

Romania Becomes an Early Test Case for the EU's Digital Identity Wallet as December Deadline Nears

Chip-based ID cards are now issuing nationwide. The harder problem is no longer forging the document, but proving who is presenting it.

BUCHAREST, BUCHAREST, ROMANIA, August 20, 2026 /EINPresswire.com/ -- With chip-based national ID cards now issuing across the country and every EU member state required to field a digital identity wallet by 6 December 2026, Romania offers an early view of what the rest of the bloc faces. Bucharest-based RegTech firm [Qoobiss](#) says the harder problem is no longer forging the document. It is proving that the person presenting it is real.

BUCHAREST, Romania, August 2026. Romania is emerging as one of the European Union's earliest practical tests of eIDAS 2.0, the regulation that will place a digital identity wallet in the hands of every EU citizen who wants one.

The country's chip-based national identity card, first piloted in Cluj county, is now issued nationally, with more than EUR 150 million in European funds financing the first batches in 2026. The chip carries biometric data in a secured zone, qualified electronic signature capability and the national health card function. Under Regulation (EU) 2024/1183, every member state must make at least one European Digital Identity Wallet available by 6 December 2026.

Documents issued earlier remain valid until the expiry date printed on them, and identity cards without a chip cease to be valid by 3 August 2031 at the latest under Regulation (EU) 2019/1157. For regulated institutions, that means years of verifying two generations of documents, with two entirely different technologies, inside the same onboarding flow.

For banks and insurers, the two timelines converge into one operational question: how do you verify a state-signed identity credential remotely and at scale, and how do you know the person presenting it is its holder?



Alexandru Bora, Qoobiss

“With a traditional document, verification is probabilistic. You analyse microtext, holograms, fonts, and the answer is that the document appears authentic to a certain degree of confidence,” said Alexandru Bora, Product Owner at Qoobiss. “With a chip, verification becomes cryptographic. The answer is no longer that it looks authentic. It is that it is authentic, signed by the state that issued it. That is a change in kind, not in precision.”

The chip closes one attack surface and exposes another. A valid chip proves the document; it proves nothing about who is holding it.

“The moment forging the document becomes impractical, the attacker moves to the only link left, which is the person,” Bora said. “That is why our investment over the past two years has shifted toward the biometric layer and toward detecting attacks on the video channel itself.”

“

The era of treating biometric verification as a solved problem is over. Generative AI has fundamentally shifted the threat model from presentation attacks to injection attacks.”

Teodor Rogojina, Chief Executive Officer, Qoobiss

“The era of treating biometric verification as a solved problem is over,” said Teodor Rogojina, Chief Executive Officer of Qoobiss. “Generative AI has fundamentally shifted the threat model from presentation attacks to injection attacks.”

The distinction is operational, not academic. A presentation attack shows a camera a mask, a photograph or a screen, and is countered by [liveness detection](#). An injection attack bypasses the camera entirely, feeding a fabricated video stream directly into the application, where liveness detection sees nothing unusual, because the

stream it analyses is precisely the one the attacker built.

[ONTRACE](#) approaches this in layers rather than as a single check. One layer validates the document, across more than 15,000 document types from over 250 countries and territories. A second matches the person in front of the camera against the photograph in the document and tests for liveness. A third examines the channel, verifying the image came from a real camera



rather than an emulator or virtual device.

Industry figures cited by Qoobiss show deepfake fraud attempts up 2,137% over three years and injection attacks up 741% year over year. Global identity fraud losses exceed USD 50 billion.

Identity-based social engineering is already effective at scale. A study presented in July 2026 under ING's SAFE Talks programme found that 42%

of frauds reported in Romania during the first half of 2026 were voice-phishing calls, ahead of phishing at 14% and SMS-based fraud at 13%, and that more than 60% of Romanians over 50 had experienced at least one form of online crime.

Qoobiss has been an accredited remote identity verification provider with Romania's Authority for Digitalisation since December 2022, and says it became the first e-KYC provider in the country to validate the new chip-based ID cards remotely by video in March 2024. Its ONTRACE product is undergoing independent evaluation for Presentation Attack Detection and Injection Attack Detection under ETSI TS 119 461 and CEN/TS 18099, targeting Extended Level with injection detection at Level High. Results will be published once the process concludes.

Under eIDAS 2.0, providers targeting that level must submit their detection mechanisms for independent testing before the end of 2026. Private-sector relying parties legally required to use strong user authentication, banks foremost among them, must accept the wallet by 6 December 2027.

"A vendor that grades its own defences is no longer sufficient for a bank," Rogojina said.

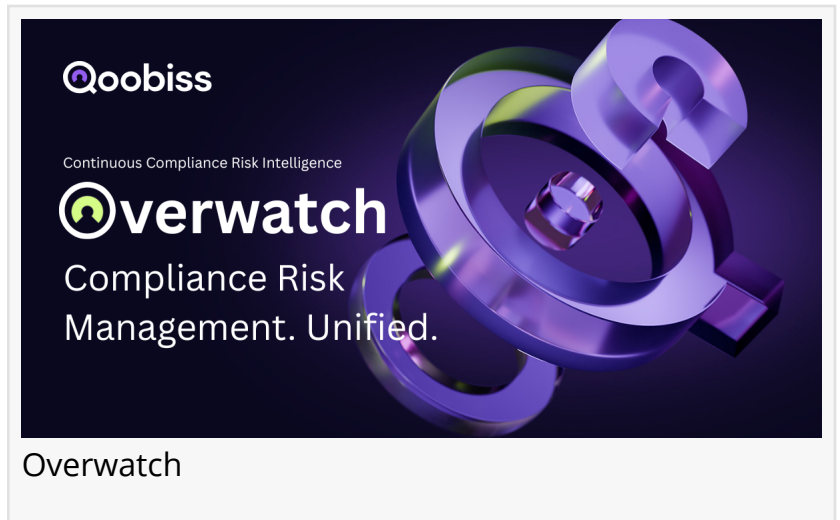
"Independent testing is the only form of proof that travels across borders and supervisors."

"Verification does not disappear once the wallet arrives. It moves," Bora said. "You are no longer checking whether a document is forged. You are checking whether the identity attestation is valid, whether it has been revoked, and whether the person presenting it is its holder. The first two are solved cryptographically. The third remains a biometric problem."

One further point rarely gets stated. Much of the technology verifying Romanian citizens' identities is being built in Romania. Where an entire population's biometric data passes through a vendor's systems, that is a question of data sovereignty, and one every member state will face as the December deadlines arrive.

ABOUT QOOBISS

Qoobiss is a Romanian RegTech company headquartered in Bucharest, building compliance and



digital onboarding infrastructure for regulated industries. Its portfolio includes ONTRACE (remote identity verification), OMNICHECK (AML and sanctions screening and ongoing monitoring), OVERWATCH (compliance risk management) and ORIGIN (onboarding orchestration). Its solutions cover more than 250 countries and territories and over 15,000 identity document types. Learn m

Ramona Voiculescu

Credimatic Network SRL

+40 745 223 105

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

[YouTube](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/935598633>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.