Best Practices for Using Biometrics for National Registry

A Documentary White Paper covering the background and providing general guidelines

This paper will outline the best practices for using the biometrics identification technology i.e. use of a personal physiological traits (fingerprints, face and/or iris biometric samples) and biographic information with unique characteristics for registering the population with the goal of issuing one identification per person. The single identity may service multiple subsequent identity applications (examples include but are not limited to birth certificates, marriage, adoption, and recognition certificates, education records, criminal records, passports, medical records, voter registration and credit bureau) as determined and implemented by the government. If the government implements the requisite legislation, information security and operational controls, the National Registry can reduce or avoid redundancy of development and maintenance of personal identification information to support each of the applications and minimize discrepancies of identity information across the applications.

The guidelines in this paper are derived from the author's lessons learned from actual system deployments over the last 20 years and extracted from extensive documented biometric performance testing that has been carried out and published by credible government institutions in various countries.

Since a national population registry system is essentially part of the given nation's infrastructure, like the roads, bridges, schools and hospitals, it has to be treated as such, planned to work reliably and economically with defined expected and stable performance for many years to come to benefit the citizens in a direct and tangible way.

This is the first publication of its kind that addresses both human factors and technical factors related to such deployments. The guidelines also consider the day-to-day operational issues such as up-keep and upgrade path. Due to the very large scope of procurement and deployment requirements and parameters for such systems and to some degree the localized nature from one country to the next, the guidelines are stated in general terms to be an applicable and appropriate starting point. This paper highlights the summary bullet point guidelines and then proceeds to provide the justifications and reasons for them in short descriptions with references to the actual extended reference reports.

Summary Guidelines:

1. **The data integrity of every individual record is essential**. Biographic and biometric data components must be captured and maintained as one record from the first enrollment through the life of the system. Standard IT guidelines for data protection, data encryption, data backups, data access, secure and well-defined roles and responsibilities of the system users and data privacy must be required and implemented in the system. The emphasis on this is due to the fact that often times the biometric data samples are extracted from record and added to the biometric matching system for the actual search and match for duplicate check. Or possibly they may be captured by one person while additional biographic data is captured or updated by another person. The maintenance of the data integrity throughout the system from the enrollment stations – fixed office – or portable field units – is a critical technical and system operational issue.
2. **The Biometric data must adhere to the published standards**. The most relevant standards are the ANSI/NIST ITL Standard for exchange of biometric data and the related Standards from ICAO / ISO. The key guide here is that no portion of the data must be kept in proprietary format. Every piece of data must be readable by Standard IT processes such as database queries by the government employees or designated other agents working for government other than the vendor who provided the system.
3. **Fingerprints are the best established biometric sample for use for these systems.** The science and technology of fingerprint has been developing for the last four decades. The fingerprint market and products are labeled as "matured" technology in the industry marketing terms as compared to the "early

stage" and "growth stage" of market and product technology. The facial recognition and iris recognition technologies are very important biometrics but technically they are in their "infancy" in the technology life cycle analysis. One important aspect of why these technologies are categorized as "early stage" products is the absence of large scale and large numbers of deployed system using the early stage technology. While, the first computerized large scale fingerprint identification system was deployed at FBI in 1975, the first large scale iris recognition was deployed in United Arab Emirate in 2004 for immigrant worker positive identification. The current size of a couple of the larger fingerprint system deployments exceeds 100M records and there are hundreds of other deployed sites around the world with databases over 1 million records working 7/24 and processing hundreds of thousands transactions daily .

