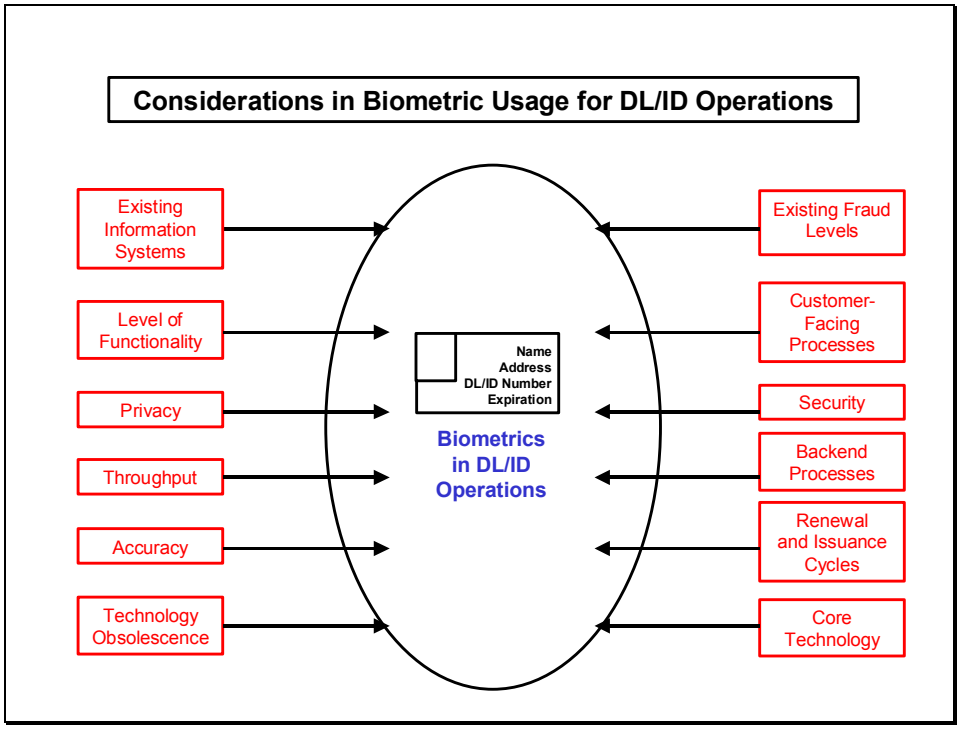
Biometrics in Driver's License Operations

An IBG White Paper

International·Biometric·Group
Research Consulting Integration

Abstract

Most U.S. states are investigating the use of biometric technologies to reduce fraud and improve efficiency in driver's license and ID card (DL/ID) issuance operations. Dozens of critical issues – from core technology performance to implementation costs to privacy impact – must be evaluated prior to deployment. This document provides decision-makers with an outline for addressing many of the complex issues involved in large-scale biometric deployment.



1. Rationale for Biometric Usage

Biometrics are deployed to detect and/or deter fraud in DL/ID issuance and usage. Biometrics, if used properly, can provide singularly reliable identification and identity verification. Because DL/IDs have become the primary method of identification in interaction with government and commercial institutions, improving the license issuance process is likely to provide positive results in a range of environments. A state may justify biometric deployment to ensure the integrity of DL/ID issuance, to reduce costs related to fraudulent DL/ID usage, to provide a more reliable means of identification for law enforcement purposes, or to extend the functionality of DL/IDs into areas that require heightened identity certainty. However, providing a rationale for biometric deployment is complicated by two factors.

First, biometrics can eliminate some, but not all, fraudulent uses of DL/IDs. Unless biometrics are placed on the DL/ID itself and are read from the card on a regular basis, biometrics cannot stop the generation and use of fake DL/IDs. Biometrics are also unable to determine whether breeder documents are valid, such that an initial "biometric identity" can be created under false pretenses[1]. Not until an individual returns to acquire a 2nd license will the biometric system identify a duplicate. Lastly, biometric systems cannot detect every duplicate enrollee – some small percentage of duplicate registrants will avoid detection.

