Cryptographic Credit Control in Pre-payment Metering Systems

Ross J. Anderson

Cambridge University Computer Laboratory
Pembroke Street
Cambridge CB2 3QG
England
rja14@cl.cam.ac.uk

S. Johann Bezuidenhout

Eskom
Megawatt Park
Sandton
South Africa
BEZUIDES@elec.eskom.co.za

Abstract

We describe the successful introduction of cryptology into a new application area - protecting pre-payment electricity meters from token fraud. These meters are used by a number of utilities from Scotland to South Africa, and they present some interesting security challenges.

1 Introduction

Cryptographic systems have been used for centuries by military and diplomatic organisations to keep messages secret, and the debate on cryptography continues to be held in the context of message secrecy [LKB+]. Over the last decade, however, these traditional systems have been overtaken, in both value and extent, by commercial applications whose goal is to prevent fraud by making payment tokens and transaction records difficult to copy or alter. Automatic teller machines were the first major instance of this and have been followed by satellite TV decoders, road toll tags, cellular telephone identity modules, building, safe and car burglar alarms, and remote replenishment of devices such as postal franking machines.

For many of these new systems, the implementers re-invent their own cryptography and operational practices from scratch. Often the cycle is one of *attempt - fail - appoint consultants - try again ... fail ....* It appears that access to experience, expertise and information could in many cases have saved a lot of money.

There is still a shortage of published information on how secure systems are constructed, and on the reliability problems they encounter in practice. Three prime contributing reasons to this shortage are:

- the perceived need for design secrecy;
- the perceived need for operational secrecy, and in particular the reluctance of most owners of commercial cryptographic systems to discuss the problems they have encountered and how these have been overcome;
- the fact that most commercial cryptographic applications have, until recently, been limited to a single environment - banking.

Recent work [A1] has documented some of the ways in which banking systems have been defrauded, and shown that their security failures are mostly due to opportunist exploitation of design and management blunders. However little is known about the problems experienced with other commercial cryptographic systems.

2 The Application

The purpose of this paper is to provide the security community with a further documented example of cryptographic payment system vuneralibilities and failures by examining a new and rapidly growing application. This is the use of cryptographically based tokens in pre-payment electricity meters.

These tokens can take the form of an EEPROM key device, a memory ('smart') card, a disposable cardboard ticket with a magnetic strip, or a 20 digit number printed on a slip of paper which is entered at a keypad on the meter. They let customers purchase credit from the electricity utility and carry the credit to the meter in their home. The token instructions are encrypted to make forgery more difficult.

Pre-paid electricity meters are installed in a number of places around the world, including Sao Paolo, Brazil; Brazzaville, Congo; Namibia; the Ivory Coast; and by various utilities in Europe (the London Electricity Board, Scottish Power, East Midlands Electric-

ity, SEEB and Electricité de France). However the largest (and most rapidly growing) single installation of pre-paid electricity meters is in South Africa, where it is a national development priority to double the number of households with electricity by 1999.

2.1 The Politics and Economics of Power

In 1990, about 2.5 million houses that were electrified in South Africa, and estimates were that around 3 million further homes would have to be electrified by the end of the century. The development of low cost electricity pre-payment meters (called Electricity Dispensers or EDs) had started in 1987, primarily as a means to provide customers with electricity without requiring an up-front deposit, and without their getting into debt.

However, with political reform during the 1990s, it became a priority to electrify homes in black townships and rural areas [B1]. The National Reconstruction and Development Programme set out by the government in 1994 aims to supply 2,550,000 more households with electricity by the end of 1999 [B2], and this means that over 1600 houses will be electrified every working day for 6 years. Already, between 1989 and 1994, the national electricity utility (Eskom) had electrified and installed pre-paid meters in 650,000 homes, and local authorities, who act as distributors in many areas, had electrified a further 150,000 homes during this period.

A decision was taken in 1988 to concentrate on pre-payment meters. Such meters had attracted some interest since 1986 when political withholding of payment became widespread in the townships; with political liberalisation the motive changed to one of economics. Reading meters is expensive, especially where access is difficult; many rural communities have no postal service or even house addresses, so a credit system would mean manual bill delivery and cash collection. Coupled to all this there is often a 90-day billing cycle which would cause many poor people to go into debt. With a national priority that 2.5 million homes should be electrified by the end of 1999, pre-payment metering was the only option.