4. **Since the National ID system will be an infrastructure component for the country and not a scientific experiment, using matured core technology is a requirement.** This does not mean other emerging technologies will be ignored. In fact use of the facial recognition and iris recognition as secondary biometrics where fingerprints fail is a normal practice for such a system deployment. The face image data in ICAO or ISO standard capture format – like for passports –are good quality biometric samples, but facial recognition is not yet a sufficiently accurate and reliable standalone biometric to be used for the general population identification and duplicate check in large scale deployments. The Iris technology products are even newer to the market and expensive. Reliability of iris technology biometrics in large scale (10 million record database) operations is not proven.
5. **The number of biometric samples must be at minimum two.** For example for fingerprints, at least two fingerprints are required for a population or system database size below 500K individuals. And for sure a single fingerprint solution such as a thumb print or one index fingerprint is not recommended for a National Registry system. The field proven deployment "golden rule" for large scale national ID and border control systems is 10 fingerprint flat capture. The development of this standard is rooted in the initial deployment of the first fingerprint national ID system in the country of Argentina in 1997 for 40 million population, and the original US INS IDENT system to check the border crossing recidivists which has turned into the US-VISIT system, one of the largest fingerprint border control ID check system using fingerprints. This guideline recommends the 10 flat fingerprints for population database record sizes of 1 million and more. The justification for this guideline is detailed out later. In short three factors stand out, one: for a reliable system we must have the data entry redundancy such as the 10 fingerprint samples from the same person, two: the demographic of the population is very critical for the successful operation of the system, a key issue is the degradation of fingerprints of much of the population due to very heavy manual labor which will be mitigated by the capture of 10 fingerprints, and three: the substantial increased probability of match due to having ten independent decision process from 10 fingerprints. These points are highlighted with reference to actual testing and analysis and the impact on the performance error rates.
6. **The capture method is the slap or flat capture of the fingerprints.** In a very large national ID system in 1997 for a 40 Million population nation, we have experimented with rolled fingerprint process and identified key ergonomic, quality and operational issues. Our findings were subsequently submitted to the FBI and DHS which formed the foundation for the new flat capture standards for fingerprint identification systems.
7. **The capture of ICAO (International Civil Aviation Organization, in French: Organisation de l'aviation civile internationale, OACI) compliant facial photograph is a viable option via good quality inexpensive web cams and must be incorporated in the enrollment process**. The use of facial recognition is not recommended as the primary biometric technology for duplicate checking in the large database. However as a secondary process for use in situations where the individuals are amputees or do not have fingerprint friction ridge formation on their fingers, the facial recognition can be used with the actual manual process as part of the standardized system exception handling and duplicate check processes.

The provision must be included in the enrollment software to check at least the basic five parameters of the face image in conformance to the ICAO standard i.e. face rotation, distance between the eyes, face center, face width and face height and provide the real time feedback to the operator to correct any of the parameters which are not conforming. For example if the face is rotated more than the limit allowed in the standard the operator will be prompted to re-take the picture directing the individual to straighten his/her face orientation.

8. **Provisions must be implemented in the system to measure the quality of the fingerprint as it is captured and in real time prompt the operator to capture a better quality fingerprint a second time when the quality is insufficient.** This process turned out to be a key success factor during a large scale deployment of fingerprint identification system for fraud detection for social services recipients' and welfare system. The intelligence must be built in the enrolment application to detect the cause of the quality defect in a just captured fingerprint and recommend a corrective action,(i.e. off-center, too-light, too much pressure, etc.), The quality check further will allow multiple sample capture – real time evaluation of the best quality sample that will be included in the registration record.
9. **Provisions must be implemented in the system to check for the system operational readiness – is the fingerprint scanner ready to be used? Is the calibration checked?**
   These are referred to as the Operational Readiness Verification (ORV) which is critical for national identification system operation where the operators have limited biometrics expertise. These are done by providing calibration targets and easy to follow procedures for the operator to follow.
10. **Provisions must be implemented in the system to check for the system backend services operational performance.** Is the matcher running as designed and configured after a period of operations – a month – six months – or a year? Has there been any degradation in accuracy and speed of the system as the database grows and updated? These are implemented by embedding known test datasets in the system and having a known number of operational support staff enroll themselves and check the performance parameters of the system.
11. **Provisions and open interfaces must be implemented so that the government agency will be able to second source components of the system.** Commercial off the shelf (COTS) components are a critical requirement. For example COTS fingerprint scanners computer platforms and servers avoid proprietary vendor locked in hardware and excessive costs.

