COM-15-3487
R. Simpson, S. Bittinger

Research Note
19 February 2002

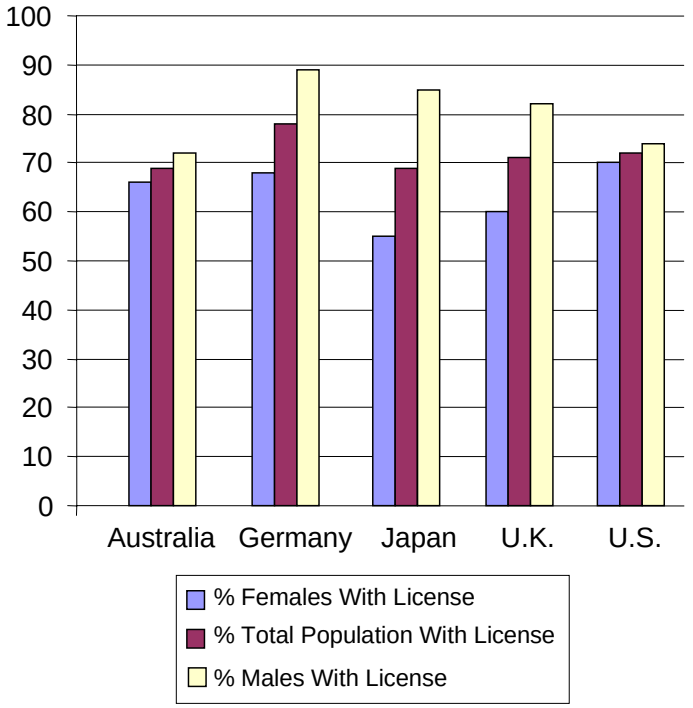
Commentary

Can the 'Smart State' Implement a Smart Driver's License?

DMVs face the problem of cutting the cost of issuing and renewing motor vehicle registrations and driver's licenses while reducing identity fraud. The Department of Transport in Queensland, Australia, may have the answer.

In the absence of a national ID, driver's licenses issued by state departments of motor vehicles (DMVs) are the default proof-of-identity and proof-of-age card in most countries worldwide. Despite this almost universal reliance on driver's licenses as the default identity card, other government agencies and private enterprise pay no fees for this publicly funded service. In many Western countries, driver's licenses are held by more than 70 percent of the population, and the identity-card features are often available to citizens who do not drive.

Figure 1
Penetration of Driver's Licenses by Country and Gender



Source: Gartner Research

Despite the generally accepted need to improve identity validation in the wake of Sept. 11, the prospect of a national ID card is causing great controversy in the United States. While driver's licenses also fulfill a default ID card role in the United States, there is little data-sharing or coordination of driver's license standards among the 51 DMVs and local, state and federal police. A recent attempt by the American Association of Motor Vehicle Administrators to create uniform standards for license design and identity validation met with considerable opposition.

Australia has a long history of cooperation between state and federal governments on road transportation matters. Although the actual license design and technology varies from state to state, a license and motor registration data exchange standard and joint service bureau was established more than 10 years ago. The National Exchange of Vehicle and Driver Information System database allows any police or emergency services worker to check registration and license validity for any driver and any vehicle, regardless of state of origin. This has recently been extended into a real-time service that can be accessed from a suitable data-enabled mobile phone (see "WAP and GPRS Help Spot Stolen Cars In Canberra," CS-14-7681).

However, license and registration fraud is increasing, due mainly to the ease of forgery of the current, laminated cards and paper-based registration stickers used in most Australian states.

The DMV Cost Problem

The typical DMV business model is inherently transactional, with very high ongoing costs. Citizens physically attend a DMV office once a year to renew registration, and once every three to five years to renew their driver's license. On each occasion, the DMV must manufacture, issue (and often distribute later by mail) a "product" — the license or registration sticker. Manufacturing and postage costs can exceed the license renewal fee. Many DMVs are exploring electronic service delivery — but even with the use of the Web or Interactive Voice Response systems, the high cost of annual renewal, manufacturing and physical distribution of the product remains. In Australia, the license fee (typically A$120 for five years) or registration fee (typically A$200 to A$300 a year plus a similar amount for compulsory insurance) also presents a significant burden for low-income earners.

