



Secure Corporate Communications and Mobility Platform

within the Company contour (On-Premises) or in a Secure Cloud (SaaS version)

 Messenger  Audio Call  Video conference  E-mail Client  Chat bots  Smart Apps

A sovereign technological stack with European go-to-market and support.

Keeps work communication inside governed infrastructure, without consumer-message risk

Multilingual interface           

Designed to support environments handling Controlled Unclassified Information (CUI-documents)

The Risk

Business communication has moved outside enterprise control and runs on third-party platforms.
That's a ticking bomb under your company.



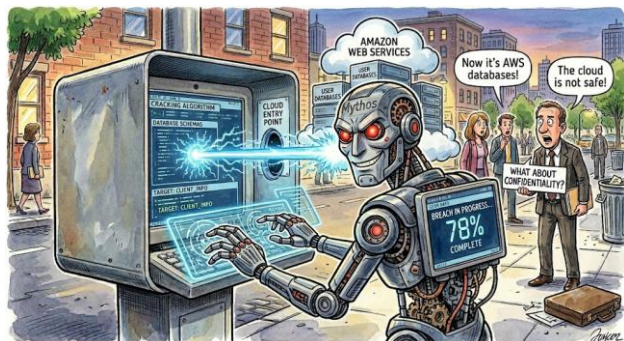
You don't own your corporate communications

- Consumer messengers were never built for business. The same account that sends a multimillion-dollar contract on Monday forwards a personal photo on Tuesday. When an employee leaves, the entire conversation history, deals, decisions, client relationships can be wiped clean before they walk out the door on Friday afternoon. **Legally, it's their account. Legally, it's their call.**
- Under GDPR, that's not a security risk! It's a compliance failure waiting to happen.



Your data lives on someone else's servers and under someone else's terms.

- MS Teams, Zoom, Google Workspace are the great products, built in the US, governed by US law. Under the US CLOUD Act, American authorities can legally demand access to your data, regardless of where it's physically stored. **That puts you in direct conflict with GDPR.**
- aXtura is non-USA (EU/KZ) -built, deployed within your own infrastructure, under EU or your country law. No jurisdictional grey zones. GDPR-compliant by design



Your data lives in the Cloud. AI is hunting there now

- Your data lives in the cloud. AI is already scanning for weak spots, exposed keys, misconfigs, and zero-day paths. The question is not if it can break in. **The question is when.**
- aXtura on prem keeps your data inside your perimeter. No cloud exposure, no easy scrape, no open playground for hostile AI

The Solution

aXtura provides secure communication across organizations where each participant retains full control over its data, identities, and infrastructure.

✓ You are really own your communications

In-perimeter, with strict personal/work separation, crypto container and remote wipe. GDPR-compliant by design.

✓ Your data, your jurisdiction

European-led compliant engineering without dependence on US cloud ecosystem. Keep somehow No US CLOUD Act exposure. EU certification underway.

aXtura is a federated, EU-built corporate communications & mobility platform. You'll have one secure workspace deployed on-premises or in a sovereign private cloud, across web, desktop, iOS and Android.



Secure messenger

1:1, group chats and channels up to 50,000 users, threads, 1 GB files, voice and burn-on-read.



Calls & video

Audio/video conferencing for 500+ participants: recording, screen share, transcription, remote desktop.



Email & Outlook

Built-in mail client with an Outlook add-in for meetings, invites and calendar sync.



Chatbots

BotX microservice and 20+ ready-made bots to automate approvals and business processes.



SmartApps

Cross-platform mini-apps with SSO, 70+ integrations and built-in LLM / AI agents / MCP.



Federation

Trusted multi-organization network for secure cross-company communication and guest access.

The Platform's Features

The aXtura corporate communications and mobility platform combines a secure corporate messenger, video conferencing, chat-bots and SmartApps mini-apps (Email, Calendar, and other corporate services on a single platform)

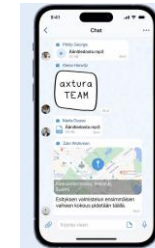


Available on:



Corporate messenger

One-on-one and group chats, channels, file sharing, threads



Audio and video calls

One-to-one and group calls



Video Conferencing

Video conferences for 500+ participants, call recording, virtual backgrounds, transcription, remote desktop



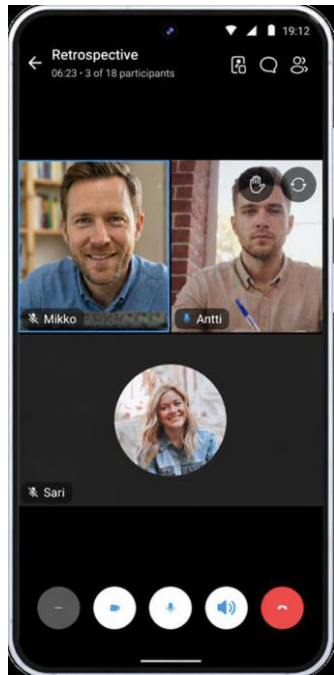
Federation

The aXtura communication protocol for communicating with colleagues and partners (including those from other companies)

