



Service Definition for GBG IDscan Enterprise

G-Cloud 15

Version 5.0 | January 2026

Contents

About GBG	3
Service Definition	3
Why GBG IDscan?	3
Document Recognition	4
Document Authentication and Validation	5
Smart Capture	5
Data Extraction.....	5
Face Match.....	6
Liveness	6
Reading Biometric Chip information	7
Investigation Studio	7
On-boarding Decision Engine	8
Digital Tamper Detection.....	8
Tolerance Levels	8
Online Forensic Document Examiners	8

About GBG

We are the experts in digital location, identity and managing fraud risk and compliance. Helping organisations across the globe eliminate customer friction and fraud from their digital experiences. GBG develop and deliver digital identity, address verification, fraud prevention and compliance software to over 20,000 customers globally.

Through the combination of the latest technology, the most accurate data and our unrivalled expertise, GBG helps organisations ranging from start-ups to the largest consumer and technology brands in the world deliver seamless experiences, so their customers can transact online with greater confidence.

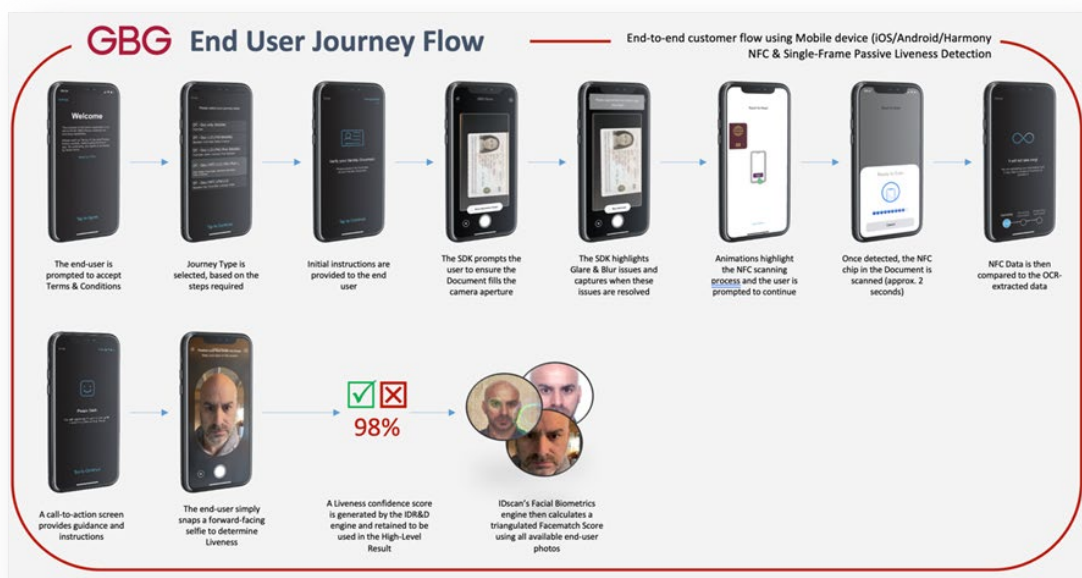
GBG is headquartered in the UK with over 1,100 team members across 17 countries.

Service Definition

FASTER DIGITAL ON-BOARDING

Why GBG IDscan?

On-boarding your customers online couldn't be easier. With GBG IDscan's mobile and web technology, you simply capture an image of your customer's ID document and our technology will do the rest. Our software will classify the document, perform a series of authentication and validation checks and extract data using Optical Character Recognition (OCR) in seconds.



Our Offer:

- Document recognition
- Smart capture
- Data extraction
- Face Match
- Liveness
- Reading biometric chip information (NFC)
- Investigation
- On-boarding decision engine
- Digital tamper detection
- Tolerance levels
- Online forensic document examiners



Our Results:

- Faster Digital on-boarding
- Fully automated solution, no manual interaction needed
- Seamless tailoring
- Compliance and results to the highest standards

Document Recognition

We can automatically tell you what type of ID document your customer has presented on device. Our software lifts the data from the document, enabling you to pre-populate your customer's information into your systems, such as registration pages and CRM platforms.

