On the Reliability of Electronic Payment Systems

Ross J. Anderson
Cambridge University Computer Laboratory
Pembroke Street
Cambridge CB2 3QG
England
ross.anderson@cl.cam.ac.uk

S. Johann Bezuidenhoudt
Eskom
Megawatt Park
Sandton
South Africa
johann@aztec.co.za

Abstract

One of the problems facing the builders of the 'Information Superhighway' is how to charge for services. The high costs of billing systems suggest that prepayment mechanisms could play a large part in the solution. Yet how does one go about making an electronic prepayment system (or indeed any kind of payment system) robust? We describe some recent systems engineering experience which may be relevant — the successful introduction of cryptology to protect 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 reliability challenges.

I. Introduction

Robust payment mechanisms will be needed if high speed network services are to realise their full potential, especially in consumer markets. One of the more serious problems may be the cost of accounting: utilities and computer bureaux find that billing systems can easily devour 20% of revenue. The exact figures vary: some telephone companies spend 30% of their revenue on administering a traditional billed system, while well run power companies might spend only 10%. So alternatives, such as prepayment systems may come to play a significant role. But not all prepayment systems are economic; in the UK, parking meters consumed 70–80% of revenue in coin collection, maintenance and administration and are now being replaced by 'pay-and-display' systems.

So it is important to know how to build prepayment mechanisms that are both reliable and cheap to administer. This paper describes a very large fielded system in which we successfully used cryptographic techniques to construct a robust prepaid accounting system with low overheads. It is not untypical of other micropayment mechanisms, which may be used as phone tokens or digital stamps [19]; these will probably also be based on cryptography.

Cryptography — the art of codes and ciphers — has been used for centuries by governments to keep messages secret [15]. Over the last decade, however, these systems have been overtaken, in both value and extent, by commercial systems. Automatic teller machines were the first major application; they have been followed by satellite TV decoders, road toll tags, cellular telephones, burglar alarms for buildings and vehicles, and remote replenishment of devices such as postal franking machines. Most commercial systems are less concerned with secrecy than with the authenticity of users and the integrity of transactions.

Reliability has been a problem for many of these systems. The implementers often invent their own cryptography and operational practices from scratch, and the cycle is often one of *attempt — fail — appoint consultants — try again ... fail ...*. Access to experience and expertise could have saved a lot of money; yet there is a serious shortage of published information on how secure systems are constructed, and on the reliability problems they encounter in practice. The prime reasons for this are:

- the perceived need for design secrecy;
- the perceived need for operational secrecy, and in particular the reluctance of most system owners to discuss the problems they have found and fixed;
- the fact that most commercial cryptographic applications were until recently limited to banking.

One of us documented some of the ways in which banking systems have been defrauded, and showed that their security failures are mostly due to opportunist exploitation of blunders in system design, implementation and management [1]. But little was known about the problems experienced with other commercial cryptographic systems.

The purpose of this paper is to provide the systems engineering community with a further documented example of electronic payment system vulnerabilities and failures by examining a new and rapidly growing application. This is the use of cryptographic tokens in prepayment electricity meters.

II. The Application

Slot meters were used in Britain for many years. The customer would insert a coin and receive a certain amount of electricity or gas, after which the meter would interrupt the supply. This was convenient for bankrupts and welfare claimants, as well as in shared premises such as student hostels where a slot meter was often used to control the water heater. However, the technology was less convenient for the utility; in addition to the high costs of coin collection, the meters were the target in 54% of theft from some local authority housing [21] and the collection staff were also vulnerable to attack [6]. These problems and their associated costs motivated the development of meters using electronic tokens.

The new meters still interrupt the supply when the customer's credit runs out, but the credit is transferred to the meter using electronic tokens that can be bought from the utility or from a distributor such as a corner shop or garage. The token can be an EEPROM key device, a memory ('smart') card, a disposable cardboard ticket with a magnetic strip, or a 20 digit number printed at the vend point on a slip of paper and which is entered by the customer at a keypad on the meter. But whatever its physical presentation, the token is really a number — typically of 64 bits or 20 decimal digits — that carries an instruction to a microcontroller in the meter. It is encrypted to make forgery more difficult.

