Task 1

What is the most widely accepted biometric authorisation technology? Why?

The answer to this relies heavily on the usage of the word "accepted".

If we are to take the meaning as acceptability to a user, according to Mattord and Whitman (2019) the most widely accepted biometric authorisation technology is iris scanning as it relies on a simple snapshot of the iris, rather than an intrusive scan. It can also be achieved with the use of inexpensive camera equipment. However a study published by IEEE (2022) indicates that finger prints were the mostly commonly accepted biometric method. An article by ABI Research (2023) suggests that this is likely due to its wide and long-established implementation.

If we are to take the meaning as accepted (and therefore implemented) by software vendors, jumpcloud (2022) stipulate that fingerprints are the most common biometric used due to the unique quality of a person's fingerprints and as they are easy to capture, both digitally and physically.

Task 2

What is the most effective biometric authorisation technology? Why?

The effectiveness of biometric technologies is measured using the crossover error rate (CER) - the point at which the number of false rejections equal the number of false acceptances. The lower the CER, the more effective the technology. Whilst it is largely recognised that the use of DNA as a biometric would result in the lowest CER, it is not currently being applied in practice as it is not easy to collect nor socially accepted (Mattord and Whitman, 2019). Of the remaining biometric measures, iris scanning is one of the most accurate, offering an CER of as little as 0.4% (NEC, 2018) - this is due to the authorisation technology relying on the random pattern of features found in the iris, which is highly unique and unlikely to change during the lifetime of a person.