DOCUMENT SECURITY ISSUES

Part of a Series of Datacard Group White Papers for the Secure Document Issuer

ID CREDENTIAL ISSUANCE: CENTRAL VS. OVER-THE-COUNTER ISSUANCE

Overview

Historically many government agencies have selected a business model for issuing personal Identification Credentials (IDs) based on policy or legislative issues, or in some cases have been driven to select a low-cost method to meet budget requirements. With growing concern over the security and effectiveness of every ID System, organizations today are increasingly requiring a broad review of business issues as a critical step in preparing for new and more secure ID issuance. This paper is intended as a reference for government officials considering how best to issue secure IDs. Because there are trade-offs with each model and different requirements for each issuing agency, there is no "best" method.

MARCH 2007

DatacardGroup

SECURE ID AND CARD PERSONALIZATION SOLUTIONS

ID CREDENTIAL ISSUANCE: CENTRAL VS. OVER-THE-COUNTER ISSUANCE

Current Business Models

Over-the-Counter (OTC) Issuance: In this process the applicant (e.g. government employee, driver license applicant, etc.) typically completes forms at a local government or government-designated office and receives an ID at the completion of the process. Completion of the process involves submission of a written application and supporting documentation, collection of the applicant's photo image and signature, processing and approval of the application and delivery of the finished ID to the applicant. Supporting documentation can range from proof-of-identity documents (e.g. birth certificate, passport, etc.) to a pre-printed form mailed from the issuing agency notifying the applicant to appear in person. This process typically requires processing and approval while the applicant waits, production of the ID, and finally delivery of the ID to the applicant. Alternatively, some agencies complete this process in two steps, where the application and data collection process take place in the first visit and the ID is delivered in a second visit following processing and approval. In this approach ID production and application processing can be done on-site or at a remote location.

Central Issuance: In this approach the applicant completes data collection forms at a local office by mail or over the Internet, and the ID is produced at a central location for delivery to the applicant. Processing the application, ID production and delivery occur after the initial visit, and delivery is typically accomplished through mail from a central production facility. In the case of mail or Internet applications, the process is the same with the exception that the customer is not required to visit any office to complete the process. In many cases a temporary credential may be issued which would be valid for a limited time following the application. Credit card companies typically use this mail or Internet application approach to issue a new card.

Combined or "Hybrid" Issuance System: This approach combines some of the characteristics of both the Central and OTC methods. Many variations of Hybrid systems are used to meet operational or policy objectives. In some instances a Central Issuance system is used for all new (initial) applications, providing additional time for application processing and review. New IDs are then delivered from a central facility. In this scenario replacement or renewal IDs can then be issued by an OTC approach. An assumption critical to this process is that the initial application process was sufficient to confirm applicant data prior to issuance and that the person receiving the ID is the legitimate ID-holder (i.e. not an imposter).

In North America, driver license issuance business models range from Central Issuance to OTC to Hybrids. Decisions about the appropriate approach in some cases are tied to legacy legislation dating from the early days of Polaroid instant photocards. Some jurisdictions have changed their approach more than once over the last 10-15 years for administrative or political reasons.

Issues relating to ID issuance approaches covered in this paper include:

A. Customer Service
B. Enrollment and Applicant Processing
C. Cost
D. Equipment & ID Production Technology
E. Quality Control
F. Program Security

ID CREDENTIAL ISSUANCE: CENTRAL VS. OVER-THE-COUNTER ISSUANCE

A. Customer Service

All government agencies today are seeking ways to improve service levels for citizens and internal users. An OTC approach which produces an ID during a single visit to a local office is viewed favorably. The ID holder has the chance to review the document immediately after it is produced, and can request a reissue if there are any quality problems with the printed data or photo. By having the customer sign a receipt that they received their ID, the issuing agency can be assured that it is given to the correct person.

However, customer service problems can arise if there is an equipment malfunction. To minimize service disruptions there is usually back-up equipment either on-line or available to be quickly put into service.

With a Central Issuance process the customer completes their transaction when they finish the application process, and does not have to wait while the source documents are checked or the ID is produced. The customer can spend less time at the local office, and the office staff will be free to work with other customers. Central Issuance though introduces a delay between application and receipt of the finished ID, and the customer may be inconvenienced by this delay. If there is a quality problem with the finished ID that was not detected during production (e.g. incorrect spelling, customer unhappy with the photo image, etc.) the customer will be further inconvenienced by going through the process again to get a new ID issued.