The largest installed base of these meters is in Britain, where there are about one million electricity meters using two proprietary schemes, and some six hundred thousand gas meters using smartcards. Pre-paid electricity meters have been installed in a number of other countries, including Brazil, Congo, Namibia, the Ivory Coast and France. However the most rapidly growing single installation is now in South Africa, where one of the national development priorities is to double the number of households with electricity by 1999.

A. The Politics and Economics of Power

The South African national electricity utility (Eskom) runs the country's generating stations and national grid, and distributes power in rural areas; urban distribution was for years the responsibility of municipal authorities. Eskom started the development of low cost electricity pre-payment meters in 1987, primarily as a means to provide poor customers with electricity, but also in response to politically motivated withholding of utility payments in the townships.

With political reform during the 1990s, 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.

At the end of 1995, about 1.4 million prepaid meters had been installed, up from 850,000 in 1994 [7]. The government's National Reconstruction and Development Programme aims to supply two million more households with electricity by the end of 1999 [8], which means that over 1600 houses will be electrified every working day. In order to meet this national priority, pre-payment metering is the only option; and by the turn of the century, over half the households in the country will be using prepaid meters.

The economics are roughly as follows. The average cost of electrifying each home is about 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, a lamp socket fitting and two or three 15 Amp power 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, a budget of at most $1000 per month is available for token sales. This is not enough to support a full time staffed office; but a 2% sales commission provides a useful extra income for a local agent, such as a shopkeeper. Most token sales are made through these agents, of whom there were around 800 at the end of 1994. The upstream costs are also favourable: it costs much less to manage a network of sales agents than to manage a network of offices staffed by employees — or to run a system that bills a comparable number of customers directly.

The longer term goal is to cut costs still further by automating token sales in urban areas. There are already two pilot schemes with self-service token dispensing machines; one in Parow municipality, Cape Town, that takes coins, and another with a local bank with machines that accept banknotes. Work on token dispensing via supermarket EFT terminals and bank ATM networks is underway, as is an interface with a local system of electronic wallets [2] [9].

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, and these are now forming alliances with overseas distributors who will make the technology available in Europe and elsewhere.

B. 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 puts pressure on the balance of payments, but is expected to provide a major boost to education efforts in a country where the literacy rate runs at about 50%.

A lot of research has been conducted into the social aspects of rapid electrification, and in particular into the relationship between Eskom and its new mass client base [22]. This showed that the customer priority is for the system to 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 operational experience has shown that security is still a significant part of the project. It interacts with reliability in various ways. For example, an attempted fraud by a customer, or even by a token vendor, should have as little effect as possible on the security of supply enjoyed by honest customers.

Fig. 1 — a rural customer in the North West Province

III. Pre-payment Meter Security

Apart from the reliability aspects, the security requirements for a prepayment meter system seem fairly straightforward: tokens should not be able to be forged, and genuine tokens should not be able to be used in the wrong meter (or in the right meter twice). This means that they should either be tamper resistant (which is expensive) or unique. However it has taken considerable field experience to develop this simple idea into a robust system, and there are a number of complexities which we shall discuss below.

From the start of the prepayment metering project in 1987, local equipment suppliers were encouraged to innovate and produce low cost meters. They designed proprietary products and set out to sell them to the municipal authorities which at that time were the main distributors of electricity. This freedom to innovate led to low cost products as well as some designs that had not been tried elsewhere, such as the numeric token. Hundreds of thousands of meters were fielded which used six different types of token.

There was benefit in this diversity — many different ideas were tested in parallel, moving the South African pre-paid meter industry rapidly up the experience curve. However, none of the encryption schemes, and none of the physical token formats, were compatible with each other. Thus all the vendor equipment was manufacturer specific, and buying meters from a given company meant buying its vending equipment as well. This meant that the manufacturers had 'captive' districts.

It also became 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. This motivated a close study of the security and robustness of the installed meter systems.

A. Environmental Robustness

Robustness was originally a matter of contract between the equipment supplier and the local electricity distributor: a broken system 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. So did the mean time to failure of the meters.

A number of problems were identified during the pilot phase — principally due to field experience:

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. The specification now calls for meters to function up to 55^0C;

Lightning protection: severe thunderstorms are common in the South African summer, and most meters are connected to overhead reticulation systems. The meter has been described as a microprocessor with a 3 kilometre lightning conductor attached! So meters needed much better electrical protection than in Europe;

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 wire 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 [5]!