Detail Supporting Argument for ten flat fingerprint enrollments

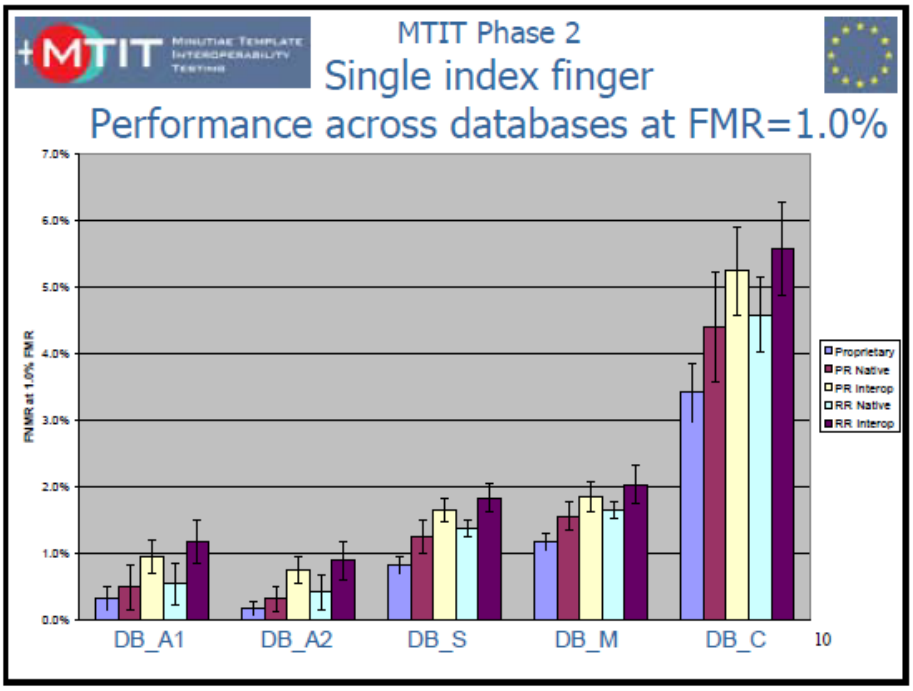
Three aspects are briefly outlined here, the actual field deployment systems requiring 10 flat fingerprints; the performance testing results from EU framework research project and US NIST testing, and the empirical results for system reliability vs. the database size growth.

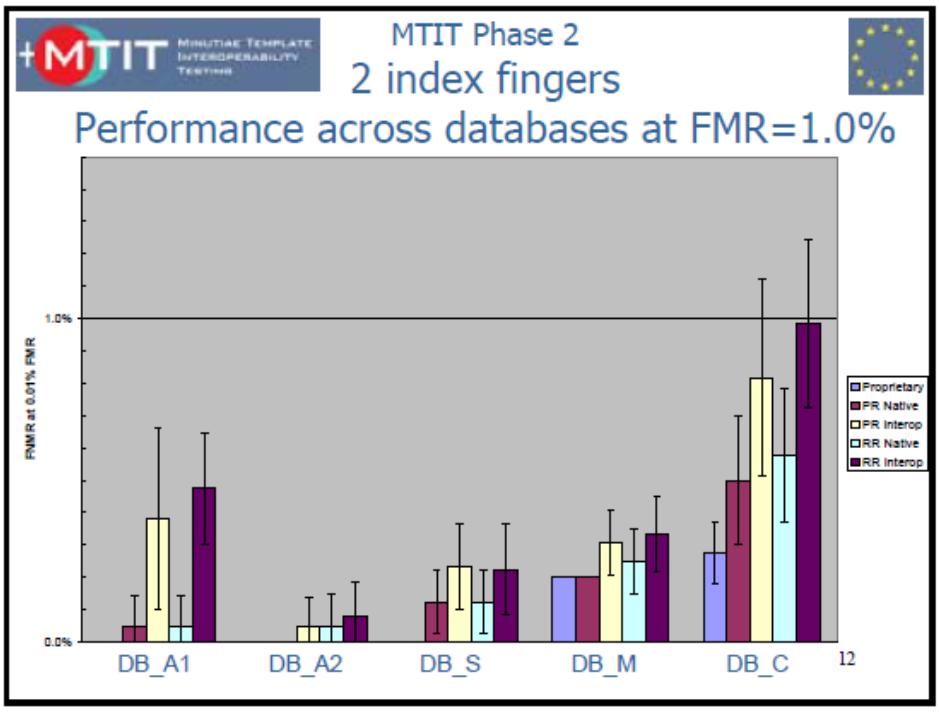
1. The field deployment reference projects for the multiple fingerprint enrolment and use of the database records for duplicate check includes:
   - In 1995, the Argentina National ID registration was the first national registry using the fingerprint biometric as part of the enrollment record. The target population of 40M records was planned including the children enrollment from the age of 8. Originally the requirement was for standard 14-set rolled and slap fingerprint card capture records. After the initial pilot deployment in 1996 it was clear that the process of rolling fingerprints is not an easy task and often times was confused both by the operator and the individual who is being printed. So flat fingerprint capture was invented and used as the ergonomically easy way to capture all the ten fingerprints. This provided compatibility with the law enforcement AFIS and turned out to be adopted as the golden standard for Civil ID AFIS procurement and deployment. The standard was added to the 2007 ANSI/NIST ITL biometric exchange standard.

