From Suspicion to Decision:

Practical Document and Identity Fraud Detection

Q&A Session

Please note that the questions have not been edited: they appear exactly as they did in the chat.

Question 1

what about counterfeited chip which it can be easily readed by NFC application

Answer

Being able to read a chip is not the same as proving that the chip is genuine. Passive Authentication checks the issuer’s digital signature and whether the chip data has been changed. However, a complete clone of a genuine chip may still pass Passive Authentication. Where the document supports them, Active Authentication or Chip Authentication are the checks designed to detect a copied chip. The chip data should also be cross-checked against the printed data, portrait, document type and physical security features. A consumer NFC app that merely displays the data is therefore not sufficient for an authenticity decision.

- Security Mechanisms for Electronic Documents
- RFID Chip Verification: How to Check Electronic Identity Documents

Question 2

In the case where certain countries are very strict regarding data residency, what measures are in place to ensure compliance?

Answer

Regula software solutions, including Document Reader SDK, Face SDK, and the IDV Platform, are deployed on premises by default. They can also be hosted in a customer-controlled cloud if the customer chooses that model.

In either case, document and biometric processing takes place within the customer's own infrastructure, not on Regula's servers. The customer controls where the data is stored, who can access it, how long it is retained, and how backups, encryption, and deletion are managed.

This architecture supports strict data residency requirements, while the customer remains responsible for configuring the deployment in accordance with applicable national laws and internal policies.

Regula IDV architecture

Question 3

Does this training teach us to detect fraud docs without the help of technology; for airport staff?

Answer

The session introduces first-line checks that can be performed without specialist equipment, such as looking for obvious inconsistencies in the document, portrait, data, validity and visible security features. It also shows when those checks are not enough and the document should be examined with equipment or referred to a specialist. A single webinar is not a substitute for an operational training programme or an airport's official SOPs. Regula provides specialized practical courses on document authentication; the exact programme and delivery format should be confirmed with the Regula training team for the organization concerned.

Regula Specialized Trainings

Question 4

regarding the scans and the app, how does it work with paper based IDs like Brazilian or Digital only like in Philippines digital IDs?

Answer

For a paper ID, the camera captures the document and the software identifies the document type, extracts the printed data and checks the available layout, data, barcode or QR-code elements against the relevant template. Because a paper document may have no chip and fewer machine-verifiable features, the result depends on what that specific document contains and on capture quality. For a digital ID, a screenshot should not be treated as proof on its own. The issuer's cryptographic mechanism must be verified. For the Philippine National ID, the official verification method relies on the QR code and its digital signature, including status/revocation checks.

Regula: paper-ID deployment case

Question 5

which of these technologies are used in digital documents?

Answer

Digital documents use a different evidence set from physical documents. Electronic passports use the chip, digital signatures and PKI-based checks such as Passive Authentication and, where supported, Active or Chip Authentication. Mobile driving licences and other digital credentials use issuer signatures, encrypted device communication, data-integrity checks and, depending on the standard, device binding and selective disclosure. Face matching and liveness may then link the credential to the person presenting it. Physical techniques such as UV, IR, laminate, paper and printing examination are relevant only when a physical document is present.

- Regula: mobile driving licences
- Regula: electronic-document security
- Regula: verifiable credentials

Question 6

Can the system detect the difference on documents that belong to twins?

Answer

Twins is a broad category, and the result depends on how similar their faces actually are. The system can verify each document and compare the person’s face with the portrait, but identical or very similar-looking twins are a particularly challenging case because their facial characteristics may be almost indistinguishable. When confirming the identity of a specific individual is essential, face comparison should be supported by other evidence and biometric modalities, such as document and chip data, prior trusted enrollment, fingerprints or iris, where legally permitted, and manual review.

For age estimation, however, this is usually less relevant: identical twins are the same age, so using a sibling’s document would not normally change the age-assurance result.

