getTrusted

PROJECT HIEROPHANT: PARTNERING FOR AFRICA'S DIGITAL SOVEREIGNTY

MAY 2025

Protect your country's most sensitive communications with Project Hierophant: a specialized messengers, software, hardware, and data exchange protocol designed to ensure total independence from foreign messaging platforms for critical missions.

All physical servers and encryption infrastructure remain under your full national jurisdiction and control. Operates securely—even over radio and offline—for government, financial, and critical infrastructure protection.

Hierophant is engineered to be resistant against sophisticated foreign intelligence threats, including scenarios where an adversary gains physical access to servers or devices.

WWW.GETTRUSTED.IO

getTrusted

EXECUTIVE SUMMARY

Africa is charting a bold course in its digital transformation. As digitalization expands, so does the imperative for nations to safeguard their digital sovereignty.

The use of communication platforms headquartered outside the continent, such as WhatsApp, Signal, WeChat and various foreign data exchange software, hardware, while offering convenience, presents inherent risks.

Globally operated platforms create an environment where critical data may be exposed to risks beyond local legal and regulatory control.

To address this challenge, Project Hierophant offers partnership to Africa: secure messengers, software, and hardware engineered for sovereign communications, protected against sophisticated intelligence threats.

getTrusted

EXECUTIVE SUMMARY

Engineered in Austria—one of the world's most democratic and constitutionally neutral countries, not a member of NATO or other military alliance—Hierophant embodies a commitment to trust, neutrality, and data protection.

We offer customer-controlled (on-premises) solutions for government, corporate sectors, financial institutions, critical infrastructure, SCADA and defense. Including, but not limited to secure messengers, telemetry security, communications encryption software and hardware.

Hierophant technology operates securely not only over standard internet, but also via radio, and even in offline or disconnected environments.

For African countries, we offer pilot projects with special terms with the same focus on long-term partnership.

getTrusted

HIEROPHANT TECHNOLOGY

The full list can be found on official website: https://gettrusted.io/technology/

No Identifiers or Accounts
No names, phone numbers, or emails are needed. No one can see who is talking to whom.

Zero Metadata Collection
The system does not record when, where, or who is communicating. No traces are left behind for interception.

Client-Side E2EE Encryption
All messages are locked (encrypted) on devices before being sent. No one else, not even us, can unlock them.

Traffic Analysis Resistant
Outsiders cannot figure out communication patterns or relationships, even if they see the data flow.

Zero-Knowledge Architecture
Even with full system access, attackers cannot see messages, data or who is using the system.

Post-Quantum Safe
Uses standardized encryption that will keep today's secrets secure even against future quantum computers in next 20-30 years.

On-Premises Data Sovereignty
All equipment and data stay under your country's control — nothing is sent abroad or stored on foreign servers.

Radio Transmission
Messages can be sent over long-range radio waves, so secure communication works even when the internet is down.

Mesh Network Support
Devices can connect to each other directly in a network, even in remote areas or if regular networks are blocked.

Serverless & P2P Capable
Can work without central servers; users can communicate directly, which means no single point of failure. Prepared for blackouts and crisis scenarios.

Software
Hierophant software can be quickly installed on existing computers or phones, no need for extra hardware.

Bare-Metal (OS-Free)
Communicate directly via Hierophant devices without any regular operating system — the highest level of isolation.

GOVERNMENT AND PUBLIC SECTOR

- Deployment of secure communication channels for ministries, agencies, and inter-agency coordination, replacing WhatsApp, Signal and other platforms with servers in the United States or China with Hierophant — **fully controlled by national authorities.**
- Establishment of resilient messaging infrastructure able to function during internet outages, blockages, or states of emergency.
- Rollout of radio and offline (mesh network, hardware) communication capabilities to ensure continuity during blackouts or crisis situations.
- Migration planning, technical onboarding, and training for all relevant personnel in secure usage and incident prevention.

TOP MANAGEMENT. STATE LEADERS

- Provision of ultra-secure, closed-loop communications for heads of state, ministers, national security councils, and senior management in key institutions.
- Distribution of dedicated devices with built-in hardware encryption, radio support, and no external dependencies for critical decision-makers.
- Establishment of exclusive, physically isolated channels for confidential, real-time dialogue between government and top business leaders.
- Personal onboarding, security briefing, and technical support for highest-level users and their designated staff.

FINANCIAL SECTOR AND BANKING

- Implementation of secure, locally hosted channels for communication between central banks, commercial banks, regulators, and critical third parties.
- Protection of payment, transaction, and client data exchange — including API and telemetry flows — against interception or data leakage.
- Integration of cryptographically authenticated remote access solutions for mobile staff and branch operations.
- Replacement of vulnerable messaging and communication platforms in compliance with data localization and sovereignty laws.

DEFENSE, STATE SECURITY

- Deployment of a military-grade, interception-resistant messaging and data exchange platform for armed forces, police, and intelligence and counterintelligence services.
- Enablement of fully autonomous, communication via software, radio and portable hardware, operational even in disconnected or adversarial environments, with privacy and anonymity.
- Secure operational planning, order transmission, and mission coordination — with zero metadata or traffic analysis risk, even during electronic warfare.
- Field pilots, scenario-based testing, custom solutions to adapt to local operational challenges.

CRITICAL INFRASTRUCTURE AND SCADA

- Protection of SCADA and industrial telemetry via autonomous, encrypted control and monitoring channels — eliminating reliance on foreign software, hardware, clouds or third-party servers.
- Integration of hardware modules for network isolation and air-gapped command separation at critical sites.
- Establishment of emergency management and operational communication over secure radio/mesh in case of power or internet loss.

ENTERPRISES, BOARD-LEVEL AND STRATEGIC BUSINESS OPERATIONS

- Secure channels for executive communications, M&A negotiations, asset management, and confidential board interactions — isolated from external monitoring.
- Migration of internal and external business messaging from foreign platforms to a corporate, locally governed instances.
- Dedicated, crisis-resilient communication lines (including offline and energy-independent options) for business continuity planning.
- Deployment of specialized secure devices and mobile terminals for C-level executives — including hardware encryption and secure radio modules.

getTrusted

TAKE THE NEXT STEP TOWARDS SOVEREIGN COMMUNICATIONS

Schedule a private consultation or pilot deployment with Oleg Shumar, CEO, GetTrusted Escrow GmbH.

EMAIL
oleg.shumar@gettrusted.io

ENCRYPTED FORM & PGP KEY
https://gettrusted.io/request-demo/

OFFICIAL WEBSITE
https://gettrusted.io/

—

GetTrusted Escrow GmbH
Zimmermanngasse 8
1090 Vienna, Austria
oleg.shumar@gettrusted.io
support@gettrusted.io
VAT ID: ATU79631025