Product Catalog

Telsy

A TIM ENTERPRISE BRAND

Born to innovate

Telsy's long history is one of innovation and the constant pursuit of excellence in data and communications security

Founded in 1971, **Telsy** is **TIM Group**'s **cryptography** and **cybersecurity** competence center operating within **TIM Enterprise**. Subject to Golden Power regulations, as a strategic asset for Italy's security, Telsy develops and provides **proprietary cybersecurity and cryptographic solutions** for government agencies, companies, institutions, and SMEs.

Telsy's portfolio comprises five operational areas: **communication security** solutions with cutting-edge cryptographic systems, **intelligence** services, **cyber professional services**, **managed detection and response** services, **SOC-integrated managed security services** with products and solutions for defense enhancement.

Telsy's core is its **engineering labs**, where security technologies are developed and tested for the most demanding clients. The company also boasts its **cyber platform**, which enables cyber-event monitoring, analysis, and response, and an outstanding team of **cyber specialists**.

1971
Founded in Turin
Telsy Elettronica e
Telecomunicazioni

1980
First **"Digital Signal**
Processor" devices

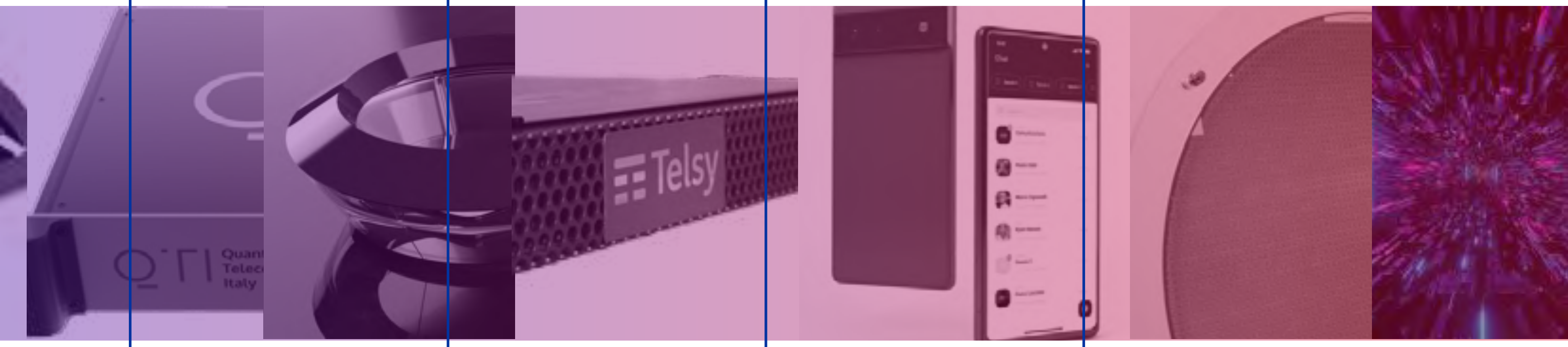
2000
First **secure VoIP**
phones

2001
Joins the
TIM Group

2017
Enters the
Golden Power
perimeter

In 2021, Telsy joined the share capital of **QTI**, a leading Italian company in **Quantum Key Distribution** technology. In 2023, Telsy acquired **TS-WAY**, an Italian company specializing in prevention services, cyber attack analysis, and **cyber threat intelligence** technologies. Furthermore, Telsy invests daily in new and exciting research areas and nurtures its dedicated **Research & Development Team**.

Thanks to its crypto, cyber, quantum, and intelligence areas, Telsy's business proposal represents a true **uniqueness in the market**. It integrates proprietary technologies and highly specialized experts to offer its customers the best security.



2021

Investment in QTI, company specializing in **Quantum Key Distribution**

2022

Evolution of the Crypto, Cyber, Quantum and Intelligence **portfolio**

2023

Acquisition of TS-Way, specializing in **Cyber Threat Intelligence**

2024

First cryptographic microprocessor designed entirely in Italy. The company **increased its stake** to 80% in **QTI**

Cybersecurity & Crypto Portfolio

Intelligence

- Red Teaming
- VIP Digital Protection
- Active Security Platform

Cyber Professional Services

- Cyber Risk Management
- Cyber Awareness & Training
- On-Site Professional Services

Managed Detection and Response (iSOC)

- Cyber Threat Intelligence
- Security Monitoring
- Incident Response

Managed Security Services

- Network Security
- Endpoint Security
- Application Security
- Mobile Security
- Industrial Security

Communication Security

- TelsyInTouch$^{\text{App}}$
- TelsyATMO
- TelsyAntares
- TelsyMusa
- TelsyInTouch$^{\text{Phone}}$
- Crypto Voice
- Secure Microchip
- Quantum Security

Intelligence

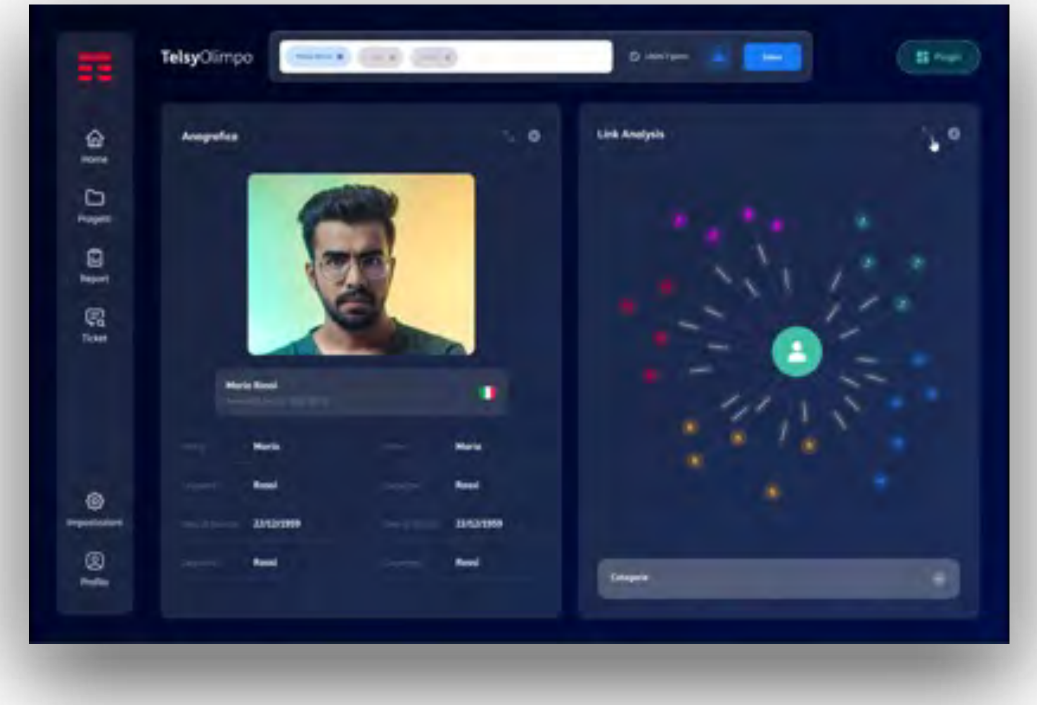
Active Security Platform

In today's rapidly evolving digital landscape, the proliferation of diverse data sources and the increasing complexity of global challenges demand advanced tools to uncover hidden patterns, mitigate risks, and support strategic decision-making. The ability to effectively analyze and correlate vast volumes of heterogeneous information is now a critical capability for organizations operating in an interconnected and data-driven world.

A modular intelligence platform powered by Machine Learning and Artificial Intelligence algorithms, designed to integrate and correlate massive volumes of heterogeneous sources (OSINT, CLOSINT, SOCMINT). It accelerates the extraction of actionable insights, providing analysts and decision-makers with a clear, precise, and cohesive understanding of the phenomena under analysis.

The platform offers enabling technologies to integrate and correlate large-scale data - structured and unstructured, internal and external to the organization - addressing the growing demand for transparency, interpretability, and reliability in decision-making.

Its integration with tools for link analysis and structured investigation further enables the exploration of hidden and latent aspects of the matters at hand. This empowers users to conduct multi-domain and multi-dimensional research, even in areas that typically require specialized expertise.



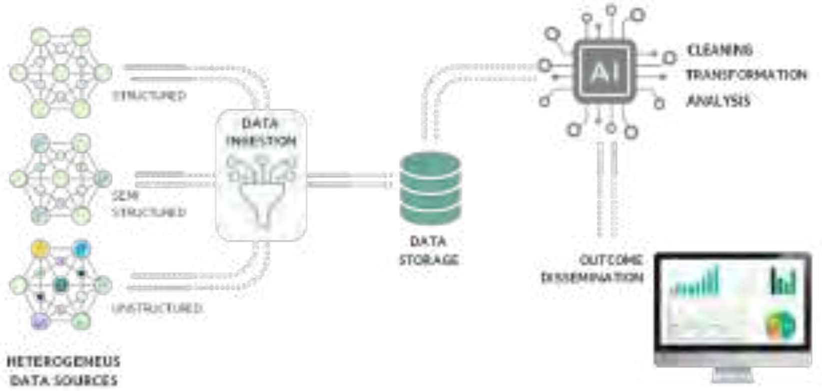
Technical features

- Machine Learning engine and AI algorithms
- Crawlers for OSINT, SOCMINT, and Deep/Dark Web sources
- Integrated Google-like search engine
- 10 analysis modules (available as plug-ins)
- Link analysis tools
- Multilingual translator integrated within the document analysis plug-in
- Source reliability ranking
- Alert modules (24/7 monitoring)

Key objectives of the solution

Enable **intelligence analysts** with advanced tools leveraging correlation algorithms and artificial intelligence to drastically reduce analysis time. The platform provides dedicated user accounts that allow analysts to intuitively create, manage, and modify analytical projects—either individually or collaboratively within defined analysis groups. Projects are composed of interactive dashboards structured using automatically populated cards, which can be customized to align with specific investigative needs.

Deliver actionable insights to **end users** (e.g., decision-makers) through clear, intuitive, and easily accessible outputs. The “end-user mode” grants read-only access to dashboards and enables external users to view and download detailed, printable reports for streamlined decision-making.



Data gathering

Open Source Intelligence (OSINT)

The OSINT module focuses on collecting, processing, and analyzing information from open and publicly accessible sources (e.g., web, media outlets, public records).