Document Authentication and Validation

Document authentication identifies a document type using the visible image of the document and comparing it against a database of over 6,500 supported identity document types.

- Based on the established document type, information is extracted from the document using OCR, barcode extraction, MRZ extraction and checking digits and electronic chip data capture methods, in the case of e-Passports and e-Identity cards.
- Finally, the document is authenticated by running numerous forensic tests, specific to the identified document type and the security features expected for that document.
- For non-electronic documents, this includes correlating the document to known security features and other intrinsic features of the document type. The results of each of these tests are calculated and then extrapolated into an overall result that indicates the likelihood that the document is authentic or fraudulent.
- For e-Passports and e-Identity cards, this constitutes performing Passive Authentication of the document security object from the chip against the e-Passport validation engine.

Through this process, the software provides an authentication of the presented document via both, a document physical security feature assessment against an authoritative database and the cryptographic evaluation of the digitally signed, electronic components of the document, including the validation of the document's cryptographic binding to a trusted issuer's Public Key Infrastructure (PKI). To complete its document authentication process, the software will confirm the security/cryptographic features of the ID matches the expected features electronically, by comparing the electronic features to the physical features. This includes performing MRZ-to-RFID, MRZ-to-VIZ (visual inspection zone), and VIZ-to-RFID comparisons

Smart Capture

Your customers will not have to worry about lining up their ID documents perfectly or trying to take a picture in focus or without glare. Our cutting-edge technology automatically detects a good frame and takes the picture! We'll capture the best quality image, first time.

Data Extraction

We recognise and extract the relevant data points from your customer's ID document including name, document number etc, using OCR. This utilises the details we have in our document library, recognising the format of the document, where the data fields are located and how it's formatted.

We ensure the data we extract is accurate by running the initial result through several layers of checks, including dictionary comparisons on the extracted words and correcting any errors. We check addresses from ID documents against our global address databases.

Some ID documents can be years old, and can become worn, damaged, mistreated and contaminated. We've got the unique technology to overcome this. Our proprietary Optical Character Recognition (OCR) system is specifically designed to meet the challenges of reading data from documents that may have been purposely designed not to be machine readable.

Face Match

GBG IDscan's extensive computer-vision developer toolset powers a wide range of face recognition applications. Our face recognition Software Development Kits (SDKs) and APIs enable comprehensive security and frictionless experiences. In addition to measuring the accuracy of face recognition across different use cases, from fully unconstrained to travel document-quality images, the National Institute of Standards & Technology (NIST) 1:1 Facial Recognition Vendor Test (FRVT) benchmark also tests demographic performance across gender, nationality, and age.

Our technology has proved to be one of the highest scoring applications in terms of demographic variety and has achieved NIST homogenous accuracy scores in line with the overall noted error rate reduction across a highly diverse range of global testing subjects. When considered across gender, age and nationality, our face recognition now shows less than 0.65% false non-match rates at 1 in 100,000 false match rates for every demographic group tested.

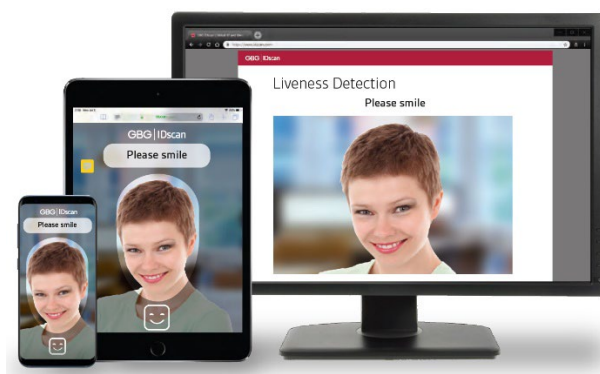
Face match is NIST accredited for 1:1 and 1:N global top 10 in the online vendor testing.