At the end of 1994, about 850,000 prepaid meters had been installed in South Africa; by the turn of the century, over half the households in the country will be using them. The additional homes will have been electrified at an average cost of US$1000; this includes reticulation hardware such as overhead cables and transformers, labour, a pre-payment meter and a 'readyboard' which typically contains an earth leakage circuit breaker and two or three 15 Amp socket outlets. For this the customer is only charged US$15; the difference is recovered over 15 years through the tariff charged.

On the revenue side, the goal is to keep collection costs to under 5% of turnover. With 1000 customers for the average retail sales outlet and an average sale of US$20 per month per customer, it is not possible to support a staffed office; but a sales commission provides a useful extra income for a local agent, such as a shopkeeper. Most token sales are thus made through these agents - of which there were around 800 at the end of 1994.

The longer term goal is to automate the sales of tokens. Investigations are proceeding into the use of bank ATM networks, automatic self-service machines that can recognise bank notes and dispense tokens, and interfaces with a fielded system of smart card based electronic wallets [A2] [B3].

On the capital side, importing meters from Europe would have cost two to three times what it is costing to have them made locally. Eskom set out from the beginning to develop local suppliers, with the result that there are now six qualified manufacturers of locally made meters.

2.2 Social Aspects

Electrification has had many unexpected political and economic side-effects. One definite result has been a huge growth in television sales; in some areas up to two thirds of newly electrified customers buy a set, bringing fortunes to importers. This is expected to provide a major boost to education efforts in a country where the literacy rate runs at about 50%.

Research has also been conducted into the social aspects of rapid electrification, and in particular into the relationship between Eskom and its new mass client base [P1]. This showed that the most important customer priority is that the system should be trustworthy. This does not just mean the computer security aspects; customers expect reliability from the tokens, meters and physical electricity supply. They also require convenient and available points of sale and courteous staff who are able to deal with customers of all ages (children are often sent to buy tokens). Yet experience from an operational and risk perspective has shown that security is still a significant part of the project.

3 Pre-payment Meter Security

The transfer of value from the point-of-sale to the meter takes place through a token, which is bought by the customer from a vendor for cash, taken home and

then entered into the meter in the customer's house. The customer is then able to consume electricity to the value of the credit contained in the ED, after which the ED interrupts the supply. A token is issued for a unique meter and should not be able to be used in the wrong meter (or in the right meter twice).

In 1987 equipment suppliers were encouraged to innovate and produce low cost pre-payment electricity meters. They designed proprietary non-standard products and then set out to sell them to the municipal authorities. This freedom to innovate led to a low cost product as well as the development of the numeric token.

By 1990 it had become clear that there was wide variation in technical quality (including security) and that the electricity supply industry would have to develop and impose some standards, not just to develop the supplier base, but also to avoid the need to maintain a large non-standard meter population. It motivated a close study of the security and robustness of the installed meter systems.

3.1 Environmental Robustness

Robustness was originally a matter of contract between the equipment supplier and the local electricity distributor: a broken scheme could lead to a claim for damages. In practice, the electricity distributors did not know how to assess the physical (and logical) security of the competing products, and the quality of protection varied quite widely between suppliers.

A number of problems were identified during 1990 - principally due to field experience:

Lightning protection: severe thunderstorms are common in the South African summer, and meters have to be much better protected than in Europe. To aggravate the problem the majority of meters are connected to overhead reticulation systems. The pre-payment meter has been described as a microprocessor with a 3 kilometre lightning conductor attached!

Tamper protection: Initial installations showed that some of the proposed schemes were inadequate:

- one of the enclosures could be opened by a brisk karate chop;
- another of the early vendors arranged that any tampering would short the live and neutral feeds together and trip the feeder circuit breaker, which would cut off perhaps 40 houses. The idea was to create a social pressure against meter tampering, but this was somewhat misplaced;
- it was also possible to insert a knife or a live cable into the card throat of one meter type and destroy the electronics immediately underneath, which had the effect of giving unlimited credit.

Fortunately, the fragmentation of the market into many small areas using incompatible meters prevented knowledge of such tricks from spreading too widely before the issues were resolved. This was a quite unexpected benefit of the four-colour theorem [AH]!