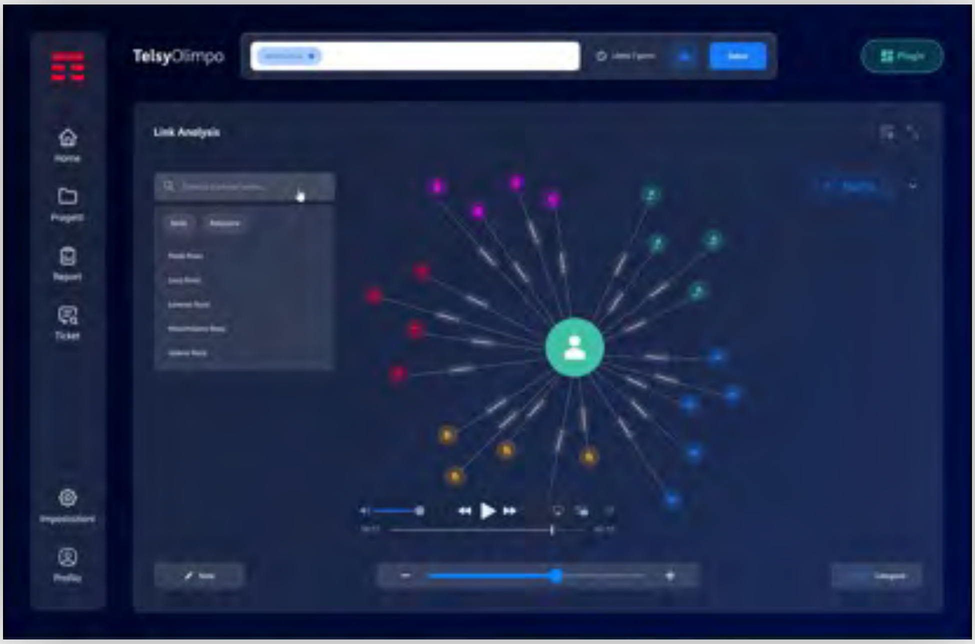
Integrated crawler ingestion capabilities empower analysts to execute web searches directly within the platform via an embedded search engine, bypassing the need to leave the platform environment. Users can also onboard new data sources seamlessly through the dashboard interface.

Social Media Intelligence (SOCMINT)

The SOCMINT module is designed to ingest, process, and analyze data from social media platforms, focusing on content shared and generated across these channels. Integrated crawlers allow seamless ingestion of social media data, enabling comprehensive analysis within the platform without requiring external tools.

Currently Integrated Social Media Platforms:

Facebook
X
Instagram
LinkedIn
Telegram
Tik Tok
VK
Reddit
YouTube
4Chan
Snapchat
Threads
Gettr
8Kun
Mastodon

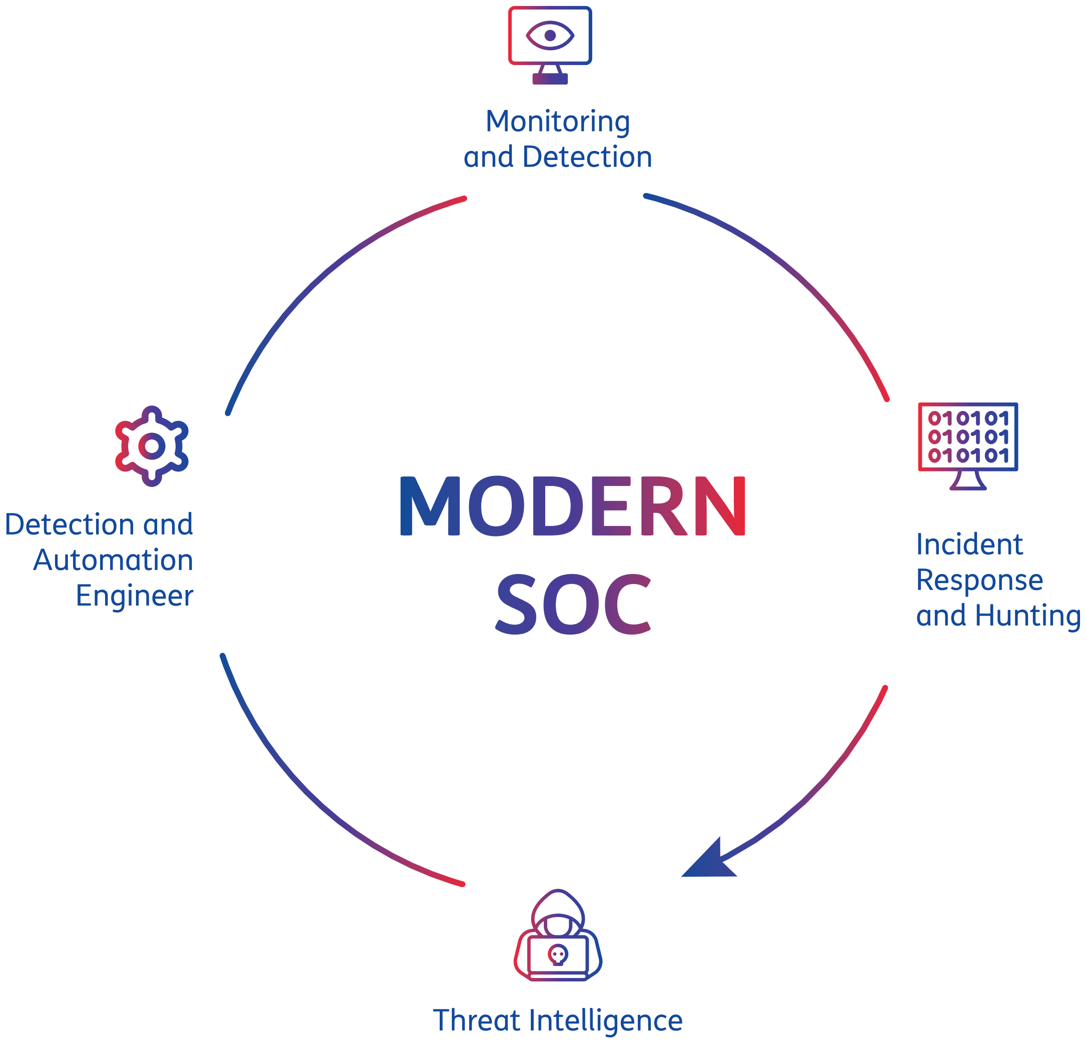


Managed Detection & Response

Cyber Threat Intelligence

Cyber threat intelligence is the knowlege that enables to identify and prevent cyber attacks

Gartner defines it as a ***«knowledge based on evidence related to an existing or emerging threat or a risk for assets»*** and, for this reason, places **CTI at the foundation of the Modern SOC**

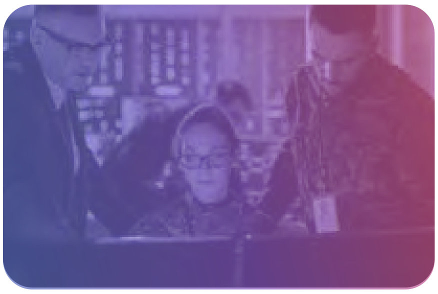


Source: Gartner 754096_C

Characteristics and functionalities of Cyber Threat Intelligence Services

A wide range of **human-validated intelligence information** from OSINT and CLOSINT sources

The **Cyber Intelligence Operations Center** (CIOC) includes specialized professionals with deep technical, investigative and contextual skills. CIOC monitors threat actors to predict their actions and assists organizations during cyber attacks



Full API Platform with unlimited users and queries

Monitoring of 300+ structured adversaries

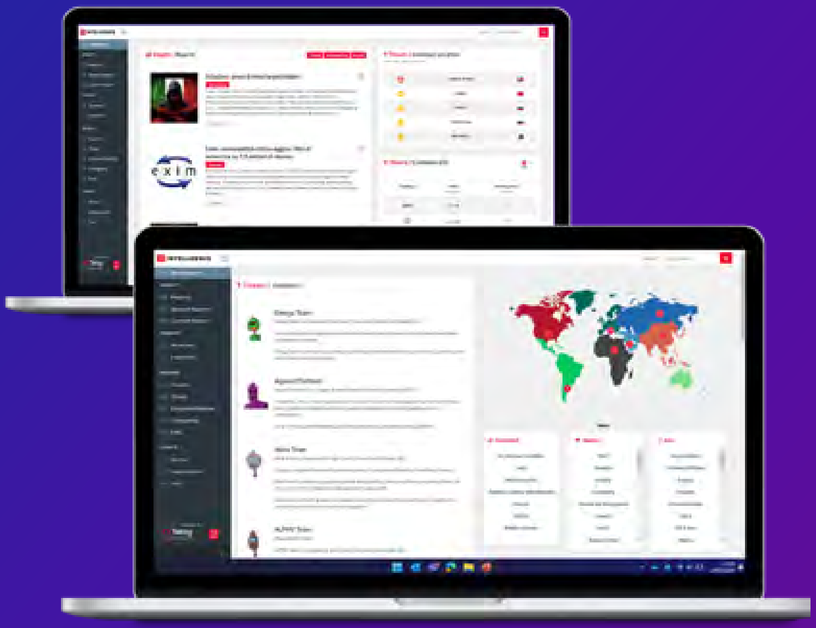
Indicators of Compromise (IoCs) constantly updated with native integration into cyber defense solutions (e.g., Firewall, XDR, SIEM)

Reduction of detection, downtime, and response times, facilitated by direct dialogue (on the platform) with the CIOC

Compliance with European regulations (NIS2) and market standards (ISO/IEC 27001)

Evolution of the defensive approach from reactive to predictive to anticipate attacks

Telsy's Cyber Threat Intelligence supports all types of organizations in any industry/region with services capable of verifying/validating information and making it available to decision makers and protection systems.



Government & Defense

Manufacturing

Pharmaceutical & Healthcare

Public Administration & Monopolies

Energy, Oil & Gas

Retail & Services

Finance & Insurance

Transportation

Information & Communication Technology

Stakeholders of tactical layer

- SOC Analyst (L1)
- SIEM and SOAR
- Firewall, IDS/IPS
- AV, EDR and XDR
- Router and other device

Stakeholders of operational layer

- Threat Hunter
- Team di Threat Investigation
- SOC Analyst (L2 ed L3)
- Incident Response Team
- Forensic Analyst

Stakeholders of strategic layer

- CISO
- CTO
- COO
- CEO
- Executive Board

CYBER INTELLIGENCE OPERATION CENTER

ALPHA TEAM
Responsible for tracking structured adversaries, advanced cyber threat intelligence activities and reverse analysis of malware samples and artefacts

BRAVO TEAM
Responsible for information enrichment in the field of Cyber Threat Intelligence and for the validation of information on all production carried out by the TS-WAY CIOC teams

CHARLIE TEAM
Responsible for managing Incident Response and Threat Hunting activities

DELTA TEAM
Responsible for information gathering, analysis and executive summary drafting activities with regard to information from mainstream open sources

ECHO TEAM
Responsible for geopolitical analysis and strategic Cyber Threat Intelligence activities

FOXTROT TEAM
Responsible for Tailored Threat Monitoring activities, monitoring and information tracking in the dark field (advanced OSINT and CLOSINT) and management of investigation activities

GOLF TEAM
Responsible for SOCMINT activities aimed at brand monitoring and sentiment analysis

Managed Security Services

TelsySpywareDetector^{Device}

The increasing reliance on mobile devices has turned smartphones into prime targets for malware creators.

In today's digital landscape, smartphones have become critical tools for business operations, significantly expanding the attack surface and introducing new risks. An unsecured or mismanaged mobile device can lead to severe consequences, including espionage, data breaches, and operational disruptions.

TelsySpywareDetector^{Device} is a solution designed to detect the potential presence of spyware on mobile devices without compromising user privacy.