Question 7

can i use idv to recover some user account? without being registered in the same way

Answer

Yes, identity verification can be one component of an account-recovery workflow, but IDV does not independently decide who owns an account. The organization must link the verification session to trusted account information and define what evidence is sufficient for recovery. If the person was originally registered through a different method, the workflow can request new document and biometric evidence and route mismatches or missing historical data to manual review. The exact policy - what data is compared, what risk controls apply and when recovery is allowed - must be designed by the account provider and reviewed by its security and compliance teams.

Question 8

You have showed the fingerprint picture. Is it taken from the document or only from a special device?

Answer

Both are technically possible, so the exact answer depends on which webinar image was being referenced. A document reader does not capture a live fingerprint from a person unless a dedicated fingerprint scanner is integrated. Some electronic identity documents contain fingerprint data in the chip, but access is normally protected and may require Extended Access Control and an authorized inspection system. Regula’s software can also be integrated with a fingerprint scanner. Therefore, the displayed image could have come from a permitted document/chip field, a sample profile or a separate scanner.

Question 9

Do you have copies of all countries' passports in your system ?

Answer

Regula does not store personal copies of every passport issued. It maintains document templates and reference specimens used to recognize document types and verify expected data and security features. The current database covers more than 16,500 document templates from 254 countries and territories.

- Regula Global Coverage of Identity Documents
- Regula Information Reference System

Question 10

Also , is it compatible with other companies and workflows?

Answer

Yes. Regula software IDV products designed to integrate with customer applications and third-party systems rather than operate as an isolated interface. Regula provides APIs, web and mobile components, SDKs and workflow actions; results can also be delivered to external systems through callbacks or webhooks. A customer can therefore place document verification, biometrics and external checks into its own onboarding, access, recovery or investigation process.

Question 11

if AI are inserted into IDV and which technique cpuld help in this devices

Answer

AI and machine-learning techniques are used where they add value—for example, identifying the document type, locating and assessing the captured document, recognizing data, comparing document patterns, matching faces and performing liveness checks. The IDV Platform orchestrates these results within a workflow. AI does not replace the original evidence source: optical checks still require the correct camera and illumination, and chip authenticity still relies on cryptographic verification. The most reliable approach combines machine-learning signals with deterministic data cross-checks, reference templates, chip signatures and manual or forensic review for uncertain cases.

Question 12

what about these checks when using a mobile phone for onboarding ?

Answer

On a mobile phone, guided capture can identify the document, assess image quality, read the visual zone, MRZ, barcode or QR code, cross-check data and examine supported visible or dynamic elements through a short capture sequence. If the phone has NFC, the chip can also be read and authenticated. A selfie can be used for liveness and face comparison. A phone does not reproduce the full UV, IR, spectral and high-magnification evidence of a specialized document reader, so the available checks depend on the document and device. High-risk or inconclusive results should be processed server-side and escalated rather than treated as automatically genuine.

Regula Automatic Authenticity Control

Question 13

how to go about those documents that are completely fake but look exactly like the original one

Answer

A convincing visual copy is precisely why the decision should not depend on appearance alone. The document should be checked across independent layers: layout and print patterns; MRZ, visual-zone, barcode and chip consistency; dynamic features; UV/IR response; chip digital signatures; and whether the portrait matches the person. A fake may imitate one layer well but is much less likely to reproduce all of them consistently. If only a photograph is available, the conclusion must be more cautious. If reasonable doubt remains after automated or first-line checks, the correct response is expert examination - not a forced pass/fail result. No product should be presented as capable of guaranteeing detection of every counterfeit.

Regula Automatic Authenticity Control

Question 14

For private Investigators, can the system's evidence be used before a competent court or one needs Certifications?

Answer

There is no universal answer because admissibility and expert-witness requirements are set by the relevant jurisdiction and court. Laboratory accreditation or a specific certification may also be required locally. A private investigator should obtain jurisdiction-specific legal advice before presenting the result as expert evidence.

Question 15

using the device to check physical documents, will it give thesame result if used on digital doc

Answer

No. A physical-document device examines evidence that exists in the object itself: substrate, printing, relief, laminate, optically variable elements, UV/IR behaviour and, where present, the chip. A digital-only credential must instead be verified through its issuer signature, trust chain, integrity, status or revocation information and, depending on the standard, device binding. A photograph or screenshot of a digital credential is not an equivalent substitute because it removes the cryptographic context. Some workflows can process both physical and digital credentials, but they use different checks and should not be expected to produce identical evidence or the same result structure.

