Service Definition for GBG IDscan Core

G-Cloud 15

Version 5.0 | January 2026

Contents

About GBG 3

Service Definition 3

Global Document Library 4

Face Match (Facial Biometrics) 5

Liveness 6

Reading Biometric Chip Information 7

Private & Confidential © GB Group plc 2026

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

IDSCAN CORE

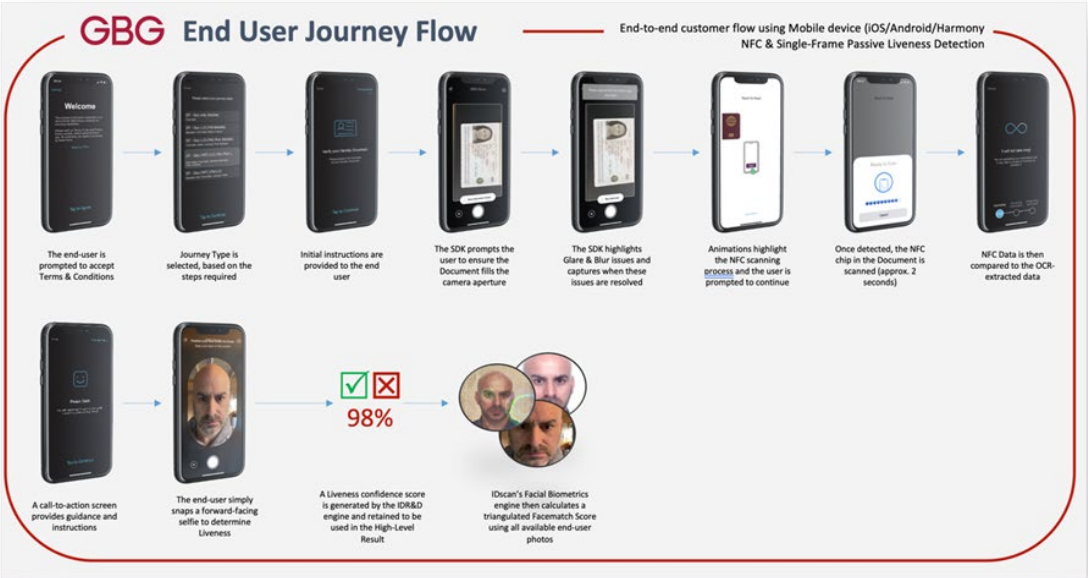
GBG IDscan Core components give you the flexibility to design and build the perfect identity platform using the best possible technology available in the market today.

IDscan Core empowers our customers with RESTful APIs that allow them to decide what level of authentication they would like to achieve, with their preferred user experience. IDscan Core allows our customers to configure their user journey and user experience as they see fit with no restrictions on the components used or the manner in which they are deployed. IDscan Core is a Server-to-Server service, that provides the below API Endpoints:

- SDKs (Native and Web) to support rapid implementation and integration.
- Global Document Authentication / Verification Library.
- Liveness Verification - iBeta Level 2 ISO 20107-3.
- Face Match (facial biometrics) Verification NIST Certified 1:1 face match.
- NFC RFID chip reading.

Private & Confidential © GB Group plc 2026

Below shows an example of a mobile application:



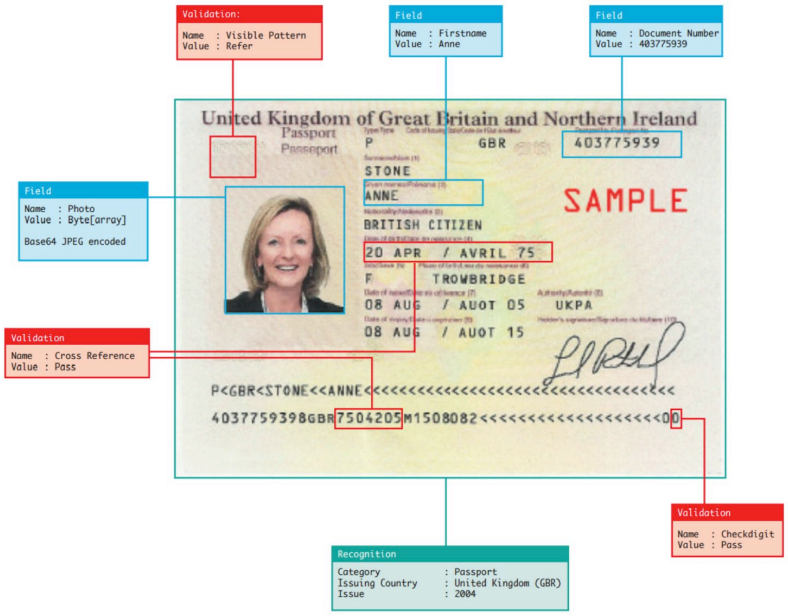
Global Document Library

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.

Private & Confidential © GB Group plc 2026



Face Match (Facial Biometrics)

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.

Private & Confidential © GB Group plc 2026

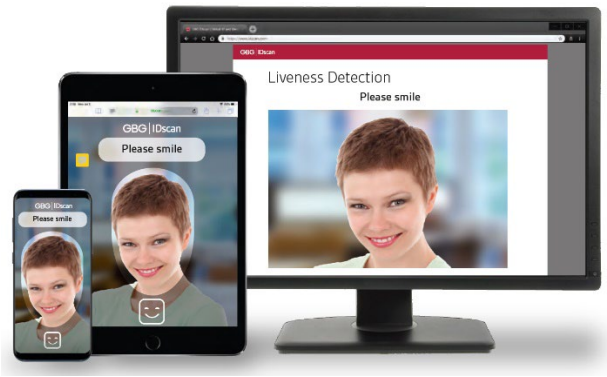


Liveness

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.



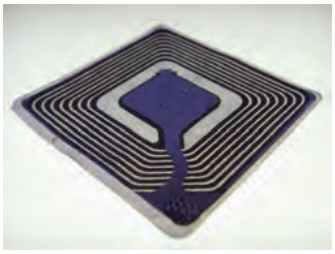
Private & Confidential © GB Group plc 2026

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.



Private & Confidential © GB Group plc 2026