B. Standardisation

The experience gained from the resolution of these initial problems led to the development of a national standard, SABS1524 part 1 [24], 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.

However, the token information and encryption method were not standardised, which meant that the suppliers used whatever algorithms and formats they felt disposed towards, and led to the compatibility and robustness problems mentioned above. The first author was therefore engaged 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 this token information [12], which was carried out with further assistance from the first author and other experts. The resulting standard, called the Standard Transfer Specification (STS) [25], is now in use; half a million meters complying with it are in the field.

C. Cryptography

The novel systems feature of prepayment meters does not concern the details of encryption algorithms or protocols, but rather with the lack of a backward communication channel from the meter to the sales point. This may be a feature of other systems too, such as the safety mechanisms for nuclear warheads, but we are not aware of any unclassified account of their design (or operational failure history).

A theory paper on forward information verification in pre-payment meters was published in 1992 [16]. 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 $K_{ID} = \{ID\}_{K_V}$; here we use the notation from [10] that $\{X\}_K$ is the result of encrypting the message X with the key K.

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 (i.e., like 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. The other instructions include engineering test functions and key changes.

The use of number-based tokens in electricity meters is unique to South Africa (although it is used in postal franking machines). 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 while in the field. It will facilitate the purchase of power through supermarkets, ATMs and other vending systems where it could be expensive to fit magnetic token encoders. The numeric token also provides a man-machine interface for the customer to communicate with the meter, and this will become important with the addition of extra functionality in the future.

There were initial worries about whether the number system would cause problems with illiterate customers. But ‘everyone can use a phone’: we found that 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 [23]. When the 5 groups were printed in a row, the centre group had an entry error rate an order higher than the others. Presumably the customers got confused while tracking and rekeying the centre digits in a 20 digit string.

Fig. 2 — a numerical meter

The cryptographic algorithms in use have included proprietary schemes as well as variants of DES [20] and Lucifer [14]. 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 [11], but as perhaps 5,000 blocks will ever be enciphered under any one meter key, this 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 changing it has turned out to be tricky. Tokens are often purchased and hoarded as a means of expenditure control, so the customer has to use all his existing tokens before entering a key change token. It was considered whether to have the equipment retain 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 integrated with several more complex security functions: to help trace revenue losses by balancing transactions with power consumption; to detect fraud by balancing transactions and cash; to impose central management on a network of diverse vending systems, and in particular to control agents' credit; to revoke 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.

Fig. 3 — vending equipment at a 'home shop' in KwaZulu-Natal

D. Security Problems - First Phase

However, it is not enough to have a system that possesses physical, electrical and cryptologic robustness. Implementation detail and operational procedures are also very important. This is where computer security failures usually occur in real systems [1] [3].

The first author was therefore engaged to examine these aspects. A number of early meter and vending system designs were examined in detail, and several 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 manipulating refunds. A refund could be granted, but the refunded token (or a copy of it) could still be used;
- some meters physically erased the token after a transaction as a first line of defence against replay. However the robustness of the erase mechanism varied considerably, and one test meter did not erase tokens at all;
- one of these meters could be fooled by duplicate tokens. Its designers had relied too much on the erase mechanism, and its software retained only the last token serial number entered. So by alternately entering duplicates of two previously used tokens it could be charged up indefinitely;
- one type of token dispensing unit had a supervisor password with which its credit could be indefinitely replenished. The theft of such a unit, with its password, would force recoding 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 trails;
- the structure of the databases used to store client information and to match the meter administration to that of the power supply varied so much between the meter vendors that it was difficult to design and operate a unified system for balancing energy and cash.

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 and no purchase reports) 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 problem this creates is that, in busy centres like Johannesburg, a vending machine might have to hold keys for as many as fifty different vend areas. How could this exposure be controlled?

E. Security Problems - Second Phase

In the year after the initial security study, field experience brought further problems to light, including:

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: customers 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;

System operational: balancing power and cash was hard because the dates on which feeder meters were read were not accurately known. Staff would vary their schedules, and 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 [1] [3]: real security breaches in payment systems result from blunders, which may be quite obscure, but which are discovered by accident and exploited in a quite opportunistic way. Security depends as much on good system engineering as on any specific technical feature such as encryption.