Question 16

What are some common red flags for further investigation

Answer

Common escalation triggers include a portrait that does not match the holder; inconsistencies between the visual zone, MRZ, barcode and chip; invalid check digits or impossible dates; unusual fonts, spacing, alignment or print quality; damaged or lifted laminate; substituted pages or photographs; missing or incorrect holographic, UV or IR features; evidence that the document is displayed on a screen or is a colour copy; and a chip failure combined with other anomalies. An expired, damaged or unfamiliar document may require further review but is not automatically fraudulent. The important point is the combination and consistency of evidence, not one isolated alert.

Question 17

Just a curiosity: how common are artifacts caused by imperfections in the printing or lamination process on genuine ID documents? I assume that it depends a lot from the issuer also.

Answer

Yes, genuine documents can contain manufacturing tolerances, batch variation, wear or isolated printing and lamination imperfections, and the level of variation depends on the issuer and production process. However, there is no reliable public statistic that would support a percentage or a general frequency for genuine IDs. This is why an examiner should not reject a document because of one imperfect feature. The document series must first be identified correctly, then the questioned area should be compared with current reference material and assessed alongside multiple independent features. If the anomaly remains unexplained, the case should be reviewed manually or compared with a trusted specimen.

Question 18

how many counteries are included in your IDV all world or not

Answer

Regula’s document database includes more than 16,500 document templates from 254 countries and territories.

Question 19

Like how many minutes can you spend to determine if doc is original

Answer

It depends on the level of examination. Automated capture and data checks are normally completed in seconds. In one Regula airport example, a first-line gate check is described as taking approximately 15–30 seconds before a questioned document is escalated. A forensic examination has no universal duration: it may take minutes, hours or longer depending on the document, the suspected alteration, comparison material and reporting requirements. The goal should not be to force a conclusion within a fixed time, but to use a fast first line and reserve deeper examination for the relatively small number of unresolved cases.

Question 20

I wanna know about twins. if missed change their passport, what's the different points to identify them quickly

Answer

If identical twins exchange genuine passports, the document itself may still pass authenticity checks; the issue is an impostor using genuine evidence. Face comparison may help, but identical twins are a known difficult case and there is no reliable set of quick visual points that guarantees separation. The officer should verify the chip portrait and document data, compare current and prior trusted records, ask questions permitted by procedure and refer the case for manual or secondary inspection. Where legally authorized and available, fingerprints are stronger evidence because identical twins do not have identical fingerprints. The exact action must follow the border authority’s SOP; facial similarity alone is not proof of fraud.

Question 21

You showed a few devices, those are awesome. And that´s great for border control, airpots, governments... But what happens when doing onborading from a cell phone? What does, say a good iphone, allow you to actually detect about the document? How realiable is the technology to analize different elements whithin the document to safely onboard a person?

Answer

A smartphone itself does not verify the document. It acts as a capture device: its camera takes images of the document and captures a selfie or video for liveness, while NFC can read the document chip where available.

The actual processing is performed by Regula IDV software. It identifies the document type, extracts the data, assesses capture quality, cross-checks the visual zone, MRZ, barcode and chip data, performs the supported authenticity checks, and processes the selfie or video for liveness and face matching.

Unlike specialized document readers, a smartphone does not provide controlled UV, IR, spectral or high-magnification images. The reliability of mobile onboarding therefore depends on the document, the quality of the captured images, NFC availability and the checks configured in the workflow. Inconclusive or high-risk results can be referred for additional review.

Question 22

Are any Risks involved if one is using AI on the same device where you have the Regula App is?

Answer

No. Regula does not monitor or control which other applications, including AI applications, are installed on the user’s phone.

Question 23

If a visa passes the initial visual checks but we still have reasonable doubts about its validity, what should be the correct escalation process before accepting the passenger?

