



KATIM® Messenger Frequently Asked Questions

1

What is the KATIM® Messenger?

KATIM® Messenger is created with one goal in mind: to provide ultra-secure communications without compromise.

It is designed to provide state-of-the-art data security, privacy, compliance and auditing capabilities. It is the solution for businesses, governments and enterprise workgroups to ensure intellectual property and decision-making information remains confidential, no matter what.

You need KATIM® Messenger when the information you are dealing with is business sensitive or has significant commercial or strategic value or when confidential information is shared. It gives you confidence that your sensitive information remains secure at all times – in transit, at rest, or wherever it may be consumed by the recipient.

2

Why should my organisation use KATIM® Messenger instead of other publicly available end-to-end encrypted messengers?

Many messaging applications claim to be secure, encrypted end-to-end and safe when dealing with sensitive data. The challenge is knowing what makes a messenger application truly private and trustworthy.

Most freemium messaging apps that claim to offer end-to-end encryption are inherently not private. These consumer-grade messaging applications may be feature-rich but they are not designed to be privacy-focused. These often free and publicly available messaging apps expose you to security risks that they were not designed to protect against. This is because these applications treat security as a feature rather than the core architectural foundation.

Free and freemium apps collect information from their users, analyse it and aggregate it, with the goal of eventually monetising that information.

KATIM® Messenger enables organisations to stay focused on their core business, knowing their confidential communications are protected, while providing a productive digital workspace. With KATIM® Messenger, organisations can verify that their mission-critical information and communications will remain private, confidential and secure – in transit and at rest, everywhere, all the time.



3

Who can I connect to using KATIM® Messenger?

With KATIM® Messenger you can communicate and collaborate only with those who have the same app and have been registered by administrators to be in your circle of peers.

The number of global data breaches has rapidly increased in the last several years, leading to an uptick in identity theft, account takeovers, and the leaking of business secrets. In many of these cases, the method of attack has been through the vulnerabilities exposed in popular consumer-grade messaging apps.

This is because an organisation cannot securely manage the users who you are able to communicate with. When users are not managed, anybody with a phone number can be added to a messenger app group chat. This leaves your communications vulnerable to phishing and social engineering attacks.

4

How are user identities managed in KATIM® Messenger?

To achieve true end-to-end security is to only trust the communication peers, not the infrastructure between peers. KATIM® Messenger is a managed collaboration and communication tool that allows communications scope to only users that are under administrative control. It lets an organisation control that scope, minimising the chance of communicating with the wrong people. It provides truly private and secure communications that are robust and manageable, in a transparent manner, while preserving a great user experience.

With KATIM® Messenger your organisation can breathe easier, knowing that a secure strategy is in place that protects the messaging platform and the users, reducing complexity, ensuring access and boosting the flexibility of mobile workers.

Strong identity protection protects access to critical resources, hence KATIM® Messenger applies a strong Public Key Infrastructure (PKI) model to ensure the identity of individual users when communicating between peers. You can connect with anyone using KATIM® Messenger who has been registered to be in your circle of peers. New contacts need to be registered to be in your circle of peers.

5

Can KATIM® Messenger connect to someone that is not part of my organisation?

As a KATIM® Messenger user, your profile can only be seen by the contacts in your administered secure circle and you can control the information about yourself that is shared with other users. To connect with peers in other organisations, a feature called 'Secure Federations' allows one organisation to trust another organisation by federating both organisations, opening secure communications between both sides. Federation allows communication between organisations with the same ultra-secure protection.



6

Can Digital14 access my chats?

No. Digital14 cannot access your chats, content or communication. This is because your communications are end-to-end encrypted. Organisations that use KATIM® Messenger can choose to have complete control of the encryption keys for both mobile devices as well as applications, preventing Digital14 (or anyone else unauthorised) from decrypting any of the users' end-to-end encrypted communications.

If your organisation chooses to take advantage of KATIM® Messenger's compliance and auditing capabilities, then only individuals who have been nominated as Compliance Officers would have secure access to the communications of individuals identified by your organisation as "Persons of Interest".

7

Where's my data stored and how do I know my communications are private?

KATIM® Messenger was developed in and is hosted in the UAE and data is kept strictly within UAE borders, and subject to UAE laws.

An organisation can choose an on-premises deployment, in which case all communications and data are stored on the organisation's own servers. With an on-premises deployment, the data remains at all times under the organisation's control.

Unlike publicly available messaging apps, KATIM® Messenger is monitored via a managed Security Operations Centre (SOC) to identify and stop attacks, and to keep your communications secure and private. KATIM® Messenger is thoroughly and independently tested and analysed against a comprehensive threat model, covering all potential attack surfaces across multiple use cases. It is further validated by the leading-edge, third-party testing and validation facility xen1thLabs for holistic security and quality assurance.

8

Why should I trust KATIM® Messenger?

KATIM® Messenger is a defence-grade end-to-end encrypted messaging service designed for private and secure enterprise communications, collaboration and decision-making.

You can trust KATIM® Messenger to offer you the highest level of protection as it engages multi-layer end-to-end encryption with optional National Cryptography and brings strong PKI-based user identity with customer-controlled Hardware Security Module based certificates. Hosted with optional behind-the-firewall control, KATIM® Messenger protects your mobile communications against sophisticated remote network, identity and man-in-the-middle attacks.

KATIM® Messenger employs two different layers of security. If there is an error or a breach in the first layer of encryption the second layer is reserved as a backup to protect data. While the odds are low that an implementation error could occur to begin with, the odds are infinitesimal that both layers could fail. This model is similar to having a primary and secondary parachute for a skydiver.



9

What is the “scrambling” feature? What is it used for?

This new functionality is called ‘message obfuscation’ and it is designed to give you the confidence that your conversations are protected while on the move, when surrounded by people and in the field.

This feature allows you to scramble chat messages on your phone’s display, and read them one line at the time, which is effective against ‘shoulder surfing’ or any other possible onlookers.

You can toggle shoulder surfing protection on by simply tapping three times on any message and observe the scrambling take place. By swiping the scrambled message, you can partly uncover a message as you read it. Tap three times again to reveal all.

10

Can documents be uploaded in the app and can they be set to self-destruct?

Yes, document and media sharing is available in the app, as well as a self-destruct feature. A user can set a timer, and the document or media file will disappear at the specified time after the recipient views it.

Uploaded documents and media files are stored on the device within the app in encrypted format. As a security feature the downloading of decrypted files from the app to the device is not permitted

11

Earlier you mentioned KATIM® Messenger has the option to encrypt with National Cryptography. What does this mean?

KATIM® Messenger is built for national security level defence. It allows an organisation or nation to use the cryptographic library of their choosing for one of the layers of cryptography. This allows the nation to benefit from the security that they have built to protect their national secrets and yet remain protected through the implementation of multiple layers of encryption, employing a second layer of conventional cryptography.



We Are Digital14

Connect with us

