an increasingly technologically advanced environment.

To ensure the authenticity and integrity of the messages, each one is digitally signed using the Dilithium algorithm. This digital signature provides an additional layer of security by ensuring that messages have not been altered during transit and are coming from the expected source.

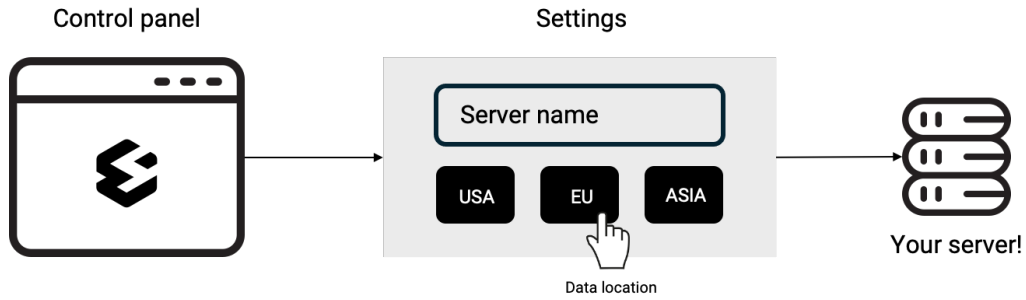
Finally, to protect the encryption keys used in our system, we implement a secrets system that distributes fragments of the keys among different authorized entities. This approach ensures that even if a key fragment is compromised, the entire key cannot be accessed without the collaboration of multiple authorized parties.

In summary, our messaging system uses a combination of AES-256 encryption, post-quantum algorithms such as Kyber, Dilithium digital signatures and a system of secrets to ensure the security and privacy of our users' communications. With these measures in place, our users can communicate with confidence, knowing that their data is always protected.

Servers

Features

Our platform also offers the flexibility and control you need through the ability to configure and manage your own servers. Any Enigm user can have their own servers, allowing full customization and control over their communications infrastructure. These servers can be deployed in the geographic location of the user's preference, facilitating compliance with local data regulations and optimizing the speed and efficiency of communications.



Through these servers, users can tell the application to connect specifically to their private server. This ensures that the user maintains complete control over their data, ensuring that the information is always under their supervision and management. This ability to direct application traffic to a specific server provides an additional layer of security and privacy.

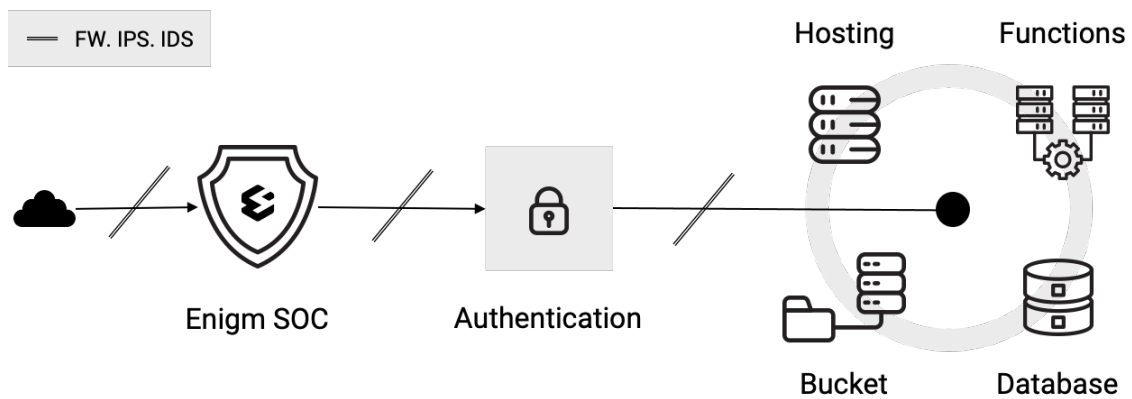
Additionally, users can delete data from their server, including all messages exchanged by members belonging to that server. This functionality is crucial to maintain data cleanliness and security, allowing the user to manage their information effectively.

Server member management is another essential feature. Users can manage who has access to the server and can kick and delete unwanted members. Additionally, they can choose to delete only the information that a specific member has left on the server without needing to delete the member entirely. This flexibility in user and data management ensures that each server can be customized to the specific needs of its owner.

In short, you can easily deploy private servers in specific geographic locations, connect the application to these servers, and manage data and members comprehensively, ensuring a secure, private, and customizable user experience.

Architecture

Our server architecture is designed with a meticulous focus on security and efficiency. We implement a series of advanced technologies and rigorous security practices to ensure that our users' data is protected at all times.





In our infrastructure, we use an application firewall system and an intrusion detection system (IDS) to protect our applications against threats and attacks. This firewall acts as the first line of defense, filtering malicious traffic and ensuring that only legitimate traffic can access our applications. Additionally, IDS allows us to quickly detect and respond to any suspicious activity that may compromise the security of our systems.