Answer

Do not clear the passenger solely because the visa passed a quick visual check. Follow the authority's SOP and refer the document to secondary inspection. There, confirm the exact visa/document series using current reference material; examine printing, laminate, security features and alterations with magnification and appropriate light sources; cross-check the visa and passport data; and verify the traveller's answers and any available system or issuer records. Record the reason for referral and the evidence examined. If doubt remains, consult a supervisor, document expert or the competent issuing/immigration authority. Only an authorized officer should make the final admit/refuse decision under national rules.

- Regula: advanced manual examination
- Regula: global reference system
- Manual vs. automated document verification

Question 24

What is the hardest altered item to identify on an ID?

Answer

There is no single feature that is always the hardest. One of the most difficult scenarios is a genuine document used by an impostor, because the substrate, printing and chip may all be authentic. Among physical alterations, a high-quality portrait or data-page substitution can be difficult when the attacker preserves surrounding laminate and security elements. Difficulty also varies with document design and examiner equipment. The practical response is to avoid relying on one feature: combine portrait/holder comparison, chip and printed-data consistency, printing and laminate examination, UV/IR behaviour and reference images. Regula has not published a universal ranking of the “hardest” alteration, so this answer should be presented as expert guidance, not a measured league table.

Trends in Identity Document Forgery

Question 25

regarding the scans and the app, how does it work with paper based IDs like Brazilian or Digital only like in Philippines digital IDs? How does it treat damaged IDs

Answer

Paper and digital IDs are verified through different evidence. A paper ID is captured by camera and checked using the data, layout, barcode/QR and visible features available for that exact document. A Philippine digital National ID should be validated through its official QR code and digital signature rather than accepted as an image. Damage does not automatically mean fraud. If enough data and security features remain readable and consistent, the system can return the checks it was able to perform. If glare, tears, abrasion, missing laminate or a damaged barcode/chip prevents reliable verification, the result should be inconclusive or routed to manual review and the organization may request another accepted document. Whether a damaged ID remains legally valid is an issuer/policy decision.

Question 26

While doing remote investigations and requesting identity documents is there an easy way to spot a fake ID or passport if they send a picture? If we can't see it in person.

Answer

Yes. In a controlled remote IDV process, the document image is not treated as just a photograph. The software guides the user through capture, assesses image quality, identifies the document type, and automatically checks its layout, data fields, portraits, MRZ, barcode, and visible security features against the relevant document template.

Document liveness checks can also verify dynamic security features and determine whether a genuine physical document is being presented rather than a screen image, printout, or replay. For biometric documents, the RFID chip can be read through NFC and its data cross-checked against the printed information. Selfie liveness and face matching then verify that the person presenting the document is its legitimate holder.

There is no single visual clue that identifies every fake. Reliability comes from combining document authenticity checks, data cross-checks, document and biometric liveness, and chip verification where available. If the captured evidence is insufficient or the results are inconsistent, the case can be flagged for recapture or further review.

Question 27

what about quantitative and qualitative magnetic features that measured if there is references between genuine and false ones

Answer

Regula 7701M can visualize magnetic patterns and measure the magnetic properties of document security features. It calculates parameters such as magnetic induction and magnetic flux and compares the results with those obtained from a genuine reference sample.

This comparative analysis helps an expert identify differences in magnetic inks, patterns and other magnetic security elements. It can support a conclusion about the document's authenticity and help distinguish counterfeiting from normal wear or damage.

Question 28

can we use it to identify VIN labels of vehicles?

Answer

Yes, but the correct tool depends on what is being examined. Printed VIN labels, manufacturer plates and related vehicle documents can be inspected for printing, laminate, alteration and optical security features using suitable document-examination equipment and reference data. For a VIN stamped or otherwise marked into metal, Regula's dedicated 7505M and 7515M solutions are designed to detect falsification and, in some cases, recover an obliterated original number without removing the paint coating. A standard IDV mobile workflow is not a substitute for this forensic examination. The material-label, aluminium plate or ferromagnetic chassis—and the suspected alteration must be established before selecting the method.

Thank you!

Regula

Identity Verification for the AI Era

Forensic Science Inside