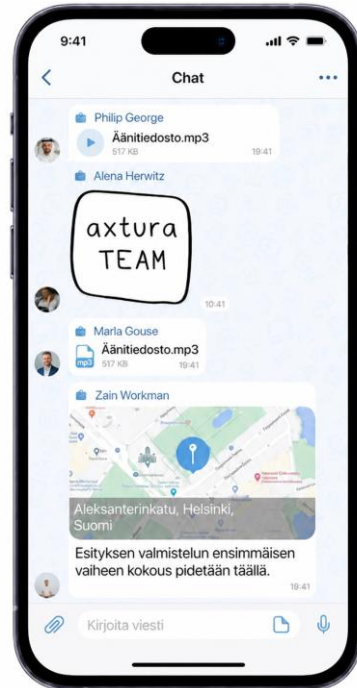


Messenger/Features

Audio/Video Calls



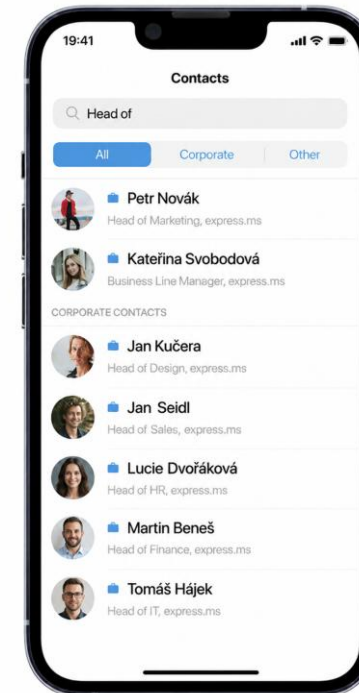
Personal and group chats



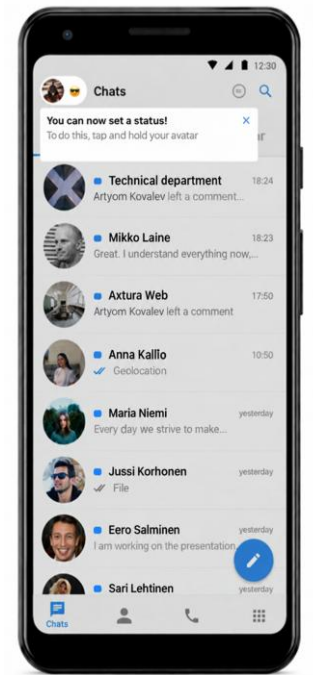
Channels



Address Books



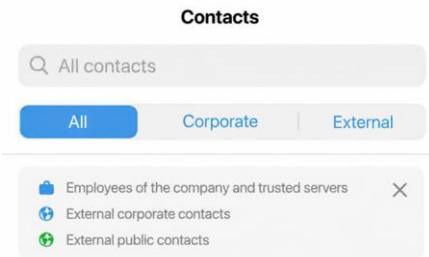
Status selection



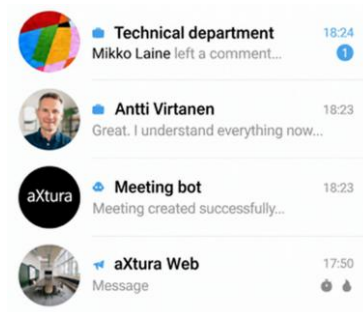
Messenger/Features

Search for users

In the corporate system (by name or title) or directory



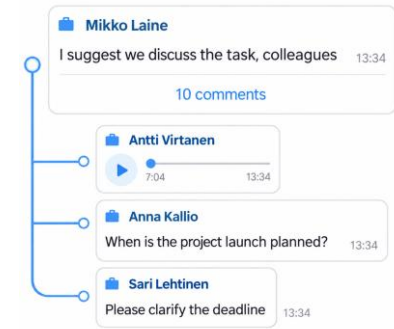
Personal and group chats, channels, and bots



Text formatting

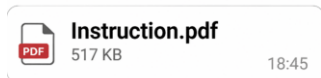


Discussions / threads



Files and documents

Sending by moving the document shortcut to the WEB window forwarding from other users, saving files