Liveness

The use of facial recognition for authentication is becoming increasingly prevalent, especially on mobile devices. However, between easy access to images on social media and advances in digital and print image resolution, biometric systems have security gaps that fraudsters can exploit to successfully spoof a facial recognition system. These spoofs, called presentation attacks (PAs), include printed photos, cut out masks, digital/video replay attacks and 3D masks.

GBG IDscan uses leading passive facial liveness detection which identifies spoofing attempts based on the same selfie used for facial matching and NO additional user participation - no smiling, blinking, head-turning, moving the camera or lights flashing which can trigger epileptic reactions. This unique single image liveness detection approach is fast, accurate and doesn't require any capture-side software. The technology uses a Deep Neural Network (DNN) based approach that examines different elements of the image to detect artefacts that help distinguish between a photo of a live person and a presentation attack. This approach further combines the facial image capture step with the Liveness Assurance step into a single process to provide a far more effective end-user experience.

Passive liveness is Level 2 ISO 20107-3 accredited.

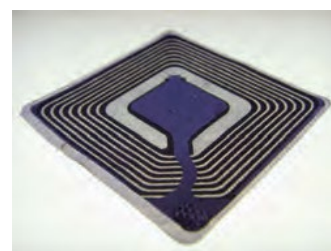


Reading Biometric Chip information

Using Near Field Communication (NFC) on Android and iOS supported devices, we extract details and Portrait Photo (Facial) images from biometric chips and compare those to the corresponding details on the document to help prevent fraud and improve extraction accuracy. We perform both Active and Passive authentication on biometric chips.

- The solution verifies data with the document (e-Passport, e-MRTD, e-ID) issuer.
- Provides cloned document and revocation checks.
- Provides document issuance checks.
- Access to high-quality image for best face match results.
- Supports all methods of access including PACE, BAC.

The NFC capability is built upon knowledge derived from millions of transactions on over 2,600 different models of smartphones. From our extensive experience with millions of scans of documents worldwide, we have learned how to deal with tremendous range. The NFC-based solution is fast and verifies the total end user journey in real time. NOTE: Biometric Chip reading through NFC devices is only available through a native App and is not currently possible via the web browsers.



Investigation Studio

Our Investigation Studio enables you to access your scanned documents quickly and easily in a secure, single platform and is available as a web-based solution or integrated API. Your employees will have access to all of the data captured in an application and be able to see the results of the security checks we perform of the ID document image. Rest assured you're compliant with a full audit trail.

Your users will be able to review:

- Personal details of a customer.
- ID document images, and the segments used for OCR.
- Authentication results, including reference images of genuine samples for the same document type.

On-boarding Decision Engine

Our work-flow tool means that you can configure a solution that suits your business needs. You can create a full On-boarding journey from initial application to final decision. As well as changing the order of events, for example asking your customer to take a selfie before capturing the ID document images, our solution provides an extensive, customisable ruleset to help you make the right decisions automatically, freeing your time and resource. Different identity documents may warrant different levels of authentication checks and different cross-referencing. Doing more checks may increase rejections but will reduce your exposure to fraud. We provide configuration that allows different levels of authentication to be set for different individual or groups of documents.

Digital Tamper Detection

Most digital image manipulation is invisible to the naked eye, but GBG IDscan can detect digitally modified images to help mitigate instances of fraud when files are being captured, as part of the onboarding process. When manipulation is detected, we highlight modified areas in the audit image in our Investigation Studio or provide warning of suspected tampering.

Tolerance Levels

Different identity documents may warrant different levels of authentication checks and cross-referencing. Performing broader checks may increase rejections but reduces exposure to fraud. Configurable authentication levels can be set for different individual or groups of documents.

Online Forensic Document Examiners

Our UK-based forensic document examiners can review images of documents in real-time. Trained to CIFAS and National Document Fraud Unit (NDFU) levels, they aim to provide an opinion within 120 seconds.