Installed on a dedicated tablet, **Telsy**SpywareDetector^{Device} software conducts automated scans of processes, executions, and file ownerships on a connected mobile device via USB. By maintaining the user's privacy and generating comprehensive reports on detected anomalies, the solution provides businesses with actionable insights through a secure, dedicated dashboard.

Malware and infection technics

Ransomware
Blackmails you

Spyware
Steals your data

Among the various types of malware, spyware poses a particularly insidious threat, as it can be deliberately installed or hidden within seemingly innocuous apps.

Adware
Spams you with adds

Trojan
Sneaks malware onto your device

Worm
Spreads across computers

‘Remote’ Infection

The device is compromised remotely, without any direct physical contact

- Social Engineering (e.g. phishing)
- Drive-by Download
- Exploiting Remote Vulnerabilities (e.g. malicious app)
- 1 Click / N Click

‘Proximity’ Infection

Attacks requiring physical proximity via wireless technologies

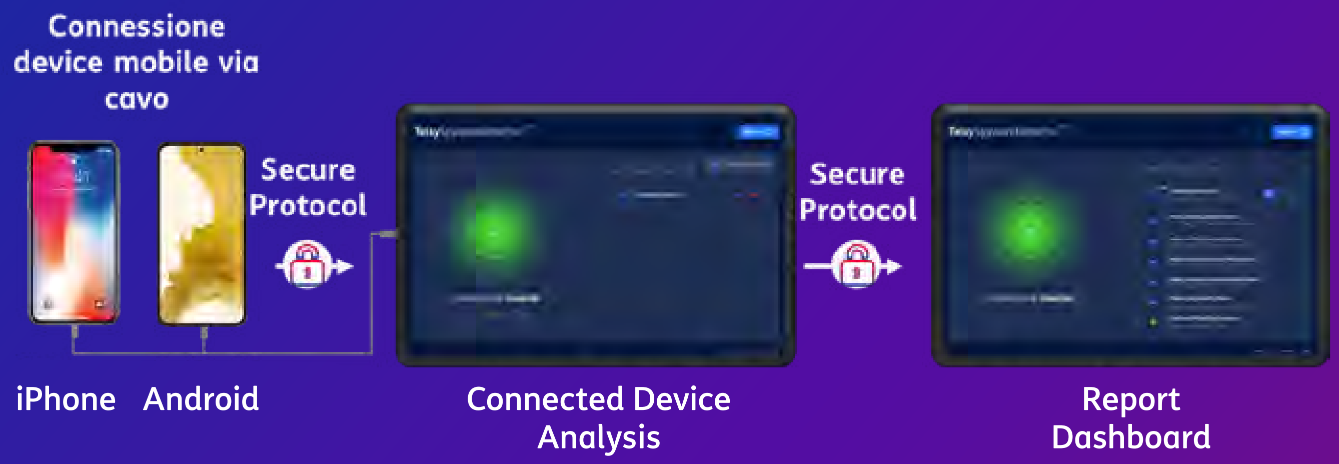
- Social Engineering (e.g. phishing)
- Man in the Middle
- Exploit 0 Click (Bluetooth)
- NFC (Near Field Communication)

‘Local’ Infection

Infections through direct physical access

- USB Malware
- Sim Swap

How it works TelsySpywareDetector$^{\text{Device}}$



Connessione device mobile via cavo

Secure Protocol

iPhone Android

Connected Device Analysis

Secure Protocol

Report Dashboard

Key Benefits

- Compromise Status Check
- No Installation Required on the Device
- No Network Connection Needed
- User Privacy Guarantee
- Quick Scanning Time

5 myths to debunk

FALSE “EMM/MDM keeps my device secure”

FALSE “Protected folders keep me safe”

FALSE “Mobile security is not a priority”

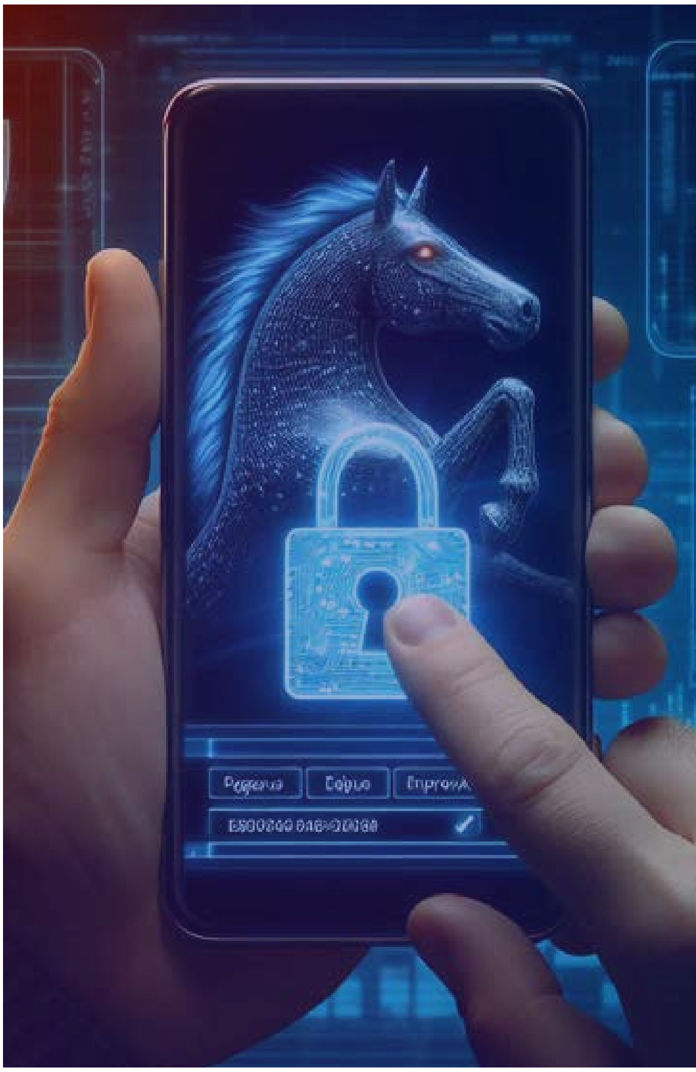
FALSE “iOS is immune to cyberattacks”

FALSE “I’m protected with antivirus software”

The Pegasus Case

In 2023, the **Telsy**SpywareDetector^{Device} solution successfully identified a suspicious process with elevated privileges on a mobile device, which was later revealed to be one of the most sophisticated spyware ever discovered, known as Pegasus*.

This discovery highlights the solution’s ability to effectively detect advanced threats even before they are publicly recognized, enabling necessary actions to prevent data exfiltration.



*__Pegasus__ is an **advanced spyware** developed by the Israeli company NSO Group, known for its ability to monitor cell phones and mobile devices. This software can infiltrate devices without the user’s knowledge, **often exploiting unknown vulnerabilities (zero-day) or phishing techniques**. Once installed, Pegasus can **gain full access to the device**, allowing attackers to **extract data** such as messages, emails, contacts, and activate the microphone and camera to monitor the surrounding environment.

Communication Security

TelsyInTouch

Answering the growing need of secure communication for mobile devices, InTouch is Telsy solution for instant messaging communication and critical information sharing.

TelsyInTouch crypto mobile solution is an integrated solution (App & Phone) designed to provide Companies and Government Agencies with a strong and secure tool for sensitive communications in all operational environments.

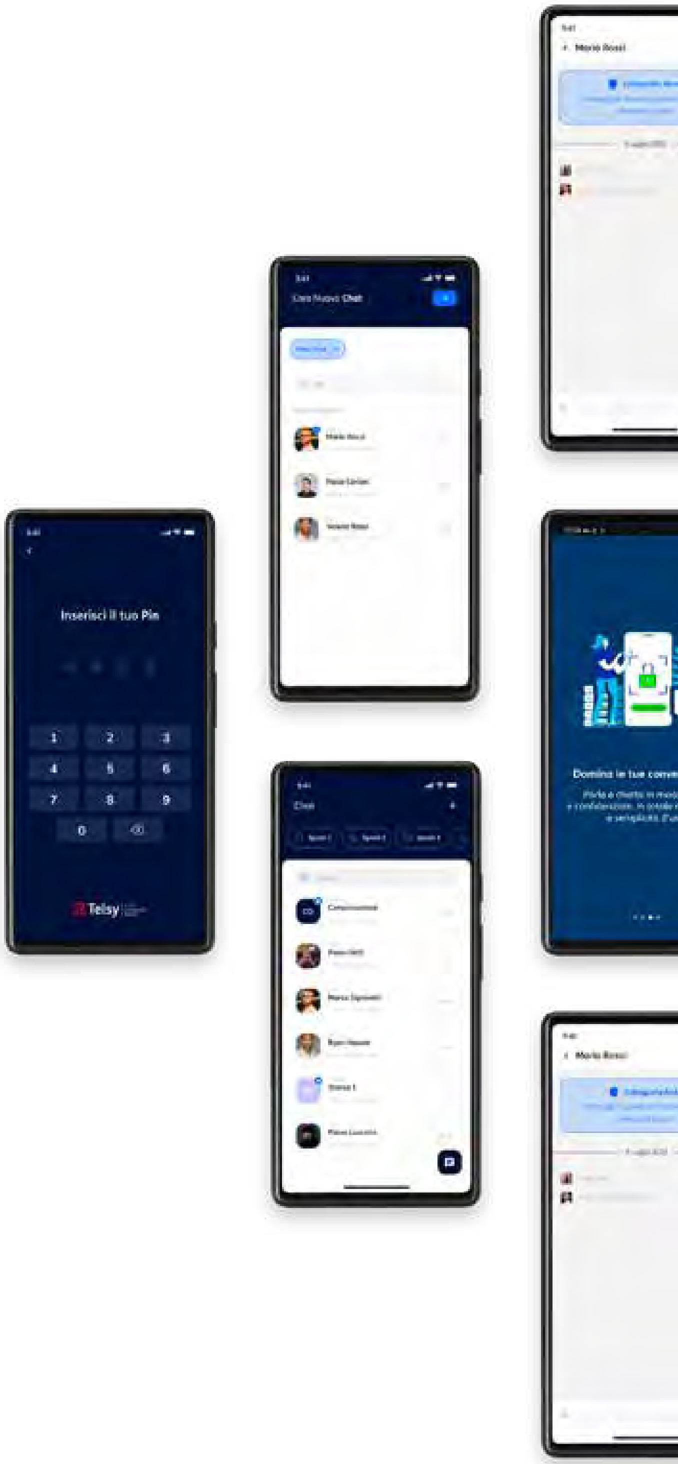
TelsyInTouch, is an innovative integrated secure collaboration solution composed by two distinct elements.

The first one is **Telsy**InTouch$^{\text{App}}$, a secure collaboration app that guarantees encrypted communication for the users. The second one is **Telsy**InTouch$^{\text{Phone}}$ terminal, compliant to Common Criteria 3.1 and 3.2 certified and appropriately configured to minimise the attack surface.

Instant messaging app

TelsyInTouch App

A secure instant messaging app that provides a user experience similar to the one of other widely diffused instant messaging apps, delivering also high audio and video quality thanks to the advanced codecs utilized. Available for both **Android** and **iOS**, the InTouch app uses E2EE for chat, VoIP calls and audio conferencing.