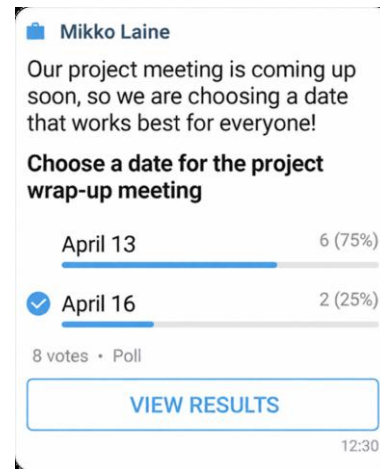


Voice messages

With listening through the phone speaker



Polls & Quizzes



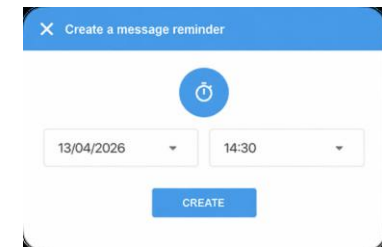
Emojis, stickers, and reactions



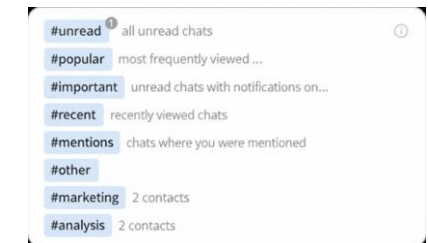
Deferred messages



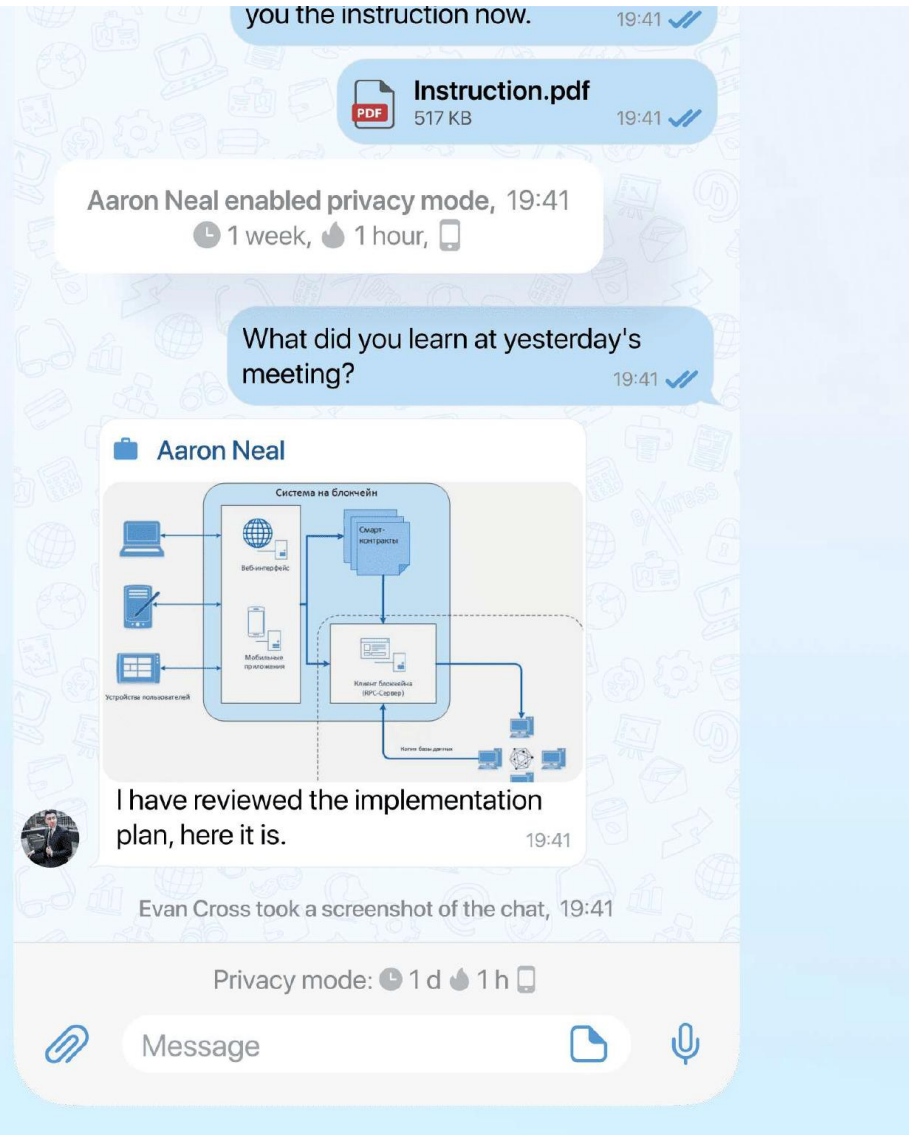
Reminders



Tags



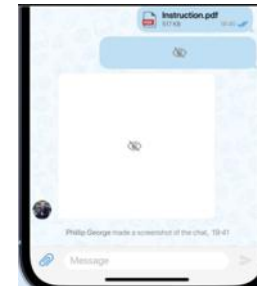
Messenger / Enhanced Privacy Mode



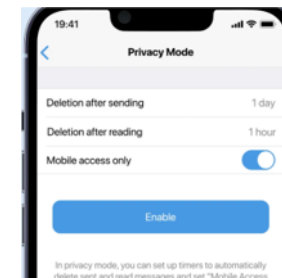
Opening files exclusively in the app



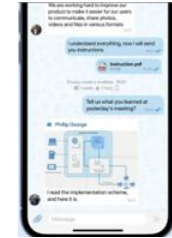
Detecting screenshot and screen recording attempts



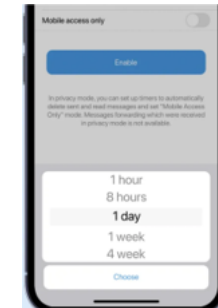
"Mobile only" restriction (messages and files are not available from Web/Desktop sessions)



Prohibition of copying, forwarding, saving messages and files, "Open in" and "Share To" functions



Setting up timer for automatic deletion of messages and files (after sending or after reading, from one minute to one month)



Ideally suited for processing sensitive information



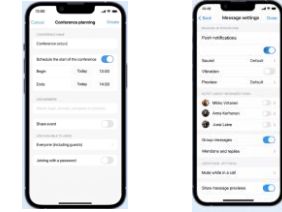
Video Conferencing / Key Features



Up to 512 participants



Planning



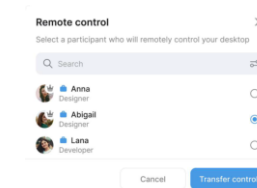
Transferring a call to a conference



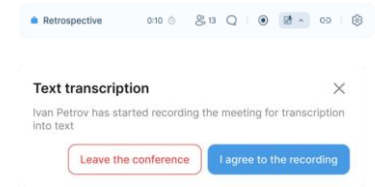
Virtual Meeting Rooms



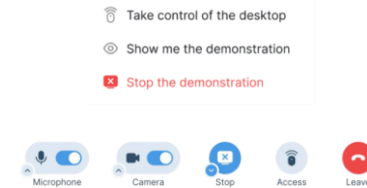
Remote Desktop



Call Recording
Call Transcription



Guest access



Alerts via chatbot



Raising Your Hand



Blur Custom background



Screen sharing



Creating a video conferencing with access by password



Live Chat



External links



Chatbots

The aXtura platform provides the ability to create chatbots using the BotX microservice or use ready-made solutions from the bot catalogue

Chatbot catalog*

Chatbot Features

Send text messages, files



Sending messages with buttons



Management of LLM/MCP and other external services



Enable/disable High Privacy Mode



Assign chat admins



Creating a chat with a user (useful for corporate chatbots)



Approvals, resolutions, etc.