Second, the benefits of biometric usage in DL/ID issuance are difficult to quantify. Biometrics both detect and deter misuse of DL/ID systems, but deterrence cannot be measured precisely. Similarly, it is difficult to assign a monetary value to increased confidence in DL/ID issuance processes. Therefore, while the costs of biometric systems are fixed and often sizeable, cost avoidance can in most cases only be generally estimated.

Key Questions

- *Have costs linked to fraudulent DL/ID issuance and usage – such as through identity theft and illegal immigration – be quantified?*
- *Has the suspected percentage of duplicate or fraudulent licenses been calculated?*
- *Is there general public awareness of problems or vulnerabilities in DL/ID issuance processes?*

[1] This problem can only realistically be addressed through intra-state data sharing, which raises additional challenges in terms of scale, interoperability, and the type of biometric collected.

2. Functionality Options

Biometrics can provide various types of functionality in DL/ID environments. The basic functional division is between identification (or 1:N), which searches a central database for duplicate biometric data, and verification (or 1:1), which confirms a claimed identity. DL/ID applications may utilize both 1:N and 1:1, or may utilize only one functional mode.

The following are the major types of biometric applications in a DL/ID environment.

- **Targeted 1:N.** In this application, biometrics are used for select 1:N searches when fraud is suspected in the DL/ID application process. For example, a transaction in which an individual presents suspect breeder documents may be flagged for a 1:N match.

- **Full 1:N.** In this application, biometrics are used to execute 1:N searches for every applicant to determine if that person's biometric data has been acquired previously.

- **Renewal and Update 1:1.** In this application, biometrics are used to confirm the identity of individuals already in possession of DL/IDs looking to renew or update DL/ID data. This type of usage can be divided into centrally-stored 1:1, in which biometric data is retrieved from a central database for matching, and token-based 1:1, in which biometric data is stored on the DL/ID itself, allowing for offline identity verification.

Additional uses of biometric data collected for DL/ID issuance law enforcement, commercial transactions, and interaction with federal government agencies are often speculated on but rarely if ever implemented.

Determining precisely what functions the biometric is to provide is a critical determinant of system costs, time to implementation, and complexity of integration.

Key Questions

- *What are the most critical problem areas to be addressed through biometrics?*

- *What processes are currently in place to detect and deter fraudulent DL/ID usage and issuance?*

- *What is the jurisdiction's tolerance for large-scale information systems deployment?*

- *What is the marginal effort to incorporate both 1:1 and 1:N functionality if one mode is the focus of DL/ID efforts?*

3. Existing Process Flows

Depending on the level of functionality that biometrics are expected to provide, incorporating biometrics in DL/ID operations may have little to no impact on current processes or may have a major impact. The areas that biometric systems may directly impact can be divided into *customer-facing* and *backend*.

In terms of customer-facing processes, incorporating biometric acquisition as well as results of 1:1 biometric matches can require substantial process reengineering. Difficulties can arise when determining where to place biometric acquisition in the customer-handling sequence, how to accommodate longer lines related to increased transaction time, and understanding how to address non-matches in 1:1 operations.

In terms of backend processes, the use of biometrics for 1:N duplicate detection requires that additional man-hours be dedicated to resolving potential fraud cases. Fully populated systems biometric systems are unable to provide real-time biometric matches with a high degree of accuracy; manual inspection is required to ensure that a "duplicate" record is truly a duplicate and not a false match. Depending on the rates of enrollment, the size of the database, the biometric data acquired, and the tolerance for false matches, a state may need to resolve dozens of such "false matches" on a daily basis. This, in turn, may impact the process of card manufacturing.

Certain technologies have the substantial advantage of limited impact on existing processes. For example, facial-scan can be implemented with almost no impact on current processes; standard facial images, already acquired in DL/ID operations, can facilitate enrollment as well as 1:1 and 1:N operations.

Key Questions

- *What are the jurisdiction's capabilities in terms of retraining employees to acquire biometric data effectively?*
- *What will be the impact of increased transaction time on overall customer handling processes?*
- *How many personnel are currently dedicated to fraud investigation and resolution?*

4. System Design

Biometric systems must be designed to operate with existing information systems – those that contain legacy transactional and DL/ID information – but still provide forward-looking scalability in anticipation of population increases and peak transaction periods.