Our experience also confirmed the value of design diversity. With a number of different designs, even a catastrophic failure has limited effects, as geographical fragmentation helps limit the spread of attack know-how (though perhaps that will change with improved communications). Another aspect is the balance of power between the utility and its suppliers. With only one supplier, a security disaster might result in protracted negotiations; but with six competing suppliers, the system operator can get them to fix faults as they arise.

The meter failure rate is now generally low, and security work is now focused on the mechanisms for key management, remote token purchase, credit control and interfacing with banking systems.

F. Lessons Learned

The general lessons emerging from this exercise are:

1. make the system operator 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 unnecessarily risky;
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. One expert alone can not usually span all the issues, and even the best will miss things;
9. do not be afraid to use multiple equipment suppliers, but be careful about the tradeoffs 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 no matter what is done, small mistakes with large consequences will still creep in. Thus, in addition to experts and methodologies, one absolutely needs prolonged field testing. This is where many errors and impracticalities will first become apparent.

The opportunity now exists for utilities and meter vendors in other countries to benefit from our experience, and we hope that the IEC working group mentioned above may help in this. In any case, software quality is of the utmost importance, as meter software is very expensive to change: there are so many meters, and entry into customers' homes is difficult. Testing must cover a wide range of conditions, from steady state through fast mains borne transients to customer interference. ISO 9001/2 compliance has been mandatory for the meter hardware since 1991, but this was found not to be enough, as there were no external controls on the implementation and modification of the meter software. So in early 1995, Eskom introduced mandatory ISO 9001/2 software certification to ensure strict change control and hopefully limit the number of bugs. It has also audited all the vendors' software maturity levels.

IV. The Medium Term

In accordance with the principle that robust security systems are explicit ones [3], the Common Vending System (as the network is now called) has an explicit threat model and security goals. The gist of it 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, credit replenishment and key management, 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 higher level secure processors which are used by the electricity distributors. The detailed design 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 related problems which emerge from this exercise, and which are likely to affect other industries using electronic vending, are vendor revocation and the control of third party credit.

A. Vendor Revocation

Recent political changes are affecting local government and utility management structures, and make it possible that a large number of former local 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, we must have robust controls. 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 contain a secret that 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 meters 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.

The point is that customers can purchase power as individuals rather than as members of a group. Each customer can nominate two alternate vendors, and her meter keys will be sent to those vendors encrypted under a suitable, time limited, master key; these master key are unique to each vending system and are only supplied so long as the vendor remains in good standing.

B. Third Party Credit

The most serious problem, and the one with major political ramifications, is that of controlling transactions by third parties. If tokens are sold by bank ATMs (or supermarket checkout terminals), how can we be sure that the bank (or supermarket) is being honest about their sales?

We already have experience of token vendors damaging their vending systems (or claiming that they were stolen) in order to avoid handing over their takings. It is also well known that disputes over the security of ATMs can be heated and difficult to resolve [2] [4], and that both the law and banking practice vary quite widely from one country to another on this point [18]. 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 the sale.

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

Such universal smartcards could be attractive to utilities: they could provide the missing return channel to report meter readings, usage statistics and tamper occurrences back to the point of sale. However, Eskom's experience 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 some serious drawbacks.

Infrastructure: many terminals will have to be in place before electronic wallets are successful, and this will be very expensive. Cash can simply be handed from one person to another.

Utility reduction: even once enough terminals have been fielded, there is a reduction of utility when one puts money into an instrument which can only buy a limited number of things. This utility reduction is marked among the poor, who might have to commit over half their wealth to a card used for rent, power and transport tickets.

Standardisation: international standards for smartcard functionality are not yet stable. This could mean reprogramming all meters if the standard changes and bank issued smartcards follow.

Politics: Who will control a 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. According to smartcard vendors, the main dispute with shared systems is over whose logo shall go on the card [17]. Meanwhile, Eskom's electrification program is a national priority and must not be held up by bickering among third parties' marketing managers!

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

Legacy of the Dompas, or pass book: South Africa had for many years a system of identity books which contained each individual's racial group, marriage certificate, residence permit, driving licence, gun licence, and so on. A multifunction card might be seen as a return to the bad old days.

