

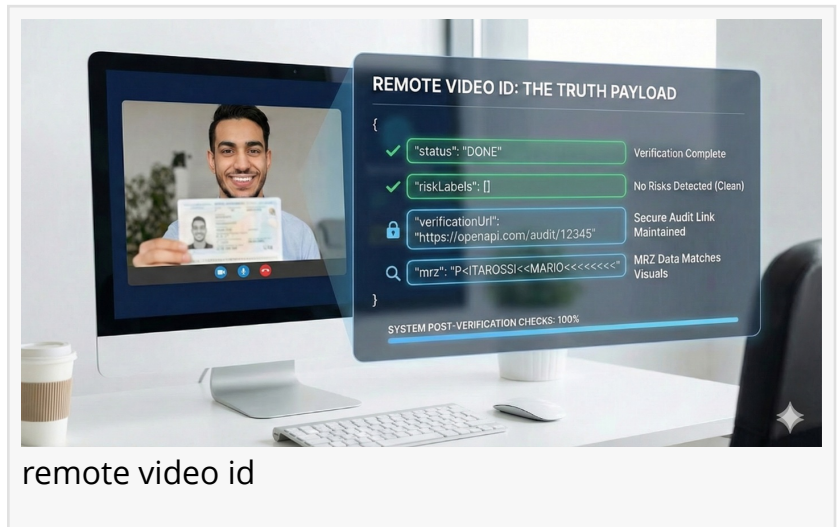
Deepfakes and identity EBA guidelines force banks to take the biometric leap

With synthetic fraud surging by 300%, static document uploads are no longer compliant. The market is shifting towards hybrid API architectures.

ENGLEWOOD CLIFFS, NJ, UNITED STATES, March 20, 2026

/EINPresswire.com/ -- The race toward business process dematerialization is unstoppable. According to the latest European DESI indices and findings from the Digital B2b Observatory, during 2019, more than 70% of SMEs

digitized their order cycles and contract management. However, hidden behind these growth charts lies a systemic legal vulnerability: evidentiary uncertainty.



The "Scanning" Paradox and the Risk of Repudiation Many companies mistakenly believe that scanning a hand-signed contract or receiving a simple "Ok" via email equates to solid proof in a court of law. Recent case law tells a different story.

“

It is no longer just about knowing who the client is, but if the client is real”

Elena Rinaldi

In practice, most of these methods fall into the weakest category of electronic signatures under EU Regulation 910/2014 (eIDAS). In many disputes, a mere claim of

"repudiation" (a denial that the signature was applied by the user) often causes the burden of proof to shift to the company. The organization is then compelled to undergo protracted and costly forensic analysis on original documents that often no longer exist.

The Solution: Advanced Electronic Signature through OTP To "armor-plate" a digital contract—whether B2B or B2C—and ensure its legal effect and admissibility as evidence under Article 25 of eIDAS, the stringent demands of Article 26 must be met:

- Unambiguous Identification: Clearly identify the signatory.
- Sole Control: Ensure the signatory has sole control over the signature creation data.

- Tamper Evidence: Ensure the document integrity so that any subsequent change is detectable.

This is where OTP (One-Time Password) technology becomes the de facto standard. Sending a unique code via SMS or Email to the signatory creates the link of "sole control" required by law, substantially elevating the legal standing of the document compared to a simple signature.

The Cybersecurity Perspective "Any sensitive transaction that requires the user to be redirected to an external domain increases abandonment rates and—more importantly—habituates users to click on external links, exposing them to phishing," explains Paul Thompson, a banking cybersecurity expert.

Until recently, adopting these technologies meant fragmenting the user experience, forcing clients to exit the company website to land on third-party signing portals or download local software. In 2025, this disjointed approach is coming under scrutiny from cybersecurity risk management.

Infrastructural Transparency via APIs The market response is infrastructural transparency via APIs. Modern solutions, devised by tech players like [OpenAPI.com](https://openapi.com) or the DocuSign eSignature API, have addressed this need for compliance and security. By using dedicated endpoints—such as the POST /EU-SES protocol—companies can directly integrate the signing process into their proprietary code. It is no longer the user "going to sign," but the certified signing technology entering the corporate management software.

The Audit Trail: The Contract's "Black Box" Beyond the interface, true legal value in court stands not in the visual PDF, but in what lawyers call the Audit Trail (or Preservation Log). Next-generation platforms create a technical evidentiary file that captures:

- IP addresses and Geolocation of the signatory.
- Electronic Time Stamps.
- Technical evidence of the dispatch and receipt of the OTP.

This data must be retained for 10 years—the standard statutory retention period in the EU for commercial and tax records—as it is the key that enables a judge to reconstruct the chain of custody.

In an increasingly "paperless" economy, it is no longer the ink that distinguishes an enforceable debt from a null and void contract, but the quality and integrity of the metadata accompanying it.

Luca Scuriatti
Openapi Spa
[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/874915319>

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.