Deploying biometrics effectively requires that issues such as scalability, throughput, transaction loads during maximum enrollment periods, interoperability, and technology obsolescence be addressed prior to implementation.

The sensitivity of biometric data is such that strict security policies must be established and enforced relating to data transmission, account access, and administrative privileges. Standards can be leveraged which provide enhanced cryptographic functionality, but these standards may increase transaction times and require implementation of new communications infrastructure.

Key Questions

- *How will biometric data be secured during storage and transmission, and in what formats will biometric data exist?*
- *How will access to biometric data be limited, and how will such access be audited?*
- *What percentage of existing communications and information systems can be leveraged in biometric deployment?*
- *What are the projected maximum throughput loads projected throughout the life of the system?*

5. Core Technology Issues

While a number of technologies compete in the biometric industry, only fingerprint-based and facial biometrics have been deployed in DL/ID applications in the U.S. Determining which technology or technologies to deploy, and more importantly determining how best to deploy a given technology, is central to effective use of biometrics in DL/ID issuance.

Facial-scan is best deployed in targeted 1:N operations in which a given applicant is suspected of attempting duplicate enrollment. Manual inspection of potential matches can occur as a backend process. While facial-scan can match images more rapidly than fingerprint-based technology[2], it is designed to return candidate lists of closest matches at opposed to a single strong match. Executing 1:N searches with every enrollment would result in an excessive number of matches requiring manual resolution, unless the matching threshold is set such that a high percentage of duplicate enrollments go undetected. Facial-scan is rarely used for 1:1 authentication, being susceptible to reduced performance over time and with modest changes in user appearance.

Fingerprint-based biometric systems offer a much higher degree of accuracy than facial-scan in both 1:N and 1:N operations, with a corresponding increase in costs, time to acquire data, and time to match data. Fingerprints can be used to facilitate very large-scale matching, up to tens of millions of people, depending on the number of fingerprints acquired and the quality of acquisition. Fingerprint-based biometric systems are also deployed for 1:1 matching in a wide variety of applications. Much more data is available regarding the accuracy of fingerprint-based biometrics than any other biometric, due to its relatively longer deployment history. Jurisdictions looking to fully embrace biometric functionality, as opposed to using biometrics in highly circumscribed and targeted searches, are more likely to adopt fingerprint-based systems than any other type, although deployers must be able to counter privacy concerns related to use in police or investigative applications.

Among alternative biometric technologies, iris-scan warrants the most serious consideration as it provides highly accurate 1:1 operations and is thought to be theoretically capable of high scalability for 1:N operations. The effort and expense of iris-scan deployment, however, combined with the absence of real-world data related to the technology's accuracy in large-scale deployments, firmly places iris-scan as an emerging technology.

Key Questions

- *What technologies are under consideration for piloting and deployment?*
- *What are the jurisdiction's target applications for biometrics?*
- *Is the jurisdiction interested in high accuracy and reliability, low cost, limited impact on processes, or long-term utility?*
- *What is the jurisdiction's approach to technology obsolescence?*

---

[2] Assuming that the same amount of computing power underlies both matching subsystems

6. Accuracy

A core consideration of any proposed biometric deployment is the system's ability to provide accurate and reliable 1:1 and 1:N operations. Biometric systems are subject to matching, non-matching, and enrollment errors; depending on the reasons for which the biometric system is deployed, it may be necessary to minimize one of these error types at the expense of an increase in other types of errors.

Biometric accuracy is a notoriously complex topic, with dozens of factors contributing to system accuracy. But a handful of these factors include (1) the quality of initial biometric data acquisition, (2) the time lapse between initial capture and subsequent verification and/or identification, (3) the type of biometric data acquired, (4) the number of biometric samples acquired, (5) the quality of training and degree of supervision, (6) the robustness of the scanning device, (7) the maximum permitted response time, (8) the demographic composition of the user population, (9) the robustness of the underlying algorithms, (10) the use of non-biometric data to limit or filter searches, (11) the amount of damage or alteration to the identifiable biometric data, and (12) changes to the operating environment.