We might try to tackle the trust problems by technical means. For example, we might draw inspiration from digital cash schemes [13] 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 insure against losses, with a sampling system to monitor a number of households; it might agree to pay compensation equal to the expected loss whenever a card or part of an audit trail goes missing. However, some modern smartcard-based banking systems have no reconciliation, and this severely limits options; in this case, the bank might have to take over as distributor and simply pay for bulk metered power from the grid.

However, shared systems could still give rise to fearful rows. If the primary operator wants to accommodate lottery ticket sales, and this meant cutting the space available for the electrical audit trail, then could 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?

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.

V. Conclusions

Many future networked applications, and indeed the charging mechanisms of the 'Information Superhighway' itself, will depend on cryptographic mechanisms to control credit and transfer value. The reliability of such systems is therefore of considerable importance. Yet most fielded commercial cryptographic systems are less reliable than one would wish. Attacks keep on being reported on systems such as satellite TV decoders, automatic teller machines and utility meters; many of these are due to their designers' ignorance of how similar systems failed. Minimising the risk of such failures is primarily a systems engineering issue, concerned with careful requirements engineering and thorough testing.

We have described a number of the specification and testing issues which we found to be important in the fastest growing 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. We finally got a robust system, but this took several years of field experience with equipment from a number of competing manufacturers working in parallel. As with other studied systems, we found that most frauds were due to errors in design and management leaving loopholes, which were discovered and exploited on a more or less opportunist basis by both operators and customers.

The most difficult remaining problem is how to control systems which involve more than one main player. At present, there is no obvious solution, and the problem may be so serious as to prevent the creation of universal payment mechanisms for the future world of networked systems. Our work at least shows that while building a reliable payment mechanism with low overheads is not simple, it is not impossible either.

Acknowledgements: we would like to acknowledge a discussion with Nick MacLaren on the administrative costs of time-sharing systems, and assistance generally from the South African meter industry and from staff at Eskom. The first author also acknowledges the Isaac Newton Institute for Mathematical Sciences for hospitality while this paper was being written.

References

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

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

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

[4] RJ Anderson, "Liability and Computer Security - Nine Principles", in *proceedings of ESORICS 94*, Springer Lecture Notes in Computer Science v 875 pp 231–245

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

[6] M Attree, K Green, "Key Budget Metering — The Total Payment System", in *Proceedings of the 6th IEE International Conference on Metering Apparatus and Tariffs for Electricity Supply* (1990) pp 139–143

[7] 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)

[8] SJ Bezuidenhout, "20 questions and answers about EDs", Eskom document sjb1995

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

[10] M Burrows, M Abadi, RM Needham, "A Logic of Authentication", in *Proceedings of the Royal Society of London A* v **426** (1989) pp 233–271

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

[12] 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)

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

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

[15] D Kahn, *The Codebreakers'*, Macmillan 1967

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

[17] P Maes, Gemplus, invited talk at Cardis 94, Lille, France

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

[19] JK MacKie-Mason, HR Varian, "Some FAQ's about usage-Based Pricing", November 4, 1994, online at `http://gopher.econ.lsa.umich.edu`

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

[21] MJA Partridge, "Prepayment Coin Meters — A Target for Burglary", *UK Home Office Crime Prevention Report no. 6* (1986)

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

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

[24] South African Bureau of Standards, *'Standard Specification - Single-Phase Electricity Dispensing Systems Part 1: Electricity Dispensers'* SABS 1524-1:1994

[25] Standard Transfer System, Eskom 1994

Ross J. Anderson received his MA and PhD degrees from Cambridge University. He is a chartered engineer and chartered mathematician, and a Member of the IEE. He has worked in computer security and cryptography for about ten years and is currently working on the robustness of cryptographic protocols. His other research interests include the analysis and design of cryptographic algorithms, the reliability of software and systems, and the failure modes of computer security systems.

S Johann Bezuidenhoudt received his BSc (Eng) Elec. from the University of the Witwatersrand in 1979 and a BCom from the University of South Africa in 1986. He has been employed by Eskom, the South African electricity utility, since 1980 and worked in nuclear reactor instrumentation, control and protection before moving to computer security in 1988. He was the project leader for and designer of the computer systems with which prepayment meters are managed. His research interests include key management in distributed off-line system architectures and time coherence of information in distributed secure databases. He is a Senior Member of the SAIEE, whose Measurement, Computation and Control Section he chairs, and is also a member of the Computer Society of South Africa.