Temperature: South Africa has a wide variety of climates, from alpine in the Maluti mountains through subtropical in Natal to desert in the Northern Cape. Temperatures can range from subzero to 45^0C or more, and again it was found that international standards for indoor credit meters were quite inadequate, especially where meters were being installed in informal housing.

3.2 Standardisation

The experience gained from the resolution of these initial problems led to the development of a national standard, SABS1524 part 1 [SABS], which at present appears to be the only national standard for pre-payment meters in the world. This covers the hardware and functionality of the meter, and has been offered as the basis for an international standard for pre-payment electricity meters to WG15 of IEC TC13, formed in September 1994.

SABS 1524 was based on a draft IEC standard for electronic meters, and covered the hardware functionality. However, the standardisation of the token information and its encryption method were not specified. This meant that each of the six active suppliers used whatever algorithms and formats they felt disposed towards. As a result, hundreds of thousands of meters were fielded using one of six different token information schemes. To add to the logical diversity, the physical token formats also differed from one manufacturer to another.

There was some benefit to this diversity - many different ideas were tested in parallel, moving the prepaid meter industry in South Africa rapidly up the experience curve. However, all the vendor equipment was manufacturer specific; buying meters from a manufacturer meant buying its vending equipment as well. This meant that the manufacturers had 'captive' sites.

This helped motivate the engagment of the first author in 1991 to carry out a preliminary study, during which the problem of standardising the token information (including encryption algorithms and protocols) was formally identified. This led to a project to standardise the token information and its associated security features [BJ], which was carried out from June 1992 through to December 1993, with further assistance from the first author and other experts. The resulting document, called the Standard Transfer Specification [STS], is now in use; meters complying with it have been in production since June 1994.

3.3 Cryptography

The novel cryptographic feature of the meter system does not have to do with the details of algorithms or protocols, but rather with the fact that there is no backward communication channel from the meter to the sales point. This may be a feature of other systems too, from satellite TV decoders to the safety mechanisms for nuclear warheads, but we are not aware of any unclassified technical exposition of the design (or operational failure history) of these systems.

A theory paper on forward information verification in pre-payment meters was published in 1992 [K]. The client purchases power from a sales agent using an identification card in ISO magnetic strip format which contains his unique meter number ID. The processor in his meter has a cryptographic key K_{ID}; and the agent also has K_{ID} (in fact, the typical system has a vendor key K_V and derives the device key when needed as $K_{ID} = \{ID\}_{K_V}$).

Thus the agent can use K_{ID} to encrypt a credit or other instruction for encoding on the meter token. In the STS standard, this may be either a number of 20 decimal digits, which is supplied to the customer on a receipt and entered at a numeric keypad, or a string of bits encoded on a disposable magnetic ticket conforming to ISO 7810/11/12 (ie similar to a subway ticket). The entered token data is then decrypted by the meter, the plaintext parsed and the instruction decoded. The typical instruction increases the credit register by a certain number of kilowatt hours. There are also other instructions such as engineering test transactions and key changes that can be issued to the meter.

The use of number-based tokens in electricity meters is unique to South Africa (although it is used in postal franking machines in the UK). The main benefit is that it allows the customer to purchase power over the phone; engineering staff can also get test and emergency credit tokens in this way while in the field. In the future, power may be purchased from supermarket checkouts and ATMs; the 20-digit code can also be printed on the transaction receipt without any need to fit token encoders.

There were initial worries about whether the number system would cause problems with illiterate customers. This turned out not to be the case: 'everyone can use a phone'. Numeracy is not an issue in South Africa, especially among children, who are often sent to buy the tokens. One interesting discovery was that the error rate was significantly reduced when the 20 digits were printed on two lines (3 and then 2 four-digit groups) rather than all on one line [P2]. When the 5 groups were printed in a row, the centre (3rd) group exhibited an entry error rate an order higher than the other groups. This was ascribed to the customers' inability to locate the digits in the centre of the string.

The cryptographic algorithms in use have included proprietary schemes as well as variants of DES [NBS] and Lucifer [F]. Because of the extreme price sensitivity of the meter, at least one manufacturer chose a Lucifer variant over DES for code size reasons (250 versus 800 bytes). Now Lucifer can be broken with about 2^{36} plaintext-ciphertext pairs [BB], but as perhaps 5,000 blocks will ever be enciphered under any one meter key, the algorithm's differential weakness is not an issue. In fact, the algorithms used on the link from the vending machine to the meter still vary with old meters, but the STS standards are imposed on new meters and from the vending machine upwards in the hierarchy.