Another aspect in this system was the inclusion of the children fingerprint records which resulted in new fingerprint scale invariant matching accommodating the growth from 8 years old and above.

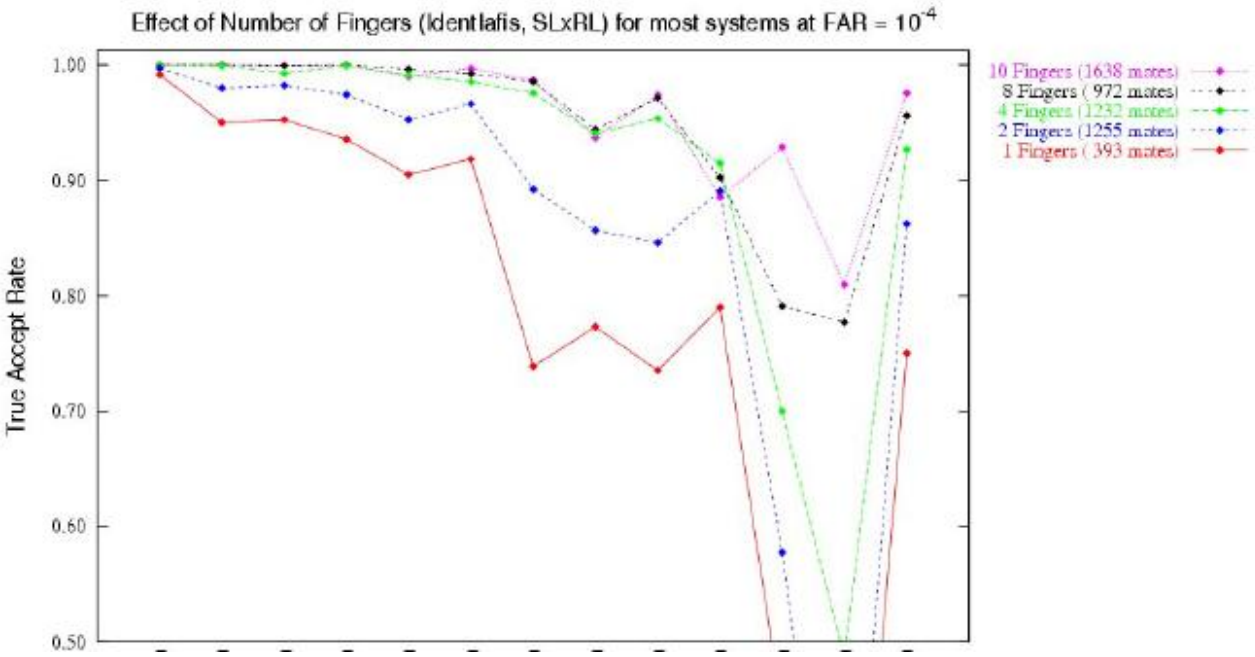
- The original US Immigration and Naturalization Services (INS) border crossing recidivist duplicate check which was first deployed in 1994 and started with two right and left indices fingerprints. The system was designed for less than 500K database and proved to be effective for positively identifying the individuals who would try to enter US with fake and multiple Id credentials. The system evolved to the IDENT program which was later used as the core for enrolling people who apply for US visa around the world – first to make sure people would not apply and get a visa under multiple ID's and second to verify the person at the point of entry with fingerprints, making sure the same person who was issued the visa was entering the country. As the database grew to the target 120M records the new standard policy was enacted in 2005 to move the system to 10 flat fingerprints captures for enrollment. The verification is done with multiple flat fingerprints.
- The European Union visa issuance and border control system contract awarded in 2006 has adopted and required the 10 flat fingerprint capture. The database size for the system is targeted for over 100M records.