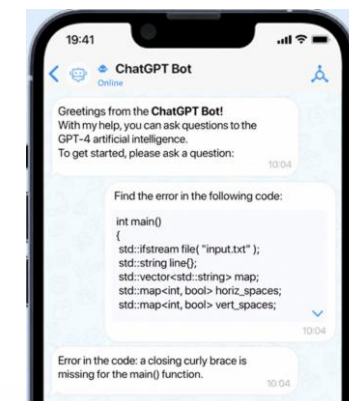
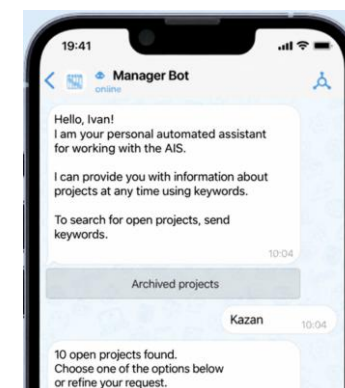
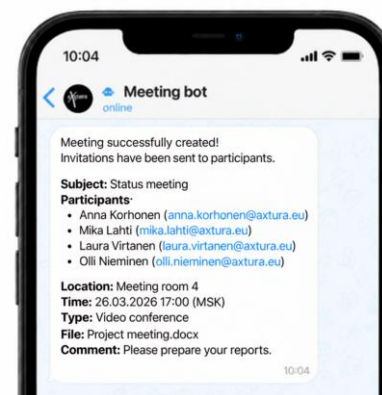
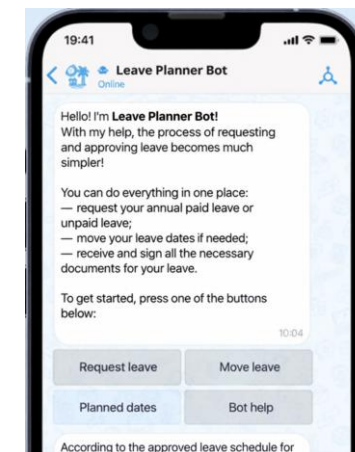
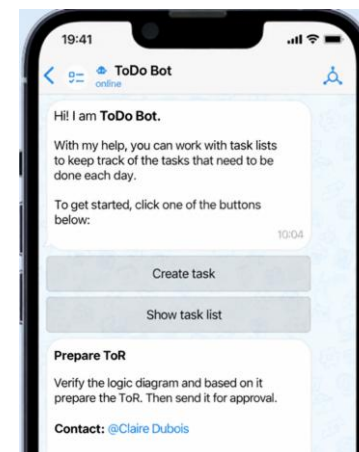
Receiving system notifications (chat creation, user login, etc.)



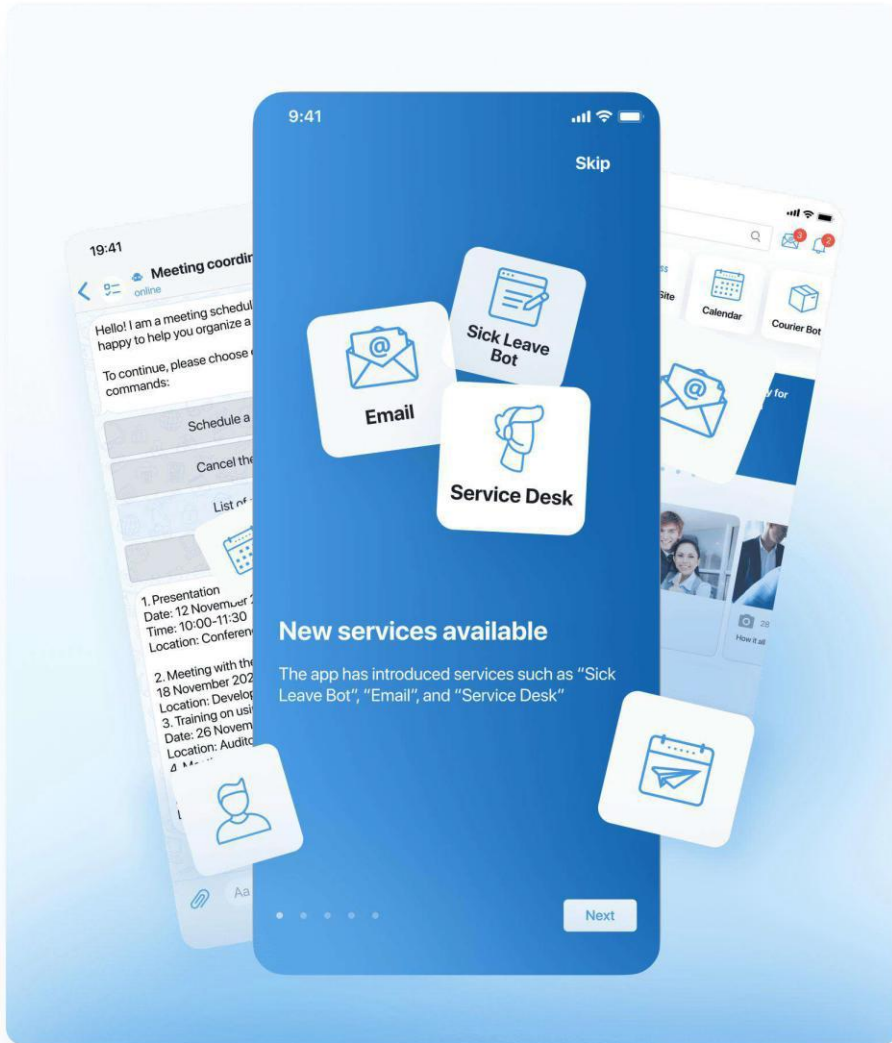
Audio translation and transcription



*More than 20 pre-installed chatbots to automate various business processes



SmartApps / Full-fledged Graphical Apps



Proprietary aXtura SmartApps technology: mini-apps that are uniform across all platforms (iOS, Android, Web, Desktop)

SmartApps help solve work tasks within the one ecosystem, provide integration with corporate and external systems, and are an alternative to developing dozens of apps for each individual task

SmartApps Benefits:

A New Level of Corporate Mobility

All the corporate services you need are available anytime and on any device in a single-window app format

Integration with 70+ systems

Including the most in-demand solutions: email clients, document management systems, antivirus software, CRM, and more

No Need to Switch Between Apps

SSO (Single Sign-On) is used, so no additional authorization is required

New AI Capabilities

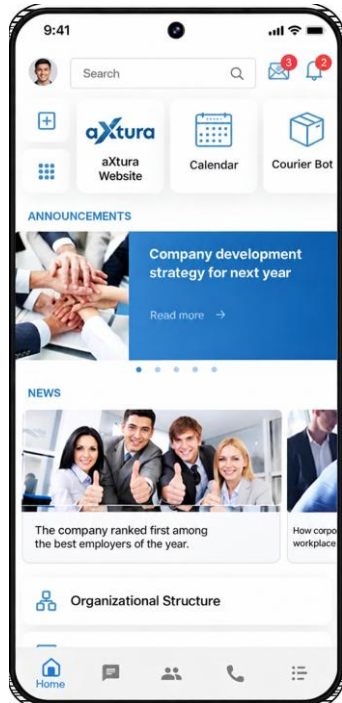
Integration with LLMs (language models), connection of AI agents, MCP servers, and more

Eliminate the labor-intensive and costly development of mobile apps

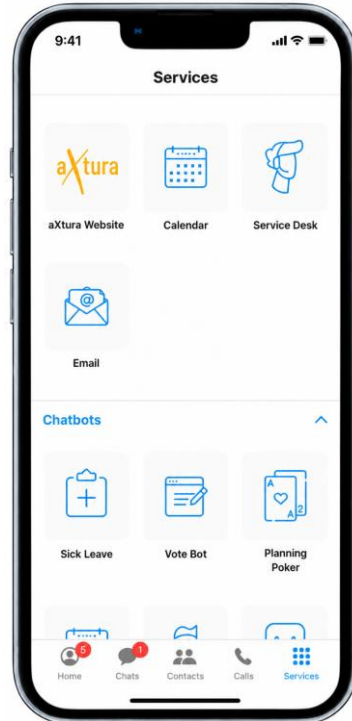
SmartApps /Feature Examples



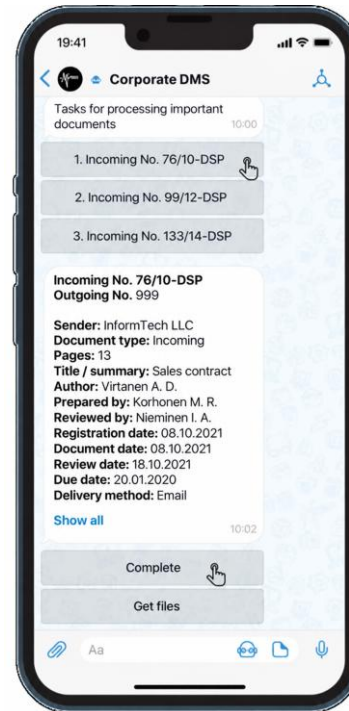
Company Portal



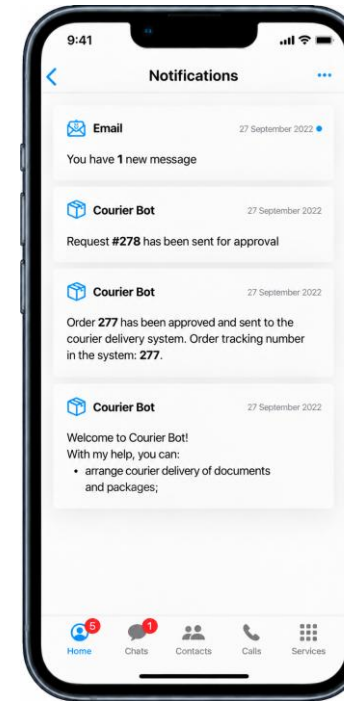
Employee's personal account



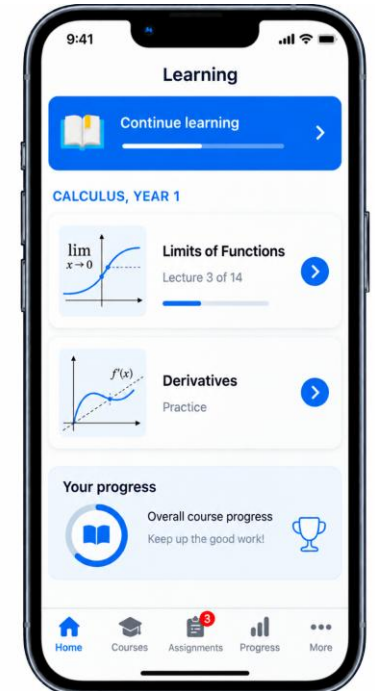
Document flow



Notifications



Training



Access to external services: CRM, accounting, training systems, etc. Working with LLM, connecting to AI agents, automation by your AI agents

Federation

Communication protocol in aXtura, which allows employees to communicate with colleagues registered on trusted corporate servers (including those from other companies) and securely interact with public users of the messenger