Key management is much more critical. The initial meter key K_{ID} is loaded in a secure cell at the factory, but doing key changes turned out to be troublesome in practice with either token technology. As tokens are often purchased and hoarded as a means of expenditure control, the customer has to use all his existing tokens before entering a key change token. It was considered whether to have the equipment remember the previous key, but this was rejected during the STS design process as it would mean that two key changes would be required to flush a compromised key from the system.

Finally, as well as preventing token forgery, the cryptography must be well integrated with several more complex security functions: to impose central management on a network of diverse vending systems; to control credit; to detect fraud by balancing transactions and cash; to revoke sales agents when required; and to find secure ways of conducting sales through

third parties such as banks. Since there will be around 4,000 to 5,000 token vending points by the end of the century, these are sizeable problems.

3.4 Security Problems - First Phase

However, it is not enough to have a system which possesses physical and electrical robustness, and a good cryptographic design. Implementation detail and operational procedures are also important; in fact, this is where computer security failures usually occur in real systems [A1]. The first author was therefore engaged in 1991 to examine these aspects.

A number of early meter and vending system designs were examined in detail, and a number of problems were found:

- one type of meter could have the tariff code set to a minute amount by vending staff, so that it would operate for an almost indefinite period;
- another could be attacked by vendor staff manipulating refund coupons. A refund could be granted, but the refunded token still used, because of the lack of a return channel from the meter to the vending system;
- another could be fooled by duplicate coupons. It remembered only the last coupon serial number entered; thus by alternately entering duplicates of two previously used coupons it could be charged up indefinitely;
- the robustness of the physical token erase mechanism varied quite considerably between vendors. One test meter did not erase them at all;
- one type of credit dispensing unit had a supervisor password with which its credit could be indefinitely replenished. The theft of such a unit, together with its password, would force replacement of all the meters it could sell to;
- there were bugs in the balancing mechanisms of some of the vending systems, as well as the usual deviations from good computer security practice such as poor password management mechanisms, weak separation of duties and inadequate audit facilities;
- the structure of the databases used to store client information and to match the meter administration to that of the power supply varied considerably between the meter vendors, which made a unified system for balancing power and cash difficult to design and operate.

These faults were fixed, and it became policy that all the cryptographic operations should be done in a secure processor, now called a Vending Secure Module (VSM), which can be implemented in a secure microcontroller or a smartcard. The principle was established that each VSM should contain a credit counter, the replenishment of which should require a transaction from a superior unit in its credit control hierarchy.

It was also established that the management functions of the vending systems should interface with the utility's own systems in order to facilitate the balancing of power and cash. It was foreseen that once the system became more complex, it would no longer be feasible to simply balance a moving average of sales against feeder meter readings, so further warning signals (such as minimum purchase level records) also had to be implemented.

It was also decided to start work on mechanisms for vending tokens for meters in other areas. This is the utility equivalent of automatic teller machine networking; the motive in South Africa is that working people often commute for two hours or more from their home to their place of work, and find it convenient to buy tokens in town rather than from a local shop.

The obvious problem this creates is that, in busy centres like Johannesburg, a vending machine might have to hold cryptographic keys for as many as fifty different vend areas. How could the resulting key exposure be controlled?

3.5 Security Problems - Second Phase

The standardisation process had to be handled carefully in order to avoid losing the confidence of the 'winners' of the technological race, and it was 1993 before a follow-up security study was undertaken to look at overall standards. By then it had become clear that multiple sales points would be needed, and some work had started on standardisation of algorithms and protocols.

The strategy adopted was inspired by the history of bank ATM networking, and was to insist on the use of standard protocols at all levels in the system. Standards were also set for the format of the meter tokens, as either 20 digit magic numbers or 66-bit subway type tickets conforming to ISO 7811/2; and for an ISO magnetic strip card to identify the customer to the vending system. As remarked above, this approach evolved into the STS specification at the end of 1993.

By the time the second study was undertaken, field experience had brought further problems to light.

Functional error: one type of meter could be set to maximum credit if the voltage was reduced to 160 - 180V. This bug was due to one wrong assembly language instruction in the meter controller; its effect was to motivate customers to throw chains over the 11KV feeders in order to 'credit' their meters, and disrupt service to neighbours in the process. Fixing this problem involved the manufacturer in swapping out its installed meter base.