Even with these factors isolated, the manner in which accuracy is statistically defined can be highly misleading. Biometric error rates may be indicative of a single template versus template comparison, or may reflect "all vs. all" test data extrapolated to larger populations. Results in the lab may not equate to real-world results due to reduced control over the operating environment. For many large-scale biometric scenarios, no independently verifiable data exists, such that deployers may not know what degree of accuracy to expect until a large number of users are enrolled.

The concept of using multiple biometric technologies has substantial appeal in applications where enrollment and false matching errors must be minimized. The rationale for multiple biometrics is that an individual unable to enroll in one technology can enroll in another, reducing outliers. In addition, large-scale matching may be eased through use of multiple biometric samples. The challenge is in acquiring multiple biometric samples rapidly while ensuring high-quality data acquisition. In addition, there is still debate as to whether combining strong and weak biometrics increases or decreases total performance.

As a baseline, deployers must reference independently generated and validated test data before making any assumptions regarding biometric performance.

Key Questions

- *What tolerance does the jurisdiction have for matching, non-matching, and enrollment errors?*
- *What quantity of biometric data can be reasonably acquired without excessively impacting customer-facing operations?*
- *What fallback processes can the jurisdiction implement for use in 1:1 operations?*
- *Can biometric data of a sufficiently high resolution and quality be acquired in DL/ID operating environments?*

7. Cost Considerations

Estimating the costs of biometric system procurement, integration, and deployment, as well as estimating the direct and indirect financial benefits of deployment, is complicated by a number of variables. For example, the processes through which biometric data will be acquired, the complexity of integration, and impact on personnel levels will likely vary according to final system design decisions. Even more fundamentally, the uses to which the biometric system will be put directly impacts implementation costs.

Major cost areas in biometric deployment within DL/ID operations include 1:1 and 1:N acquisition and matching components (both hardware and software), professional services and support, and integration of hardware in the field. In addition, substantial costs may be associated with increased staff for training and duplicate resolution.

In addition, there is the issue of initial versus ongoing costs. A day-forward system, one unable to leverage legacy biometric data, will require the implementation of a large infrastructure. The primary area in which costs can be deferred is in 1:N matching components, as large-scale match volumes are not achieved until a substantial percentage of individuals are enrolled, a process likely to take years.

Key Questions

- *What budgetary constraints are present limiting long-term expenditures?*
- *What cost savings or other metrics are used to justify system costs?*
- *Can the system be phased in incrementally or is major hardware and software expense incurred prior to seeing benefits?*
- *What infrastructure and platforms are present in customer-facing and backend operations?*

8. Piloting and Testing

Once decided on a technology and high-level system design, jurisdictions are advised to pilot biometric technology in operational environments in order to validate assumptions regarding the impact on process flow. Piloting the technology across DMV facilities representative of statewide operations – for example in both high traffic / low traffic and in "high-tech" and "low-tech" facilities – will give the clearest indication of full deployment impact.

Because full systems integration cannot normally be executed prior to piloting (being a major expense in many systems), piloting does not validate assumptions related to integration with legacy systems. However, one-off integration at client terminals may be viable depending on the age of existing information systems. This would validate assumptions related to process flows, if not overall information systems impact.

- *Has the jurisdiction conducted accuracy and performance testing, or does it have access to such data?*
- *Has the jurisdiction budgeted for piloting?*
- *How is the jurisdiction evaluating the results of piloting and test efforts, and are these results being validated by an independent 3rd party?*

9. Conclusion

While the preceding represents only a percentage of the issues to be addressed in biometric usage in DL/ID environments, areas such as standards, interstate and federal interoperability, and privacy and policy impact must also be addressed to gain a full understanding of if and how to deploy biometrics in DL/ID operations.

Biometrics are not the right solution for every state's DL/ID program. However, the maturation of biometric technologies, combined with the need for identity certainty in an increasingly broad range of applications, makes biometrics a valuable solution for many state-level deployers.

Contact IBG for information on the services we provide to states investigating or deploying biometrics in DL/ID operations.