Trusted communication loop inside and outside the company

Independence

Secure On-Premise servers in-house
No external servers = no hidden connection

Guest's accounts

Temporary accounts for project team members

Effective communication

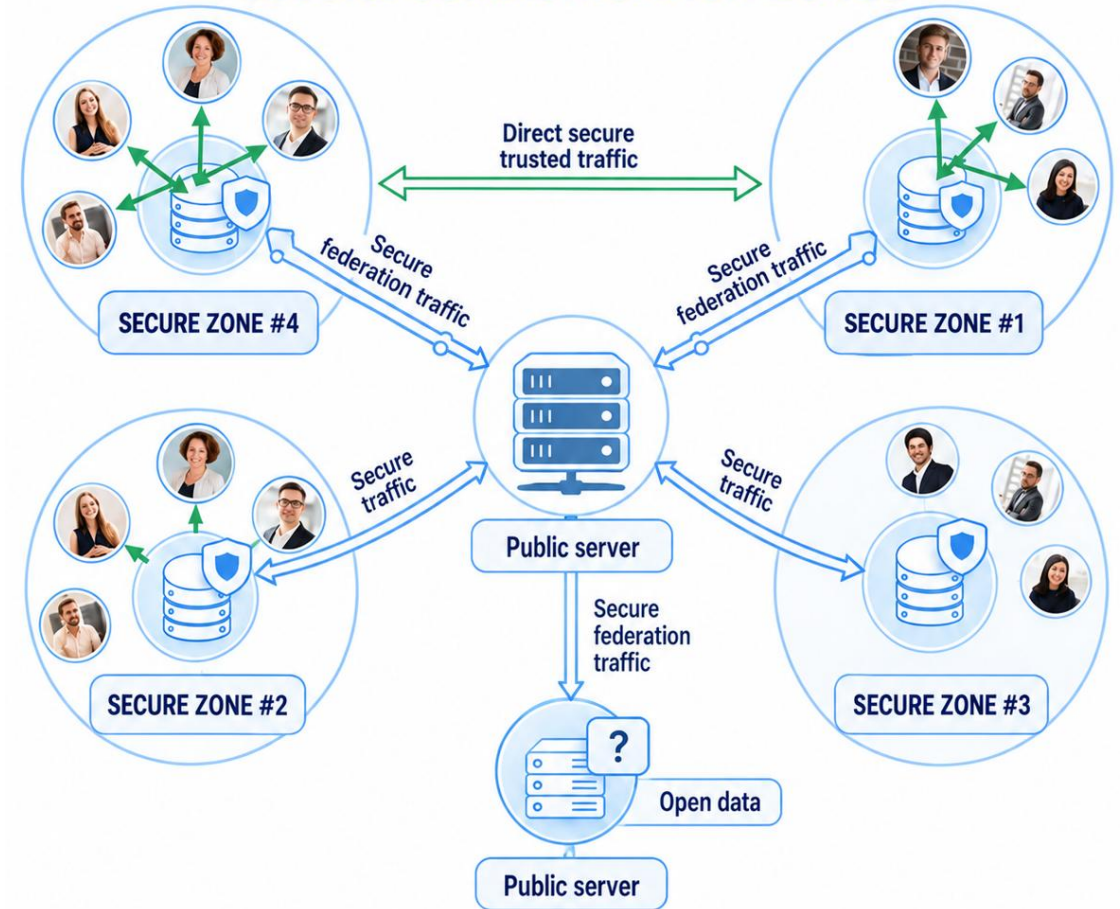
Ability to create a working group in-house and with external aXtura users

Security

Full control of data flows and strong encryption for external communication



FEDERATION ARCHITECTURE: SECURE COMMUNICATION ZONES



- **Central public server:** Coordinates federation and open data.
- **Secure zones (#1-#4):** Isolated segments for local teams.
- **Secure trusted traffic:** Direct channels between zones #1 and #4, and within these zones, enabling trusted communication that bypasses the core for specific tasks.

Federation / Internal and external contacts

Friends. Colleagues. Partners and clients

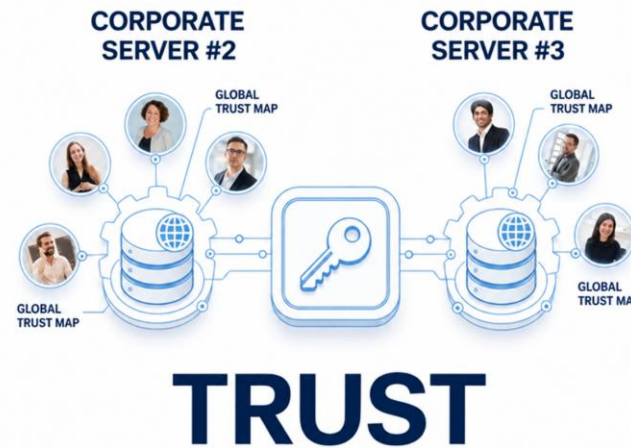
Available only to those who
You have entrusted your phone number

Instant search for contacts on servers
connected by trust

Full integration with Active Directory /
OpenID, search by name, position,
department and other fields

Acquaintances. Colleagues Partners and clients

Only accessible to those
you have trusted with
your phone number



Mobile Security

A super-app in the "online communication" class, prepared for certification at the 4th level of trust.

Certification in Kazakhstan and the EU is planned for 2027



User Authentication

3FA via three completely independent channels:

- Corporate account in Active Directory (NTLMv2 pass-through authentication) / OpenID or one-time password entry from corporate email
- One-time password from SMS (linking to a phone number)
- Personal user password (not available to system administrators)



Absolute data transfer security

- TLS
- **End-to-end encryption**
- Secure push notifications without transferring content to them
- Encryption in accordance with the requirements of the local regulator - on request



Crypto container

- Encrypted storage of all data on the mobile device (container)
- Deletion of all data on the MU on command from the server (or one session if the phone was lost, or all sessions if the employee was fired)
- Open files inside the app container
aXtura, prohibition of transfer and storage "externally"
- Control of system functions (screenshot, screen recording, clipboard)

Enterprise Security

Active Integration Directory / OpenID

Provides secure
synchronization of corporate
user directories



DLP integration systems

Detects and prevents unauthorized
use, transmission, and storage of
sensitive data