Although it is possible to issue a temporary ID while the customer is present, there are significant security concerns over any temporary document. The most critical concern is the counterfeiting or alteration of temporary documents, as they are not likely to incorporate the security features included on a permanent ID issued from a secure facility. Central issuance also introduces the risk of theft of the genuine ID during the delivery process, and the risk that the intended recipient may not even be aware that the ID has been compromised.

B. Enrollment and Applicant Processing

In an OTC environment a decision must be made quickly about the validity of the documents presented with the application. Although online services can be used to expedite this process, the responsibility for issuing an ID is delegated to office staff at each location. If there is a question about the validity of a document submitted as proof-of-identity, well-trained staff can enhance customer service levels by reviewing issues with the customer to help them understand requirements. The accuracy and security of the application process then is dependent upon the skills and motivation of each staff person charged with authenticating proof-of-identity documents.

With sufficient training and experience, many staff learn to “read” the behavior of applicants, and may use more thorough verification procedures if they sense something unusual about an applicant’s behavior. However, there is no margin for error in this process, as an applicant receives a genuine ID at the conclusion of the process. Thorough training about document verification is a requirement, combined with regular auditing and supervisory interaction.

Staff motivation is also a critical issue, as the process can break down unintentionally under periods of high stress (e.g. large queues of customers, delays caused by equipment malfunction, personnel issues, etc.) or intentionally because of compromised staff. Genuine documents are highly valued by fraudsters, and the temptations that can be offered to circumvent a complete application review create real security concerns in application processing.

ID renewals or replacements (i.e. after the applicant is already enrolled) can be much simpler to administer with lower security risk, and are generally provided under OTC or Hybrid systems. The process should be driven by automated on-line retrieval of the applicant photo and signature for comparison to the person, and for verification that there are no regulatory issues with reissuance (e.g. license suspension).

Application processing in a Central Issuance model can supplement the benefits of personal interaction with an applicant (as noted above) with additional time to complete a verification process for submitted documentation. Depending upon the information provided by the applicant, additional time can be devoted to communicating with issuers of the documents or with other government agencies. The added steps in the verification process are a primary reason for adoption of Hybrid Systems where a thorough check is made for initial enrollment. When IDs are produced separately, staff can focus more on data collection and document screening.

C. Cost

The primary cost differences between OTC and Central Issuance are tied to the equipment and personnel necessary to produce IDs. In an OTC environment, each issuing office must have the appropriate equipment for ID production. Because ID issuance volumes can vary significantly on a day-by-day basis, it is usually necessary to have excess production capacity at each issuing location.

There are additional costs directly related to security policies, and include components such as secure delivery of all security supplies (e.g. blank IDs, security laminates, etc.), a vault to store supplies, destruction or collection of any defective IDs, and the cost to conduct regular audits of the supplies and ID issuance documentation. Further indirect costs are associated with additional staff training for equipment operation and routine maintenance, and for additional office space for the equipment and supplies storage.

Equipment maintenance that covers all issuing locations represents an additional cost in an OTC approach. Part of the service requirement can be handled by local staff (e.g. routine maintenance and cleaning) but the use of office staff adds to indirect costs related to time and training.

Central Issuance allows optimization of production equipment to meet daily issuance requirements for the entire ID program. Depending upon issuance policies, this process also provides greater flexibility in smoothing production peaks, with the result that the total equipment requirement will generally be lower than OTC. Delivery of finished documents may be a significant ongoing operating expense, and there may be a need for fraud control efforts to investigate any undelivered documents.

Central Issuance requires use of a secure facility with appropriate facility protection and security monitoring hardware and software. Some indirect costs should be associated with contingency or disaster planning in the event of a major event at the central site.

Other indirect costs with central issuance are lower, as there is generally more staff assigned for production, providing greater flexibility to cover vacations, illnesses, etc. Similarly, the indirect costs for auditing and dual control at a central facility are lower in comparison to the costs for those functions at every OTC issuing location.

D. Equipment and ID Production Technology

The choice of ID production technology for OTC production is generally constrained by costs, limiting alternatives to solutions that are generally:

- Simple to operate, with minimal operator intervention
- Relatively compact, and operate within an office environment
- Relatively lower in cost (in comparison to large-scale production equipment)
- Generally less flexible in the range of security technologies offered

Because of cost considerations, OTC ID production equipment is more likely to be the same or very similar to commercial off-the-shelf desktop printers, using many of the same supply items. The ability to create unique security features then may be more limited in an OTC environment. In addition to hardware considerations, there is also a need for an inventory tracking system at each OTC location to track daily usage of supplies and to plan replenishment. If security laminates or pre-printed blank IDs are used, there is also a requirement for vaults and increased access control security at each location.

