



Trantor®

ENCRYPTED QR CODES · WEB AND MOBILE APP

QRcode

The QR code that can be read only if you are authorized.

Inside, encrypted information; outside, for anyone without the app and the password, nothing but random characters. It is generated and read with the Trantor® application (web or mobile), and every piece of content has its own password.



ENCRYPTED, NOT HIDDEN

MULTIPLE PASSWORDS

PAPER AND DIGITAL

THE RIGHT QUESTION

Who can read that sheet of paper? With Trantor® QRcode, you choose the answer: person by person, content by content.

trantor.it · info@trantor.it

10 August 2026

The contents of this brochure (text, graphics, logos) are the property of PetaBit S.r.l. and are protected by copyright and industrial property law; they may not be reproduced without written permission. All other trademarks cited belong to their respective owners. The information published is for information purposes only and does not constitute a contractual offer, and PetaBit does not warrant the absence of inaccuracies. All prices shown are subject to change and do not constitute a contractual offer.

What it is, how it works

Trantor® QRcode is a special QR code: it holds **encrypted information**, and it can be read only by authorized people, not by anyone who happens to point a camera at it (as happens with ordinary QR codes). Anyone trying to read it without our application sees nothing but **random characters**.

AN ORDINARY QR CODE

Anyone who scans it reads everything: it was born to be read.

A TRANTOR QR CODE

Without the app and the password: k7Xq2fLw9Rp... random characters, by design.

How it works

Generated and read from the app

With the Trantor® application (web or mobile) you create a QR code holding your content, then print it or attach it. To read it, you scan it: the app asks for the password and shows the content.

Multiple passwords, separate contents

A single QR code can hold several pieces of content, each protected by a different password: every person reads only what they are authorized to read, and the rest stays secret.

When the content grows, it splits

When a QR code becomes too large, it is automatically split into several smaller QR codes, which can be scanned **in any order**: the application puts them back together on its own, and discards duplicates scanned twice by mistake.

THE PHILOSOPHY

«The QR code was born to be read by everyone. With Trantor®, you decide who can read it.»

Where confidential stays confidential

The QR code lives happily on paper and in digital channels: Trantor® QRcode brings encryption exactly where documents travel, get handed around and get filed.

On paper

It is printed on the paper document to conceal the most sensitive information: the sheet circulates, the confidential part does not. Anyone reading it without authorization finds an ordinary-looking QR code and, inside it, nothing.

Filed and in transit

Documents can be filed without worrying about who has access to the archive, and sent from one site to another without the courier or an office employee being able to read the confidential information.

In meetings

Printed documents are handed around the table: each participant scans and reads **only the information they are authorized to see**. One single sheet, different levels of reading.

In digital channels

The QR code is attached as an image on websites, email and chat: the information stays protected even from the companies running those channels (the email provider, the messaging service, and so on).

ONE SHEET, MANY TRUTHS

The same page can say different things to different people, and nothing at all to everyone else. It is the paper document acquiring the confidentiality of serious systems.

Under the hood

The last page is for those who want the names of the algorithms, because in cryptography trust is given to standards, not to promises.

AES-256-GCM

Contents are encrypted and **authenticated**: tampering is not suffered, it is detected. The standard of symmetric encryption, in the mode that verifies the integrity of what you decrypt.

Argon2id

From password to key with the winner of the Password Hashing Competition: **memory-hard**, designed to make brute-force attacks expensive even with GPUs and dedicated hardware.

One password, one key

Every piece of content has its own key, derived from its own password: passwords do not travel and are not stored in the QR code.

Random by design

Without the password, the content is indistinguishable from random text: this is not obfuscation to be worked around, it is cryptography to be respected.

One line of honesty: the security of a piece of content is also the security of its password. Choose them well; the algorithm is our job.

THE NEXT MOVE

Bring us a document, we will make it confidential.

A trial with a real sheet of paper: we generate it, print it, hand out the passwords, and each person reads their own part.

trantor.it
info@trantor.it