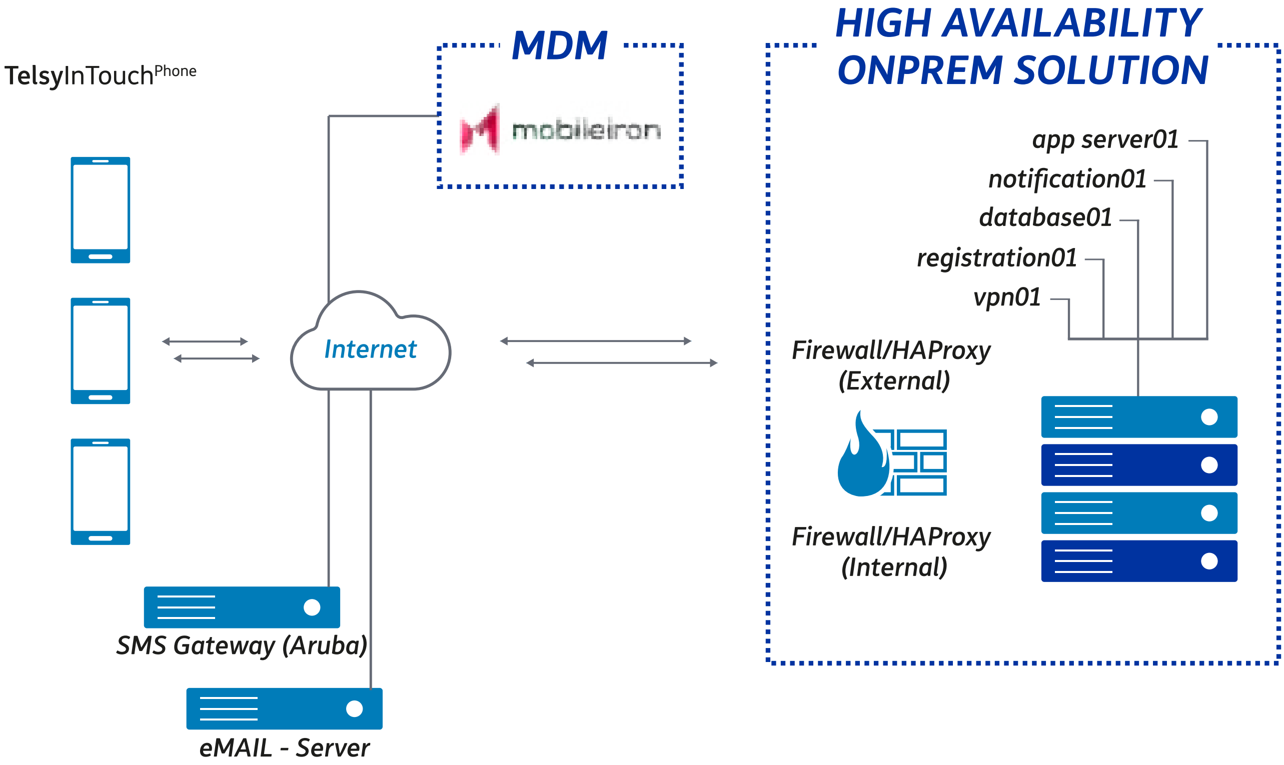


Secure smartphone

TelsyInTouch Phone

Kernel-level configured, Common Criteria certified, last generation smartphones for maximum **COMSEC** and **CIS** security. The device attack surface is reduced to the minimum by enabling only the features required by the customer in order to achieve high security and confidentiality.

Functionality of **Telsy**InTouch^{App}



Characteristics

- The iOS and Android terminals are compliant to Common Criteria 3.1 and 3.2 certified for mobiles (which not only guarantee the highest security standards but also facilitate the approval process)
- Security over the entire communication flow (multi-layer) enabled by the integration of **Telsy**InTouch^{Phone} and **Telsy**InTouch^{App}
- The obsolescence of mobile terminals does not entail any problems
- Multi-vendor and multi-operating system (Android and iOS) cross-platform solution
- Use of the proprietary **Telsy**Guard protocol for the secure communication part (COMSEC+), hence full interoperability with the entire ecosystem of Telsy solutions
- Firmware security patch update with ‘zero delay’ after release by the terminal vendor
- Management, maintenance and configuration of the system in “MDM as-a-service” mode by outsourcing responsibilities and costs related to deploying physical and human resources to Telsy

Technical data sheet

TelsyInTouch

	Object	Quantity	Model
Hardware composition of the system	Server	2	PowerEdge R350 Server (or similars)
	Log Server	1	Smart Value PowerEdge R350 Server Basic
	NAS	2	RS820xs
	Dischi per NAS	8	Seagate IronWolf Pro, 4TB
	Firewall	2	Server DELL R250-CPU E-14 16GB RAM - 1X1 TB HDD SATA-Intel i350 Quad Port 1GB
	Switch	2	CISCO CBS350 MANAGED 24 - Port GE, FULL POE, 4XG
	Armadio	1	Rack da 19 24RU 1000
	UPS (optional)	1	APC - 3000 VA
	KVM	1	Console KVM Modulare con LCD 17” da Rack 19”

Employed technologies	**KVM** virtualization environment **Matrix** Specification compliancy **TelsyGuard** VPN 3 Diffie-Hellman Rooms Session Encryption **AES256** message encryption WebRTC Communication Online or fully offline mobile ativation

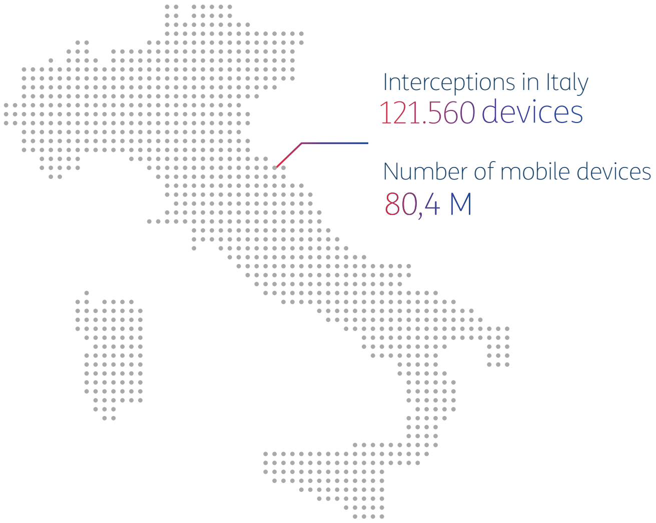
Communication Security

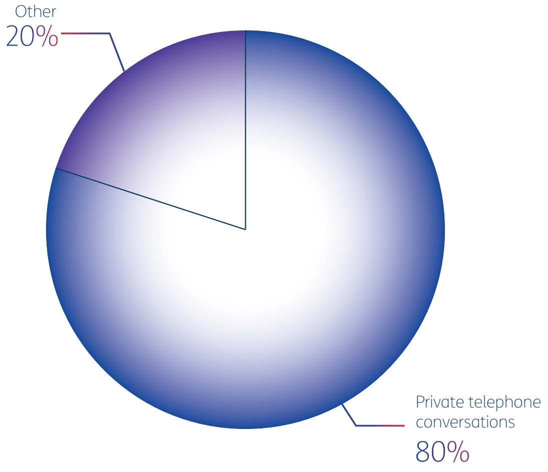
TelsyATMO

During business meetings, we are often exposed to the risk of eavesdropping with the purpose of espionage or information theft. In this scenario, all mobile digital devices such as smartphones and smartwatches are potential attack vectors. They can be exploited as gateways by attackers, that can access the device microphone and record conversations remaining undetected.

In the early 2000s, approximately 70,000 telephones were tapped during the year. Today, an average of around 130,000 phones are intercepted annually.

In 2022, the “targets” of wiretapping in Italy totalled 121,560 devices. Of these, more than 80% were private telephone conversations, corresponding to more than 61,000 persons (considering that the wiretapping affected persons holding several telephone numbers at the same time).





***Source:** How many people are tapped on the phone in Italy, 2022, Digital 2022 political report in Italy, 2022, DGline*

This data shows how the need to hold discussions in a safe and secure manner requires focused precautions, especially in situations of strategic importance or in confidential contexts.

The **Telsy**ATMO system arose from the need to protect sensitive or confidential information and communications against the risks of eavesdropping.

Outwardly a hi-tech gadget holder, **Telsy**ATMO is actually an ultrasonic audio jammer that inhibits malicious applications on compromised smartphones from listening in ongoing voice conversations. Thanks to this capability, the system prevents any conversation held in the presence of mobile devices from being intercepted.

TelsyATMO is capable of emitting very high frequencies, so as to provide a sonic shield for any incoming acoustic signal from the mobile device housed inside.

Features

System concept

TelsyATMO consists of an open housing in which one or more mobile devices, such as smartphones or smartwatches, can be stored, ensuring that they remain visible, accessible and reachable thanks to its transparent structure.

In this way, it is always possible to have evidence of any notifications, communications and system status at a glance.

How it works

Within the housing space, **Telsy**ATMO emits ultrasonic noise signals that are inaudible to the human ear.

These ultrasounds saturate the microphones of the hosed devices to such an extent that all other ambient sounds are distorted and rendered unintelligible to any listening device. This technique guarantees confidentiality in sensitive situations

Ease of use

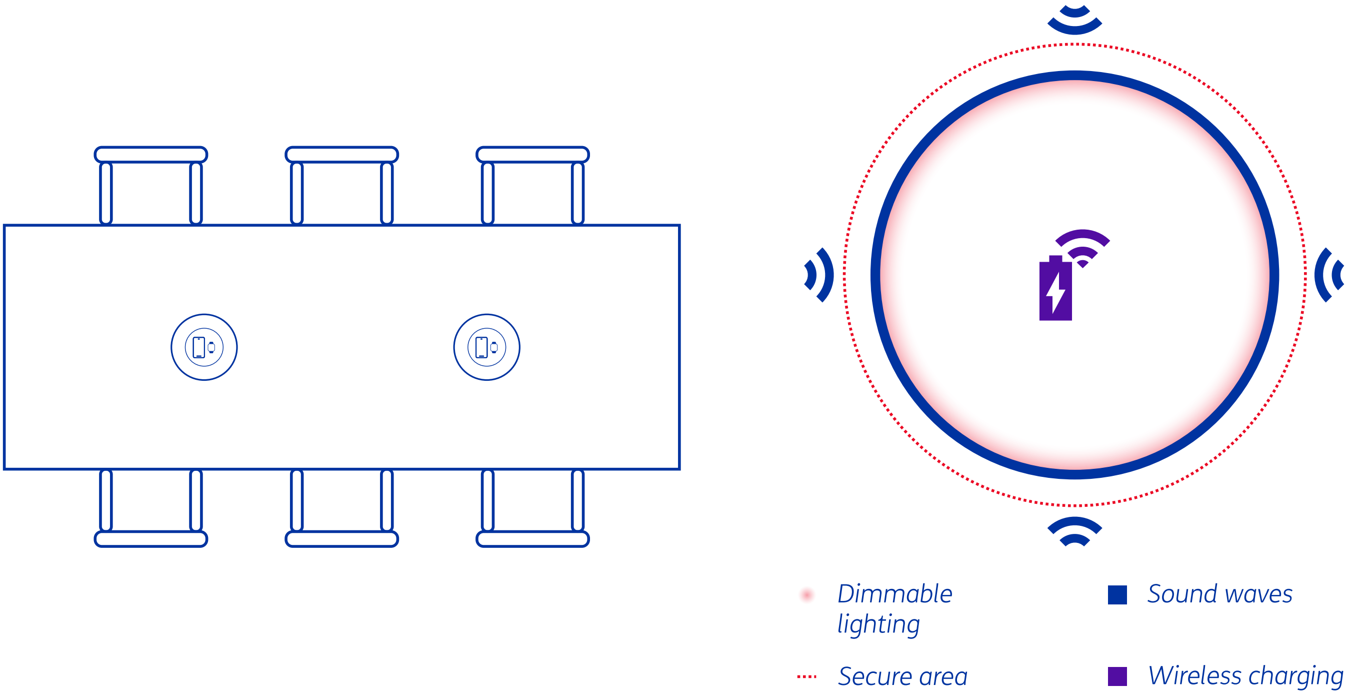
TelsyATMO is equipped with a wireless charger for the battery of the devices housed in it, together with a dimmable diffuse lighting system that can be controlled remotely via a dedicated remote control unit. The sonic protection function and wireless charging for devices can also be switched off via a simple switch.