2. The two major independent testings are referenced here with the associated related results;
   - European funded framework project Minutia Template Interoperability Test (MTIT) conducted in 2006-7 with four vendors participating – Cogent, Morpho, NEC, and Motorola. The primary objective was the investigation of template interoperability; however a good portion of the accuracy analysis was dedicated to the accuracy improvements going from single fingerprint matching to multiple fingerprint matching. The following two graphs show that using two fingerprints will reduce the average false non-match rate i.e. missing a person in the database by order of magnitude, for example for DB_C database from around 5% to less than 0.5%.





- The US National Institute of Standards and technology (NIST) Fingerprint Vendor Technology Evaluation (FpVTE) test conducted in 2003. Eighteen companies attended the test. The test included small (1000 records), medium (10K records) and large (64K records) scale database sizes. The test results for 1, 2, 4 and up to 10 fingerprints are reported.
  For one of the major vendors the match rate for single fingerprint was 91.5% improving to 97.8% for two fingerprints and 99.5% for 10 fingerprints matching for the operational databases.
  The following graph shows the effect of Number of Fingerprints used in matching on the true match rate. The performance has drops of over 50% going from 10 fingerprints to single fingerprint used in the matching.
  It must be noted that this FpVTE was funded partly by the US Department of Homeland Security and these results were a key input for the decision to go from a two-fingerprint system to 10-fingerprint system for the US-VISIT border control visa issuance and checking system.



3. The third aspect of the reliability of the using fingerprint biometrics is the empirical fact that for the 1 to N matching identification system the duplicate missing error rates increased by 1% as the database size doubles. So if the matching rate is at 92% – which is typical for a good quality single fingerprint matching algorithm in a 100K background database, the rate drops to 91% for 200K database and approximately to 85% for the 10M record database. So using two fingerprints which generally represents two independent decision variables will improve the joint match probably rate back to 97% and using the ten fingerprints better that 99.99% match rate reliability. This has been primarily the reason for the classical police AFIS products using multiple fingerprints to carry out the duplicate check for a new booking. The early practice used two rolled thumb fingerprints, and the current systems use 3, 4, and up to 10 fingerprints based on the quality of fingerprints to achieve very high accuracy referred to “lights out” tenprint operation.

References

1. ANSI/NIST ITL-2011 Standards for exchange of biometrics data, in publication.
2. MTIT – Minutiae template interoperability test – European Union Framework research project 2006;
3. MINEX – National Institute of Standards and Technology ongoing fingerprint interoperability performance test.
4. FpVTE - C. Wilson, et al; Fingerprint Vendor Technology Evaluation 2003, NISTIR 7123. June 2004. http://fpvte.nist.gov/
5. GAO - GAO; “Border Security: Challenges in Implementing Border Technology,” Statement of Nancy Kingsbury, Managing Director Applied Research and Methods, Testimony Before the Subcommittee on Terrorism, Technology, and Homeland Security and Subcommittee on Border Security, Immigration, and Citizenship, Committee on the Judiciary, United States Senate; March 12, 2003. http://www.gao.gov/new.items/d03546t.pdf

6. IQS - R.A. Hicklin, et al; Implications of the IDENT/IAFIS Image Quality Study for Visa Fingerprint Processing, October 2002. http://www.mitretek.org/publications/biometrics/NIST-IQS.pdf
7. NFIQ - E. Tabassi, et al; Fingerprint Image Quality NIST IR 7151, August 2004. ftp://sequoyah.nist.gov/pub/nist_internal_reports/ir_7151/ir_7151.pdf
8. SDK - C. Watson, et al; NIST Fingerprint SDK (Software Development Kit) Testing, NISTIR 7119. June 2004. http://fingerprint.nist.gov/SDK/