Integration with antivirus By means

Protect your corporate
environment from malware



Integration with SIEM systems

Allows you to monitor events
and respond to security incidents
in time



Integration with 70+ platforms and systems at the request of the customer

Integrations with external services

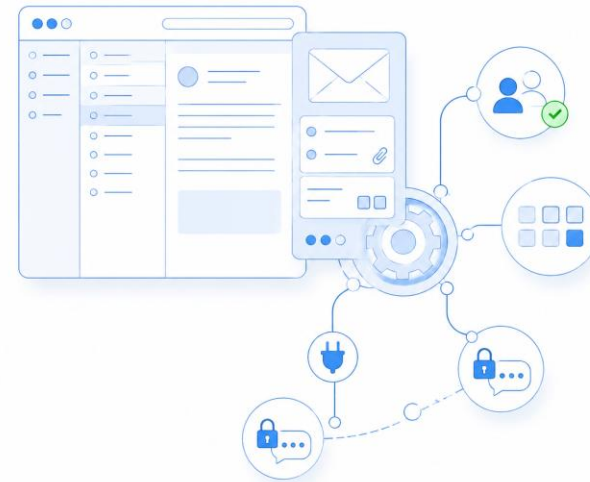
Integration with SIP telephony



Integrations with Communicate, Exchange mail servers (via SmartApp Email)



Integration with MS Outlook email client (plugin)



Integrations with external video conferencing systems Vinteo / Communicate

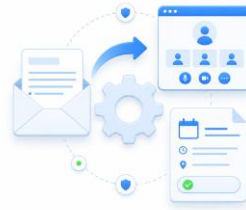


Outlook Add-in / Integration Example

Create public, private, and recurring aXtura conferences from Outlook clients (Create Meeting feature)



Create conferences directly in response to a received email in Outlook (Invite a meeting, the text of the received email will be in the invitation)



Flexible configuration of video conferencing links for all aXtura users (even guests), for users of trusted servers, for users of corporate servers



Create password-protected conferences



Editable invitation email template



Intuitive and familiar conference management



Create an event in your Outlook calendar when you create and edit a conference



Convenient administration

Role model

axTura uses a role-based model to flexibly differentiate access rights. The tasks of the role-based model are to prevent file leakage, speed up the processes of granting rights/prohibitions to employees, and manage access to application functions.

Rules for users or groups

- Flexible configuration of access to attachments (files) with indication of types, sizes and extensions
- Restriction on access to chats
- restriction on access to calls;
- Generating a list of SmartApps displayed to users
- Create user groups (without device ID) with platform type
- Enabling a mandatory PIN code for access to the application with the ability to configure the timeout time

info@axtura.eu

Users

Chats

Open Chats

Calls

Conferences

Requests for change list

Logout requests

Administrators

Servers

Bots

Internal Bots

External Client Users

Containers

Role Model

Create a new rule

Rule name

Block video sending over 200MB

Rule description

Size limit for sent videos for the marketing department

User groups

Marketing

Scope of action

In messenger

Rule type

Block attachment sending or forwarding

Block attachment sending or forwarding

Block attachment uploading or viewing

Block attachment forwarding and saving

Block attachment downloading from users with cts

Mandatory PIN-code for access

What to block

Block clarification

Here, select the user group to which the rule will apply

Choose where the rule will operate - in messenger or SmartApps

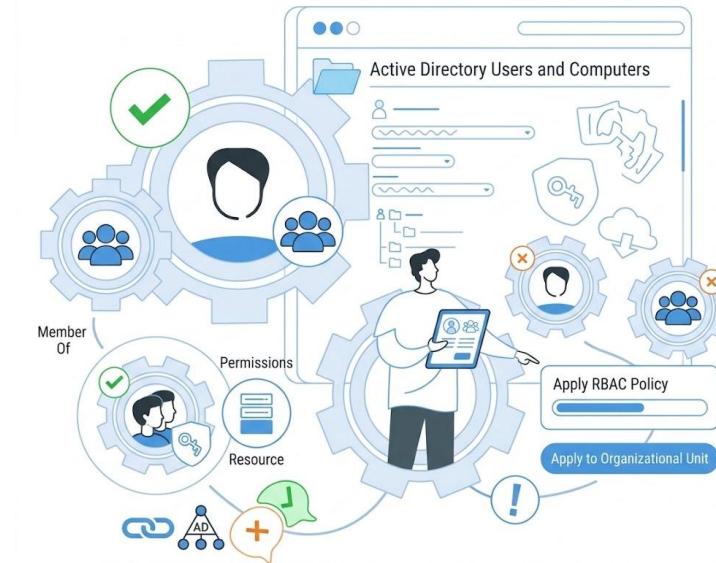
Select the rule type we need

Administrative role model

The privilege differentiation functionality allows you to create different roles for administrative users depending on their responsibilities:

- Server Administrator
- Security Administrator
- SmartApps Administrator

Active Directory or Key Cloak directories for user management



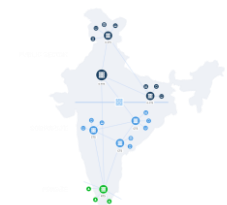
Admin's Dashboard



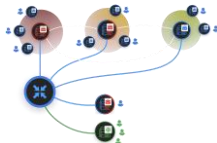
Possible systems configurations



A **system for critical infrastructure** with strong requirements for operational continuity: a distributed system across multiple data centres, resistant to disasters (the destruction of one or more data centres)



Corporate + SmartApps: Corporate super apps: messenger, video conferencing, smart apps (mail, calendar, integration with company systems and services). On-premise or protected cloud



Corporate: A communications platform with an admin panel and integrations with DLP and antivirus software. On-premise or protected cloud



Lite: Cloud-based team messaging and video conferencing for small and medium businesses Protected cloud only



Free: A simple and convenient messenger with calls for individuals (*not available in some countries)

Migration from Telegram to aXtura



Migration of correspondence and bots from Telegram

The aXtura messenger for business allows you to transfer business communications from Telegram to a secure solution with the preservation of the history of correspondence and the main chatbots.