Elegant, transparent and robust safeguard

Conversations and privacy

Incomparable ease of use

Use case



TelsyATMO is designed to protect all conversations during meetings, briefings or calls.

Whether it is a table with more than one person talking or a video conference from your personal location, **Telsy**ATMO provides an efficient acoustic shield capable of blocking any incoming sound waves to your device, preventing any unwanted apps or malware from recording confidential sounds or conversations.

Communication Security

TelsyAntares

As remote working continues to expand, virtual meeting is becoming an integral part of business operations where video conferencing is expected to play a crucial role in shaping the future of team collaboration.

TelsyAntares is a web conferencing system developed on an open-source platform named Jitsi. Asymmetric cryptography protocols are used to implement participant authentication.

This platform can be easily deployed on different customer infrastructures, providing higher security levels than other video conferencing solutions available on the market.

Encryption keys are managed exclusively by the customer, and the system installation is fully implemented on customer premises.

Charateristics

- *Available on the customer-dedicated hardware platform and installed on-site*
- *Availability of videoconferencing with mixed traffic (traffic from an internal network, traffic from an external network, traffic from an internal and external network)*
- *Platform monitoring by forwarding logs to SIEM (syslog) or Stack ELK*
- *Three categories of users are available: administrator, moderator and guest*
- *Password management conforming to IAM best practices*
- *Dashboard displaying platform statistics*
- *Management dashboard for user and room management*
- *Videoconferencing with no time limit and up to 50 participants*
- *Use of WebRTC technology*
- *End-to-end connection encryption mechanisms can be activated to ensure maximum privacy and security of communication (participant limit set to 20, Chrome/Chromium browser or derivatives required)*
- *Most common features of videoconferencing systems*

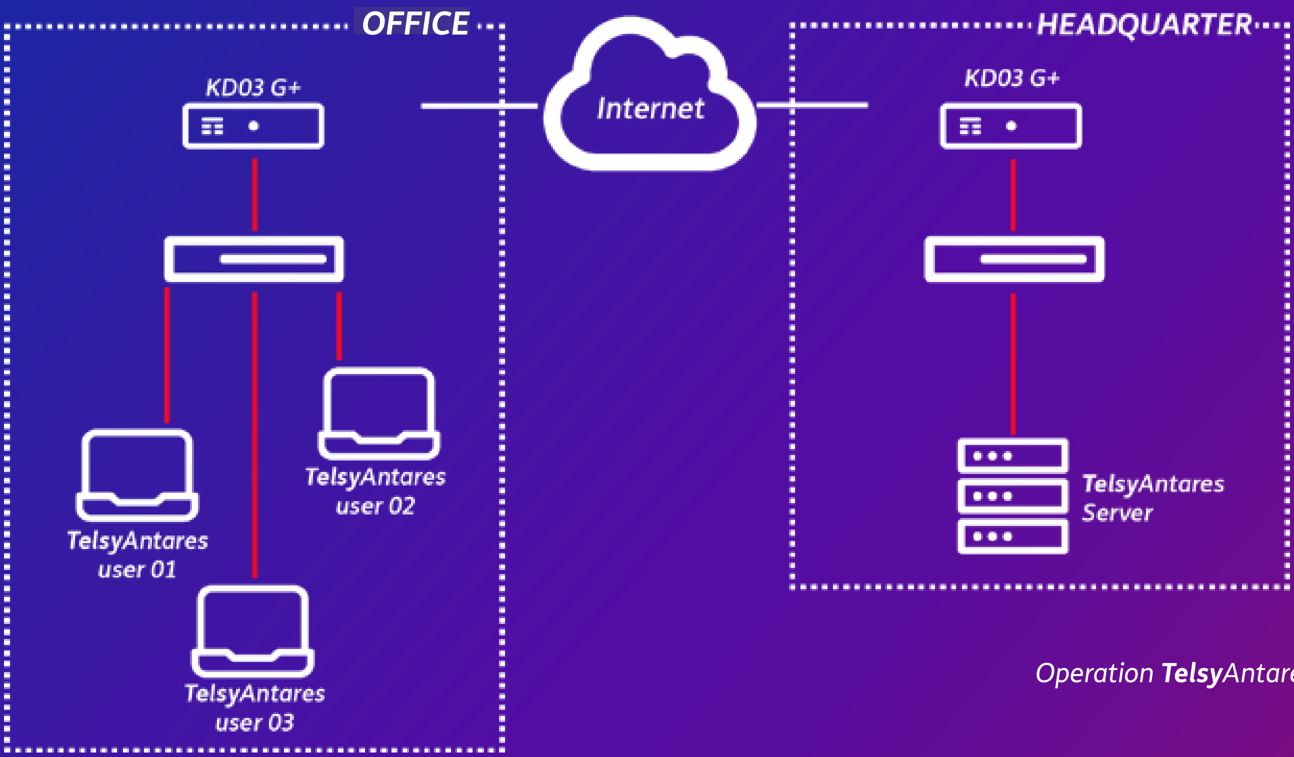
Cryptography and security

The underlying approach used in developing the **Telsy**Antares component is Zero Trust. For this reason, all internal and external flows (relating to **Telsy**Antares) are encrypted.

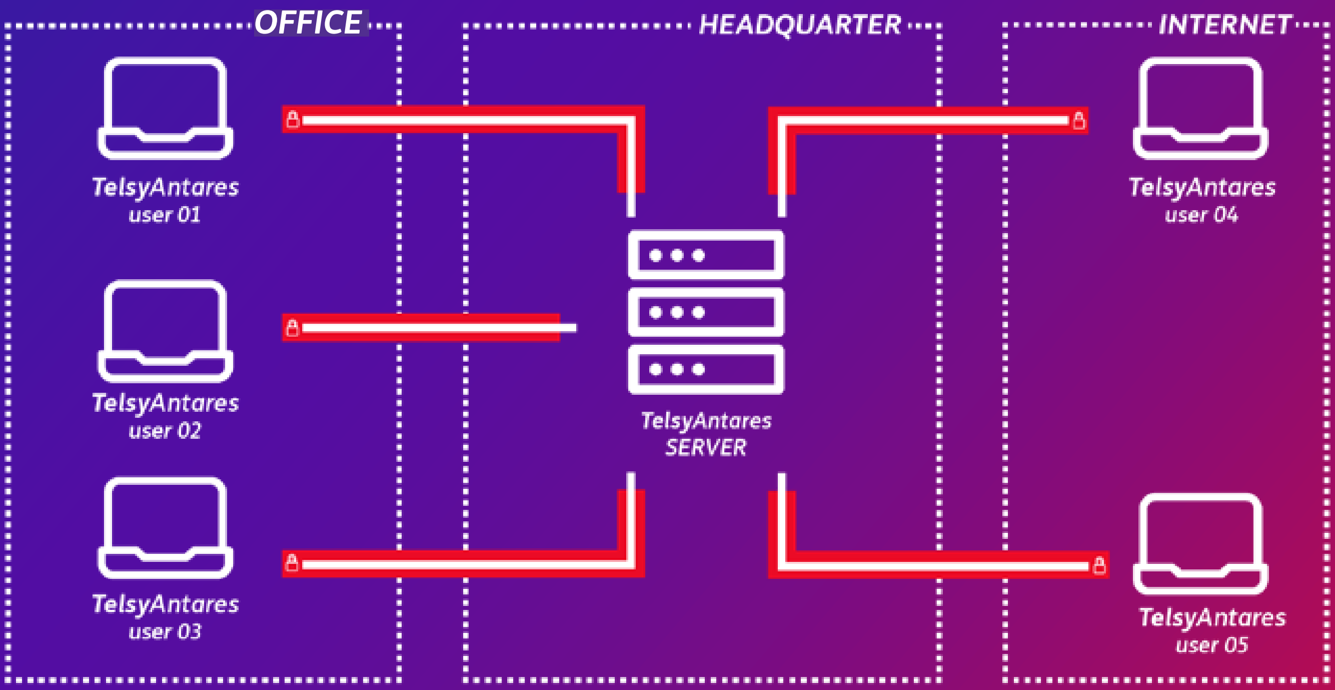
Keys and passwords are loaded into the system and protected with strong access privileges or stored in encrypted key-value databases.

The externally exposed **Telsy**Antares Rest APIs are authenticated with JWT **Telsy**Antares tokens of Bearer type, passed in the HTTP Authorisation header. In addition, sensitive public APIs are protected with API throttling mechanisms.

Operation & case study



*Operation **Telsy**Antares*



🟥 DTLS-SRTP

— E2EE AES-GCM

*Case study **Telsy**Antares*

Technical data sheet

TelsyAntares

	Quantity	Item
Hardware composition of the system The system is installed on a customer-dedicated hardware platform and installed on-site with the following components:	3	Dell PowerEdge R340 servers (or similar)
	2	24p switches with 10GbE capacity in HA
	2	Firewall with 10GbE capacity in HA
Used technologies		KVM for stack virtualisation
		Jitsi CE for the videoconference component (SFU architecture)
		Docker Swarm as the infrastructure of TelsyAntares
		MariaDB Galera Cluster as a database
		Other software: Nginx, HAProxy, GOlang, React
		JSON Web Token-based authentication with RS256 signature
		Database encryption with AES256
		Hashing database with 10 round Bcrypt
		DTLS-SRTP client-server encryption
		End-to-end AES-GCM encryption using 128-bit keys with key rotation
Network exposure The following ports must be available (and reachable) to access the platform.		TCP 80
		TCP 443
		UDP 10000 (videobridge)
		UDP 3478 (turn server)

Communication Security

Quantum Key Distribution

The tremendous computational potential provided by innovative technologies such as Quantum Computing puts the security of classical cryptography at serious risk. In response to this problem, Telsy and QTI are taking the field with Quantum Key Distribution.