The "Smart State" Solution

In the Australian state of Queensland (which calls itself the "Smart State"; www.qld.gov.au/), Queensland Transport (QT) has spent the last 12 months studying the application of smart-card technology for driver's licenses. Even for a small state like Queensland (population four million), the cost of license renewals totals millions of dollars per year; QT believes it can financially justify implementing a smart-card license system independent of other states.

The study has developed recommendations that, if adopted by the government, will:

- Reduce the ongoing cost of license renewal, manufacturing and distribution
- Reduce the fee burden by allowing automatic payment by installments
- Improve driver's license ID security
- Provide benefits to drivers
- Recover some of QT's infrastructure costs

Reducing Ongoing Department Costs and License Fees

The physical product (the authentication card) can be separated from the formal authority to drive and the vehicle registration function. Once issued, the life of the card is independent of the life of the license. Rather than requiring a large lump-sum renewal, license and registration fees can be paid monthly, similar to mobile-phone billing. The authentication card becomes a customer card used to manage the department's relationship with the citizen and to access and update current license and registration status electronically. The physical card would last up to 10 years, depending on the technology chosen.

Improving Security

The department has no legal mandate to provide a proof-of-identity function to the public, but it recognizes its de facto responsibility to do so with a high degree of integrity and security. While initial license issue procedures are tight, QT is contemplating a smart card with a digitally stored photograph to reduce identity fraud. Gartner believes stronger biometric authentication would be required to guarantee integrity and security. QT's market research has also shown public support among women for name and address data to be stored digitally but not printed on the card, as is now the case. The card would, however, retain the current human-readable information such as a photograph, name and license number for low-security visual ID validation.

Providing Benefits for Drivers

Automobile accidents are a daily challenge for police and emergency service workers. Most critically injured roadside trauma victims die within the first 30 minutes of an accident. While some citizens already carry medical and next-of-kin details in an "SOS" bracelet or in their wallets, QT's market research has shown community support for including healthcare and emergency contact information in the smart-card driver's license.

Recovering QT Infrastructure Costs

Assuming QT is able to sway government and public opinion in favor of the modest benefits we have detailed, the department has also explored other possible uses of a smart-card license.

To date, most single-purpose smart-card initiatives have failed to build a satisfactory business case to cover the costs of issue and infrastructure deployment. QT already enjoys a level of public trust in its de facto identity authentication role, and by its own estimate reaches more than 80 percent of the population. It is therefore ideally placed to extend its role to that of a smart-card services common carrier. QT does not see itself as the sole provider of common carrier or commercial identity services, but it could offset some of its infrastructure costs by providing an attractive, government-endorsed service to organizations that could not otherwise justify the costs of smart-card deployment.

The Challenge: Building Broad Support and Public Trust

Other smart-card projects are under consideration by different state and federal departments, including several public-transportation ticketing initiatives. In Gartner's experience, even the most visionary e-government strategies can fall prey to interdepartmental "turf wars" unless there is strong coordination and visionary leadership at state and federal levels.

Multiapplication uses beyond the road accident example also bring a raft of legislative, management, security, privacy and public-trust issues that would need to be overcome. Any organization that hopes to

play a trusted smart-card common-carrier role will need to be simultaneously superb at security, privacy and customer relationship management. The government of Hong Kong's open, innovative approach to these issues provides useful guidelines (see "Hong Kong's Multiapplication Smart ID Card," COM-15-4907).

Nevertheless, QT and many other DMVs already enjoy some degree of public trust. If implemented in a staged fashion as currently envisioned, the QT license card could benefit Queensland citizens and government agencies — and, eventually, private enterprises. The staged smart-card implementation strategy suggested is simple, practical and has a reasonable chance of achieving public acceptance due to the benefits to road accident victims.

Bottom Line: With 70 percent to 80 percent population penetration and a "social contract" to provide default ID card services to government and enterprise, DMVs that successfully introduce a multiapplication smart-card driver's license will find themselves in a strong position to provide common carrier services, provided they can prove their "trust" credentials. They can leverage their investment in smart-card infrastructure and ID services by offering value-added services to citizens and selling application space to other agencies and enterprises that otherwise would have no hope of making a business case for the required infrastructure investment. In a world concerned about terrorism, DMV-initiated smart-card identity services represent a small, positive step toward improved identity authentication that will be perceived as less threatening than a national ID card.