We employ over 4,000 people in a network of offices across the UK.

Issues circa 6 million passports

Responds to over 6 million passport validation service requests.

Other government departments and a credit-reference agency to help us check your identity. We may also pass the information you give us to UK law enforcement agencies or government departments involved in preventing fraud to help prevent or detect identity theft, fraud or other criminal activity. You can find details about the personal information we hold, how we protect it, who we pass it to and how you can get a copy of that information and other rights in our Privacy Information Notice (PIN) on our website

* <https://assets.publishing.service.gov.uk/media/636e1326e90e07618e6ae553/09.22_Guidance_Booklet_IND.pdf>
* Verification System – verify authenticity of supporting documents – needs optical character recognition technologies (OCR) to automate the process/detect issues
* Payment system – process payments, interface with banks, generates invoices and receipts
* Biometric data systems – could be lumped in with the rest of them
* Database – for all the info – needs to be secure – a database management system – to assure CIA and backup
* Processing system (more web focused)

MySQL Enterprise Masking and De-identification

MySQL Enterprise Edition

**Type of Information gathered: - personal identifiable information (PII)**

* Full name
* House address
* **Race - NON**
* Gender - NON
* Date of birth - NON
* Place of birth - NON
* Contact details

**Biometric information (photo ID, fingerprints, iris scan, facial recognition data)**

* Credit card info/payment info (both for paying, but also for renewing ur passport)
* Documentary data (birth certificates, identification documents (like driver’s licences)
* Application history (previous application info for passports)
  + <https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en#:~:text=trade%2Dunion%20membership%3B,sex%20life%20or%20sexual%20orientation>.
  + <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/special-category-data/>
    - Statutory and government purposes - substantial public interest conditions

Different Systems in place:

* Verification System – verify authenticity of supporting documents – needs optical character recognition technologies (OCR) to automate the process/detect issues
* Payment system – process payments, interface with banks, generates invoices and receipts
* Biometric data systems – could be lumped in with the rest of them
* Database – for all the info – needs to be secure – a database management system – to assure CIA and backup
* Processing system (more web focused)

**Abstract:**

This document presents my background research, as well as the proposed system for the Passport Office business. I consider the threats and vulnerabilities of the system, as well as proposing alternate methods to secure, and protect the service from threats. I will then detail a threat and risk analysis, using multiple methods, including SD3, STRIDE, a Risk Severity Matrix and DREAD. Finally, a secure design specification will be included, in order to further patch possible vulnerabilities that may be present within the system.

**Describe the business of the passport office and the different types of data that are held by them. This includes what you have learnt through background research.**

**An Introduction, a description of the system/service, and a summary of your background research [10%].**

The passport office is an institution that is inextricably linked with the systems of our government. Their role is to gather information about people, whether that be provided by the customer, or information gathered through other governmental departments POSSIBLE CITATION/THING. They then analyse this information, determining if it is both accurate and also meets the requirements for a valid passport. If so, they are in charge of printing and issuing said passport to the customer in question, and securely storing all the information for future use, or for verification purposes.

They hold many different types of data, most of which are counted as personal identifiable information (PII). Some of this data is considered ‘sensitive PII’, such as biometric information (photo ID, fingerprints, iris scan, facial recognition data) or information regarding racial origin or ethnicity. To process said sensitive information, the organisation is required to have ‘Reasons of substantial public interest (with a basis in law)’. An example of a substantial public interest reason would be for any ‘Statutory and government purposes’, for which the passport office would apply. While the other types of data are still PII, they are not sensitive, and the processing and security requirements are somewhat lessened, although strict privacy rights must still be enforced. Other types of data include but are not limited to: Full name, address, gender, date of birth, place of birth, contact details, payment information, documentary data (such as supporting documents like a driver’s license) and application history (regarding previous passport applications).

While it is unknown the exact processes and protocols that the Passport Office maintains, due to secrecy and privacy reasons (not to mention proprietary technologies), we can make some educated and accurate guesses at who what types of systems they would be required to have in place.

Firstly, our proposed service would require a Database Management System (DMS) to store all the data discussed above. Due to the size, but also the privacy and security concerns, access to such a system would need to be privileged and highly vetted. A DMS system like this would also work towards CIA (Confidentiality, Data Integrity and Availability) – as efficient addressing would allow for high-rate availability, while the principle of service separation and elevated privilege levelled access requirement would maintain Confidentiality. In addition, our proposed DMS system would require several backups, both due to its large size, but also the importance of the data stored therein. These backups would be both online and offline, cloud and local. Based on the UK Passport Office’s own numbers, they issue around 6 million passports per year, while servicing over that amount of passport validation service requests. As such, it would be prudent to have the system backup modifications to the files daily, with additional complete backups taken at various times. This would ensure Data Integrity, as any lost or corrupted data could be retrieved from one of the several backups available.

Our proposed system would require a way of intaking, processing and generating payment information, to interface with banks, generate invoices and receipts, and process payments for the services rendered.

We would require Biometric data systems, for the generation and confirmation of biometric information, such as iris scans, fingerprint, and facial recognition data. Given the updated biometric passports provided in the UK since 2010, this information needs to be accessible in order to be applied to the requisite passport. <https://www.postoffice.co.uk/identity/biometric-passports>

A primary password application processing system would be needed, in order to track, verify and process the status of applications throughout the entire work-process. In addition, audit and logging systems would be essential, in order to provide Repudiation should something go awry.

Finally, a verification system would be required, in order to verify authenticity of supporting documents (such as driver’s licenses and birth certificates). It would be this system that is capable of sending automated requests to other governmental bodies, in order to verify the authenticity of the provided information, and gather other sensitive personal identifiable information. This system would require Optical Character Recognition system (OCR’s) in order to automate the process, and detect issues with the provided documents.