One of the most significant vulnerabilities in today's cryptographic security lies in the exchange of encryption keys.

These keys are cryptographic codes required to validate the security and non-compromise nature of the data and information being exchanged by the communicating parties, sender and receiver.

Quantum Key Distribution (QKD) is a physical layer method that provides an unconditionally secure distribution of random keys between remote users.

In short, QKD is a technology that exploits the physical properties of photons to distribute secret keys between encryptors to secure ongoing communication.

Thanks to the laws of quantum physics, the slightest perturbation in the communication channel (due, for example, to a hostile attacker intruding into the communication to exfiltrate sensitive or confidential information) causes the system to discard the compromised key, interrupting the transmission itself and making any theft of data or information impossible.

Quantum Key Distribution System

Quell-X

Quell-X is a complete **QKD** system consisting of one Alice unit and one Bob unit capable of generating secure quantum keys for ultra-secure data communication.

Main features:

- It can be implemented on existing networks, even in complex architectures, and can implement trusted nodes to reach long distances.
- An ultra-versatile solution that can be used in any network configuration: point-to-point links, trusted node configuration, and more advanced network topologies (e.g., ring or star networks).
- It's fully integrable into existing telecommunications networks due to the flexibility of the equipment operating in both C-band and O-band.

Available in two main versions:

- Quell-X is the core product of the family. It guarantees reliable and high-performance QKD quantum key generation. It includes a standardised key management entity compatible with third-party encryption units.
- Quell-XR is the Quell-X version for academic and research activities. It generates raw key data for customised post-processing protocols and future developments. Quell-XR is a customisable platform and can be interfaced with third-party detectors.

QTI & Telsy

The complete system

In 2021, Telsy S.p.A. - the cybersecurity and encryption competence center of the TIM Group - acquired part of QTI's shares, reaching the 80% of the company share in 2024.

This partnership enabled the development of a fully reliable end-to-end encryption system compatible with current telecommunication infrastructures for civil and military applications. This solution integrates Quell-XC, an optimised version of the QTI QKD system, with Telsy's high-speed Layer 3 encryptors (throughput up to 1Gbps and latency of ~1ms).

Applications:

- Cryptographic key distribution infrastructures
- Data center security
- Medical data protection
- National and cross-border backbones
- Long-distance key distribution based on trusted nodes
- Key distribution over advanced reconfigurable networks (star, ring, software-defined networks)
- Security of government and financial data
- Security of critical infrastructure: airports, ports, gas distribution and electricity grids.

Beyond point-to-point networks

QKME and QSDN

Current telecommunications infrastructures rely on **complex multi-point networks**. For guaranteeing the ultimate security of telecommunications, Quantum Key Distribution (QKD) needs to be compatible with existing architectures. QTI and Telsy meet the challenge of bringing QKD in the **real world** through their **Key Management Entity (QKME)** and **Software Defined Network QKD solution (QSDN)**.

QKME is a state-of-the-art network appliance able to perform secure key storage and key deployment following the latest standards in the QKD field.

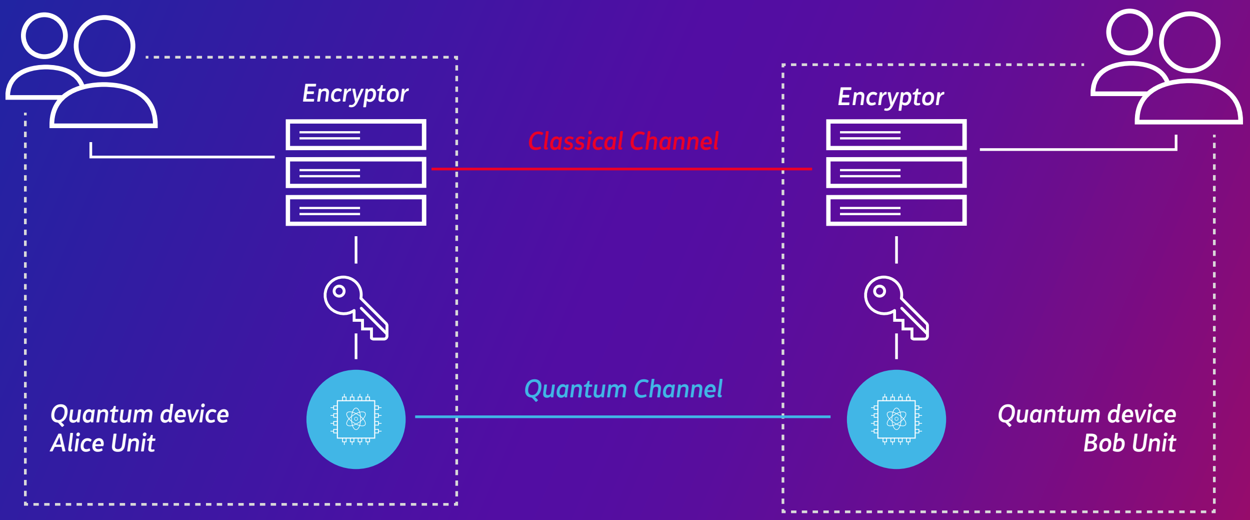
KME allows the integration between classical and QKD technology, abstracting the key-generation process and providing simple REST APIs. QKME can manage multiple clients and allows communications between clients using different standards (ETSI GS QKD 014; ETSI GS QKD 004; Cisco SKIP).

QKME can be fully integrated with QTI Quell-X QKD systems and it is an essential component of SDN configuration for a complete QTI turn key solution.

Software Defined Network (SDN) is a technology that centralizes the management of a network and allows to dynamically configure it. This is done by a SDN controller that can understand what kinds of devices are present in the network and configure them in the most efficient way.

QSDN implements the latest SD-QKD standard available (ETSI GS QKD 015). The standard brings also the possibility to interconnect QKD networks from different vendors, with different protocols, using Gateway nodes.

Basic use case



Technical data sheet

Quell-X

		Quantity	Object
Specifications	Interfaces	1	Duplex/Simplex single-mode fiber (Upon request)
		2	1Gb Ethernet ports
			Operating LEDs Outputs
	Quantum state a preparation:		Up to 600 MHz
	Quantum protocol:		Discrete-variable BB84 with time-bin encoding and decoy states
	Key security parameter:		10^{-9}
	Link budget:		Up to 30 dB
	Secret key rate:		2.4 kb/s @ 10dB
			1.7 kb/s @ 20dB
			500 b/s @ 25 dB
			150 b/s @ 30 dB
	Key management protocol:		ETSI GS QKD 014
			ETSI GS QKD 004
			ETSI GS QKD 015
			Cisco Secure Key Integration protocol Skip
	WDM compatibility:		Operating with non-dark fibers upon request (C/O-band wavelengths and ITU channels customized)
	Operating temperature:		10°C to 35°C with no direct sunlight on the equipment
	Operating humidity:		0% to 85% relative humidity with 29°C maximum dew point
Dimensions			Standard 19" rack mount, height = 2U, 650 mm depth

Communication Security

TelsyMusa

Ensuring adequate security standards for your servers is essential. This need, coupled with the growth rate of cyber threats and, above all, the increasingly varied nature of the vulnerability surfaces targeted by attacks, calls for considerable expense and continuous support.

The **Telsy**Musa range of encryptors includes Rack, Desk and **Telsy**MusaX designed to be integrated with the Quantum Key Distribution system. They are IP Layer 3 encryptors, designed to cover usage cases such as a point-to-point configuration for connecting headquarters to its data centre, up to complex centre-to-station systems.

The practical and innovative form factor of **Telsy**Musa Desk makes it unique, offering the extreme manageability of hardware designed to be used even on a desk along with extremely high throughput and security performance values.

Like all the devices belonging to this range of encryptors, **Telsy**Musa and TelsyMusaX use the proprietary **Telsy**Guard protocol, optimised to maximise performance in terms of throughput while still maintaining high security standards.

The **Telsy**Musa encryptor

TelsyMusa is a software solution designed and developed by Telsy, implemented on various COTS devices selected by our Engineering department and, for this reason, very versatile in covering different usage situations.

Particularly in its desk-top form factor, **Telsy**Musa Desk optimises its practical nature by helping the user to organise, protect and quickly access confidential and sensitive data, making daily work more efficient and secure.

It has three network interfaces: one for local management, one for LAN unencrypted traffic, and one for WAN encrypted traffic.

For the lifecycle of the cryptographic keys, **Telsy**Musa uses two separate smartcards: IT (Initialisation Token) for the initialisation phase, and CIK (Crypto Ignition Key) during operation. The removal of the CIK smartcard renders the device inert, blocking the movement of network traffic in both directions.

Management console

TelsyMusa encryptors provide a specific physical port for local management of the device. This port gives access to a graphic interface allowing the operator - with the appropriate credentials - to carry out the following operations:

- Device initialisation
- Uploading of the cryptographic material
- Uploading of the network configurations
- Visualisation of non-sensitive details on the loaded traffic keys
- Visualisation of the traffic statistics
- Device zeroisation
- Device restart

TelsyGuard protocol

TelsyMusa is a network encryptor based on **Telsy**Guard, a proprietary protocol developed by Telsy. The **Telsy**Guard protocol guarantees:

- Post-quantum confidentiality
- Different and unique communication keys for each session
- *Perfect forward secrecy* (PFS)
- Mutual authentication between the parties
- *Handshake* in 1-RTT
- *Throughput* of 850 Mbps @ MTU 1420
- Latency less than 2 ms

Key Distribution Center (KDC)

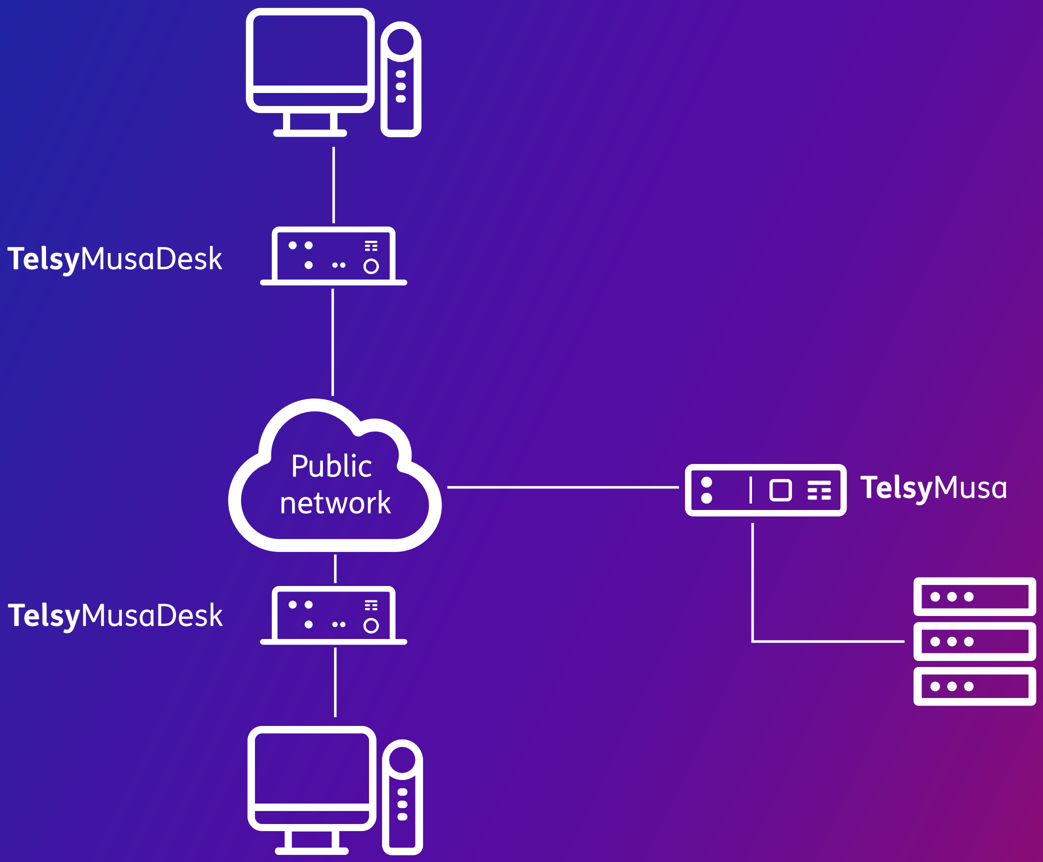
To support **Telsy**Musa encryptors, the system has a specific solution for managing the cryptographic parameters: the **Key Distribution Centre** (KDC) for generating and distributing cypher keys.

