

# 👉 ELECTRONIC SECURITY DOCUMENTS

TOMORROW'S TECHNOLOGIES WITH TODAY'S CHALLENGES

By Allan Harle, Chairman, Inspectron Holding plc.

By its very nature, the production of electronic documents such as ePassports, eID Cards and contactless smart cards is a relatively new industry. Whatever the application, the introduction of a chip into such documents brings challenges to manufacturing, management and security. More and more new security features are being incorporated, but the basic demands of production integrity remain the same. The traditional methods and skills appropriate to preparation of paper-based security documents must now be upgraded to allow for the IT aspect of the embedded chip.



The combination of variable data and personalization demand that each item is accounted for and verified, and that any errors, rejects or unusual manufacturing events are immediately identified and corrected. Traditionally this has involved reading and recognizing printed codes and data streams, using cameras, barcode readers and a variety of database and decision making software. With the addition of a chip to such documents, it has become necessary to add chip readers and associated security software to the solution set.

## Typical problem areas

Security documents must be perfect as government credibility is at stake. Where machines and human operators are involved during production, things can go wrong:

- The chip/inlay is often exposed to severe mechanical stress. Sometimes it breaks, and becomes unreadable;
- When printing, the document number gets out of synch with its other pages (e.g. wrong data on the right photograph page);
- When remaking damaged items, the wrong numbers are typed in, leading to missing or duplicate documents;

- Quality control is essential. With high volumes being made daily, it is not enough to rely upon human monitoring alone.

## Next generation security features

Security features are continually under development, with the target of making fraud more difficult. But the document itself must be used by anyone, and therefore needs to be as simple as possible. As the chip begins to dominate these features, it becomes necessary to relate the chip itself to the document structure, and the variable data contained in it.

## What happens if a chip is dead after the document has been issued?

The purpose of a chip embedded into a document is to add security and more data capability. ID Cards and passports must be usable for up to 10 years, and they must outlast potential abuse from day to day exposure to the real world.

One particular problem arises if the chip cannot be read during its operational lifetime. Normally this can be for one of two reasons: either the chip, or its associated electronic apparatus, is damaged through wear and tear, or it has been purposefully damaged by

☞ someone with bad motives. A security officer or border agent will normally rely upon the printed information to decide upon what happens next, but more importantly, he or she will be required to note the offending document for forensic evaluation.

The relationship between ease of inspection and adequate levels of security demands that simple solutions are used wherever possible. If a document has been falsified, it is necessary to find out when and where this may have happened. One valuable tool in this process allows the investigator to trace the original source of the main component of the document: the inlay.

### **The inlay birth certificate – tracing a dead chip**

When an inlay is manufactured, possibly months before it goes into a security document somewhere else

---

**The purpose of a chip embedded into a document is to add security and more data capability.**

---

in the world, it is tested for electrical operation. This is the first time the chip becomes viable for use in a later document. When the chip is energized for the first time, its unique serial number becomes available for

recording. An interesting innovation allows this number, together with other manufacturing history data, to be recorded within the inlay for immediate future reference. This is achieved by printing the data in barcode format, using a specially developed magnetic ink, alongside the chip on the inlay. When the inlay is later built into a security document, its barcode is hidden within the laminated document material. Thus it is available to be swiped with a special reader for the life of the document. If the chip is dead, this barcode provides a tracing route to confirm the provenance of the document for forensic purposes.

### **Personalized holograms**

Holograms have been in use for some time in the security document environment. To date, they have

---

**Holograms have been identical, and act as a security feature for the materials used in the document.**

---

been identical, and act as a security feature for the materials used in the document. It is now possible to 'print a



*Variable Data can now be embedded in a high quality Hologram.*

hologram on demand' and embed into it a series of variable data. In this way, the material security aspect is further enhanced by tying each hologram to the actual item to which it is attached.

### **Putting this all together**

During document manufacture, when the inlay is incorporated, its birth certificate is read and the number is passed to a machine which 'burns' a personalized hologram. This hologram now contains a copy of the birth certificate, which can be read by human eyes. Once this hologram is attached to the document, it enables the inspecting officer to simply compare the hologram number with the 'birth certificate' to establish whether the document is genuine.





Source: Bundesdruckerei GmbH, Berlin

In the background, a manufacturing tracking system has recorded all important events of the document's manufacture. This database is available for future investigation, and can be accessed to help identify the provenance of any document.

A local 'quick check' comparison of the 'birth certificate', printed data and hologram, supported by the manufacturer's database if necessary, which enables the inspector to continue his or her work with ease, whilst relying upon the latest and best available security features.

### Tracking during manufacturing

An electronic security document can be described simply as a traditional paper document with a chip built in. During manufacture, it is necessary

to ensure that the chip is readable, that the printed personal and variable data is readable and correct, and that a permanent record of the two related pieces of data is created.

If a unique item is rejected during manufacture, it is necessary to re-make it later. This can often be complicated, since there is always the risk of a mistake in setting up the exact remake criteria, and the need to reconcile the remakes to the original production batch.

Because of the security involved, it is also necessary to account for all rejected and wasted production items.

Human beings can read printed numbers, but they need help when it comes to identifying chips!

Before the chip can be built into a document, it must be built into an inlay, which includes the antenna and a suitable mechanical support. Inlays are typically made by specialist manufacturers, and supplied in packs to the document manufacturer. Each pack will usually be delivered with a packing list, containing information, sometimes called a manifest, about the pack and its contents.

A further complication is the need to ensure that if the document is stolen or lost, security items and components are not useful if they fall into the wrong hands. This is often achieved by adding electronic keys and special software to the chip. These keys are used typically when items move from one secure area to another, for example between inlay supplier and document manufacturer. When tracking each item, it is often necessary to use these keys, sometimes to change them, and certainly to account for them.

### The manufacturing audit trail

To overcome these challenges, a computer-based tracking system follows each stage of production. Sensors, whether cameras, chip readers or other information gathering devices 'watch' each item as it is

produced. Real time decision-making logic makes a good/bad determination and the item continues or is rejected. At all stages, an audit trail is recorded,

---

**That components are not useful if they fall into the wrong hands is often achieved by adding electronic keys and special software to the chip.**

---

so that, at the end of a batch, all good, bad and rejected items can be reconciled, and a complete history of the document's source is recorded for future reference.

### Summary

The ever increasing volumes of personal ID documents demand ease of use, accuracy and the highest level of data integrity. Confidence by the general public must be maintained. Behind such demands lies a specialist industry, where security, operational experience and the flexibility to respond to evolving technological innovations mandate perfection of product and record keeping. ■