Customer operational: people who ran out of credit would report the meter as broken. Such reports were also made in the case of a protective trip. Education of customers and maintenance staff was the answer to this expensive operational problem.

System operational: balancing power and cash was made difficult by the fact that the dates on which feeder meters were read was not accurately known. Staff would vary their schedules, with the result that instead of showing a steady low level of technical losses, an area might show a large loss in one accounting period and sometimes even a gain in the next. The current remedy consists of procedural controls.

The overall experience confirmed the first author's ATM threat model [A1]: real security breaches in payment systems result from errors by development staff or in management procedures, which may be quite obscure, but which are accidentally discovered by users and exploited opportunistically.

It also confirmed the value of design diversity. With a number of different designs, even a catastrophic failure has limited effects, and geographical fragmentation helps here too. Another aspect is the ability to get a supplier to fix a problem. With only one supplier, protracted negotiations might have ensued; but with six competing suppliers, the balance of power favours the system operator.

In any case, the meter failure rate is now generally low, and security work is now focused on mechanisms for key management, remote token purchase, credit management and interfaces with banking systems.

3.6 Lessons Learned

The general lessons emerging from this exercise are:

1. make the end user understand that the buck for the correct operation of the system stops at his or her doorstep, and that this accountability can not be contracted out;
2. use an appropriate project engineering discipline;
3. be extremely sure that the planned business process is viable before starting crypto design. For example, off-line key update can cause havoc with a design that should have had this as an initial constraint;
4. someone has usually applied the technique that you need before - spend time to find them! Blank sheet approaches are dangerous;
5. accept that crypto work is not cheap and takes time - initial estimates were an order of magnitude out;
6. use trusted encryption algorithms where possible, not just for assurance against cryptanalysis, but also for due diligence reasons;
7. accept that there are no 'plug-and-play' solutions available for distributed key management, which is not a mature applications field (although there may be interesting research ideas and prototype products);
8. do not be afraid to use multiple experts from both industry and academia. One expert alone can not usually span all the issues from the perspective of both theory and experience, and even the best can make mistakes;
9. do not be afraid to use multiple suppliers, but be careful about the trade-offs between design diversity and compatibility;
10. use simulators to test communication protocols, especially those written by independent third parties, as they often find the hard to detect common-mode errors which arise when the same people design and implement a system;
11. expose the design to as much security review as you can, especially if the reviewers are independent peers (the exposure of STS to the review of six manufacturers definitely added value);
12. accept that small mistakes with large consequences will still creep in, no matter what is done to stop this. Thus, in addition to experts and methodologies, one absolutely needs prolonged field testing. This is where many errors and impracticalities will first become apparent.

With the formation of the IEC working group mentioned above, the opportunity now exists for utilities and meter vendors in other countries to benefit from this experience.

4 The Medium Term

In accordance with the principle that robust security systems are explicit ones [A3], the Common Vending System (as the network is now called) has an explicit threat model and security goals. The details are confidential but the gist is that large scale threats above the level of the meter-token dispenser link are likely to involve either insider dishonesty or litigation. The security mechanisms must therefore isolate all the players from each other, and be able to discover losses quickly.

A surprisingly large number of transactions need to be protected. These include not just sales to customers, key management and credit replenishment, but also all transactions which alter credit limits or tariffs. The trusted computing base consists of the VSMs in the vending systems, plus a number of secure processors which are specially programmed for use by the electricity distributors.

The detailed design of the system follows established banking principles. End-to-end authentication is used wherever possible; and it is an explicit goal that the system should recover from the compromise of any secure module with a minimum of disruption.

Two problems which emerge from this exercise, and which are likely to affect other industries using cryptographically based vending, are vendor revocation and the control of third party credit.

4.1 Vendor Revocation

Recent political changes make it possible that a large number of municipalities and former homeland authorities will cease vending power in the next few years and transfer their systems to metropolitan authorities and/or Eskom. When this happens, how can one be sure that no official has made off with a credit dispensing unit (or its keys) which he might continue to use for his own benefit?

At present, the fine granularity of vending areas means that the damage which such a villain could do is fairly limited. However, once vendors can sell on each others' behalf, one must be sure that proper controls are in place. Ideally, each key in the system should have a limited life, so that even if the tamper protection of a vending system is broken, it does not become necessary to replace a large number of meters.