This sub-system manages all the operations aimed at ensuring the correct lifecycle of the cryptographic material and configuration parameters in relation to the operation of the encryptor network:

- Management of the cryptographic security parameters
- Smartcard programming for the initialisation (IT) and use (CIK) of the device
- Generation of device configuration files

The system is offline and therefore air-gap; all the CSP cryptographic material is distributed to the encryptors via **IT (initialisation tokens)**, **CIK (cryptographic ignition keys)**, and the encryptor configuration file. The smartcards and file are required during the commissioning and initial configuration of the encryptor in the device configuration wizard on the control console.

Use case



Technical data sheet

TelsyMusa Desk

Cryptography and security		Cypher algorithm standard AES256
		Set-up via *smartcards* programmed by KDC. Keys distributed by KDC
		Access control via ISO7816 *smartcard*, with PIN defined by KDC
Performance		Maximum throughput 850 Mbps @ MTU 1420. Latency less than 2 ms
		Latenza inferiore a 2 ms
Installation	Dimension	Form factor: desktop, with removable slots 170mm x 69mm x 135mm (WxHxD)
		Weight 1.3 kg
Interfaces used		2 Gigabit Ethernet interfaces
		1 Ethernet *management* interface.
		Power supply connector
Processor	CPU	Intel® Celeron® processor 6305E; Single-socket FCBGA-1449 supported, CPU TDP supports up to 15W TDP
	Core	Up to 2 cores, 2 threads / 4MB Cache
Environmental operating conditions	Operating Temperature Range	0°C - 60°C (32°F - 140°F)
	Non-Operating Temperature Range	-40°C - 85°C (-40°F - 185°F)
	Operating Relative Humidity Range	8% - 90% (non-condensing)
	Non-Operating Relative Humidity Range	10% - 95% (non-condensing)

Communication Security

TelsyMusaX

Ensuring adequate security standards for your servers and networks is essential. Achieving this goal, however, requires considerable investment and operational costs especially taking into account the growth of cyber threats and the increasingly variety of the vulnerability surfaces targeted by attacks.

The **Telsy**Musa family of ciphers provides a complete range of IP-based encryption solutions for application in large-scale network architectures.

This family includes the **Telsy**Musa and **Telsy**MusaX, IP layer 3 encryptors designed to cover simple use cases, such as a point-to-point configuration for connecting a head office to its data centre, up to complex spoke-hub star networks.

Like all devices belonging to this family of encryptors, **Telsy**Musa and **Telsy**MusaX use the proprietary **Telsy**Guard protocol, optimised to maximise performance in terms of throughputwhile maintaining high security standards.

TelsyMusaX Encryptors

Management console

TelsyMusaX is a software solution designed and developed by Telsy, implemented on DELL SERVERS of the PowerEdge family. It has four Ethernet network interfaces: one for local management, one for unencrypted LAN traffic, one for encrypted WAN traffic, and one dedicated to the QKD system (Alice and Bob).

For the encryption keys lifecycle, **Telsy**Musa encryptors use a USB token into which two separate smartcards are inserted: IT (Initialisation Token) for the initialisation phase and a CIK (Crypto Ignition Key) during operation. Removing the CIK smartcard token renders the device inactive, blocking the passage of network traffic in both directions.

TelsyGuard Protocol

TelsyMusaX is a network encryptor that uses a derivative of TelsyGuard, a proprietary protocol developed by Telsy. This particular version of the protocol integrates quantum keys generated by the QKD Quell-X system to which the **Telsy**MusaX encryptor is linked. Thanks to the optimisations implemented to maximise performance in terms of throughput, **Telsy**MusaX can reach 1 Gbps with latencies of less than 2 ms.

The **Telsy**Guard protocol guarantees:

- Post-quantum confidentiality
- Different and unique communication keys for each session
- Perfect forward secrecy (PFS)
- Mutual authentication between the parties
- Handshake in 1-RTT
- Throughput exceeding 1 Gbps with 1420-byte packets
- Latency lower than 2 ms

Management console

TelsyMusa encryptors are equipped with a physical port for local device management. This port provides access to a graphical interface that enables an operator with appropriate credentials to perform the following operations:

- Device initialisation
- Uploading of cryptographic material from the KDC
- Configuration loading
- Review of non-sensitive details on loaded traffic keys
- Review of traffic statistics
- Device Zeroisation

The **Telsy**Musa System

To support **Telsy**Musa encryptors, the system provides a specific solution for the management of cryptographic parameters:

- *Key Distribution Center (KDC)*, per la generazione e la distribuzione delle chiavi di cifratura.

Key Distribution Center (KDC)

This subsystem manages all operations to ensure the proper lifecycle of the cryptographic material and configuration parameters in relation to the operation of the encryptor network:

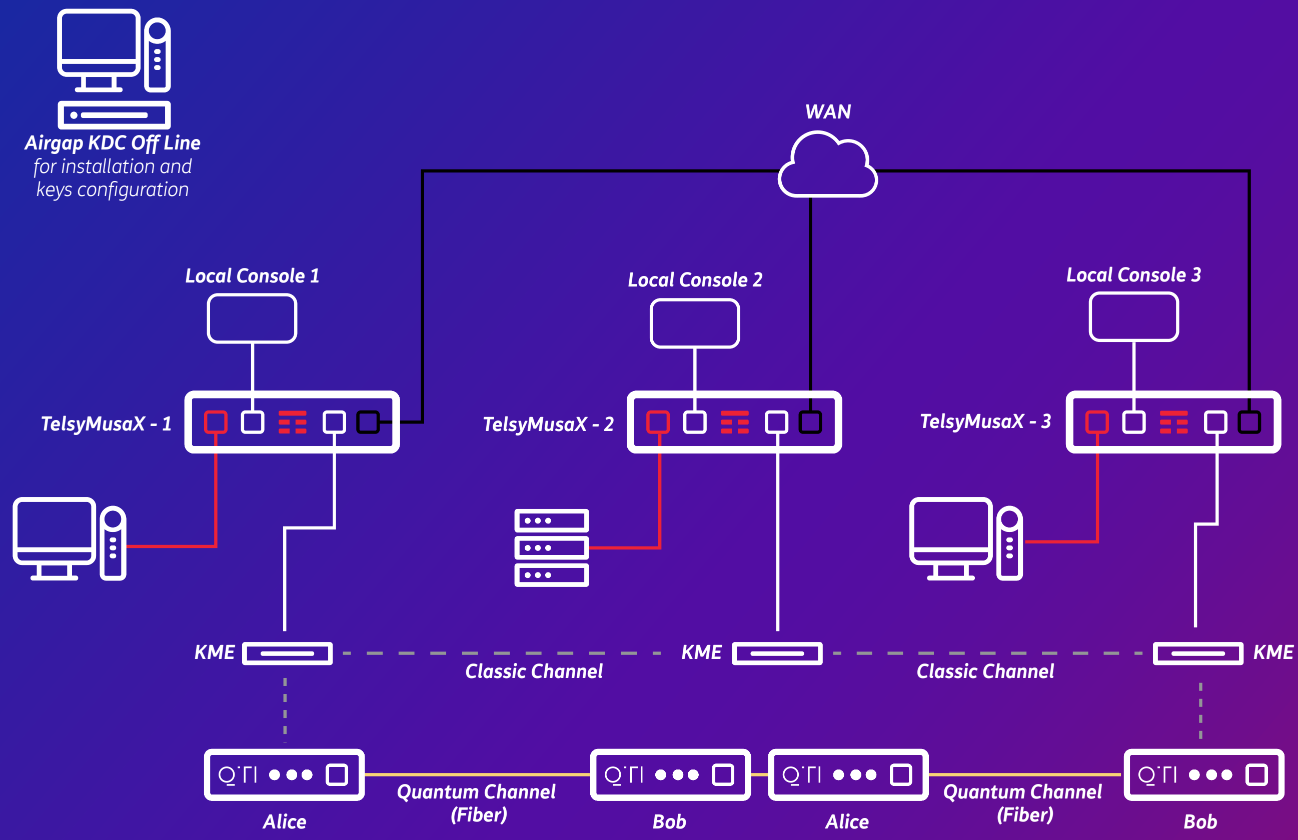
- Management of cryptographic security parameters.
- Smartcard programming for initialisation (IT) and use (CIK) of the device.

Cryptography

Like all devices belonging to the **Telsy**Musa family of encryptors, **Telsy**MusaX uses the proprietary **Telsy**Guard protocol, in this case specially modified for the QKD system. For this protocol, in addition to the communication keys provided by KDC, **Telsy**MusaX uses the QKD component keys provided by the Quell-X solution.

The encryption algorithm used is standard AES256.