With the help of a special bot, administrators can perform:

- Automatic transfer of an individual chat

- mass transfer of several chats from Telegram in chronological order; add users to an already created aXtura chat using an Excel file or manually.

- SDK is provided to adapt existing Telegram bots to work on the aXtura platform without completely rewriting the integration code.

Why Choose aXtura



Safe Environment for Communications

Prepared for certification at trust levels 6 and 4

A single window for communications and secure access to corporate systems

Crypto container

And more:

A platform that combining a messenger, chats, video conferencing, an email client, and chatbots

EU (non-USA) software

Multi –language interface

MS Teams / Zoom/ Telegram Alternative — the closest possible solution

On-premises or SaaS deployment

Support for any device type

Three-factor authentication

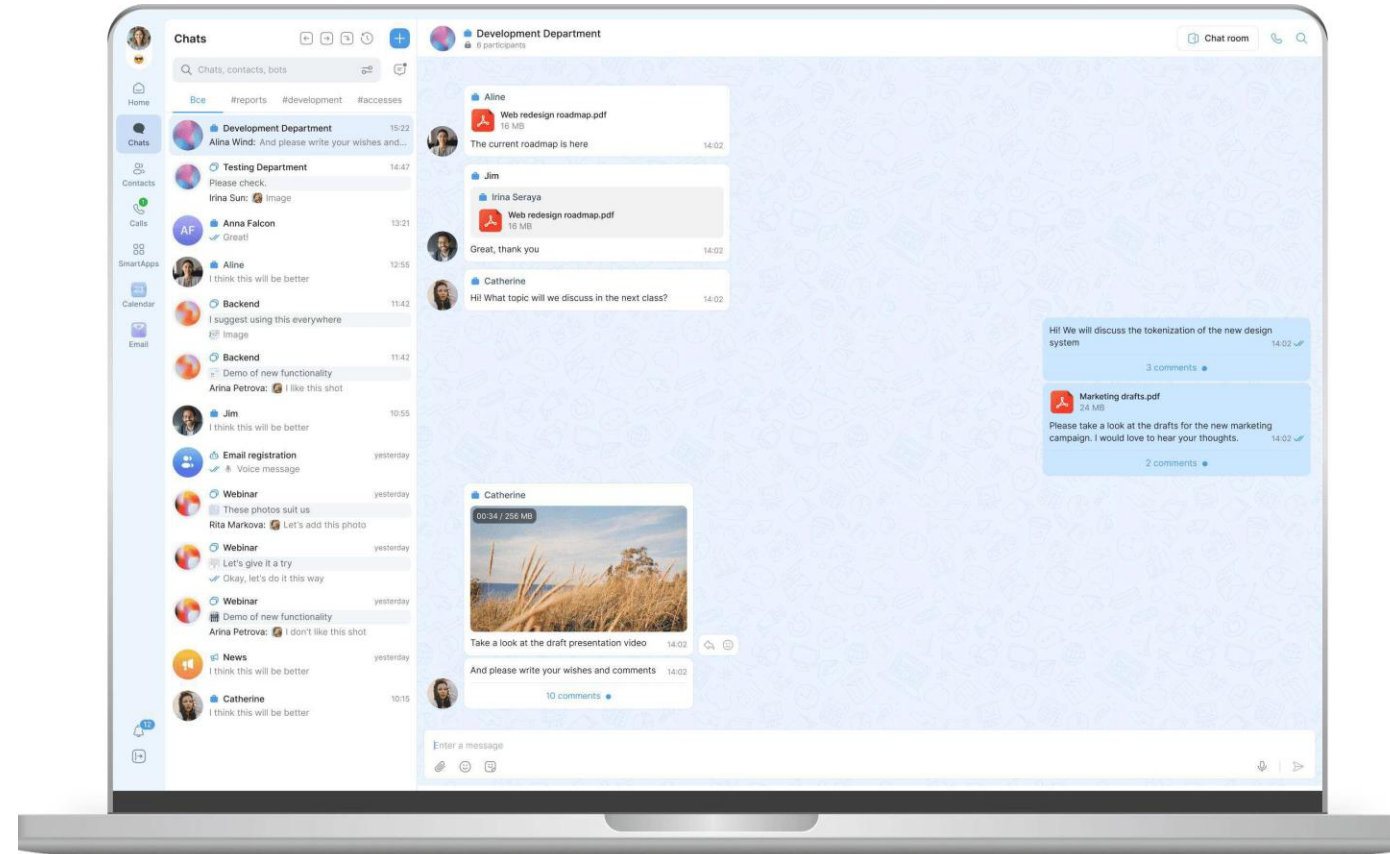
Integration with information security systems, DLP

Designed to support environments handling Control Unclassified Information

Possibility to integrate your own information systems via SmartApps

Federation

We are constantly working on improvements



Contacts and regional presence



Finland and EU

Legal name	Astrokvantit Oy
D-U-N-S	369028850
Business ID	3321009-8
Address	Hietaniemenkatu 14A 208, 00100 Helsinki, Finland
Telephone	+33 745 15 26 36
WhatsApp/Telegram only	+358 46 890 4791
Website	axtura.eu
Sales and support	info@axtura.eu



Kazakhstan and EMEA

Company	Astrokvanta LLP
Astana Hub Member	№ 2946
Business ID	250940000062
Address	Kazakhstan Uralsk
WhatsApp / Telegram only	+7-775-915-7869
Websites	astrokvanta.kz axtura.kz info@astrokvanta.kz info@akstura.kz
Commercial Department	
Sales and technical support	

Contacts for investors

Founder	Vadim Veshchezerov
Tel	+33 745 15 26 36
WhatsApp/Telegram only	+358 46 890 4791
E-mail	vvv@astrokvanta.com