Our backend is built on a platform that offers authentication, real-time databases, storage and cloud functions. Authentication ensures that only authorized users can access our services. Real-time databases allow us to manage and synchronize data efficiently, ensuring a fluid and responsive user experience. Cloud storage is used to handle files and other user data, while cloud functions allow us to execute backend logic in a secure and scalable manner.

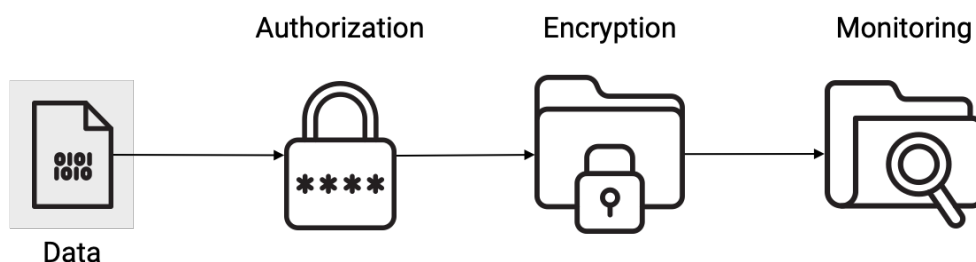
All this infrastructure is protected under an application validation system and configured with strict security rules. These rules apply to both storage buckets and databases, ensuring that data can only be accessed by authorized users and processes. This ensures that data is protected from unauthorized access and meets the highest security standards.

In addition, we implement AI security monitoring systems to constantly monitor the status of our infrastructure and detect possible vulnerabilities. However, it is important to highlight that these monitoring systems do not store or analyze any data that could identify our clients. We focus on maintaining the privacy of our users, ensuring that all personal information remains confidential and secure.

In short, our server architecture is carefully designed to combine high security with operational efficiency. From perimeter protection to secure backend and continuous monitoring, every component of our infrastructure works together to provide a secure and reliable environment for our applications and our users' data.

Data protection

Protecting data on our servers is one of our top priorities. In a digital environment where security threats are increasingly sophisticated and persistent, we have implemented a series of advanced measures to ensure that our users' information remains secure and private at all times.



DATA FLOW



Authorization

To ensure maximum security and privacy of the data hosted on our servers, we have implemented a rigorous access control system at the record level in our database. These rules, meticulously defined and managed through our backend platform, play a critical role in protecting sensitive information. Each time a read or write operation is performed, these rules are thoroughly evaluated, ensuring that only authenticated and properly authorized users can access the corresponding data. This approach not only provides precise control over who can access what information, but also allows for dynamic adaptation as access requirements change. In this way, our systems guarantee the integrity and confidentiality of data, ensuring that only those with the appropriate permissions can interact with it, thus strengthening security and privacy at all stages of data management.

Encryption

To protect data on our servers, we use an advanced encryption approach. Data at rest is encrypted at the data level with AES-256 and then has a second level of encryption applied by our backend platform, providing a double layer of security. Additionally, at the disk level, we apply additional encryption, ensuring that data is protected across all storage layers. This triple encryption ensures that even if one level of encryption were compromised, the data would remain protected.

For data that does not need to be reversible, we employ a hashing process with randomly generated dynamic jumps to increase resistance against brute force attacks. Each hash is additionally encrypted with AES-256, increasing its security.

Data in transit is protected using TLS 1.3, and we apply extra transactional encryption to protect data in the payload and prevent sniffing attacks. This ensures maximum security at all stages of information transmission and storage.

Additionally, we implement a policy of regular key rotation through our secrets system, which further increases security. We conduct regular audits of our encryption and security systems to ensure their effectiveness and update our practices to include algorithms resistant to quantum attacks, strengthening long-term data protection.

“ **Data** stored on our servers can only be decrypted with your phone's keys and our secrets system. **Not even Enigm can decipher them.** ”



Monitoring

To further strengthen Enigm security, we have a monitoring system backed by artificial intelligence, designed to proactively detect and respond to new threats. This system guarantees the continuous protection of our environment against any potential risk. Additionally, we implemented a maximum log retention of 30 days to ensure the availability of necessary logs for subsequent analysis and security audits. It is important to note that no data that could identify our users is stored in our logs, and all metadata is anonymized before being recorded by our security monitoring systems and our Security Operations (SOC) team. This measure adds an additional layer of privacy protection for our users, ensuring that their personal data is completely secure and protected against any potential risk of exposure.



OUR CERTIFICATIONS

Privacy and compliance

Enigm complies with applicable data privacy and security regulations, such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). We are committed to complying with relevant laws and regulations to protect the rights and privacy of our users around the world.

With Enigm, users can communicate with peace of mind, knowing that their data is protected by a cutting-edge security infrastructure that prioritizes privacy and confidentiality.