To achieve this, the meter must clearly contain some secret which is not known to the vendor. A simple solution is to use an initial factory key K_F to update the meter key monthly, so that for example $K_{ID}^{JULY} = \{K_{ID}^{JUNE}\}_{K_F}$. However, it is then no longer possible for K_{ID} to be derived from the vend key K_V unless one uses public key techniques, such as a one-way function based on the discrete logarithm problem. The cost of upgrading the meter controllers to cope with modular arithmetic would be prohibitive, and so the currently favoured solution is to supply each vending system with a database of time limited keys. Keys for each time period are encrypted under a key which is unique to each vending system (and time limited) and which is only released provided that the vendor remains in good standing.

The main point of this scheme is that people who wish to purchase power can do so as individuals rather than as members of a group. Each customer can be invited to nominate two alternate vendors, and her meter keys will be sent to that vendor encrypted under the appropriately time limited vendor key.

4.2 Third Party Credit

The most serious problem, and the one with major ramifications for the smartcard industry, is that of controlling transactions by third parties. If tokens are sold by third party devices such as bank ATMs or supermarket checkout terminals, how can we be sure that the operator is being honest about how many have been sold, further than to simply trust them?

There is already some experience of token vendors damaging their credit dispensing units (or claiming that they were stolen) in order to avoid handing over their takings to the electricity distributor. It is also well known that disputes over the security of ATMs can be heated and difficult to resolve [A2] [A4], and that both the law and banking practice vary quite widely from one country to another on this point [MR]. With a system which has no return channel, there is no way for the operator to know if a third party sells a token and then destroys the evidence of this sale.

The significance of this does not seem to have been fully grasped yet by industry. Smartcard promoters have for years envisaged a world in which their cards become multifunction 'electronic wallets', which are not limited to ATM and EFTPOS transactions, but also double as transport tickets and parking tokens; count up air miles; control utilities; manage student, corporate and bulk discounts; and handle monthly credit payments for appliance purchases.

It really would be ideal for the utility industry if everyone had a smartcard; it could provide a return channel to take meter readings, usage statistics, tamper occurrences and so on back to the point of sale. However, Eskom's experience in this regard has so far been negative; a proprietary meter smartcard token

was considered in 1991 but not adopted. The alternative - a multifunction smartcard - was also considered, but has the following serious drawbacks.

Infrastructure: a massive infrastructure will have to be in place before electronic wallet smartcards are successful, and this will be extremely expensive. For funds to be transferred a terminal is necessary, unlike with cash which is simply handed from one person to another.

Utility reduction: even once a large number of terminals have been fielded, there is a reduction of utility when one commits funds to an instrument such as a smartcard which can only be used to buy a limited number of things. This utility reduction is marked among the poor, who might well have to commit over half their wealth to a card which would only be used for rent, power and transport ticket payments.

Standardisation: the functional specification for smartcards (ISO DIS 7816-4) is not yet stable. This implies reprogramming all meters using smartcard tokens if the standard changes and bank issued smartcards follow.

Politics: of the inter-organisational and inter-sector variety. Who will control this universal card? The banks want to, but so do the retailers. In some countries, the government wants to drive the project and use it for tax collection and law enforcement. Meanwhile, South Africa's electrification program is a national priority and it cannot be held up by bickering among third parties over who will control the mailing list!

Legacy of the Dompas, or pass book: in South Africa, there was for many years a system of identity books which contained all the information about an individual which was of interest to the state - identity, racial group, marriage certificate, residence permit, driving licence, gun licence etc. A multifunction card might well be seen as a return to the bad old days.

Trust: how can one trust the smartcard's primary operator not to lose transactions? How can complaints be arbitrated?

We might use purely technical means to tackle the trust problem, which is essentially that of how to provide a reliable audit trail. For example, we might draw inspiration from digital cash schemes [C] and have both the bank and the utility contribute a processor to a secure device. We might also use a mixture of technical and contractual measures: the bank might simply insure against losses, with a sampling system whereby a number of households were monitored closely; or it might agree to pay compensation equal to the expected loss whenever a card or part of an audit trail goes missing.

However, a moment's thought will indicate that shared systems could still give rise to fearful rows. If the primary operator wants to change the card design to accommodate lottery ticket sales, and this means cutting the space available for the electrical audit trail, then can the utility veto this? If so, would the primary operator ever let their system be shared and if not would a utility want to share it?