A Central Issuance approach offers the widest latitude, allowing an agency to select from a range of security and personalization technologies. Centralized systems can range from custom-built systems to meet specific requirements to large-scale standard production equipment. For example, the Datacard® MX6000™ Card Issuance System is a high-speed modular card production system that can be configured to produce a range of features on a secure ID. Because of its high throughput and corresponding higher price, this type of equipment is best suited for central or regional production centers.

High capacity production centers can alternatively be configured with numerous networked desktop printers, similar to those used in an OTC environment. This approach generally involves a trade-off between a lower initial capital investment and increased labor and control concerns. As noted earlier, it may also limit the choice of security technologies available for personalizing the ID document.

In a centralized environment, production downtime and equipment problems are less visible to customers and under most circumstances can be managed without creating delivery delays. Peak volumes can be processed by adding production shifts.

E. Quality Control

Quality control is a critical issue for any secure document. If sub-standard documents are distributed, it becomes easier for fraudsters to pass off reasonable facsimiles of genuine IDs.

One of the primary benefits of an OTC approach is the opportunity to conduct visual inspection of every document produced. An ID can be checked first by the issuing agency official, and then by the document holder. As noted earlier, if there is incorrect or missing information, or if the photo or signature is not clear a replacement can be issued immediately and the defective ID destroyed. The challenge though is assuring that the same quality standards are enforced uniformly at every issuing office.

If any of the critical components (e.g. camera capture or ID printer) begin to deviate from initial configurations, it is possible for IDs to be produced that meet most of the quality standards but still are not uniform in appearance. A key example would be variation in colors printed on an ID, where the customer and agency official may not notice a deviation from standards.

Quality control at a centralized production facility will always be easier to manage. Staff can be assigned with specific responsibilities for quality assurance. In some cases specialized equipment can be utilized to automate the inspection process.

Combined or Hybrid systems require that identical documents are issued from OTC or centralized production equipment. The quality control process must assure consistency between documents produced at any location.

F. Program Security

An OTC approach creates significant management challenges to assure that key elements of the program are secure. Managing security across multiple locations will always be more complex, and introduces more opportunities for security lapses or breaches. Security policies and procedures must already be in place around data access at each location. Additional security issues tied to the OTC environment include:

- Administration of passwords or keys required to operate the equipment
- Protecting the ID printer from unauthorized use during the day, and from theft or use when the office is closed (if removed from the office, the printer should not be able to produce legitimate IDs without being re-installed by a government officer)
- Vault storage of blank IDs and/or security laminates, and daily procedures for removing and returning security supplies (enforcing dual-control procedures for activities such as vault access may be a management burden in small offices dealing with staff vacations and absences)
- Managing the application process to assure that all applicants are screened and authorized prior to issuance of an ID
- Tracking the daily usage of issued IDs, and storage of defective IDs
- Controlled disposal of any supplies (e.g. printer ribbons) which may retain images of personal data printed on issued IDs

Central Issuance requires use of a secured facility. Administration of security policies and procedures will be simpler than in an OTC environment as the staff is all in a controlled facility. A security background check can be done for only the staff requiring access to secured areas, and then access can be managed through an access control system. All activities, equipment and access points can be monitored, and security procedures customized to the facility and type of ID production chosen.

The major security risks in a Central Issuance environment are related to internal fraud. Security is generally improved by limiting the number of times documents are handled, reducing potential points of compromise. In-line highly automated personalization systems tend to provide greater control than using multiple steps during the document production process. Security policies and procedures must be in place to address the threats from internal fraud.

Summary

As shown in the following table, there are benefits and drawbacks for each ID issuance approach covered in this paper. The security advantages of a Central Issuance system are significant, and should be weighed strongly against any policy considerations which may favor an OTC approach. The EU Council and ICAO (International Civil Aviation Organization) both favor centralized production for high security documents such as passports and visas.

Table 1. Summary Comparison: OTC vs. Central Issuance

ISSUE	OVER-THE-COUNTER	CENTRAL ISSUANCE
Customer Service	**+ Immediate**	**-** Process/delivery delay
Enrollment and Applicant Processing	**-** Higher risk when done quickly	**+ More time for thorough verification process**
Cost	**-** Usually Higher	**+ Usually Lower**
Equipment and ID Production Technology	**-** Fewer choices	**+ More choices**
Quality Control	**+ Immediate (100%) inspection**	- Centralized
Program Security	**-** More complex	**+ Simpler at a single site**