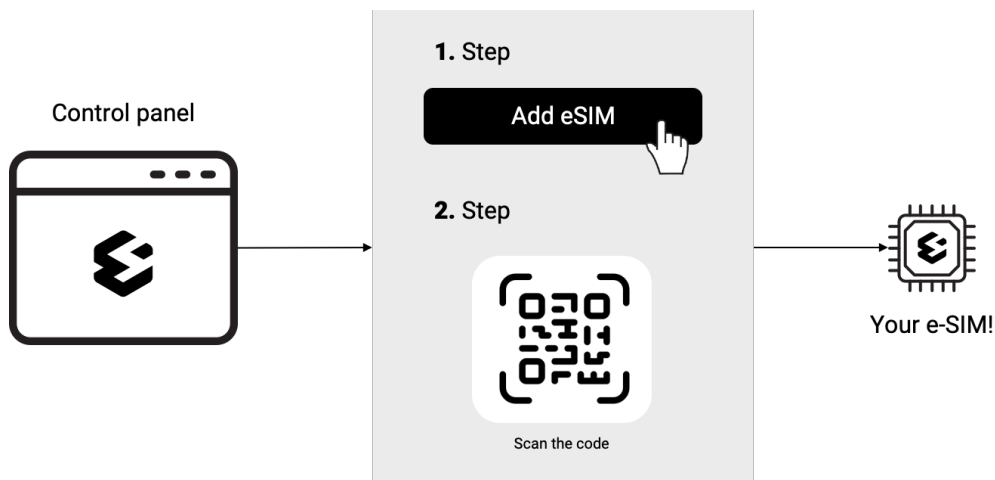
“ We do **not compromise** or **sell** user data to third parties. ”



eSIM

Features

Our anonymous eSIM offers a number of unique features that ensure the safety and protection of your data online.



FLOW CREATE AN ESIM

By using this eSIM, your local mobile network provider does not know your real mobile number, since you are roaming. This ensures that attacks such as the SimToolKit Attack cannot be carried out, ensuring the integrity and confidentiality of your communications.

Additionally, our app has a built-in VPN that adds significant value to the security of your data. The VPN encrypts all communications on your device, ensuring that your online activity is protected from intrusions and malicious attacks, even on public or unsecured Wi-Fi networks. This provides an additional layer of security when using our eSIM, ensuring your data is always protected.

Our eSIM also protects against subscriber location monitoring and logging of calls, messages and data sessions, ensuring the privacy and confidentiality of your online activities. In short, our anonymous eSIM combined with our in-app VPN offers a complete solution to protect your data and ensure your safety online.

Privacy and anonymity

Our eSIM technology stands out for offering a service exclusively focused on data, eliminating the phone number. This innovative solution allows you to instantly connect your device to the Global Mobile Data network, giving you fast and reliable access to mobile data in almost any country in the world, without requiring identity verification, SIM cards or documents. Our service stands out for its complete privacy, since we do not collect any user data.



Network

Features

At Enigm, we are committed to providing you with not only a secure communication platform, but also an additional layer of protection through our built-in VPN and network of proxies that protect your complete anonymity between you and our systems.



VPN CONNECTION FLOW

Our VPN offers a variety of features to suit each user's security and privacy needs. One of the key features is the ability to choose whether you want only our app to use the secure VPN channel or whether you want all apps installed on your device to benefit from this additional protection.

Additionally, our VPN is designed to always stay active, ensuring that all your communications are always protected. Even if you disconnect from the server for any reason, our application will automatically connect to another server immediately, ensuring constant and uninterrupted protection.

For emergencies, our built-in VPN has a Kill Switch feature, which acts as a safety switch in situations where the VPN connection is lost. This feature automatically blocks all traffic on your device to protect your online identity and data, preventing any unwanted exposure in unexpected disconnection situations.

Privacy and anonymity

We do not store records or logs of any kind on our servers. This means that we do not have access to details about our users' connections or browsing activities. Your information, including communications and online activity, remains completely private while you use this service.

In addition, our servers are located offshore to maximize data privacy and protection. This means that they are subject to laws and regulations that promote data confidentiality, providing a safe and secure environment to store information.





Using our VPN adds an additional layer of encryption to data transport, ensuring greater security in your online communications and preventing your service provider from knowing your connection destinations, further preserving your online privacy.



Annex

Comparison with competitors

In this comparison, we will look at the key functionalities and security aspects of our app in comparison to some of the top competitors in the market. This will help you make an informed decision about which is the best option for your online security and communication needs.

				
No data required	✓	✗	✓	✗
Message anti-recovery	✓	✗	✗	✗
End-to-end encryption	✓	✓	✓	✓
Post-quantum cryptography	✓	✓	✗	✗
Integrated VPN service	✓	✗	✗	✗
Voice modulator	✓	✗	✗	✗
Recording inhibitor	✓	✗	✗	✗
Anti-screenshot	✓	✓	✗	✗
Private servers	✓	✗	✓	✗
GDPR Compliance	✓	✗	✓	✗