It may be significant that smartcard vendors have been trying to sell multifunction cards for many years, but with little success. Perhaps the whole concept of shared service tokens needs a rethink.

5 Conclusions

The majority of fielded cryptographic systems are not used in message secrecy applications, but to provide trust and to prevent fraud. Yet attacks keep on being reported on these systems, which include satellite TV decoders, automatic teller machines and utility meters. Many of the frauds seem to be due to their designers' ignorance of how similar systems failed.

We have described the largest single installation of pre-payment utility meters in the world. This has been running for some five years, and considerable experience of security issues has been accumulated.

It turned out that the threats which led to real losses followed much the same pattern as had been previously reported for automatic teller machines - errors in design and management left loopholes which were exploited on a more or less opportunist basis by both operators and customers. South Africa did end up with a robust system, but this took several years of field experience with equipment from a number of competing manufacturers working in parallel.

The most difficult remaining problem is how to control a system which involves more than one main player. At present, there is no obvious solution, and this problem may extend to make multi-issuer tokens pointless. At any rate, system builders might like to consider whether a single smartcard serving as a multiple service token is even a desirable goal.

References

[A1] RJ Anderson, "Why Cryptosystems Fail", in *Proceedings of the 1st ACM Conference on Computer and Communications Security* (November 1993) pp 215 - 227

[A2] RJ Anderson, "UEPS - A Second Generation Electronic Wallet". in *Computer Security - ESORICS 92*, Springer Lecture Notes in Computer Science v **648**, pp 411 - 418

[A3] RJ Anderson, "Why Cryptosystems Fail", in *Communications of the ACM* v **37** no 11 (November 1994) pp 32 - 40

[A4] RJ Anderson, "Liability and Computer Security - Nine Principles", in *proceedings of ESORICS 94*, to be published by Springer in the Lecture Notes in Computer Science series

[AH] K Appel, W Haken, "The solution to the four colour problem", in *Scientific American* v **27** no 4 (1977) pp 108 - 121

[B1] SJ Bezuidenhout, "Serving the needs of newly electrified customers with the latest in electricity sales systems - the retail business", in *53rd AMEU Convention, Durban* (October 1993)

[B2] SJ Bezuidenhout, "20 questions and answers about EDs", Eskom document sjb94/07/01

[B3] SJ Bezuidenhout, "Card Use in Electricity Payment", in *Proceedings of 2nd Plastic Cards Conference*, Johannesburg (November 1993)

[BJ] SJ Bezuidenhout, PA Johnson, "Towards the Standardization of Electricity Sales & Dispensing Systems in South Africa", in *Proceedings of SAIEE Electricity Tariffs and Metering (ETAM)* (March 1992)

[BB] I Ben-Aroya, E Biham, "Differential Cryptanalysis of Lucifer" *Technical report no* **753**, *Technion, Haifa*

[C] D Chaum, "Encrypted IDs for Digital Privacy", in *Scientific American* v **267** no 2 (August 1992) pp 76 - 81

[F] H Feistel, "Cryptography and Data Security", in *Scientific American* v **228** no **5** (May 1973) pp 15 - 23

[K] GJ Kuhn, "The Use of Secret-key Techniques in Forward Information Verification", in *Proceedings of 1992 South African COMSIG* (IEEE) pp 165 - 168

[LKB+] S Landau, S Kent, C Brooks, S Charney, D Denning, W Diffie, A Lauck, D Miller, P Neumann, D Sobel, "Codes, Keys and Conflicts: Issues in US Crypto Policy", *Report of the ACM US Public Policy Committee June 1994*

[MR] E McCullagh, I Ryan, "Who pays the bills?". in *Cards International no* **108** *(April 25 1994)* pp 8 - 11

[NBS] National Bureau of Standards, *'Data Encryption Standard'* FIPS Publication no **46** (January 1977)

[P1] MW Pickering, "Customer Acceptance of Prepaid Metering Systems", in *Proceedings of SAIEE Electricity Tariffs and Metering (ETAM) March 1992*

[P2] RH Price, STS numeric token field research (1993)

[SABS] South African Bureau of Standards, *'Standard Specification - Single-Phase Electricity Dispensing Systems Part 1: Electricity Dispensers'* SABS **1524-1:1990**

[STS] Standard Transfer System, Eskom 1994