Use Case



🟥 Unencrypted traffic

⬜ Local management control (opt)

🟪 KME

⬛ Encrypted traffic

Technical data sheet

TelsyMusaX

Installation	Form factor	Rack 19”, 1 RU W x H x D: 482 mm x 42,8 mm x 734.95mm (without Bezel)
	Mounting	Mounting brackets for the rack: ReadyRails Sliding Rails with Cable Management Arm
	Weight	18.62 kg (max)
Power supply	AC power supply units	Power Supplies options: 600W Platinum Mixed Mode (100-240Vac or 240Vdc) hot swap redundant 800W Platinum Mixed Mode (100-240Vac or 240Vdc) hot swap redundant 1100W -48Vdc hot swap redundant (CAUTION: only works with -48Vdc to -60Vdc power input)
Climatic and environmental conditions	Ambient temperature	Storage: –40°C to 65°C Operating temperature (for altitude less than 950 m or 3117 ft): 10°C to 35°C °C
	Humidity	Operating (Without condensation): 8% RH with -12°C minimum dew point to 80% RH with 21°C (69.8°F) maximum dew point
Data ports	Number of ports	Data lines: 2 10Gbit/s RJ45 ports 1 “Red” private/unencrypted 1 “Black” public/encrypted
	Maximum Throughput	Black Traffic - UDP max 3Gbit/s Red Traffic – TCP/IP max 3Gbit/s

Device management

Management ports	Number of ports	1Gbit/s Management port for Local management
Connections to the security management Remote/ Online management	Access	In-band: Configurable on customer request TLS 1.2, HTTPS through **Telsy**Guard encrypted channel
Local management	Access	Through local port or Red Network: TLS 1.2, HTTPS

Crypto Token	Format	USB 3.0: USB adapter with 2 smart cards IP (for initialization) and CIK (for Operation)
Keys and Management	Management station	For appliance initial configuration and Smart card programming: **Telsy**KDC
	Security anchor	PFor initialization and operation: Smart card, secure configuration memory

Cryptography and security

Operational mode	Protocol	**Telsy**Guard VPN Proprietary protocol integrated with QDK. (quantum safe cryptography included from next release)
	Supported architecture	Point to point, Star, Mesh
	Latency	<2ms
Symmetric cryptography	Algorithm	AES (NIST Standard)
	Key length	256 bits
	Mode	GCM
Key retrieval	Interface	1 Gbit/s RJ45 interface to KME supporting ETSI 014 Standard
Additional functions	Device security	Zeroize: **Telsy**MusaX can be zeroized upon request from management portal

Approvals and certificates*

	Safety	EN 62368-1:2014 +A11:2017
		EN IEC 62368-1:2020 +A11:2020
		EN IEC 62311:2020
		EN 62479:2010
	RoHS	EN 55032:2015 +A11:2020
		EN 55035:2017 +A11:2020
		EN 61000-3-2:2014
		EN 61000-3-3:2013
	Environmental	EN IEC 63000:2018
	Energy	Commission Regulation (EU) No. 2019/424

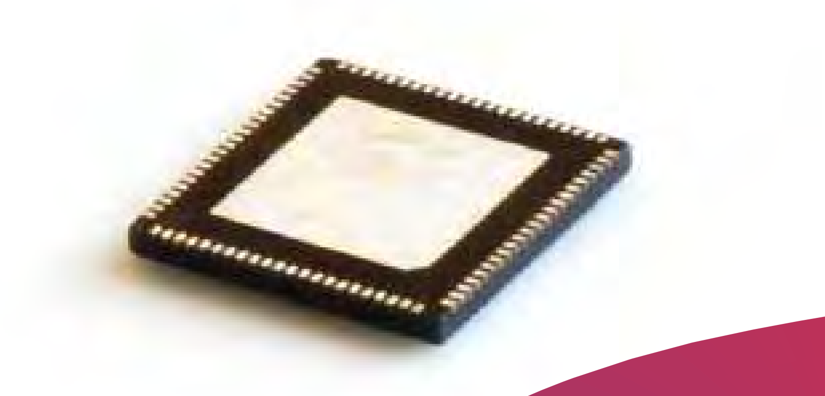
**Provided as reference only Considering a Dell R450 platform using the provided data available on manufacturer site www.dell.com data may vary based on installation platform.*

Communication Security

Secure Microchip

An unbreakable secured enclave

The **Secure Microchip** offers a comprehensive and integrated secure element solution in a LGA-64 format and it is able to provide multiple security features in order to protect IoT and dependable systems, providing a wide portfolio of standard cryptographic functions, allowing cryptographic-grade key generation and encrypted storing of key credentials.



The first microcontroller developed in Italy

The Secure Microchip is a micro-platform, programmable and secure by-design, which enables the implementation of various security solutions for multiple applications and technology services.

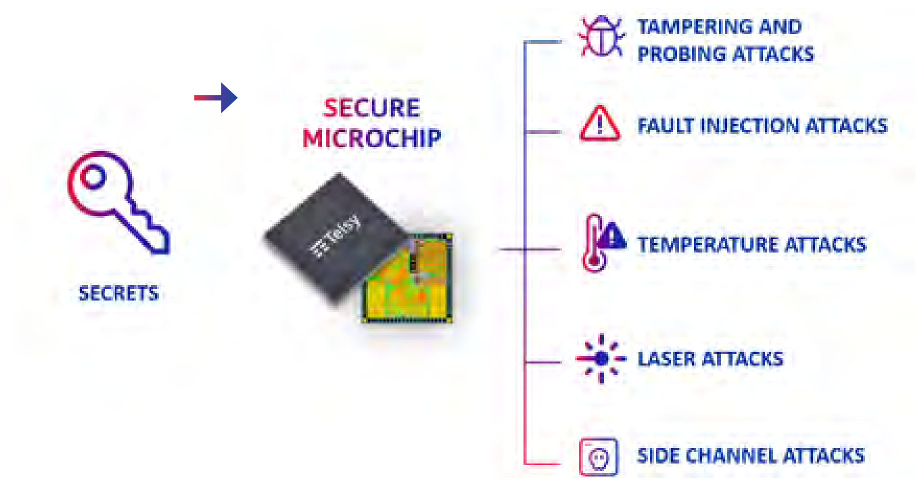
It ensures the logical and physical security of cryptographic operations underlying the security architectures of any computer system, or communication system, dealing with sensitive information.

The solution elevates security measures derived from the cryptographic domain, in terms of confidentiality, integrity and authenticity, both in the cyber and physical security domains.

Below are the application areas distinguished by technology types:

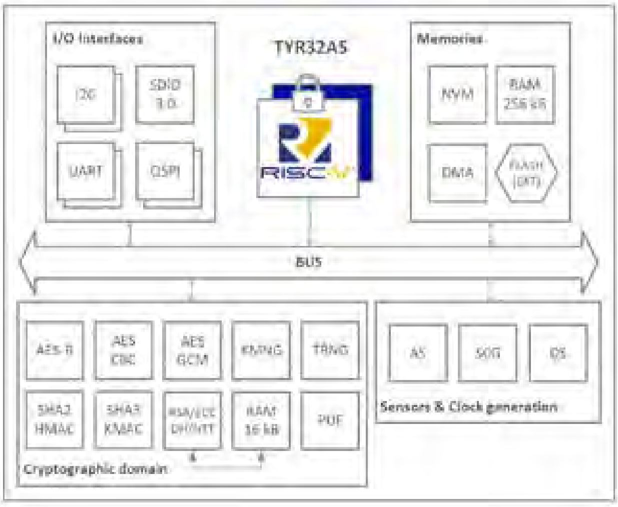
- **Information Technology** – IT (network, cloud)
- **Operational Technology** – OT (critical infrastructure, SCADA)
- **Internet of Things –** IoT (smart city, military wearable device, M2M)
- **Security for mobile devices**
- **Military assets and weapon systems** – (digitized weapon systems, drones)

Telsy's Secure Microchip protects your sensitive data, from tampering and probing attacks, fault injection attacks, temperature attacks, laser attacks, side channel attack.



Technical specifications

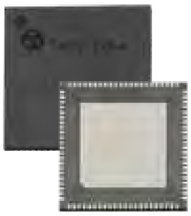
The hardware architecture of Telsy's Secure Microchip implements a programmable and configurable solution that includes a microcontroller with RISC-V Instruction Set, a series of cryptographic accelerators, analog security modules such as a random number generator (TRNG), an identity module cryptographic interface (PUF), various input and output interfaces and finally various modules for the physical protection of the device.



Architecture and formats

BASICS

- 32-bit RISC-V with Lockstep processor
- Internally generated clock at 166 MHz
- 128kB code RAM
- 128kB data RAM
- System-in-Package 1MB ENC flash
- 128-bit user-available One-Time Programmable (OTP) memory



64-pad LGA package.

INDUSTRIAL QUALIFICATION:

HTOL, LU, ESD, HBM, ESD CDM, MSL3, HAST, TC, HTSL

SECURITY CERTIFICATION :

EAL 5+ (on-going)

Use case

Cryptographic authentication

USB Token: Enables secure access to cloud services such as email, video conferencing, messaging, and file storage on laptops.

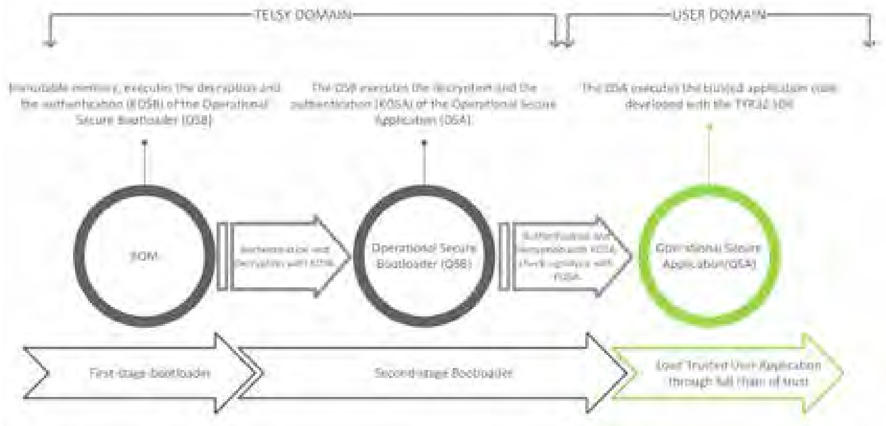
Authentication and Confidentiality: Secures IP networks by managing and protecting VPN keys, such as **Telsy**Guard (Telsy's proprietary cryptographic protocol), for sensitive data handling.

Main Features

Secure Microchip

Hardware supported cryptographic primitives	Key Manager	Keccak-based AEAD
	Analog Crypto Cores	PUF, TRNG
	Symmetric Encryption	AES 128/256: ECB, CBC, GCM:CTR,CCM, CMAC
	Asymmetric cryptography	RSA, ECDH, ECDSA
	Hash	SHA2, HMAC, SHA3, KMAC, SHAKE, cSHAKE
	Post Quantum Cryptography	Crystal Kyber

Secure Boot Loader and Secure SDK


TELSY DOMAIN
USER DOMAIN
Immutable memory, executes the decryption and the authentication (EOSB) of the Operational Secure Bootloader (OSB)
The OSB executes the decryption and the authentication (KOSA) of the Operational Secure Application (OSA)
The OSA executes the trusted application code developed with the TYRJ2 SDK
ROM
Authentication and Decryption with KEMK
Operational Secure Bootloader (OSB)
Authentication and decryption with KOSA, check signature with RSA
Operational Secure Application(OSA)
First-stage bootloader
Second-stage Bootloader
Load Trusted User Application through full chain of trust

Physical Security FI and SCA Tolerance	Active Shielding: Keccak-based AEAD
	Digital Sensors monitoring clock, power supply, temperature and radiation
	Error Detection mechanisms
	Lock Step Processor
	Processor never executes crypto functions (Timing analysis)
	Secure Clock (Jitter, Stealing)

ACTIVE SHIELDING

Top-metal mesh sensor

DIGITAL SENSOR

SECURED CLOCK

contact@telsy.it